On Generalizations of the Lai-Massey Scheme

Lorenzo Grassi

Ruhr University Bochum, Bochum, Germany
Lorenzo.Grassi@ruhr-uni-bochum.de

Abstract. In this paper, we re-investigate the Lai-Massey scheme, originally proposed in the cipher IDEA. Due to the similarity with the Feistel networks, and due to the existence of invariant subspace attacks as originally pointed out by Vaudenay at FSE 1999, the Lai-Massey scheme has received only little attention by the community. As first contribution, we propose two new generalizations of such scheme that are not (extended) affine equivalent to any generalized Feistel network proposed in the literature so far. Then, inspired by the recent `Horst` construction, we propose the `Amaryllises` structure as a generalization of the Lai-Massey scheme, in which the linear combination in the Lai-Massey scheme can be replaced by a non-linear one. Besides proposing concrete examples of the `Amaryllises` construction, we analyze its cryptographic properties, and we compare them with the ones of other existing schemes/constructions published in the literature. Our results show that the `Amaryllises` construction could have concrete advantages especially in the context of MPC-/FHE-/ZK-friendly primitives.

Keywords: Generalized/Redundant Lai-Massey · Amaryllises · Generalized Feistel · Horst

1 Introduction

Probably, the two most popular design frameworks for iterated symmetric primitives are the Substitution-Permutation Network (SPN) and the Feistel one (FN). In the SPN case, the input of each round is divided into multiple small sub-blocks, a non-linear function (called S-Box) is applied on each sub-block, followed by an affine transformation that mixes the sub-blocks.[1] The invertibility of the entire construction depends on the invertibility of each sub-component. The scenario is different in the FN case. In each round of a Feistel network, the input is split into two halves, a function $\mathcal{F}$ is applied on one of the two halves, which is successively mixed with the other part, just before the two halves are swapped, that is, $[x_0, x_1] \mapsto [y_0, y_1] := [x_1 + \mathcal{F}(x_0), x_0]$. With respect to the SPN case, FNs are invertible by construction independently of the details of the $\mathcal{F}$-function. Hence, the designer can choose among a larger class of non-linear functions in order to instantiate a FN with respect to what happens in SPNs, since no condition on the invertibility is imposed. Moreover, the costs of computing a Feistel network in the forward and in the backward direction are very similar (even identical in some cases), since the same $\mathcal{F}$-function is computed in the two processes. Due to these facts, a large proportion of symmetric primitives adopts the Feistel design approach, including DES, Blowfish [Sch93], MISTY [Mat97], among others, and several generalizations have been proposed in the literature, including Type-I/-II/-III Feistel networks [ZMI90, Nyb96]

Another design strategy that has many points in common with the FNs is the Lai-Massey one [Vau99], introduced after the design of IDEA [LM90]. As in the case of a FN,

[1] In this paper, we do not make any distinction between the case in which this affine permutation is just a shuffle plus a round-constant addition as in Present [BKL+07], or a more complex affine transformation as in AES [DR00, DR20].

the input is first split into two halves, but in this case a function $\mathcal{F}$ is applied on their difference, and the result of such function is then added to each input, that is,

$$[x_0, x_1] \mapsto [y_0, y_1] := [x_0 + \mathcal{F}(x_0 - x_1), x_1 + \mathcal{F}(x_0 - x_1)] \,. \tag{1}$$

Analogous to the FNs, the invertibility of Lai-Massey schemes follows from its construction, that is, it is independent of details of the function $\mathcal{F}$. However, compared to the FNs, the Lai-Massey scheme is much less studied in the literature, and only few concrete Lai-Massey schemes have been proposed in the literature. This is due to several factors, including the following:

1. a Lai-Massey scheme as the one just proposed can be easily broken due to the existence of an invariant subspace attack, as first pointed out by Vaudenay [Vau99];
2. it seems that Lai-Massey schemes do not have any concrete advantage with respect to Feistel networks, as stated by Yun et al. in [YPL11, Sect. 8]: "*as a cryptographic design, the Lai-Massey cipher does not have any advantage over the Feistel in terms of the Luby-Rackoff model*".

In this paper, we re-consider the Lai-Massey construction, and we present new generalizations of it that are not affine equivalent to any generalized Feistel network proposed in the literature so far. Moreover, we introduce the generalized `Amaryllises` construction, a new generalization of the Lai-Massey one in which the linear combination between the function $\mathcal{F}$ and the halves that composed the input can be replaced by a non-linear combination.

1.1 Generalized and Redundant Lai-Massey Schemes

Relation between Generalized Feistel and Lai-Massey Schemes

The simplest generalization of a Lai-Massey scheme recently proposed in [GØSW23] and recalled in Sect. 3 works as following:

1. first, the input message is divided in $n \geq 2$ sub-blocks;
2. a function $\mathcal{F}$ is applied to zero-sum linear combinations of such sub-blocks (that is, the sum of the coefficients that define the linear combination is zero);
3. the result of such function is then added to each input.

In Sect. 3.2, we prove that any Lai-Massey scheme of that form is *affine equivalent* to a generalized Feistel network, that is, a Lai-Massey scheme of this form is equal to a generalized FN pre- and post-processed with affine invertible transformations. Equivalently, any iterated symmetric primitive instantiated with a Lai-Massey scheme is equivalent to an iterated scheme whose round function is a Feistel network followed by an affine invertible operation (besides an initial and a final invertible affine transformation).

As a direct consequence of this, it follows that the linear and the differential properties of any Lai-Massey scheme are equal to the ones of the affine equivalent Feistel network.

New Generalizations of the Lai-Massey Schemes

Based on the previous results, it seems there is no concrete reason to prefer a Lai-Massey scheme with respect to a Feistel network. Still, it is possible that generalizations of the Lai-Massey schemes exist such that are not affine equivalent to any Feistel network (hence, they can potentially have better linear and differential properties), but still they preserve the "properties" tat characterize a Lai-Massey scheme.

For this reason, as next step, in Sect. 4 and 5, we propose two new generalizations of the Lai-Massey scheme with the aim to capture the "essence" of a Lai-Massey scheme. They are:

- the **generalized Lai-Massey schemes**: instead of adding the same fixed function to each input, we allow for *different functions that still take zero-sum linear combinations of the sub-blocks, under the condition that the entire scheme is invertible*;
- the **redundant Lai-Massey schemes**: instead of limiting ourselves to consider a function which takes as inputs zero-sum linear combinations of the sub-blocks, we allow for *any fixed function F for which the entire construction is invertible.*

Formal definitions are given in Sect. 4 and 5, respectively Def. 4 and Def. 5. Concrete examples of generalized and redundant Lai-Massey schemes over a field $\mathbb{F}_q^n$ (where $q = p^s$ for a prime $p \geq 2$ and a positive integer s) that are *not* extended affine equivalent to any generalized Feistel network are also given in Sect. 4 and 5.

1.2 `Amaryllises` for MPC-/FHE-/ZK-Friendly Symmetric Primitives

MPC-/FHE-/ZK-Friendly Symmetric Primitives

Currently, one of the hottest topics in symmetric cryptography regards the design and the analysis of symmetric primitives for applications such as Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge (ZK). Those applications require dedicated symmetric primitives that *minimize the number of field multiplications required to compute and/or to verify the primitive in its natural algorithmic description.*

In contrast to traditional/classical symmetric primitives like AES and Keccak/SHA-3 defined over $\mathbb{F}_{2^n}^t$ for small $n \in \{3, 4, \ldots, 8\}$, these new MPC-/FHE-/ZK-friendly primitives usually operate over a vector space $\mathbb{F}_p^t$ for a huge prime p such as $p \approx 2^{128}$ or $p \approx 2^{256}$. The main reason behind this regards the fact that such applications make use of primitives from public-key cryptography as well, which are in general defined over prime fields. Hence, when working with such applications, it is more convenient to deal with a symmetric primitive that works directly over a prime field, rather than one instantiated over $\mathbb{F}_{2^n}^t$ and that requires a conversion from/to the vector space over the prime field. Before going on, we limit ourselves to recall that, unlike in the case of traditional symmetric primitives, the size of the field over which the symmetric primitive is defined has usually a small impact on the overall cost of the considered applications.

The particular cost metric these MPC-/FHE-/ZK-friendly symmetric primitives aim to minimize has a crucial impact on their design strategy. Due to the huge size of p, no function can be pre-computed and stored as a look-up table. Hence, a MPC-/FHE-/ZK-friendly symmetric primitive must admit a *simple algebraic expression.* For example, the majority of the MPC-/FHE-/ZK-friendly symmetric primitives are instantiated with invertible power maps $x \mapsto x^d$ over $\mathbb{F}_p$. (We emphasize that a simple algebraic expression does not imply low-degree in general.) Besides, this design approach also allows to minimize the *multiplicative complexity*, that is, the number of multiplications for evaluating and/or verifying the system of polynomials equations associated to the symmetric primitive.

As a direct consequence of this fact, algebraic attacks are usually much stronger than statistical attacks in the case of MPC-/FHE-/ZK-friendly primitives. As designing symmetric primitives in this domain is relatively new and not well understood yet, several algebraic attacks have recently been proposed in the literature, breaking the security claims of many of the proposed primitives. Just to cite some of them, Gröbner basis attacks have been recently proposed on full *Jarvis* and *Friday* [ACG+19], on some (weak) instances of Poseidon and Starkad [BCD+20, BBLP22], on full *Grendel* [GKRS22], and on Ciminion [BBLP22, Bar23].

Dedicated Design Strategies

Due to all these facts, the different cost metrics these primitives aim to minimize pushed the designers to look for new design strategies. Concretely, let's consider the case of

Advanced Encryption Standard (AES) [DR00, DR20], probably the most well studied and used block cipher. As it is well known, the design principle of the AES is the "wide-trail design" strategy [DR01, DR02], which allows the designer to provide simple, elegant and formal arguments for guaranteeing security against two of the most powerful statistical attacks, namely, the linear [Mat93] and the differential [BS90, BS93] attacks. Even if several MPC-/FHE-/ZK-friendly symmetric primitives make use of the "wide-trail design" strategy, such strategy by itself does not provide any concrete argument for guaranteeing security against the algebraic attacks, which – as we recalled before – are the *main threats* for these dedicated symmetric primitives.

