`Horst and Amaryllises`: Possible Generalizations of the Feistel and of the Lai-Massey Schemes

ASK 2023, December 2023

Lorenzo Grassi
Ruhr-Universität Bochum, Germany

CASA
Cyber Security in the Age of Large-Scale Adversaries

Ruhr Universität Bochum RUB
Gefördert durch DFG Deutsche Forschungsgemeinschaft
Horst Görtz Institut

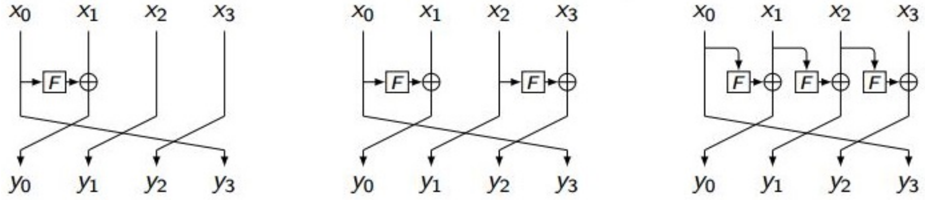
SPN and Feistel Schemes

The majority of the symmetric schemes follows one of the two following design strategies:

- Substitution Permutation Network (SPN):

$$(x_0, x_1, \ldots, x_{n-1}) \mapsto c + M \times (\mathsf{S}(x_0), \mathsf{S}(x_1), \ldots, \mathsf{S}(x_{n-1}))$$

- Feistel schemes:



Motivation

CASA — Cyber Security in the Age of Large-Scale Adversaries

New applications such as Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge proofs (ZK) require symmetric-key primitives that

- are naturally defined over $\mathbb{F}_p^n$ for a large prime p (such as $p \approx 2^{128}$ or 2^{256})
- minimize their *multiplicative complexity*, i.e., the number of multiplications (= non-linear operations) required to compute and/or verify them.

Questions:

1. Is it possible to set up *new invertible non-linear layers* over $\mathbb{F}_q^n$ for $q = p^s$?
2. Is it possible to achieve better security argument and/or performances via them?

Motivation

CASA
Cyber Security in the Age of Large-Scale Adversaries

New applications such as Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge proofs (ZK) require symmetric-key primitives that

- are naturally defined over $\mathbb{F}_p^n$ for a large prime p (such as $p \approx 2^{128}$ or 2^{256})
- minimize their *multiplicative complexity*, i.e., the number of multiplications (= non-linear operations) required to compute and/or verify them.

Questions:

1. Is it possible to set up *new invertible non-linear layers* over $\mathbb{F}_q^n$ for $q = p^s$?
2. Is it possible to achieve better security argument and/or performances via them?

Table of Contents

Table of Contents

From Feistel to Horst Schemes

Feistel scheme $\mathcal{F}$ over $\mathbb{F}_q^2$ (where $q = p^s$ for $s \geq 1$ and a prime $p \geq 2$):

$$(x_0, x_1) \mapsto (y_0, y_1) = (x_1, x_0 + \mathrm{F}(x_1)),$$

where $\mathrm{F} : \mathbb{F}_q \to \mathbb{F}_q$. *Always invertible independently of* F*:* $x_0 = y_1 - \mathrm{F}(x_1) = y_1 - \mathrm{F}(y_0)$.

Horst as a possible generalization:

$$(x_0, x_1) \mapsto (y_0, y_1) := (x_1, x_0 \cdot \mathrm{G}(x_1) + \mathrm{F}(x_1)),$$

where $\mathrm{G} : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$. Invertible as well:

$$(x_0, x_1) = \left(\frac{y_1 - \mathrm{F}(y_0)}{\mathrm{G}(y_0)}, y_0\right).$$

From Feistel to Horst Schemes

Feistel scheme $\mathcal{F}$ over $\mathbb{F}_q^2$ (where $q = p^s$ for $s \geq 1$ and a prime $p \geq 2$):

$$(x_0, x_1) \mapsto (y_0, y_1) = (x_1, x_0 + \mathsf{F}(x_1)) \, ,$$

where $\mathsf{F} : \mathbb{F}_q \to \mathbb{F}_q$. *Always invertible independently of* F*:* $x_0 = y_1 - \mathsf{F}(x_1) = y_1 - \mathsf{F}(y_0)$.

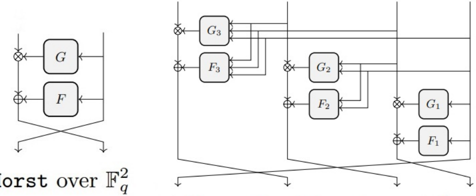
Horst as a possible generalization:

$$(x_0, x_1) \mapsto (y_0, y_1) := (x_1, x_0 \cdot \mathsf{G}(x_1) + \mathsf{F}(x_1)) \, ,$$

where $\mathsf{G} : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$. Invertible as well:

$$(x_0, x_1) = \left(\frac{y_1 - \mathsf{F}(y_0)}{\mathsf{G}(y_0)}, y_0 \right) \, .$$

Horst Schemes over $\mathbb{F}_q^n$ [GHR+23]



Horst over $\mathbb{F}_q^2$

Generalized Horst over $\mathbb{F}_q^4$

The Horst scheme over $\mathbb{F}_q^n$:

$$y_i := \begin{cases} x_{i+1} \cdot \mathsf{G}^{(i+1)}(x_i, x_{i-1}, \ldots, x_0) + \mathsf{F}^{(i+1)}(x_i, x_{i-1}, \ldots, x_0) & \text{otherwise } (i \in \{0, 1, \ldots, n-2\}), \\ x_0 & \text{if } i = n-1, \end{cases}$$

where $\mathsf{F}^{(j)} : \mathbb{F}_q^j \to \mathbb{F}_q$ and $\mathsf{G}^{(j)} : \mathbb{F}_q^j \to \mathbb{F}_q \setminus \{\mathbf{0}\}$.

Constructing $G : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$ (1/3)

If q small (e.g., $q \approx 2^8$) and no particular condition on G: easy task! (E.g., brute force).
Our Goal: *construct low-degree* G *over any* $\mathbb{F}_q$.

1st Example: Let $q = p \geq 3$ be a prime. Remember: $x \mapsto x^2$ is not invertible.
Define

$$G(x) := x^2 + \alpha \cdot x + \beta$$

such that $\alpha, \beta \in \mathbb{F}_p$ satisfies $\alpha^2 - 4 \cdot \beta \neq z^2$ for each $z \in \mathbb{F}_p$.
Then, $G(x) = 0$ if and only if

$$x = (-\alpha \pm \sqrt{\alpha^2 - 4 \cdot \beta})/2\,,$$

which do not exist!

Constructing $\mathrm{G} : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$ (1/3)

If q small (e.g., $q \approx 2^8$) and no particular condition on G: easy task! (E.g., brute force).
Our Goal: *construct low-degree* G *over any* $\mathbb{F}_q$.

1st Example: Let $q = p \geq 3$ be a prime. Remember: $x \mapsto x^2$ is not invertible.
Define

$$\mathrm{G}(x) := x^2 + \alpha \cdot x + \beta$$

such that $\alpha, \beta \in \mathbb{F}_p$ satisfies $\alpha^2 - 4 \cdot \beta \neq z^2$ for each $z \in \mathbb{F}_p$.
Then, $\mathrm{G}(x) = 0$ if and only if

$$x = (-\alpha \pm \sqrt{\alpha^2 - 4 \cdot \beta})/2\,,$$

which do not exist!

Constructing $\mathsf{G} : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$ (2/3)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Given a generic G over $\mathbb{F}_q$: very expensive to check if G returns zero or not!

Lemma 1

Let $\mathsf{G} : \mathbb{F}_q \to \mathbb{F}_q$ be such that (i) $\mathsf{G}(0) \neq 0$ and (ii) $\mathsf{H}(x) := x \cdot \mathsf{G}(x)$ is a permutation. Then, $\mathsf{G}(x) \neq 0$ for each $x \in \mathbb{F}_q$.

Proof.

Obviously, $\mathsf{H}(0) = 0$. Since H is a permutation, then $\mathsf{H}(x) \neq 0$ for each $x \in \mathbb{F}_q \setminus \{0\}$. Hence:

$$\forall x \in \mathbb{F}_q \setminus \{0\} : \qquad \mathsf{G}(x) = \frac{\mathsf{H}(x)}{x} \neq 0\,.$$

By assumption, $\mathsf{G}(0) \neq 0$. Hence, $\mathsf{G}(x) \neq 0$ for each x. □

Constructing $\mathsf{G} : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$ (2/3)

Given a generic G over $\mathbb{F}_q$: very expensive to check if G returns zero or not!

Lemma 1

Let $\mathsf{G} : \mathbb{F}_q \to \mathbb{F}_q$ *be such that (i)* $\mathsf{G}(0) \neq 0$ *and (ii)* $\mathsf{H}(x) := x \cdot \mathsf{G}(x)$ *is a permutation. Then,* $\mathsf{G}(x) \neq 0$ *for each* $x \in \mathbb{F}_q$*.*

Proof.

Obviously, $\mathsf{H}(0) = 0$. Since H is a permutation, then $\mathsf{H}(x) \neq 0$ for each $x \in \mathbb{F}_q \setminus \{0\}$. Hence:

$$\forall x \in \mathbb{F}_q \setminus \{0\} : \qquad \mathsf{G}(x) = \frac{\mathsf{H}(x)}{x} \neq 0\,.$$

By assumption, $\mathsf{G}(0) \neq 0$. Hence, $\mathsf{G}(x) \neq 0$ for each x. □

Constructing $G : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$ (3/3)

CASA — Cyber Security in the Age of Large-Scale Adversaries

2nd Example: Let $x \mapsto x^d$ be a permutation over $\mathbb{F}_q$, and let $\alpha \in \mathbb{F}_q \setminus \{0\}$. The function

$$G(x) := \frac{(x+\alpha)^d - \alpha^d}{x} = \sum_{i=1}^{d} \binom{d}{i} \cdot \alpha^i \cdot x^{d-1-i}$$

never returns zero (since $G(0) = d \cdot \alpha \neq 0$ and $G(x) \cdot x = (x+\alpha)^d - \alpha^d$ is invertible).