For this reason, the research of symmetric primitives that minimize the multiplicative complexity while providing a sufficient security level is an opportunity for exploring and evaluating innovative and dedicated design strategies. Without going into the details, examples of some recent innovative and dedicated design strategies include:

- **`Horst` in Griffin**: the `Horst` construction recently introduced by Grassi et al. [GHR+23] is a variant of the Feistel network, in which a non-linear mixing takes place. In particular, it is defined over $\mathbb{F}_q^2$ as $[x_0, x_1] \mapsto [y_0, y_1] := [x_1 \cdot \mathcal{G}(x_0) + \mathcal{F}(x_0), x_0]$. Even if a single round of `Horst` is obviously more expensive than a single round of a Feistel network, the Griffin's designers showed that such construction has concrete advantages in order to defeat the Gröbner basis attack over multiple rounds, making it overall more efficient than a Feistel network;
- **`Flystel` in Anemoi**: the `Flystel` [BBC+23] is a particular 3-round Feistel network over $\mathbb{F}_q^2$. Over a prime field, its rounds are instantiated via the power maps $x \mapsto x^2$ and $x \mapsto x^{1/d}$, where $d \geq 3$ is the smallest integer co-prime with $p-1$. The advantage of such non-linear function relies on the cheap cost necessary to verify it. For this reason, it is used to instantiate the S-Boxes of the SPN Anemoi;
- **Generalized Triangular Dynamical System (GTDS) in Arion**: the GTDS [RS22] is a general non-linear layer defined as the combination of a SPN' S-Box layer with a `Horst` construction (see App. A for more details). It instantiates the non-linear of the hash function Arion [RST23].

We limit ourselves to mention that particular mode of operations (such as a modified version of Farfalle [BDH+17] in Ciminion [DGGK21], or Megafono in Hydra [GØSW23]) have been also introduced in order to guarantee security and/or to increase the efficiency of the proposed primitives. However, since they are out of the scope of this paper, we omit their details.

The Blooming of `Amaryllises`

The details of the non-linear layer of a MPC-/FHE-/ZK-friendly primitive plays a crucial role for what concerning the security and the performance of the primitive itself. Indeed, remember that such primitives aim to minimize the multiplicative complexity, and at the same time that they are particularly vulnerable to algebraic attacks. Both these two facts are strictly related to the details of the non-linear layer that instantiates the primitive itself. Based on this, it is crucial to design new and innovative dedicate non-linear layers that can be used to design new MPC-/FHE-/ZK-friendly primitive in such a way to improve their efficiency without affecting the security.

We concretely face this problem in this paper. Taking inspiration from the `Horst` construction, we propose a variant of the Lai-Massey scheme in which the linear combinations can be replaced with non-invertible ones. We call this new construction as the "`Amaryllises`" construction.[2] A formal definition is given in Theorem 4 – see Sect. 6. In

[2]We decided to call it as the flowers *ama(r)yl(l)ises*, since such word is (almost) the anagram of Lai-Massey.

there, we also show how to concrete instantiate it in an efficient way. Next, in Sect. 7, we propose an initial generic analysis of its statistical and algebraic properties, and we discuss its possible advantages and disadvantages with respect to other non-linear layer constructions proposed in the literature so far.

2 Preliminary

In this initial section, we introduce the notation and recall some well-known results that we are going to use in the following.

Notation. Let $q = p^s$ where $p \geq 2$ is a prime number and $s \geq 1$ is a positive integer. Let $\mathbb{F}_q$ denote the Galois Field of order q. We use small letters to denote both indexes and variables, and greek letters to denote fixed elements (as parameters) in $\mathbb{F}_q$. We use the calligraphic font to denote functions, with the only exceptions of linear/affine functions denoted via the capital font. We use the frankfurt font (e.g., $\mathfrak{X}$) to denote sets of elements, and $|\cdot|$ to denote their cardinality. Given $x \in \mathbb{F}_q^n$, we denote by x_i its i-th component for each $i \in \{0, 1, \ldots, n-1\}$, that is, $x = [x_0, x_1, \ldots, x_{n-1}] \equiv x_0 \| x_1 \| \ldots \| x_{n-1}$, where the symbol $\cdot\|\cdot$ denotes concatenation. Given a matrix $M \in \mathbb{F}_q^{n\times m}$, we denote the entry in the r-th row and in the c-th column by $M_{r,c}$. We use $\langle s^{(0)}, s^{(1)}, \ldots, s^{(t-1)} \rangle \subseteq \mathbb{F}_q^n$ to denote the linear span of the vectors $s^{(0)}, s^{(1)}, \ldots, s^{(t-1)} \in \mathbb{F}_q^n$.

For the follow-up, we introduce the following definition.

Definition 1. Let $n \geq 2$ be an integer, and let $q = p^s$ be as before. Let $1 \leq l \leq n-1$. We say that the sets $\{\lambda_j^{(0)}\}_{j\in\{0,1,\ldots,n-1\}}, \{\lambda_j^{(1)}\}_{j\in\{0,1,\ldots,n-1\}}, \ldots, \{\lambda_j^{(l-1)}\}_{j\in\{0,1,\ldots,n-1\}}$ with $\lambda_j^{(i)} \in \mathbb{F}_q$ for each i, j are "*zero-sum linearly independent*" if the following conditions are satisfied:

- for each $i \in \{0, 1, \ldots, l-1\}$: $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$;
- the vectors $[\lambda_0^{(0)}, \lambda_1^{(0)}, \ldots, \lambda_{n-1}^{(0)}]$, $[\lambda_0^{(1)}, \lambda_1^{(1)}, \ldots, \lambda_{n-1}^{(1)}]$, $\ldots$, $[\lambda_0^{(l-1)}, \lambda_1^{(l-1)}, \ldots, \lambda_{n-1}^{(l-1)}]$ are linearly independent.

We point out that the range of l follows from the fact that there are *at most* $n-1$ $\mathbb{F}_q^n$-vectors such that (i) their entries sum to zero, and that (ii) they are linearly independent.

Generalized Feistel Networks and Horst Constructions

Regarding the definition of generalized Feistel networks, we propose the following:

Definition 2 (Generalized Feistel Schemes)**.** Let $q = p^s$ be as before, and let $n \geq 2$. For each $i \in \{1, 2, \ldots, n-1\}$, let $\mathcal{F}_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be a function. The generalized Feistel network $\mathtt{F}_\mathrm{G}$ over $\mathbb{F}_q^n$ is defined as $\mathtt{F}_\mathrm{G}(x_0, x_1, \ldots, x_{n-1}) := y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i := \begin{cases} x_{i+1} + \mathcal{F}_{i+1}(x_0, x_1, \ldots, x_i) & \text{if } i \in \{0, 1, \ldots, n-2\}\,; \\ x_0 & \text{otherwise (if } i = n-1)\,. \end{cases}$$

It is not difficult to check that any Feistel network proposed in the literature including [ZMI90, Nyb96, HR10, BS13] satisfy the definition just given. As it is well known, the invertibility of the entire construction is independent of the details of $\mathcal{F}_0, \ldots, \mathcal{F}_{n-2}$. Indeed, we have that (i) $x_0 = y_{n-1}$, and (ii) for each $i \geq 1$, $x_i = y_{i-1} - \mathcal{F}_i(x_0, x_1, \ldots, x_{i-1})$ where y_{i-1} and $x_0, x_1, \ldots, x_{i-1}$ are given.

The `Horst` construction recently proposed by Grassi et al. [GHR+23] is a generalization of the Feistel networks in which the linear combination is replaced by a linear one. As a concrete example over $\mathbb{F}_q^2$:

$$(x_0, x_1) \mapsto (x_1 + \mathcal{F}(x_0), x_0) \qquad \textit{versus} \qquad (x_0, x_1) \mapsto (x_1 \cdot \mathcal{G}(x_0) + \mathcal{F}(x_0), x_0)$$

for $\mathcal{F}, \mathcal{G}$ over $\mathbb{F}_q$. More formally:

Theorem 1 (`Horst` [GHR+23])**.** *Let $q = p^s$ be as before, and let $n \geq 2$ be an integer. For each $i \in \{1, 2, \ldots, n-2\}$, let $\mathcal{F}_i, \mathcal{G}_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be $2 \cdot (n-1)$ functions, where $\mathcal{G}_i(x_0, x_1, \ldots, x_{i-1}) \neq 0$ for each $x_0, x_1, \ldots, x_{i-1} \in \mathbb{F}_q$. The `Horst` construction $\mathtt{H}$ over $\mathbb{F}_q^n$ defined as $\mathtt{H}(x_0, x_1, \ldots, x_{n-1}) := y_0 \| y_1 \| \ldots \| y_{n-1}$ where*

$$y_i := \begin{cases} x_{i+1} \cdot \mathcal{G}_{i+1}(x_0, x_1, \ldots, x_i) + \mathcal{F}_{i+1}(x_0, x_1, \ldots, x_i) & \text{if } i \in \{0, 1, \ldots, n-2\} \\ x_0 & \text{otherwise } (i = n-1) \end{cases}$$

is invertible.

The invertibility holds due to the same argument previously given for the Feistel networks, and since $\mathcal{G}$ always returns a non-zero element.

Extended-Affine (EA) Equivalence

Two functions $\mathcal{F}$ and $\mathcal{G}$ are Extended-Affine (EA) equivalent if they satisfy the following requirement.

Definition 3 (EA-Equivalence)**.** Let $q = p^s$ be as before. Let $n, m \geq 1$, and let $\mathcal{F}, \mathcal{G} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be two functions. $\mathcal{F}$ and $\mathcal{G}$ are *extended-affine equivalent* (EA-equivalent) if there exist two affine permutations $A : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $B : \mathbb{F}_q^m \to \mathbb{F}_q^m$, and an affine function $C : \mathbb{F}_q^n \to \mathbb{F}_q^m$ such that

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

If C is identically equal to zero, then we speak of affine equivalence (A-equivalence).

We limit ourselves to recall that if two functions $\mathcal{F}$ and $\mathcal{G}$ are EA-equivalent, then they share several statistical properties (besides e.g. having the same degree). As a concrete example, the maximum differential probability $\text{DP}_{\max}$ of $\mathcal{F}$ and of $\mathcal{G}$ are equal, where $\text{DP}_{\max}(\mathcal{H}) := \max_{\delta \neq 0, \Delta} |\{x \in \mathbb{F}_q^n \mid \mathcal{H}(x+\delta) - \mathcal{H}(x) = \Delta\}| / q^n$. We refer to [CCZ98, CP19] for more details.

3 Lai-Massey Schemes in the Literature

Given a function $\mathcal{F}$ over $\mathbb{F}_q$ for $q = p^s$ as before, the Lai-Massey scheme over $\mathbb{F}_q^2$ introduced in [LM90] is defined as in (1). Its invertibility follows from the fact that $y_0 - y_1 = x_0 - x_1$, and so $x_j = y_j - \mathcal{F}(y_0 - y_1)$ for each $j \in \{0, 1\}$.

3.1 Lai-Massey Schemes over $\mathbb{F}_q^{\geq 2}$ from [GØSW23]

A possible generalization of the Lai-Massey scheme over $\mathbb{F}_q^n$ for $n \geq 2$ has been recently proposed in [GØSW23].[3]

[3] To be precise, the following proposition is a slightly modified version of the result proposed in [GØSW23]. In there, authors assume $\alpha_i = 1$ for each $i \in \{0, 1, \ldots, n-1\}$.