3rd Example: Over $\mathbb{F}_{2^n}$, let

$$G(x) = \sum_{i=0}^{d} \alpha_i \cdot x^{2^i - 1}.$$

for $\alpha_0 \neq 0$. Choose $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{F}_{2^n}$ such that $G(x) \cdot x = \sum_{i=0}^{d} \alpha_i \cdot x^{2^i}$ is invertible (note that $x \cdot G(x)$ is a linear map $\to$ easy to check!). Then, G never returns zero.

Constructing $G : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$ (3/3)

CASA — Cyber Security in the Age of Large-Scale Adversaries

2nd Example: Let $x \mapsto x^d$ be a permutation over $\mathbb{F}_q$, and let $\alpha \in \mathbb{F}_q \setminus \{0\}$. The function

$$G(x) := \frac{(x+\alpha)^d - \alpha^d}{x} = \sum_{i=1}^{d} \binom{d}{i} \cdot \alpha^i \cdot x^{d-1-i}$$

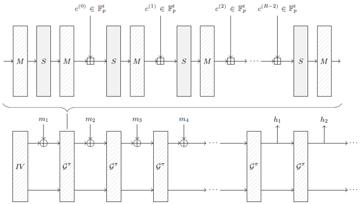
never returns zero (since $G(0) = d \cdot \alpha \neq 0$ and $G(x) \cdot x = (x+\alpha)^d - \alpha^d$ is invertible).

3rd Example: Over $\mathbb{F}_{2^n}$, let

$$G(x) = \sum_{i=0}^{d} \alpha_i \cdot x^{2^i - 1}.$$

for $\alpha_0 \neq 0$. Choose $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{F}_{2^n}$ such that $G(x) \cdot x = \sum_{i=0}^{d} \alpha_i \cdot x^{2^i}$ is invertible (note that $x \cdot G(x)$ is a linear map $\to$ easy to check!). Then, G never returns zero.

Feistel versus Horst in GRIFFIN [GHR+23] (1/2)



Non-linear layer $S(x_0, x_1, \ldots, x_{t-1}) = y_0 \| y_1 \| \ldots \| y_{t-1}$ over $\mathbb{F}_p^t$ defined as

$$y_i = \begin{cases} {x_0}^{1/d} & \text{if } i = 0, \\ {x_1}^{d} & \text{if } i = 1, \\ x_2 \cdot \left((L_i(y_0, y_1, 0))^2 + \alpha_2 \cdot L_i(y_0, y_1, 0) + \beta_2 \right) & \text{if } i = 2, \\ x_i \cdot \left((L_i(y_0, y_1, x_{i-1}))^2 + \alpha_i \cdot L_i(y_0, y_1, x_{i-1}) + \beta_i \right) & \text{otherwise,} \end{cases}$$

where $\gcd(d, p-1) = 1$ and $L_i : \mathbb{F}_p^3 \to \mathbb{F}_p$ are linear functions.

Feistel versus Horst in Griffin [GHR+23] (2/2)

$x \mapsto x^{1/d}$ is quite expensive $\longrightarrow$ *our goal:* minimize the number of rounds!

Griffin$^\times$ instantiated with Horst allows *stronger security argument* against Gröbner basis attacks w.r.t. Griffin$^+$ instantiated with Feistel:

- roughly speaking, cost of Gröbner basis attacks given by

$$\mathcal{O}\left(\binom{D_{\text{reg}} + n_v}{n_v}^2\right),$$

  where D_{reg} = degree of regularity, and n_v = number of variables;
- Griffin$^+$: D_{reg} remains almost constant w.r.t. the number of rounds $\longrightarrow$ *hard to estimate* the minimum number for guaranteeing security!
- Griffin$^\times$: D_{reg} *growths with the number of rounds.*

Feistel versus Horst in Griffin [GHR+23] (2/2)

$x \mapsto x^{1/d}$ is quite expensive $\longrightarrow$ *our goal:* minimize the number of rounds!

Griffin$^{\times}$ instantiated with Horst allows *stronger security argument* against Gröbner basis attacks w.r.t. Griffin^{+} instantiated with Feistel:

- roughly speaking, cost of Gröbner basis attacks given by

$$\mathcal{O}\left(\binom{D_{\text{reg}} + n_v}{n_v}^2\right),$$

where D_{reg} = degree of regularity, and n_v = number of variables;

- Griffin^{+}: D_{reg} remains almost constant w.r.t. the number of rounds $\longrightarrow$ *hard to estimate* the minimum number for guaranteeing security!
- Griffin$^{\times}$: D_{reg} *growths with the number of rounds.*

Feistel versus Horst in GRIFFIN [GHR+23] (2/2)

$x \mapsto x^{1/d}$ is quite expensive $\longrightarrow$ *our goal:* minimize the number of rounds!

GRIFFIN$^{\times}$ instantiated with Horst allows *stronger security argument* against Gröbner basis attacks w.r.t. GRIFFIN^{+} instantiated with Feistel:

- roughly speaking, cost of Gröbner basis attacks given by

$$\mathcal{O}\left(\binom{D_{\text{reg}} + n_v}{n_v}^2\right),$$

  where D_{reg} = degree of regularity, and n_v = number of variables;
- GRIFFIN^{+}: D_{reg} remains almost constant w.r.t. the number of rounds $\longrightarrow$ *hard to estimate* the minimum number for guaranteeing security!
- GRIFFIN$^{\times}$: D_{reg} *growths with the number of rounds.*

Feistel versus Horst in GRIFFIN [GHR+23] (2/2)

$x \mapsto x^{1/d}$ is quite expensive $\longrightarrow$ *our goal:* minimize the number of rounds!

GRIFFIN$^{\times}$ instantiated with Horst allows *stronger security argument* against Gröbner basis attacks w.r.t. GRIFFIN^{+} instantiated with Feistel:

- roughly speaking, cost of Gröbner basis attacks given by

$$\mathcal{O}\left(\binom{D_{\text{reg}} + n_v}{n_v}^2\right),$$

  where D_{reg} = degree of regularity, and n_v = number of variables;
- GRIFFIN^{+}: D_{reg} remains almost constant w.r.t. the number of rounds $\longrightarrow$ *hard to estimate* the minimum number for guaranteeing security!
- GRIFFIN$^{\times}$: D_{reg} *growths with the number of rounds.*

Table of Contents

Lai-Massey Schemes over $\mathbb{F}_q^2$

Let $q = p^s$ be as before. Lai-Massey scheme $\mathcal{LM}$ over $\mathbb{F}_q^2$:

$$(x_0, x_1) \mapsto (y_0, y_1) = (\alpha \cdot (x_0 + \mathrm{F}(x_0 - x_1)), x_1 + \mathrm{F}(x_0 - x_1)) \; ,$$

where $\mathrm{F} : \mathbb{F}_q \to \mathbb{F}_q$ and $\alpha \neq 0$. $\mathcal{LM}$ is invertible independently of the details of F:

$$(x_0, x_1) = (y_0' - \mathrm{F}(y_0' - y_1), y_1 - \mathrm{F}(y_0' - y_1)) \, ,$$

since $x_0 - x_1 = y_0' - y_1$ where $y_0' = y_0/\alpha$.

Remark: $\alpha \notin \{0, 1\}$ crucial for *destroying the invariant subspace* $\langle [1, 1] \rangle \subseteq \mathbb{F}_q^2$.
($\alpha = 1$ fixed in the following for simplicity!)

Lai-Massey Schemes over $\mathbb{F}_q^2$

Let $q = p^s$ be as before. Lai-Massey scheme $\mathcal{LM}$ over $\mathbb{F}_q^2$:

$$(x_0, x_1) \mapsto (y_0, y_1) = (\alpha \cdot (x_0 + \mathrm{F}(x_0 - x_1)), x_1 + \mathrm{F}(x_0 - x_1)) \ ,$$

where $\mathrm{F} : \mathbb{F}_q \to \mathbb{F}_q$ and $\alpha \neq 0$. $\mathcal{LM}$ is invertible independently of the details of F:

$$(x_0, x_1) = (y_0' - \mathrm{F}(y_0' - y_1), y_1 - \mathrm{F}(y_0' - y_1)) \, ,$$

since $x_0 - x_1 = y_0' - y_1$ where $y_0' = y_0/\alpha$.

Remark: $\alpha \notin \{0, 1\}$ crucial for *destroying the invariant subspace* $\langle [1, 1] \rangle \subseteq \mathbb{F}_q^2$.
($\alpha = 1$ fixed in the following for simplicity!)

Lai-Massey Schemes over $\mathbb{F}_q^n$

Let $n \geq 3$. For each $i \in \{0, 1, \ldots, n-2\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)} \in \mathbb{F}_q$ be such that

$$\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0 \,.$$

The Lai-Massey scheme over $\mathbb{F}_q^n$ is defined as $(x_0, x_1, \ldots, x_{n-1}) \mapsto (y_0, y_1, \ldots, y_{n-1})$ where

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := x_i + \mathrm{F}\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\right)$$

where $\mathrm{F} : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$. As before, invertibility follows from $\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j = \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot y_j$.

Lai-Massey Schemes over $\mathbb{F}_q^n$

CASA — Cyber Security in the Age of Large-Scale Adversaries

Let $n \geq 3$. For each $i \in \{0, 1, \ldots, n-2\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)} \in \mathbb{F}_q$ be such that

$$\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0\,.$$

The Lai-Massey scheme over $\mathbb{F}_q^n$ is defined as $(x_0, x_1, \ldots, x_{n-1}) \mapsto (y_0, y_1, \ldots, y_{n-1})$ where

$$\forall i \in \{0, 1, \ldots, n-1\}: \qquad y_i := x_i + \mathsf{F}\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\right)$$

where $\mathsf{F} : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$. As before, invertibility follows from $\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j = \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot y_j$.

Relation between Feistel and Lai-Massey Schemes

Theorem 2 ([Gra22])

A Lai-Massey scheme $\mathcal{LM}$ over $\mathbb{F}_q^n$ is extended Affine-Equivalent (AE) to a generalized Feistel scheme $\mathcal{F}$ over $\mathbb{F}_q^n$, that is, there exists two affine permutation A, B and an affine function C over $\mathbb{F}_q^n$ such that

$$\forall x \in \mathbb{F}_q^n : \qquad \mathcal{F}(x) = B \circ \mathcal{LM} \circ A(x) + C(x)\,.$$