Proposition 1 (Prop. 1, [GØSW23]). *Let $n \geq 2$ be an integer, and let $q = p^s$ be as before. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_p \setminus \{0\}$. Let $l \in \{1, 2, \ldots, n-1\}$. Let $\mathcal{F} : \mathbb{F}_q^l \to \mathbb{F}_q$ be a function. Let $\{\lambda_j^{(i)}\}_{j\in\{0,1,\ldots,n-1\}, i\in\{0,1,\ldots,l-1\}}$ be l "zero-sum linearly independent" sets as in Def. 1.*

The Lai-Massey scheme `LM` *over $\mathbb{F}_q^n$ defined as $\texttt{LM}(x_0, x_1, \ldots, x_{n-1}) := y_0\|y_1\| \ldots \|y_{n-1}$ where*

$$y_i := \alpha_i \cdot \left(x_i + \mathcal{F}\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot x_j\right)\right)$$

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

As for the case of the Lai-Massey scheme over $\mathbb{F}_q^2$, the invertibility holds since

$$\forall i \in \{0, 1, \ldots, l-1\} : \qquad \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j = \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot \frac{y_j}{\alpha_j}\,.$$

Existence of Invariant Subspace Trails

As already pointed out by Vaudenay in [Vau99] for the $\mathbb{F}_q^2$ case, there could exist invariant subspaces for the Lai-Massey scheme proposed in Prop. 1. Following [GRR16],[4] we recall that a set $\mathfrak{X}$ is *invariant* for a keyed/unkeyed function $\mathcal{F}_k$ over $\mathbb{F}_q^n$ if for each key/constant $k \in \mathbb{F}_q^n$ and for each $\beta \in \mathbb{F}_q^n$, there exists $\gamma \in \mathbb{F}_q^n$ such that

$$\mathcal{F}_k(\mathfrak{X} + \beta) := \{\mathcal{F}_k(x) \mid x \in \mathfrak{X} + \beta\} = \mathfrak{X} + \gamma\,.$$

As a concrete example, the Lai-Massey scheme `LM` defined as in Prop. 1 over $\mathbb{F}_q^n$ and instantiated by $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$ admits

$$\mathfrak{X} := \left\{x \in \mathbb{F}_q^n \mid \forall i \in \{0, 1, \ldots, l-1\} : \quad \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j = 0\right\}$$

as an *invariant* subspace. Note that such set is never empty as $\langle[1, 1, \ldots, 1]\rangle \equiv \{[x, x, \ldots, x] \in \mathbb{F}_q^n \mid x \in \mathbb{F}_q\} \subseteq \mathfrak{X}$ independently of the values of $\lambda_j^{(i)}$, since $\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x = x \cdot \sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$ for each $i \in \{0, 1, \ldots, l-1\}$, due to the assumption on $\lambda_j^{(i)}$. More generally, it is not hard to check that $\dim(\mathfrak{X}) = n - \dim(\langle[\lambda_0^{(0)}, \lambda_1^{(0)}, \ldots, \lambda_{n-1}^{(0)}], \ldots, [\lambda_0^{(l-1)}, \lambda_1^{(l-1)}, \ldots, \lambda_{n-1}^{(l-1)}]\rangle) = n - l \geq 1$, where the equality follows from the linear-independent assumption on the sets $\{\lambda_j^{(i)}\}_{j\in\{0,1,\ldots,n-1\}}$.

How to Break such Invariant Subspaces? Several strategies are possible for destroying such invariant subspace trails. One possibility consists in applying an invertible linear layer defined via the multiplication with an invertible matrix $M \in \mathbb{F}_q^{n\times n}$ that does not admit any invariant subspace (i.e., such that no subspace $\mathfrak{Z} \subseteq \mathbb{F}_q^n$ satisfies $M \times \mathfrak{Z} = \mathfrak{Z}$) after each `LM` round. Since this topic is out of the scope of this paper, we refer to [GØSW23] for more details.

We limit ourselves to analyze in more details the case $l = n-1$, that is, the case in which $\mathcal{F}$ depends on *all* the zero-sum linearly independent combinations of $\{x_0, x_1, \ldots, x_{n-1}\}$. In such a case, the invariant subspace $\mathfrak{X}$ coincides with $\langle[1, 1, \ldots, 1]\rangle$. In order to destroy

[4] For completeness, we point out that we limit ourselves to consider subspaces that are invariant independently of the value of the secret key. In this sense, the definition used here is different from the one proposed in [LAAZ11, LMR15], in which it is assumed that weak keys exist for which the subspace is invariant.

it, it is sufficient to impose that at least two coefficients α_i and α_j are different,[5] besides adding round constants that are not in the subspace $\langle[1, 1, \dots, 1]\rangle$ itself. We emphasize that this corresponds to the solution proposed by Vaudenay in [Vau99] (and recently re-considered in [AC21]) for breaking the invariant subspace $\langle[1, 1]\rangle$ of the Lai-Massey scheme over $\mathbb{F}_q^2$. Indeed, Vaudenay showed that the invariant subspace can be broken by applying an *orthomorphism* $\mathcal{S}$ on one of the two output of the Lai-Massey scheme, that is, $[x_0, x_1] \mapsto [\mathcal{S}(x_0 + \mathcal{F}(x_0 - x_1)), x_1 + \mathcal{H}(x_0 - x_1)]$. It is easy to check that $x \mapsto \alpha \cdot x + \beta$ for $\alpha \notin \{0, 1\}$ and $\beta \neq 0$ is an orthomorphism (we recall that a function $\mathcal{S}$ is an orthomorphism if and only if both $\mathcal{S}$ and $\mathcal{S}'(x) := \mathcal{S}(x) - x$ are permutations).

3.2 Relation between Feistel Networks and Lai-Massey Schemes

Next, we prove that the Lai-Massey scheme over $\mathbb{F}_q^n$ proposed in Prop. 1 is affine equivalent to a generalized Feistel network. More formally:

Proposition 2. *Let $q = p^s$ be as before, and let $n \geq 2$ be an integer. The Lai-Massey scheme over $\mathbb{F}_q^n$ defined as in Prop. 1 is affine equivalent to the generalized Feistel network defined in Def. 2.*

Proof. Here we limit ourselves to propose the proof for the case $n = 2$ only, that is, the A-equivalence between $[x_0, x_1] \mapsto [\alpha_0 \cdot (x_0 + \mathcal{F}(x_0 - x_1)), \alpha_1 \cdot (x_1 + \mathcal{F}(x_0 - x_1))]$ and $[x_0, x_1] \mapsto [x_1 + \mathcal{F}(x_0), x_0]$. The proof for the cases $n \geq 3$ is analogous, and it is proposed in App. B. In all cases, the proof reduces to find affine invertible transformations A and B over $\mathbb{F}_q^n$ for which the affine equivalence holds (C is always equal to 0 in the following). Since we only deal with linear invertible transformations $A, B : \mathbb{F}_q^n \to \mathbb{F}_q^n$, we simply identify them with the corresponding matrices in $\mathbb{F}_q^{n \times n}$.

Focusing on the Lai-Massey scheme `LM` over $\mathbb{F}_q^2$, it is easy to check that it is affine equivalent to the Feistel network `F` defined as $[x_0, x_1] \mapsto [x_1 + \mathcal{F}(x_0), x_0]$ via the invertible linear transformations

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} \alpha_0 & \alpha_0 \\ \alpha_1 & 0 \end{bmatrix}$$

and $C = 0$. Indeed,

$$\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \xrightarrow{A\times\cdot} \begin{bmatrix} x_0 - x_1 \\ x_1 \end{bmatrix} \xrightarrow{\texttt{F}(\cdot)} \begin{bmatrix} x_1 + \mathcal{F}(x_0 - x_1) \\ x_0 - x_1 \end{bmatrix} \xrightarrow{B\times\cdot} \begin{bmatrix} \alpha_0 \cdot (x_0 + \mathcal{F}(x_0 - x_1)) \\ \alpha_1 \cdot (x_1 + \mathcal{F}(x_0 - x_1)) \end{bmatrix},$$

which is the Lai-Massey scheme. That is, the Lai-Massey scheme is a Feistel network pre- and post-processed with two invertible linear functions. □

Remark 1. For completeness, we point out that the result just proposed is not new in the literature. For example, in [YPL11], Yun et al. introduced the concept of "quasi-Feistel" networks, a generic class of primitives over finite quasi-groups that includes as special cases both the Feistel networks and the Lai-Massey schemes. With respect to such result, this and the proof given in App. B point out the relation between Feistel networks and Lai-Massey schemes by directly showing the affine equivalence, without introducing any new function/construction.

[5] We suggest to impose all coefficients $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ to be pair-wise distinct. Moreover, we point out that the multiplications with the coefficients $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ correspond to multiply the `LM` scheme instantiated by $\alpha_0 = \alpha_1 = \dots = \alpha_{n-1} = 1$ with the diagonal matrix $M = \text{diag}(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in \mathbb{F}_q^{n \times n}$.

4 Generalized Lai-Massey Schemes

As next step, we discuss possible generalizations of the Lai-Massey scheme. Our goal is to introduce schemes that (i) capture the main idea of the Lai-Massey scheme, and that (ii) are not EA-equivalent to any Feistel network. (In the following, we denote the “EA-equivalence class” (or“EA-class” for brevity) of generalized Feistel networks as “Feistel EA-class”.) In this section, we focus on the "generalized Lai-Massey" schemes, while the "redundant Lai-Massey" schemes is discussed in the next one.

4.1 Definition of Generalized Lai-Massey Schemes

One main feature of the Lai-Massey scheme proposed in Prop. 1 regards the fact that the inputs of the function $\mathcal{F}$ are linear combinations of the inputs x_i defined via coefficients $\lambda_i^{(j)}$ that sum to zero (that is, $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$ for each $i \in \{0, 1, \ldots, l-1\}$). A possible generalization of such design could consist in allowing for n different functions $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_{n-1}$, under the restriction that their inputs are zero-sum linear combinations of x_i as before. More formally:

Definition 4 (Generalized Lai-Massey)**.** Let $q = p^s$ be as before, and let $n \geq 2$ be an integer. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q \backslash \{0\}$. Let $l \in \{1, 2, \ldots, n-1\}$. Let $\{\lambda_j^{(i)}\}_{j \in \{0,1,\ldots,n-1\}, i \in \{0,1,\ldots,l-1\}}$ be l "zero-sum linearly independent" sets as in Def. 1. Given n function $\mathcal{F}^{(0)}, \mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(n-1)} : \mathbb{F}_q^l \to \mathbb{F}_q$, let $\texttt{LM}_\text{G} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be defined as $\texttt{LM}_\text{G}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| y_2 \| \ldots \| y_{n-1}$ where for each $i \in \{0, 1, \ldots, n-1\}$:

$$y_i := \alpha_i \cdot \left(x_i + \mathcal{F}^{(i)} \left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot x_j \right) \right) .$$

We say that $\texttt{LM}_\text{G}$ is a generalized Lai-Massey scheme *if* it is invertible.

Obviously, the Lai-Massey scheme defined in Prop. 1 satisfies this definition. Other examples of invertible generalized Lai-Massey constructions over $\mathbb{F}_q^4$ (analogous over $\mathbb{F}_q^n$ for $n \geq 2$) include

$$[y_0, y_1, y_2, y_3] = [x_0 + \mathcal{F}(x_0 - x_1), x_1 + \mathcal{F}(x_0 - x_1), x_2, x_3] \,,$$
$$[y_0, y_1, y_2, y_3] = [x_0 + \mathcal{F}(x_0 - x_1), x_1 + \mathcal{F}(x_0 - x_1), x_2 + \mathcal{F}'(x_2 - x_3), x_3 + \mathcal{F}'(x_2 - x_3)] \,,$$

where $\mathcal{F}, \mathcal{F}' : \mathbb{F}_q \to \mathbb{F}_q$. It is not difficult to check that such two constructions are invertible, and that they are A-equivalent to a generalized Feistel scheme defined over $\mathbb{F}_q^4$.

4.2 A Generalized Lai-Massey Scheme *Not* Belonging into the “Feistel EA-Class”

Next, we propose a concrete example of a generalized Lai-Massey scheme as in Def. 4 over $\mathbb{F}_q^n$ that is *not* EA-equivalent to any generalized Feistel network. We first propose it over $\mathbb{F}_q^4$ in Prop. 3, and then we iteratively generalize it over $\mathbb{F}_q^n$ for each $n = 2 \cdot n' \geq 6$ even.[6]

Proposition 3 ($\texttt{GLM}_4$)**.** *Given $q = p^s$ as before, let $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q \setminus \{0\}$. For each $i \in \{1, 2, 3\}$, let $\mathcal{F}_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be a function. The generalized Lai-Massey scheme*

[6]We limit ourselves to mention that it is possible to set up an analogous invertible scheme that is *not* EA-equivalent to any generalized Feistel network over $\mathbb{F}_q^n$ for each $n = 2 \cdot n' + 1 \geq 5$ odd as well.

$\texttt{GLM}_4(x_0, x_1, x_2, x_3) = y_0 \| y_1 \| y_2 \| y_3$ *over* $\mathbb{F}_q^4$ *defined as*

$$\begin{aligned}
y_0 &:= \alpha_0 \cdot (x_0 + \mathcal{F}_1(x_0 - x_1) + \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \ , \\
y_1 &:= \alpha_1 \cdot (x_1 + \mathcal{F}_1(x_0 - x_1) + \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \ , \\
y_2 &:= \alpha_2 \cdot (x_2 + \mathcal{F}_2(x_0 - x_1, x_2 - x_3) + \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \ , \\
y_3 &:= \alpha_3 \cdot (x_3 + \mathcal{F}_2(x_0 - x_1, x_2 - x_3) + \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \ ;
\end{aligned}$$

is invertible.

Proof. The invertibility follows from the following facts:

$$\begin{aligned}
x_0 - x_1 &= \frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1} \ , \qquad x_2 - x_3 = \frac{y_2}{\alpha_2} - \frac{y_3}{\alpha_3} \ , \\
x_1 - x_2 &= \frac{y_1}{\alpha_1} - \frac{y_2}{\alpha_2} - \mathcal{F}_1\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}\right) - \mathcal{F}_2\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}, \frac{y_2}{\alpha_2} - \frac{y_3}{\alpha_3}\right) .
\end{aligned}$$

By making use of the same strategy exploited for the Lai-Massey scheme e.g. in Prop. 1, these information are sufficient for recovering x_0, x_1, x_2, x_3. ☐

Working iteratively, we set up a similar construction over $\mathbb{F}_q^n$ for n even.

Proposition 4 ($\texttt{GLM}_n$)**.** *Let* $q = p^s$ *be as before, and let* $n = 2 \cdot n' \geq 6$*. Let* $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$*. For each* $i \in \{1, 2, \ldots, n-1\}$*, let* $\mathcal{F}_i : \mathbb{F}_q^i \to \mathbb{F}_q$ *be a function.*

For each even integer $n = 2 \cdot n' \geq 6$*, the generalized Lai-Massey scheme* $\texttt{GLM}_n(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ *over* $\mathbb{F}_q^n$ *defined as*

$$y_i := \begin{cases} z_i + \alpha_i \cdot \mathcal{F}_{n-1}(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w_{n-2}) & \text{if } i \in \{0, 1, \ldots, n-3\} \, , \\ \alpha_i \cdot \big(x_i + \mathcal{F}_{n-2}(w_0, w_1, \ldots, w_{n-4}, w_{n-2}) & \text{otherwise } (i \in \{n-2, n-1\}) \\ \qquad + \mathcal{F}_{n-1}(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w_{n-2})\big) & \end{cases}$$

where $w_i := x_i - x_{i+1}$ *and where*

$$[z_0, z_1, \ldots, z_{n-3}] := \texttt{GLM}_{n-2}(x_0, x_1, \ldots, x_{n-3})$$

is the output of the generalized Lai-Massey scheme $\texttt{GLM}_{n-2}$ *over* $\mathbb{F}_q^{n-2}$*, is invertible.*

The proof – analogous to the one for the case $n = 4$ – is given in App. C.2.

As before, we point out that any difference in the subspace $\langle [1, 1, \ldots, 1] \rangle \equiv \{[x, x, \ldots, x] \mid x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ does not activate any function $\mathcal{F}_i$ of the generalized Lai-Massey schemes $\texttt{GLM}_n$. Such subspace can be broken by imposing that at least two coefficients α_i and α_j for $i \neq j$ are different, and by adding proper round constants.

About the EA-Equivalence

The generalized Lai-Massey schemes just proposed in Prop. 3 – 4 are not EA-equivalent to any generalized Feistel network.

Theorem 2. *Let* $q = p^s$ *be as before, and let* $n \geq 4$*. The generalized Lai-Massey constructions* $\texttt{GLM}_n$ *proposed in Prop. 3 – 4 are* ***not*** *extended affine equivalent to any generalized Feistel network.*

Proof. Let's start by analyzing the case $n = 4$. If the EA-equivalence holds, then there must exist invertible affine layers A, B and an affine layer C over $\mathbb{F}_q^4$ such that $\texttt{GLM}_4(x) = B \circ \texttt{F}_{\text{G}} \circ A(x) + C(x)$, where $\texttt{F}_{\text{G}}$ is defined in Def. 2. Let's first consider the case in which

A, B, C are linear. Since GLM_4 depends on $x_0 - x_1$, $x_1 - x_2$, $x_2 - x_3$, then the invertible matrix A must be of the form

$$A = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 1 & -1 & 0 \\ \psi_0 & \psi_1 & \psi_2 & \psi_3 \end{bmatrix}$$

up to shuffle (or linear combinations) of the rows, where $\psi_0, \psi_1, \psi_2, \psi_3 \in \mathbb{F}_q$ must satisfy $\det(A) = -(\psi_0 + \psi_1 + \psi_2 + \psi_3) \neq 0$. Given A, we have that

$$\texttt{F}_{\text{G}} \circ A(x) = \begin{bmatrix} x_2 - x_3 + \mathcal{F}_1(x_0 - x_1) \\ x_1 - x_2 + \mathcal{F}_2(x_0 - x_1, x_2 - x_3) \\ \psi_0 \cdot x_0 + \psi_1 \cdot x_1 + \psi_2 \cdot x_2 + \psi_3 \cdot x_3 + \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3) \\ x_0 - x_1 \end{bmatrix}.$$

In order to realize the EA-equivalence, the matrix B must be of the form

$$B = \begin{bmatrix} \alpha_0 \cdot \varphi_0 & 0 & \alpha_0 \cdot \varphi_2 & \varphi_3 \\ \alpha_1 \cdot \varphi_0 & 0 & \alpha_1 \cdot \varphi_2 & \varphi_4 \\ 0 & \alpha_3 \cdot \varphi_1 & \alpha_2 \cdot \varphi_2 & \varphi_5 \\ 0 & \alpha_3 \cdot \varphi_1 & \alpha_3 \cdot \varphi_2 & \varphi_6 \end{bmatrix} \tag{2}$$

for $\varphi_0, \varphi_1, \ldots, \varphi_6 \in \mathbb{F}_q$. Indeed, due to the distribution of the functions $\mathcal{F}_i$ in $\texttt{GLM}_4$, we have that $B \circ \texttt{F}_{\text{G}} \circ A(x)$ is equal to

$$\begin{bmatrix} L^{(0)}(x_0, x_1, x_2, x_3) + \alpha_0 \cdot (\varphi_0 \cdot \mathcal{F}_1(x_0 - x_1) + \varphi_2 \cdot \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \\ L^{(1)}(x_0, x_1, x_2, x_3) + \alpha_1 \cdot (\varphi_0 \cdot \mathcal{F}_1(x_0 - x_1) + \varphi_2 \cdot \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \\ L^{(2)}(x_0, x_1, x_2, x_3) + \alpha_2 \cdot (\varphi_1 \cdot \mathcal{F}_2(x_0 - x_1, x_2 - x_3) + \varphi_2 \cdot \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \\ L^{(3)}(x_0, x_1, x_2, x_3) + \alpha_3 \cdot (\varphi_1 \cdot \mathcal{F}_2(x_0 - x_1, x_2 - x_3) + \varphi_2 \cdot \mathcal{F}_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \end{bmatrix},$$

where $L^{(i)} : \mathbb{F}_q^4 \to \mathbb{F}_q$ is a linear function for each $i \in \{0, 1, 2, 3\}$. Independently of the value of φ_i, the matrix B is never invertible, since the first three columns are always linearly dependent:

$$\forall i \in \{0, 1, 2, 3\} : \qquad \varphi_1 \cdot \varphi_2 \cdot B_{i,0} + \varphi_0 \cdot \varphi_2 \cdot B_{i,1} - \varphi_0 \cdot \varphi_1 \cdot B_{i,2} = 0\,.$$

The result does not change when considering affine layers A, B over $\mathbb{F}_q^4$. We point out that the affine layer C only affects the linear/affine combination of the inputs x_0, x_1, x_2, x_3, hence, it does not change the previous conclusion.