For each $j \in \{1, 2, \ldots, n-1\}$, let $\mathrm{F}^{(j)} : \mathbb{F}_q^j \to \mathbb{F}_q$. The generalized Feistel scheme over $\mathbb{F}_q^n$ is defined as $(x_0, x_1, \ldots, x_{n-1}) \mapsto (y_0, y_1, \ldots, y_{n-1})$ where:

$$y_i := \begin{cases} x_{i+1} + \mathrm{F}^{(i+1)}(x_i, x_{i-1}, \ldots, x_0) & \text{otherwise } (i \in \{0, 1, \ldots, n-2\})\,, \\ x_0 & \text{if } i = n-1\,, \end{cases}$$

Relation between Feistel and Lai-Massey Schemes

Theorem 2 ([Gra22])

A Lai-Massey scheme $\mathcal{LM}$ over $\mathbb{F}_q^n$ is extended Affine-Equivalent (AE) to a generalized Feistel scheme $\mathcal{F}$ over $\mathbb{F}_q^n$, that is, there exists two affine permutation A, B and an affine function C over $\mathbb{F}_q^n$ such that

$$\forall x \in \mathbb{F}_q^n : \qquad \mathcal{F}(x) = B \circ \mathcal{LM} \circ A(x) + C(x) .$$

For each $j \in \{1, 2, \ldots, n-1\}$, let $\mathrm{F}^{(j)} : \mathbb{F}_q^j \to \mathbb{F}_q$. The generalized Feistel scheme over $\mathbb{F}_q^n$ is defined as $(x_0, x_1, \ldots, x_{n-1}) \mapsto (y_0, y_1, \ldots, y_{n-1})$ where:

$$y_i := \begin{cases} x_{i+1} + \mathrm{F}^{(i+1)}(x_i, x_{i-1}, \ldots, x_0) & \text{otherwise } (i \in \{0, 1, \ldots, n-2\}) , \\ x_0 & \text{if } i = n-1 , \end{cases}$$

Proof of the Relation $\mathbb{F}_q^2$

CASA — Cyber Security in the Age of Large-Scale Adversaries

$\mathcal{LM}$ over $\mathbb{F}_q^2$ defined as $(x_0, x_1) \mapsto (x_0 + \mathsf{F}(x_0 - x_1), x_1 + \mathsf{F}(x_0 - x_1))$ is *affine-equivalent* to $(x_0, x_1) \mapsto (x_1 + \mathsf{F}(x_0), x_0)$ via the invertible linear transformations

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

and $C = 0$. Indeed:

$$\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \xrightarrow{A \times \cdot} \begin{bmatrix} x_0 - x_1 \\ x_1 \end{bmatrix} \xrightarrow{\mathcal{F}(\cdot)} \begin{bmatrix} x_1 + \mathsf{F}(x_0 - x_1) \\ x_0 - x_1 \end{bmatrix} \xrightarrow{B \times \cdot} \begin{bmatrix} x_0 + \mathsf{F}(x_0 - x_1) \\ x_1 + \mathsf{F}(x_0 - x_1) \end{bmatrix} .$$

(See [Gra22] for the proof regarding the general case $\mathbb{F}_q^n$.)

Open Questions

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Is it possible to transfer the results published in the literature (including indistinguishability, indifferentiability, ...) for Feistel schemes to Lai-Massey schemes?
- Is it possible to *generalize* the Lai-Massey scheme such that the (extended) affine equivalence to Feistel schemes does **not** hold?

Generalized Lai-Massey Scheme

Definition 3 ([Gra22])

Let $n \geq 2$. For each $i \in \{0, 1, \ldots, n-2\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)} \in \mathbb{F}_q$ be s.t. $\sum_{l=0}^{t-1} \lambda_l^{(i)} = 0$.

We say that the scheme $(x_0, x_1, \ldots, x_{n-1}) \mapsto (y_0, y_1, \ldots, y_{n-1}) := \mathcal{LM}^G(x_0, x_1, \ldots, x_{n-1})$ where

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := x_i + \mathsf{F}_i(z_0, z_1, \ldots, z_{n-2})$$

such that $\mathsf{F}_0, \mathsf{F}_1, \ldots, \mathsf{F}_{n-1} : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ and

$$\forall j \in \{0, 1, \ldots, n-2\} : \qquad z_j := \sum_{l=0}^{n-1} \lambda_l^{(j)} x_l$$

is a “Generalized Lai-Massey” scheme **if** it is invertible.

Generalized Lai-Massey Scheme: Example

Let $p \geq 3$. The generalized Lai-Massey scheme defined as

$$\begin{aligned} y_0 &= x_0 + F^{(1)}(x_0 - x_1) + F^{(3)}(x_0 - x_1, x_1 - x_2, x_2 - x_3) \\ y_1 &= x_1 + F^{(1)}(x_0 - x_1) + F^{(3)}(x_0 - x_1, x_1 - x_2, x_2 - x_3) \\ y_2 &= x_2 + F^{(2)}(x_0 - x_1, x_2 - x_3) + F^{(3)}(x_0 - x_1, x_1 - x_2, x_2 - x_3) \\ y_3 &= x_3 + F^{(2)}(x_0 - x_1, x_2 - x_3) + F^{(3)}(x_0 - x_1, x_1 - x_2, x_2 - x_3) \end{aligned}$$

for $F^{(i)} : \mathbb{F}_p^i \to \mathbb{F}_p$ with $i \in \{1, 2, 3\}$ is

- invertible:

$$x_0 - x_1 = y_0 - y_1 ; \qquad x_2 - x_3 = y_2 - y_3 ;$$
$$x_1 - x_2 = y_1 - y_2 - F^{(1)}(y_0 - y_1) - F^{(2)}(y_0 - y_1, y_2 - y_3) ;$$

- **not** extended affine equivalent to any Feistel scheme (see [Gra22] for the proof).