The scenario is similar for the case $n = 2 \cdot n' \geq 6$ even. In such a case, the problem regards again the invertibility of the matrix B. By working as before, it is possible to construct an invertible matrix $A \in \mathbb{F}_q^{n \times n}$ that returns all the combinations $x_i - x_{i+1}$ for each $i \in \{0, 1, \ldots, n-2\}$. Let $B^{(4)} \in \mathbb{F}_q^{4 \times 3}$ be the matrix corresponding to the first three columns of $B \in \mathbb{F}_q^{4 \times 4}$ as defined in (2). For each $n = 2 \cdot n' \geq 6$, we define $B \in \mathbb{F}_q^{n \times n}$ via $B^{(n)} \in \mathbb{F}_q^{n \times (n-1)}$ as

$$B = \left[\begin{array}{c|c} & \varphi_{n-1} \\ & \varphi_n \\ B^{(n)} & \vdots \\ & \varphi_{2n-2} \\ & \varphi_{2n-1} \end{array}\right], \qquad \text{where}$$

$$B^{(n)} := \left[\begin{array}{ccc|cc} & & & 0 & \alpha_0 \cdot \varphi_{n-2} \\ & B^{(n-2)} & & \vdots & \vdots \\ & & & 0 & \alpha_{n-3} \cdot \varphi_{n-2} \\ \hline 0 & \ldots & 0 & \alpha_{n-2} \cdot \varphi_{n-3} & \alpha_{n-2} \cdot \varphi_{n-2} \\ 0 & \ldots & 0 & \alpha_{n-1} \cdot \varphi_{n-3} & \alpha_{n-1} \cdot \varphi_{n-2} \end{array}\right].$$

It is easy to check that the columns of $B^{(n)}$ are linearly dependent due to the fact that the columns of $B^{(n-2)}$ are linearly dependent. As before, B is never invertible since the columns of $B^{(n)}$ are linearly dependent. $\square$

5 Redundant Lai-Massey Schemes

5.1 Definition of Redundant Lai-Massey Schemes

Focusing again on Prop. 1, another main feature of such Lai-Massey schemes $[x_0, x_1, \ldots, x_{n-1}] \mapsto [y_0, y_1, \ldots, y_{n-1}]$ regards the fact that each output y_i is defined as the sum of the corresponding input x_i and of a certain element $z = \mathcal{F}(x_0, x_1, \ldots, x_{n-1})$, that is, $y_i = x_i + z$ where z is fixed for each $i \in \{0, 1, \ldots, n-1\}$. In the original Lai-Massey scheme, the inputs of the function $\mathcal{F}$ must be of a particular form in order to guarantee the inveritibility. In the following definition, we remove such a restriction, allowing for a more general scheme.

Definition 5 (Redundant Lai-Massey)**.** Let $q = p^s$ be as before, and let $n \geq 2$ be an integer. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Given a function $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q$, let $\texttt{LM}_\text{R} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be defined as $\texttt{LM}_\text{R}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| y_2 \| \ldots \| y_{n-1}$ where

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

We say that $\texttt{LM}_\text{R}$ is a redundant[7] Lai-Massey scheme *if* it is invertible.

Obviously, the Lai-Massey scheme defined in Prop. 1 satisfies this definition. At the same time, there exist redundant Lai-Massey schemes that are not of the same form given in Prop. 1, that is, invertible schemes in which the inputs of the function $\mathcal{F}$ are not necessarily zero-sum linear combinations of $x_0, x_1, \ldots, x_{n-1}$. A concrete example is the following.

Lemma 1. *Let $q = p^s$ be as before, and let $n \geq 2$ be an integer. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Let $\mu_0, \mu_1, \ldots, \mu_{n-1} \in \mathbb{F}_q$ be such that $\sum_{i=0}^{n-1} \mu_i \neq 0$. Let $\mathcal{H} : \mathbb{F}_q \to \mathbb{F}_q$ be a permutation. The redundant Lai-Massey scheme $[x_0, x_1, \ldots, x_{n-1}] \mapsto [y_0, y_1, \ldots, y_{n-1}]$ over $\mathbb{F}_q^n$ defined as*

$$\forall i \in \{0, 1, \ldots, n-1\} : \quad y_i = \alpha_i \cdot \left(x_i + \frac{1}{\sum_{j=0}^{n-1} \mu_j} \cdot \left(\mathcal{H}\left(\sum_{j=0}^{n-1} \mu_j \cdot x_j \right) - \sum_{j=0}^{n-1} \mu_j \cdot x_j \right) \right)$$

is invertible.

The proof – given in App. C.1 – relies on the fact that $\sum_{j=0}^{n-1} \mu_j \cdot x_j = \mathcal{H}^{-1}\left(\sum_{j=0}^{n-1} \mu_j \cdot \frac{y_j}{\alpha_j} \right)$. In there, we also show that such scheme is EA-equivalent to a Feistel network.

5.2 A Redundant Lai-Massey Scheme *Not* Belonging into the "Feistel EA-Class"

Next, we propose an example of a redundant Lai-Massey scheme as in Def. 5 over $\mathbb{F}_q^n$ that is *not* EA-equivalent to any generalized Feistel network.

[7] For differentiating it from the previous generalized Lai-Massey scheme, we decided to call this one as "redundant" Lai-Massey scheme to capture the fact that the same function $\mathcal{F}(x_0, x_1, \ldots, x_{n-1})$ is repeatedly used for building/defining the output.

Proposition 5 (RLM). *Let $p \geq 3$ be a prime integer, and let $n \geq 2$. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_p \setminus \{0\}$. Let $l \in \{1, 2, \ldots, n-1\}$. Let $\{\lambda_j^{(i)}\}_{j\in\{0,1,\ldots,n-1\}, i\in\{0,1,\ldots,l-1\}}$ be l "zero-sum linearly independent" sets as in Def. 1. Let $\mathcal{G} : \mathbb{F}_p^l \to \mathbb{F}_p$ be any function.*

*Let $\psi_0, \psi_1, \ldots, \psi_{n-1} \in \mathbb{F}_p$ (**no** condition on $\sum_{j=0}^{n-1} \psi_j$). Let $\beta \in \mathbb{F}_p \setminus \{0\}$ be such that $-\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j\right)$ is a quadratic **non**-residue if $\sum_{j=0}^{n-1} \psi_j \neq 0$.*[8]

The redundant Lai-Massey scheme RLM *over $\mathbb{F}_p^n$ defined as* $\texttt{RLM}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ *where*

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := \alpha_i \cdot \left(x_i + \beta \cdot z^2_{x_0, x_1, \ldots, x_{n-1}} \cdot \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j \right) \right)$$

where

$$z_{x_0, x_1, \ldots, x_{n-1}} \equiv z := \mathcal{G} \left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot x_j \right)$$

is invertible.

Proof. If $\sum_{j=0}^{n-1} \psi_j = 0 \mod p$, then the invertibility follows from Prop. 1. Hence, let's focus on $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$. Similarly to before, in order to invert it, it is sufficient to find the linear combinations of x_i both with respect to $\lambda_i^{(j)}$ and with respect to ψ_i. Given $y_0, y_1, \ldots, y_{n-1}$ as before, we have

$$\sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot \frac{y_i}{\alpha_i} = \sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot x_i + \beta \cdot \underbrace{\sum_{i=0}^{n-1} \lambda_i^{(j)}}_{=0} \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j \right) = \sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot x_i$$

for each $j \in \{0, 1, \ldots, l-1\}$, where $\sum_{i=0}^{n-1} \lambda_i^{(j)} = 0$ by assumption. It follows that $z = \mathcal{G}\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot \frac{y_j}{\alpha_j}, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot \frac{y_j}{\alpha_j}, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot \frac{y_j}{\alpha_j} \right)$.

If $z = 0$, then $x_i = y_i / \alpha_i$ for each $i \in \{0, 1, \ldots, n-1\}$. Otherwise, if $z \neq 0$, note that

$$\sum_{j=0}^{n-1} \psi_j \cdot \frac{y_j}{\alpha_j} = \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j \right) \cdot \left(1 + \beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \right) \right) .$$

Such equality is invertible with respect to $\sum_{j=0}^{n-1} \psi_j \cdot x_j$ if

$$1 + \beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \right) \neq 0 \qquad \Longrightarrow \qquad -\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j \right) \neq (\pm 1/z)^2$$

for each $z \in \mathbb{F}_p$. This condition is always satisfied under the assumption that $-\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j\right)$ is a quadratic **non**-residue modulo p.

Given both z and $\sum_{j=0}^{n-1} \psi_j \cdot x_j$, it is trivial to invert the system. □

[8] We recall that $\eta \in \mathbb{F}_p$ is a quadratic non-residue if and only if $x^2 \neq \eta \mod p$ for each $x \in \mathbb{F}_p$.

About the EA-Equivalence

Here we show that the redundant Lai-Massey scheme just defined is not EA-equivalent to any generalized Feistel network.

Theorem 3. *Let $p \geq 3$ be a prime integer, and let $n \geq 2$. The redundant Lai-Massey scheme* `RLM` *defined in Prop. 5 for which*

- $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$
- $l = n-1$ *(where $\mathcal{G}$ is a non-trivial function that depends on $l = n-1$ inputs)*

is not EA-equivalent to any generalized Feistel network.

Proof. The proof follows from the fact that

- the functions $\mathcal{F}_i$ in any generalized Feistel network as in Def. 2 depend on at most $i \leq n-1$ linearly-independent inputs;
- the function $\mathcal{F}(x_0, \ldots, x_{n-1}) := \beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j\right)$ in Prop. 5 (where $z := \mathcal{G}\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\right)$) depend on n linearly-independent inputs.

As a result, the equivalence $\texttt{RLM}(x) = B \circ \texttt{F}_{\text{G}} \circ A(x) + C(x)$ is never realized for any invertible affine layer A, B and for any affine layer C. □

6 The Blooming of the `Amaryllises` Construction

In this section, we present a new variant of the Lai-Massey scheme called `Amaryllises` that takes inspiration from the `Horst` construction previously recalled.

6.1 The `Amaryllises` Construction

The main feature of a `Horst` construction regards the fact that the linear combination that takes place in a Feistel network can be replaced by a non-linear combination. As we are going to discuss in more details in the following, such construction can have some concrete advantages with respect to the Feistel networks when the goal is to guarantee security against algebraic attacks in an efficient way.

Here, we apply a similar design strategy on a Lai-Massey scheme in order to set up a construction – called `Amaryllises` – with similar advantages. Our result is presented in the following Theorem.