Redundant Lai-Massey Scheme

Definition 4 ([Gra22])

Let $n \geq 2$.
We say that the scheme $(x_0, x_1, \ldots, x_{n-1}) \mapsto (y_0, y_1, \ldots, y_{n-1}) := \mathcal{LM}^R(x_0, x_1, \ldots, x_{n-1})$ where

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := x_i + \mathsf{F}(x_0, x_1, \ldots, x_{n-1})$$

such that $\mathsf{F} : \mathbb{F}_q^n \to \mathbb{F}_q$ is a "Redundant Lai-Massey" scheme **if** it is invertible.

Redundant Lai–Massey Scheme: Example (1/2)

Let $p \geq 3$ be a prime integer. Let $\alpha \in \mathbb{F}_p \setminus \{0\}$ be such that $-2 \cdot \alpha \neq z^2$ for each $z \in \mathbb{F}_p$. Then,

$$(x_0, x_1) \mapsto (y_0, y_1) := (x_0 + z, x_1 + z)$$

where

$$z := \alpha \cdot (x_0 - x_1)^2 \cdot (x_0 + x_1)$$

is a redundant Lai-Massey scheme. Invertibility follows from:

- $y_0 - y_1 = x_0 - x_1$;
- hence, $y_0 + y_1 = (x_0 + x_1) \cdot (1 + 2\alpha \cdot (y_0 - y_1)^2)$, which implies

$$x_0 + x_1 = \frac{y_0 + y_1}{1 + 2\alpha \cdot (y_0 - y_1)^2}$$

where $1 + 2\alpha \cdot z^2 \neq 0$ by assumption on α.

Redundant Lai–Massey Scheme: Example (1/2)

CASA — Cyber Security in the Age of Large-Scale Adversaries

Let $p \geq 3$ be a prime integer. Let $\alpha \in \mathbb{F}_p \setminus \{0\}$ be such that $-2 \cdot \alpha \neq z^2$ for each $z \in \mathbb{F}_p$. Then,

$$(x_0, x_1) \mapsto (y_0, y_1) := (x_0 + z, x_1 + z)$$

where

$$z := \alpha \cdot (x_0 - x_1)^2 \cdot (x_0 + x_1)$$

is a redundant Lai-Massey scheme. Invertibility follows from:

- $y_0 - y_1 = x_0 - x_1$;
- hence, $y_0 + y_1 = (x_0 + x_1) \cdot (1 + 2\alpha \cdot (y_0 - y_1)^2)$, which implies

$$x_0 + x_1 = \frac{y_0 + y_1}{1 + 2\alpha \cdot (y_0 - y_1)^2}$$

  where $1 + 2\alpha \cdot z^2 \neq 0$ by assumption on α.

Redundant Lai-Massey Scheme: Example (2/2)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

It is **not** extended affine equivalent to any Feistel scheme over $\mathbb{F}_p^2$.

Roughly speaking, reason:

- Feistel $\mathcal{F}(x_0, x_1) = (x_1 + \mathrm{F}(x_0), x_0)$: F depends on one input only;
- redundant Lai-Massey $\mathcal{LM}^R(x_0, x_1) = (x_0 + \mathrm{G}(x_0, x_1), x_1 + \mathrm{G}(x_0, x_1))$ just proposed:

$$\mathrm{G}(x_0, x_1) = \alpha \cdot (x_0 - x_1)^2 \cdot (x_0 + x_1)$$

  depends on two inputs.

(Note that $x_0 - x_1$ and $x_0 + x_1$ are linearly independent)

Table of Contents

Amaryllises Schemes [Gra22]

Let $q = p^s$ as before, and let $n \geq 2$. Let

1. $\mathrm{F} : \mathbb{F}_q \to \mathbb{F}_q$ be a function s.t. (i) $\mathrm{F}(0) \neq 0$ and (ii) $\mathrm{G}(x) := x \cdot \mathrm{F}(x)$ is invertible over $\mathbb{F}_q$ *(similar to before!)*;
2. $\mathrm{H} : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ be any function;
3. $\beta_0, \beta_1, \ldots, \beta_{n-1} \in \mathbb{F}_q \setminus \{0\}$ s.t. $\sum_{i=0}^{n-1} \beta_i = 0$ **if** H is *not* identically equal to zero ;
4. $\forall j \in \{0, 1, \ldots, n-2\}$, let $\{\gamma_i^{(j)}\}_{i \in \{0,1,\ldots,n-1\}}$ be s.t. $\gamma_i^{(j)} \in \mathbb{F}_q$ and $\sum_{i=0}^{n-1} \gamma_i^{(j)} = 0$.