Theorem 4 (`Amaryllises`)**.** *Let $q = p^s$ be as before, and let $n \geq 2$ be an integer. Assume the following conditions:*

- *let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$ and $l \in \{1, 2, \ldots, n-1\}$;*
- *let $\{\lambda_j^{(i)}\}_{j \in \{0,1,\ldots,n-1\}, i \in \{0,1,\ldots,l-1\}}$ be l "zero-sum linearly independent" sets as in Def. 1;*
- *let $\mathcal{H} : \mathbb{F}_q^l \to \mathbb{F}_q$ be any function;*
- *let $\mathcal{F} : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that (1st) $\mathcal{F}(0) \neq 0$ and (2nd) $\mathcal{G}(x) := x \cdot \mathcal{F}(x)$ is invertible over $\mathbb{F}_q$;*
- *let $\beta_0, \beta_1, \ldots, \beta_{n-1} \in \mathbb{F}_q \setminus \{0\}$ such that $\sum_{i=0}^{n-1} \beta_i = 0$ **if** $\mathcal{H}$ is not identically equal to zero (equivalently, no condition on $\sum_{i=0}^{n-1} \beta_i$ is imposed if $\mathcal{H}(z) = 0$ for each $z \in \mathbb{F}_q$).*

The `Amaryllises` *construction* $\mathtt{A}$ *over* $\mathbb{F}_q^n$ *defined as* $\mathtt{A}(x_0, \ldots, x_{n-1}) = y_0 \| \ldots \| y_{n-1}$ *where*

$$y_i := \alpha_i \cdot \left(x_i \cdot \mathcal{F}\left(\sum_{j=0}^{n-1} \beta_j \cdot x_j \right) + \mathcal{H}\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot x_j \right) \right) \tag{3}$$

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

Proof. Firstly, *we prove that* $\mathcal{F}(z) \neq 0$ *for each* $z \in \mathbb{F}_q$. Since $\mathcal{G}$ is a permutation and since $\mathcal{G}(0) = \mathcal{F}(0) \cdot 0 = 0$ by definition, then $\mathcal{G}(x) \neq 0$ for each $x \neq 0$. It follows that $\mathcal{F}(x) = \mathcal{G}(x)/x \neq 0$ for any $x \in \mathbb{F} \setminus \{0\}$, while $\mathcal{F}(0) \neq 0$ by assumption.

As before, the inverse can be constructed once the linear combinations of y_i with respect to β_i and to $\lambda_i^{(j)}$ are known. Given $y_0, y_1, \ldots, y_{n-1}$, it is possible to recover $\sum_{i=0}^{n-1} \beta_i \cdot x_i$ by noting the following:

$$\begin{aligned} \sum_{i=0}^{n-1} \beta_i \cdot \frac{y_i}{\alpha_i} = & \left(\sum_{i=0}^{n-1} \beta_i \cdot x_i \right) \cdot \mathcal{F}\left(\sum_{i=0}^{n-1} \beta_i \cdot x_i \right) \\ & \underbrace{+ \mathcal{H}\left(\sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i, \sum_{i=0}^{n-1} \lambda_i^{(1)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \lambda_i^{(l-1)} \cdot x_i \right) \cdot \sum_{i=0}^{n-1} \beta_i}_{=0} \\ = & \mathcal{G}\left(\sum_{i=0}^{n-1} \beta_i \cdot x_i \right) \qquad \longrightarrow \qquad \sum_{i=0}^{n-1} \beta_i \cdot x_i = \mathcal{G}^{-1}\left(\sum_{i=0}^{n-1} \beta_i \cdot \frac{y_i}{\alpha_i} \right), \end{aligned}$$

where $\mathcal{G}$ is invertible by definition. Note that either $\mathcal{H}$ always returns zero (that is, $\mathcal{H}(x) = 0$ for each $x \in \mathbb{F}_q$) or $\sum_{i=0}^{n-1} \beta_i = 0$ by assumption.

In a similar way, since $\sum_{i=0}^{n-1} \lambda_i^{(j)} = 0$, it is possible to recover $\sum_{i=0}^{n-1} \gamma_i^{(j)} \cdot x_i$ for each $j \in \{0, 1, \ldots, l-1\}$:

$$\begin{aligned} \sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot \frac{y_i}{\alpha_i} = & \sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot x_i \cdot \mathcal{F}\left(\mathcal{G}^{-1}\left(\sum_{l=0}^{n-1} \beta_l \cdot y_l \right) \right) \\ \longrightarrow \qquad & \sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot x_i = \frac{1}{z} \cdot \left(\sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot \frac{y_i}{\alpha_i} \right), \end{aligned}$$

where $z := \mathcal{F}\left(\mathcal{G}^{-1}\left(\sum_{i=0}^{n-1} \beta_i \cdot \frac{y_i}{\alpha_i} \right) \right) \neq 0$ (remember that $\mathcal{F}$ never returns zero).

Given z as before, it follows that for each $i \in \{0, \ldots, n-1\}$:

$$x_i = \frac{1}{z} \cdot \left(\frac{y_i}{\alpha_i} - \mathcal{H}\left(\frac{\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot y_j/\alpha_j}{z}, \ldots, \frac{\sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot y_j/\alpha_j}{z} \right) \right). \qquad \square$$

Multiplicative Complexity of `Amaryllises`**.** Before going on, we point out that the cost of computing `Amaryllises` corresponds to (i) the cost of computing $\mathcal{F}$ and $\mathcal{G}$, and (ii) n (non-linear) $\mathbb{F}_q$-multiplications[9] and n $\mathbb{F}_q$-sums.

6.2 Suitable Functions for the `Amaryllises` Construction

As next step, we show how to construct functions $\mathcal{F}$ that satisfy the required assumptions of the previous Theorem 4.

[9] We add the term "non-linear" for emphasizing that it is not a multiplication with a constant.

Lemma 2. *Let $q = p^s$ be as before. Let $\mathcal{P}$ be a permutation over $\mathbb{F}_q$. Let $\psi \in \mathbb{F}_q \setminus \{0\}$. The function $\mathcal{F}$ over $\mathbb{F}_q$ defined as*

$$\mathcal{F}(x) := \begin{cases} \frac{\mathcal{P}(x)-\mathcal{P}(0)}{x} & \text{if } x \neq 0 \\ \psi & \text{otherwise } (x = 0) \end{cases}$$

satisfies the requirements of Theorem 4.

Proof. The proof trivially follows from the facts that (i) $\mathcal{F}(0) = \psi \neq 0$ and (ii)

$$x \mapsto x \cdot \mathcal{F}(x) = \begin{cases} \mathcal{P}(x) - \mathcal{P}(0) & \text{if } x \neq 0 \\ x \cdot \psi = 0 & \text{if } x = 0 \end{cases} = \mathcal{P}(x) - \mathcal{P}(0)$$

is a permutation. □

By exploiting this result, concrete examples of functions $\mathcal{F}$ that satisfy the assumptions of Theorem 4 and that are cheap to compute from the point of view of the *multiplicative complexity* can be set up via the power maps.

Lemma 3. *Let $q = p^s$, where $p \geq 2$ is a prime and $s \geq 1$. Let $d \geq 3$ be an integer for which $x \mapsto x^d$ is invertible over $\mathbb{F}_q$, hence $\gcd(d, q-1) = 1$. Let $\alpha \in \mathbb{F}_q \setminus \{0\}$. The function*

$$\mathcal{F}(x) = \sum_{i=1}^{d} \binom{d}{i} x^{i-1} \cdot (\pm\alpha)^{d-i} = \begin{cases} \frac{(x\pm\alpha)^d \mp \alpha^d}{x} & \text{if } x \neq 0\,, \\ \pm d \cdot \alpha^{d-1} & \text{otherwise} \end{cases} \tag{4}$$

satisfies the requirements of Prop. 4.

Proof. In order to prove the result, it is sufficient to note that (i) $\mathcal{F}(0) = \pm d \cdot \alpha^{d-1} \neq 0$ (since $\alpha \neq 0$) and that (ii) $\mathcal{F}(x) \cdot x = (x \pm \alpha)^d \mp \alpha^d$ is invertible since $x \mapsto x^d$ is invertible by assumption on d. □

7 Properties of the `Amaryllises` Constructions

In this section, we analyze the statistical and the algebraic properties of `Amaryllises`, and we discuss its advantages and the disadvantages with respect to other non-linear layers used in the literature. For this goal, we mainly focus on the case of SPN, Feistel networks, Lai-Massey schemes, and `Horst` constructions.

Remark 2. We emphasize that the following observations are based on the assumption that the following schemes are used for instantiating a MPC-/FHE-/ZK-friendly primitive.

Remark 3. We emphasize that the following observations do not take into account the details of the sub-components of the considered schemes. Hence, it is possible that the following results do not hold for some specific instances.

7.1 Initial Remarks: Invertibility and Full Diffusion

About the Invertibility. Let's start by comparing the conditions required by each scheme for being invertible.

As well known, Feistel networks and Lai-Massey schemes are always invertible independently of the details of the functions that instantiate them. In the case of `Horst`, the construction is invertible even if its internal functions are not permutation, but not all non-invertible functions are possible (it is required that the functions $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_{n-2}$ in Theorem 1 never return zero). For comparison, both SPN and `Amaryllises` constructions are invertible only if their internal functions satisfy some specific conditions. In the case of SPNs, the non-linear layer over $\mathbb{F}_q^n$ defined as $[x_0, x_1, \ldots, x_{n-1}] \mapsto [\mathcal{S}^{(0)}(x_0), \mathcal{S}^{(1)}(x_1), \ldots, \mathcal{S}^{(n-1)}(x_{n-1})]$ is invertible if and only if all its internal functions $\mathcal{S}^{(i)}$ are invertible. In the case of `Amaryllises`, we just showed that any permutation $\mathcal{P}$ can be turned into a function $\mathcal{F}$ that can instantiate an invertible `Amaryllises` scheme.

It follows that, from a designer point of view, the number of possible choices for the internal functions of Feistel networks, Lai-Massey schemes, and also `Horst` constructions is much larger than the corresponding number for SPN and `Amaryllises` constructions. This could represent a significant advantage, since the designers can e.g. choose functions that are cheaper to evaluate/implement with respect to the SPN case, without sacrificing the invertibility (and potentially the security) of the resulting primitive.

Moreover, computing the inverse of Feistel networks, Lai-Massey schemes, and also `Horst` constructions does *not* require computing the inverse of their internal functions. As a direct consequence (and by construction), the costs of computing Feistel networks, Lai-Massey schemes, and (partially of) `Horst` constructions in the forward and in the backward direction are almost the same, which is in general a desirable property when both the encryption and the decryption phases are required. The same cannot be said in general for SPN and `Amaryllises` constructions. As a concrete example, the majority of MPC-/FHE-/ZK-friendly primitives are instantiated with power maps $x \mapsto x^d$, where d is usually the smallest positive integer co-prime with $p-1$. The inverse of $x \mapsto x^d$ is $x \mapsto x^{1/d} \equiv x^{\hat{d}}$ where $\hat{d}$ is the smallest integer for which $d \cdot \hat{d} - 1$ is a multiple of $q-1$ (due to Fermat's Little Theorem). In the case $q \gg d$, then $\hat{d}$ is of the same order of q, making $x \mapsto x^{1/d}$ much more expensive to compute with respect to $x \mapsto x^d$. Having said that, computing the inverse of a such schemes is not required in many applications, as for example:

- stream ciphers instantiated via a cipher $E_k(\cdot)$ used in a mode of operation that does not require the computation of the inverse, as the counter-mode one $(x, N) \mapsto (x + E_k(N), N)$ for a nonce N and a secret key k;[10]

- sponge hash functions [BDPA08] instantiated with permutations. In such a case, no inverse computation of the permutation is performed for computing the hash value.

Hence, the fact that computing the inverse could be very expensive does not represent a disadvantage in many practical use cases.

About the Full Diffusion. Regarding the internal diffusion, we highlight that full diffusion is achieved in Feistel, Lai-Massey, `Horst`, and `Amaryllises` without any additional linear layer (different than the shuffle). Obviously, this is not the case for SPN schemes, for which a linear layer is crucial for achieving full diffusion. As a result, even if a significant amount of research has been already done in order to classify and find the best linear layers both in terms of security/diffusion and cost, it is important to keep in mind that the efficiency and the security of a SPN scheme depend also on the details of the linear layer, while this is not the case for the other schemes considered here.

7.2 Statistical Attacks

Regarding the statistical attacks, we focus on classical differential attacks and invariant subspace trails (related to truncated differential attacks).

[10] We refer to [Gra23] for examples of MPC-/FHE-/ZK-friendly symmetric primitives instantiated with non-invertible non-linear layers.

7.2.1 Differential (and Linear) Attacks

In a differential attack [BS90, BS93], the attack exploits the probability distribution of the output differences produced by the analyzed cryptographic primitive for given input differences. Let $\delta, \Delta \in \mathbb{F}_q^n$ be respectively the input and the output differences. We recall that the differential probability (DP) of having a certain output difference Δ given a particular input difference δ for a permutation $\mathcal{P}$ over $\mathbb{F}_q^n$ is equal to

$$\text{Prob}(\delta \neq 0 \to \Delta) = |\{x \in \mathbb{F}_q^n \mid \mathcal{P}(x+\delta) - \mathcal{P}(x) = \Delta\}|/q^n \,.$$

In the case of a `Amaryllises` construction, the following result holds:

Proposition 6. *The maximum DP of any* `Amaryllises` *construction over* $\mathbb{F}_q^n$ *defined as in Theorem 4 is*

$$\leq \begin{cases} \frac{\deg(\mathcal{F})}{q} \in \mathcal{O}(q^{-1}) & \textit{if } \deg(\mathcal{H}) \leq 1 \textit{ (that is, if } \mathcal{H} \textit{ is an affine function)}\,, \\ \frac{\deg(\mathcal{F})\cdot(\deg(\mathcal{H})-1)}{q^2} \in \mathcal{O}(q^{-2}) & \textit{otherwise}\,. \end{cases}$$

Before proving such result, we highlight that it is meaningful only in the case in which the degrees of the involved functions $\mathcal{F}$ and $\mathcal{H}$ are small. For example, in the case of the AES S-Box $x \mapsto x^{-1} \equiv x^{q-2}$, the just given results would be completely meaningless from a practical point of view. However, the large majority of the MPC-/FHE-/ZK-friendly primitives are (at least, partially) instantiated with low degree functions. As a result, in the case of an iterated primitive, the given bounds combined with the huge size of q are usually sufficient for guaranteeing security against differential cryptanalysis within few rounds.

Proof. Let $\delta \neq 0$ and Δ be respectively the input and the output differences. Each differential characteristic is defined by a system of n equations of the form

$$\begin{aligned} x_i \cdot \left(\mathcal{F}\left(\sum_j \beta_j \cdot x_j + \sum_j \beta_j \cdot \delta_j\right) - \mathcal{F}\left(\sum_j \beta_j \cdot x_j\right)\right) + \delta_i \cdot \mathcal{F}\left(\sum_j \beta_j \cdot x_j + \sum_j \beta_j \cdot \delta_j\right) \\ + \mathcal{H}\left(\sum_j \lambda_j^{(0)} \cdot (x_j+\delta_j), \sum_j \lambda_j^{(1)} \cdot (x_j+\delta_j), \ldots, \sum_j \lambda_j^{(l-1)} \cdot (x_j+\delta_j)\right) \\ - \mathcal{H}\left(\sum_j \lambda_j^{(0)} \cdot x_j, \sum_j \lambda_j^{(1)} \cdot x_j, \ldots, \sum_j \lambda_j^{(l-1)} \cdot x_j\right) = \frac{\Delta_i}{\alpha_i} \end{aligned} \tag{5}$$

for each $i \in \{0, 1, \ldots, n-1\}$. In order to prove the result, we bound the number of possible solutions in $x_0, x_1, \ldots, x_{n-1}$ of such systems of equations.

First of all, one of such equations can be replaced by their linear combination with respect to $\beta_0, \beta_1, \ldots, \beta_{n-1}$. This corresponds to

$$y \cdot \left(\mathcal{F}\left(y + \sum_j \beta_j \cdot \delta_j\right) - \mathcal{F}(y)\right) + \sum_i \beta_i \cdot \delta_i \cdot \mathcal{F}\left(y + \sum_j \beta_j \cdot \delta_j\right) = \sum_i \beta_i \cdot \frac{\Delta_i}{\alpha_i}$$

where $y := \sum_i \beta_i \cdot x_i$, and where either $\sum_i \beta_i = 0$ or $\mathcal{H}$ is identically equal to zero. Since such equation is of degree $\deg(\mathcal{F})$, it admits at most $\deg(\mathcal{F})$ solutions in $y = \sum_i \beta_i \cdot x_i$.

Case: $\mathcal{F}\left(\sum_j \beta_j \cdot x_j + \sum_j \beta_j \cdot \delta_j\right) \neq \mathcal{F}\left(\sum_j \beta_j \cdot x_j\right)$. Let's assume that $\mathcal{F}(\sum_j \beta_j \cdot x_j + \sum_j \beta_j \cdot \delta_j) \neq \mathcal{F}(\sum_j \beta_j \cdot x_j)$ for each found value of $\sum_i \beta_i \cdot x_i$. Then:

- assume $\mathcal{H}$ is identically equal to zero. Since $\mathcal{F}\left(\sum_j \beta_j \cdot x_j + \sum_j \beta_j \cdot \delta_j\right) \neq \mathcal{F}\left(\sum_j \beta_j \cdot x_j\right)$, for each found value of $\sum_i \beta_i \cdot x_i$, it is possible to find the values of the remaining $n-1$ variables x_i that satisfy the system of equations in (5) by inverting $n-1$ equations. This implies that the number of solutions is $\leq \deg(\mathcal{F})$, or equivalently that the probability of the corresponding differential characteristic is of order $\mathcal{O}(q^{-n})$;

- if $\mathcal{H}$ is not identically equal to zero, we consider the linear combinations of the equations that compose the system of equations in (5) with respect to $\lambda_0^{(j)}, \lambda_1^{(j)}, \ldots, \lambda_{n-1}^{(j)}$ for each $j \in \{0, 1, \ldots, l-1\}$, that is,

$$z \cdot \left(\mathcal{F}\left(y + \sum_j \beta_j \cdot \delta_j\right) - \mathcal{F}(y)\right) + \sum_i \lambda_i^{(j)} \cdot \delta_i \cdot \mathcal{F}\left(y + \sum_j \beta_j \cdot \delta_j\right) = \sum_i \lambda_i^{(j)} \cdot \frac{\Delta_i}{\alpha_i}$$

  where $z := \sum_i \lambda_i^{(j)} \cdot x_i$ and $y = \sum_j \beta_j \cdot x_j$ as before (remember that $\sum_i \lambda_i^{(j)} = 0$ by assumption). Since $\mathcal{F}\left(\sum_j \beta_j \cdot x_j + \sum_j \beta_j \cdot \delta_j\right) \neq \mathcal{F}\left(\sum_j \beta_j \cdot x_j\right)$, it is possible to find $\sum_i \lambda_i^{(j)} \cdot x_i$ for each $j \in \{0, 1, \ldots, l-1\}$. If $l = n-1$, this information together with the knowledge of $\sum_i \beta_i \cdot x_i$ is sufficient to recover $x_0, x_1, \ldots, x_{n-1}$. If $l < n-1$, it is possible to find the remaining $n-(l+1)$ values of $x_0, x_1, \ldots, x_{n-1}$ by inverting $n-(l+1)$ equations. In both cases, this implies that the number of solutions is $\leq \deg(\mathcal{F})$, or equivalently that the probability of the corresponding differential characteristic is of order $\mathcal{O}(q^{-n})$.

Case: $\mathcal{F}\left(\sum_j \beta_j \cdot x_j + \sum_j \beta_j \cdot \delta_j\right) = \mathcal{F}\left(\sum_j \beta_j \cdot x_j\right)$. Let's assume that $\mathcal{F}(\sum_j \beta_j \cdot x_j + \sum_j \beta_j \cdot \delta_j) = \mathcal{F}(\sum_j \beta_j \cdot x_j)$ for at least one the found values among $\sum_i \beta_i \cdot x_i$. (This scenario occurs if e.g. $\sum_j \beta_j \cdot \delta_j = 0$. However, we emphasize that such equality can occur also in the case in which $\sum_j \beta_j \cdot \delta_j \neq 0$, since $\mathcal{F}$ is not bijective in general.) In such a case, by considering any difference of two equations that compose (5), note that the system of equations (5) admits a solution only if

$$\forall i, l \in \{0, 1, \ldots, n-1\}: \qquad (\delta_i - \delta_l) \cdot \mathcal{F}\left(\sum_j \beta_j \cdot x_j\right) = \frac{\Delta_i}{\alpha_i} - \frac{\Delta_l}{\alpha_l}.$$

If all these equalities are satisfied (note that they are independent of $x_0, x_1, \ldots, x_{n-1}$, then for each found value of $\sum_j \beta_j \cdot x_j$:

- if $\mathcal{H}$ is an affine function, that is,[11]

$$\begin{aligned}
&\mathcal{H}\left(\sum_j \lambda_j^{(0)} \cdot (x_j + \delta_j), \sum_j \lambda_j^{(1)} \cdot (x_j + \delta_j), \ldots, \sum_j \lambda_j^{(l-1)} \cdot (x_j + \delta_j)\right) \\
&- \mathcal{H}\left(\sum_j \lambda_j^{(0)} \cdot x_j, \sum_j \lambda_j^{(1)} \cdot x_j, \ldots, \sum_j \lambda_j^{(l-1)} \cdot x_j\right) \\
=&\mathcal{H}\left(\sum_j \lambda_j^{(0)} \cdot \delta_j, \sum_j \lambda_j^{(1)} \cdot \delta_j, \ldots, \sum_j \lambda_j^{(l-1)} \cdot \delta_j\right) - \mathcal{H}(0, 0, \ldots, 0),
\end{aligned}$$

  then no other condition on $n-1$ variables x_i is imposed. Hence, the number of solutions is $\leq \deg(\mathcal{F}) \cdot q^{n-1}$, and the probability of the corresponding differential characteristic is of order $\mathcal{O}(q^{-1})$;

[11] Note that $\mathcal{H}(0, 0, \ldots, 0) = 0$ if $\mathcal{H}$ is a linear function.