The Amaryllises scheme $\mathcal{A}$ over $\mathbb{F}_q^n$ defined as $\mathcal{A}(x_0, x_1, \ldots, x_{t-1}) := y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i = x_i \cdot \mathrm{F}\left(\sum_{j=0}^{n-1} \beta_j \cdot x_j\right) + \mathrm{H}\left(\sum_{j=0}^{n-1} \gamma_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \gamma_j^{(n-2)} \cdot x_j\right)$$

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

Amaryllises Schemes [Gra22]

Let $q = p^s$ as before, and let $n \geq 2$. Let

1. $\mathsf{F} : \mathbb{F}_q \to \mathbb{F}_q$ be a function s.t. (i) $\mathsf{F}(0) \neq 0$ and (ii) $\mathsf{G}(x) := x \cdot \mathsf{F}(x)$ is invertible over $\mathbb{F}_q$ *(similar to before!)*;
2. $\mathsf{H} : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ be any function;
3. $\beta_0, \beta_1, \ldots, \beta_{n-1} \in \mathbb{F}_q \setminus \{0\}$ s.t. $\sum_{i=0}^{n-1} \beta_i = 0$ **if** H is *not* identically equal to zero ;
4. $\forall j \in \{0, 1, \ldots, n-2\}$, let $\{\gamma_i^{(j)}\}_{i\in\{0,1,\ldots,n-1\}}$ be s.t. $\gamma_i^{(j)} \in \mathbb{F}_q$ and $\sum_{i=0}^{n-1} \gamma_i^{(j)} = 0$.

The Amaryllises scheme $\mathcal{A}$ over $\mathbb{F}_q^n$ defined as $\mathcal{A}(x_0, x_1, \ldots, x_{t-1}) := y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i = x_i \cdot \mathsf{F}\left(\sum_{j=0}^{n-1} \beta_j \cdot x_j\right) + \mathsf{H}\left(\sum_{j=0}^{n-1} \gamma_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \gamma_j^{(n-2)} \cdot x_j\right)$$

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

Invertibility of Amaryllises Schemes

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Invertibility follows from:

- recover $\sum_{i=0}^{n-1} \beta_i \cdot x_i$ by exploiting (1) and (3):

$$\sum_{i=0}^{n-1} \beta_i \cdot y_i = \left(\sum_{i=0}^{n-1} \beta_i \cdot x_i\right) \cdot \mathrm{F}\left(\sum_{i=0}^{n-1} \beta_i \cdot x_i\right) + \mathrm{H}\left(\sum_{i=0}^{n-1} \gamma_i^{(0)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \gamma_i^{(n-1)} \cdot x_i\right) \cdot \underbrace{\sum_{i=0}^{n-1} \beta_i}_{=0}$$

$$= \mathrm{G}\left(\sum_{i=0}^{n-1} \beta_i \cdot x_i\right) \quad \longrightarrow \quad \sum_{i=0}^{n-1} \beta_i \cdot x_i = \mathrm{G}^{-1}\left(\sum_{i=0}^{n-1} \beta_i \cdot y_i\right);$$

- given $\sum_{i=0}^{n-1} \beta_i \cdot x_i$ and since $\mathrm{F}(z) \neq 0$ for each $z \in \mathbb{F}_q$, recover $\sum_{j=0}^{n-1} \gamma_j^{(i)} \cdot x_j$ as in a standard Lai-Massey scheme.

Contracting-Amaryllises Schemes [Gra22]

Let $q = p^s$ as before, and let $n \geq 2$. Let

1. $e \geq 1$ be an integer such that $\gcd(e, q-1) = 1$;
2. $F : \mathbb{F}_q^n \to \mathbb{F}_q \setminus \{0\}$ be a function that (i) never returns zero for any non-zero input (i.e., $F(x) = 0$ if only if $x = 0 \in \mathbb{F}_q^n$), and s.t. (ii) the function $G_{\alpha_0,\alpha_1,\ldots,\alpha_{n-1}}(x) : \mathbb{F}_q \to \mathbb{F}_q$ defined as
$$G_{\alpha_0,\alpha_1,\ldots,\alpha_{n-1}}(x) := x^e \cdot F(\alpha_0 \cdot x, \alpha_1 \cdot x, \ldots, \alpha_{n-1} \cdot x)$$
is invertible for each arbitrary fixed non-null $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n \setminus \{(0, 0, \ldots, 0)\}$.

The Contracting-Amaryllises scheme $\mathcal{A}_C$ over $\mathbb{F}_q^n$ defined as $\mathcal{A}_C(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i = x_i^e \cdot F(x_0, x_1, \ldots, x_{n-1})$$

is invertible.

Contracting-Amaryllises Schemes [Gra22]

Let $q = p^s$ as before, and let $n \geq 2$. Let

1. $e \geq 1$ be an integer such that $\gcd(e, q-1) = 1$;
2. $F : \mathbb{F}_q^n \to \mathbb{F}_q \setminus \{0\}$ be a function that (i) never returns zero for any non-zero input (i.e., $F(x) = 0$ if only if $x = 0 \in \mathbb{F}_q^n$), and s.t. (ii) the function $G_{\alpha_0,\alpha_1,\ldots,\alpha_{n-1}}(x) : \mathbb{F}_q \to \mathbb{F}_q$ defined as

$$G_{\alpha_0,\alpha_1,\ldots,\alpha_{n-1}}(x) := x^e \cdot F(\alpha_0 \cdot x, \alpha_1 \cdot x, \ldots, \alpha_{n-1} \cdot x)$$

   is invertible for each arbitrary fixed non-null $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n \setminus \{(0, 0, \ldots, 0)\}$.

The Contracting-Amaryllises scheme $\mathcal{A}_C$ over $\mathbb{F}_q^n$ defined as $\mathcal{A}_C(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i = x_i^e \cdot F(x_0, x_1, \ldots, x_{n-1})$$

is invertible.

Invertibility of Contracting-Amaryllises Schemes

Note:

1. $y_i = 0 \qquad \longleftrightarrow \qquad x_i = 0$;
2. since F never returns zero, then for each $i, j \in \{0, 1, \ldots, n-1\}$:

$$y_i \cdot x_j^e = y_j \cdot x_i^e \,.$$

Assume $y_i \neq 0$. Since $x \mapsto x^e$ is invertible, then

$$\begin{aligned} y_i &= x_i^e \cdot \mathrm{F}\left(\left(\frac{y_0}{y_i}\right)^{\frac{1}{e}} \cdot x_i, \ldots, \left(\frac{y_{i-1}}{y_i}\right)^{\frac{1}{e}} \cdot x_i, x_i, \left(\frac{y_{i+1}}{y_i}\right)^{\frac{1}{e}} \cdot x_i, \ldots, \left(\frac{y_{n-1}}{y_i}\right)^{\frac{1}{e}} \cdot x_i\right) \\ &\equiv \mathrm{G}_{\left(\frac{y_0}{y_i}\right)^{\frac{1}{e}}, \ldots, \left(\frac{y_{i-1}}{y_i}\right)^{\frac{1}{e}}, 1, \left(\frac{y_{i+1}}{y_i}\right)^{\frac{1}{e}}, \ldots, \left(\frac{y_{n-1}}{y_i}\right)^{\frac{1}{e}}}(x_i) \,. \end{aligned}$$

By inverting G, it is possible to find x_i.

Invertibility of Contracting-Amaryllises Schemes

Note:

1. $y_i = 0 \quad \longleftrightarrow \quad x_i = 0$;
2. since F never returns zero, then for each $i, j \in \{0, 1, \dots, n-1\}$:

$$y_i \cdot x_j^e = y_j \cdot x_i^e \,.$$

Assume $y_i \neq 0$. Since $x \mapsto x^e$ is invertible, then

$$\begin{aligned} y_i &= x_i^e \cdot \mathrm{F}\left(\left(\frac{y_0}{y_i}\right)^{\frac{1}{e}} \cdot x_i, \dots, \left(\frac{y_{i-1}}{y_i}\right)^{\frac{1}{e}} \cdot x_i, x_i, \left(\frac{y_{i+1}}{y_i}\right)^{\frac{1}{e}} \cdot x_i, \dots, \left(\frac{y_{n-1}}{y_i}\right)^{\frac{1}{e}} \cdot x_i\right) \\ &\equiv \mathrm{G}_{\left(\frac{y_0}{y_i}\right)^{\frac{1}{e}}, \dots, \left(\frac{y_{i-1}}{y_i}\right)^{\frac{1}{e}}, 1, \left(\frac{y_{i+1}}{y_i}\right)^{\frac{1}{e}}, \dots, \left(\frac{y_{n-1}}{y_i}\right)^{\frac{1}{e}}}(x_i)\,. \end{aligned}$$

By inverting G, it is possible to find x_i.

Constructing $G_{\alpha_0,\alpha_1,\ldots,\alpha_{n-1}}(x) : \mathbb{F}_q \to \mathbb{F}_q$

CASA
Cyber Security in the Age of Large-Scale Adversaries

Let $d \geq 3$ be such that $\gcd(d, q-1) = 1$. Let $F : \mathbb{F}_q^n \to \mathbb{F}_q$ be an **homogeneous function** of degree $d - e$ (i.e., it contains only monomial of degree $d - e$) such that $F(x) = 0$ if only if $x = 0 \in \mathbb{F}_q^n$. Then:

$$\begin{aligned} G_{\alpha_0,\alpha_1,\ldots,\alpha_{n-1}}(x) &= x^e \cdot F(\alpha_0 \cdot x, \alpha_1 \cdot x, \ldots, \alpha_{n-1} \cdot x) \\ &= x^d \cdot F(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \end{aligned}$$

is invertible (since $x \mapsto x^d$ is invertible, and $F(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \neq 0$ by assumption).

(See [Gra22] for other concrete examples.)

Table of Contents

Summary and Open Problems

New invertible non-linear layers for symmetric schemes!

Open Problems:

1. exploit the EA-equivalence (and/or the CCZ one?) between Feistel and Lai-Massey schemes for transferring known results;
2. analyze the *statistical and the algebraic cryptographic properties* of the proposed schemes:
   - an initial study proposed in [Gra22] and in [RS22];
   - what about the degree of regularity over multiple rounds?
3. analyze the *impact* on the design: is it possible to improve the performances of current schemes?
4. set up other invertible non-linear schemes.

References I

- L. Grassi
  On Generalizations of the Lai-Massey Scheme: the Blooming of Amaryllises.
  IACR Cryptol. ePrint Arch. 2022/1245
- L. Grassi, Y. Hao, C. Rechberger, M. Schofnegger, R. Walch, Q. Wang
  Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications.
  CRYPTO 2023
- A. Roy, M. J. Steiner
  Generalized Triangular Dynamical System: An Algebraic System for Constructing Cryptographic Permutations over Finite Fields.
  Corr arXiv:2204.01802

Thanks for your attention!

Questions?

Comments?