- otherwise, the system of equations (5) reduces to a single equation, that is,

$$\begin{aligned}&\mathcal{H}\left(\sum_j \lambda_j^{(0)} \cdot (x_j+\delta_j), \sum_j \lambda_j^{(1)} \cdot (x_j+\delta_j), \ldots, \sum_j \lambda_j^{(l-1)} \cdot (x_j+\delta_j)\right)\\ &-\mathcal{H}\left(\sum_j \lambda_j^{(0)} \cdot x_j, \sum_j \lambda_j^{(1)} \cdot x_j, \ldots, \sum_j \lambda_j^{(l-1)} \cdot x_j\right) = \frac{\Delta_i}{\alpha_i}\,,\end{aligned}$$

  which admits at most $q^{n-2} \cdot (\deg(\mathcal{H})-1)$. It follows that the total number of solutions is $\leq \deg(\mathcal{F}) \cdot (\deg(\mathcal{H})-1) \cdot q^{n-2}$, and the probability of the corresponding differential characteristic is of order $\mathcal{O}(q^{-2})$.

□

Before going on, we point out that an analogous analysis and result can be derived for what concerning linear attacks [Mat93] as well.

Comparison with Other Networks/Schemes/Constructions. A general comparison with other networks/schemes/constructions is not an easy task, since too many factors can play a decisive role. For example, in the case of a SPN, at least one S-Box is active every round. However, the details of the linear layer crucially impacts the number of active S-Boxes over multiple rounds, and so the probability of any differential characteristic over multiple rounds as well. Besides that, a comparison between schemes that have a different implementation cost is not very meaningful.

For this reason, we decided to omit such comparison. We limit ourselves to recall that in the case of MPC-/FHE-/ZK-friendly primitives, the combination of the huge size of q (e.g., 2^{128} or even more) and the low degree of the non-linear scheme that instantiate the MPC-/FHE-/ZK-friendly primitives usually allow to achieve good bounds against classical differential (and linear) attacks within few rounds.

7.2.2 Invariant Subspace (and Truncated Differential) Attacks

Let's analyze separately the case $\sum_{i=0}^{n-1} \beta_i = 0$ from $\sum_{i=0}^{n-1} \beta_i \neq 0$.

Case: $\sum_{i=0}^{n-1} \beta_i = 0$. Similar to what happens for the case of Lai-Massey schemes, it is not hard to check that if $\sum_{i=0}^{n-1} \beta_i = 0$, then any difference in the subspace $\langle [1,1,\ldots,1]\rangle \equiv \{[x,x,\ldots,x] \mid x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ does not activate the function $\mathcal{F}$ and $\mathcal{H}$ of `Amaryllises`. Hence, if $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$, then $\langle [1,1,\ldots,1]\rangle$ is an invariant subspace, since

$$\forall i \in \{0,1,\ldots,n-1\}: \qquad y_i = x \cdot \underbrace{\mathcal{F}(0)}_{\neq 0} + \mathcal{H}(0,0,\ldots,0)\,,$$

that is, $y_i = y_j$ for each $i,j \in \{0,1,\ldots,n-1\}$ (remember that $\sum_{i=0}^{n-1} \beta_i = \sum_{i=0}^{n-1} \lambda_i^{(0)} = \sum_{i=0}^{n-1} \lambda_i^{(1)} = \ldots = \sum_{i=0}^{n-1} \lambda_i^{(l-1)} = 0$ for guaranteeing the invertibility). As before, if $l = n-1$, then it is possible to destroy such invariant subspace by imposing that at least two coefficients α_i and α_j are different, besides choosing proper round constants. If this is not the case, a proper linear layer must be chosen in order to destroy such invariant subspaces. The open problem to analyze which conditions are necessary and/or sufficient for such a goal is out of the scope of this paper, and it is left for future work.

For completeness, note that this is related to the existence of a truncated differential [Knu94] with probability 1 of the form:

$$[\delta,\delta,\ldots,\delta] \in \mathbb{F}_q^n \longrightarrow [\Delta\cdot\alpha_0, \Delta\cdot\alpha_1, \ldots, \Delta\cdot\alpha_{n-1}] \in \mathbb{F}_q^n$$

where $\delta, \Delta \in \mathbb{F}_q$ are *not* fixed – see [LTW18] for more details about the relation between truncated differentials and subspace trails.

Case: $\sum_{i=0}^{n-1} \beta_i \neq 0$. As we have seen before, this condition implies $\mathcal{H}$ to be equal to zero. Also in this case, $\langle [1, 1, \ldots, 1] \rangle$ is an invariant subspace since

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i = x \cdot \mathcal{F}\left(x \cdot \sum_{i=0}^{n-1} \beta_i\right) ,$$

that is, $y_i = y_j$ for each i, j, and since $x \mapsto x \cdot \mathcal{F}\left(x \cdot \sum_{i=0}^{n-1} \beta_i\right)$ is a bijective function. Indeed, since $\mathcal{G}(x) = x \cdot \mathcal{F}(x)$ is bijective, then $\frac{\mathcal{G}\left(x \cdot \sum_{i=0}^{n-1} \beta_i\right)}{\sum_{i=0}^{n-1} \beta_i} = x \cdot \mathcal{F}\left(x \cdot \sum_{i=0}^{n-1} \beta_i\right)$ is bijective as well (note that $\sum_{i=0}^{n-1} \beta_i \neq 0$). With respect to the previous case, $\mathcal{F}$ is an active function. Hence, it is not hard to check that a proper constant addition is sufficient to destroy such invariant subspace.

Comparison with Other Networks/Schemes/Constructions. As we already discussed before, Lai-Massey schemes admit invariant subspace trails as well. This problem does not arise in general for Feistel networks, `Horst` constructions or SPN schemes (instantiated with a proper linear layer), for which the subspace trails can usually cover only a limited number of rounds. Hence, this could be a disadvantage for the Lai-Massey schemes and the `Amaryllises` constructions.

For completeness, we point out that a similar problem arises in the case of Partial-SPN and Hades-like primitives [GLR+20], in which the non-linear layer is only partial and not full, that is,

$$[x_0, x_1, \ldots, x_{s-1}, x_s, \ldots, x_{n-1}] \mapsto [\mathcal{S}_0(x_0), \mathcal{S}_1(x_1), \ldots, \mathcal{S}_{s-1}(x_{s-1}), x_s, \ldots, x_{n-1}]$$

for $1 \leq s < n$. In such a case, the details of the linear layer plays a crucial role in order to destroy the invariant subspace trails. We refer to [BCD+20, GRS21, GSW+21, KR21] for more details about this topic.

7.3 Algebraic Attacks

Next, we propose some considerations about the security of `Amaryllises` schemes against algebraic attacks. With respect to statistical attacks, algebraic attacks exploit the simple algebraic structure of the attacked schemes. Due to this reason, MPC-/FHE-/ZK-friendly primitives are usually more vulnerable to algebraic attacks rather than to statistical ones.

7.3.1 Growth of the Degree

The two key-ingredients for setting up an algebraic attacks are the growth of the degree and the density of the interpolation polynomials that describe the analyzed iterative primitive. Here we focus on the growth of the degree for the `Amaryllises` construction. Regarding the forward direction, the degree of each round is obviously $\max\{1+\deg(\mathcal{F}), \deg(\mathcal{H})\}$, while the degree over $r \geq 1$ rounds is obviously upper bounded by $(\max\{1 + \deg(\mathcal{F}), \deg(\mathcal{H})\})^r$. Better bounds can be potentially obtained by considering the details of the involved functions.

Let's hence focus on the backward direction. Referring to the proof of Theorem 4, we highlight that, while $x \mapsto x \cdot \mathcal{F}(x)$ is evaluated in the forward direction, the function $x \mapsto \mathcal{F}(\mathcal{G}^{-1}(x))$ is evaluated in the backward one (where $\mathcal{G}(x) := x \cdot \mathcal{F}(x)$). The crucial point we aim to emphasize is that the degree of $\mathcal{F} \circ \mathcal{G}^{-1}$ could be much higher than the degree of $\mathcal{F}$, that is, $\deg(\mathcal{F} \circ \mathcal{G}^{-1}) \gg \deg(\mathcal{F})$. As a concrete example, consider the case in which $\mathcal{F}$ is defined via an invertible power map as in (4), where $d \geq 3$ is the smallest integer co-prime with $q-1$. (We recall that the inverse of $x \mapsto x^d$ is $x \mapsto x^{1/d} \equiv x^{\hat{d}}$ where $\hat{d}$ is the smallest integer for which $d \cdot \hat{d} - 1$ is a multiple of $q-1$ – due to Fermat's Little Theorem. In the case $q \gg d$, then $\hat{d}$ is of the same order of q.) In such a case, we have that

$$\mathcal{F} \circ \mathcal{G}^{-1}(x) := \begin{cases} \left(\left((x \pm \alpha^d)^{1/d} \mp \alpha\right)^d \pm \alpha^d\right) \cdot \left((x \pm \alpha^d)^{1/d} \mp \alpha\right)^{-1} & \text{if } x \neq 0\,, \\ \pm d \cdot \alpha^{d-1} & \text{otherwise} \end{cases}$$

which implies that $\deg(\mathcal{F} \circ \mathcal{G}^{-1})$ is close to maximum (hence, close to q), that is, much higher than the degree $d-1$ of $\mathcal{F}$.

This fact has a crucial impact in the security against e.g. Meet-in-the-Middle (MitM) algebraic attacks. In such a case, it is crucial to reach the maximum degree (or a sufficiently high degree, if e.g. the security level is smaller than the maximum possible degree) both in the forward and in the backward direction. *The `Amaryllises` constructions guarantee that the maximum degree can be reached within few rounds in the backward direction even if the degree of $\mathcal{F}$ is small.* This could have a crucial impact on the total number of rounds, hence, having concrete benefits for what concerning the multiplicative complexity of `Amaryllises`. As we are going to discuss next, this could be a concrete advantage of `Amaryllises` with respect to other non-linear schemes/networks/constructions in the literature.

Comparison with Other Networks/Schemes/Constructions. Focusing on the growth of the degree, a similar conclusion holds for the SPN schemes as well. Indeed, while the S-Box is computed in the forward direction, the inverse S-Box is computed in the backward direction. If the inverse S-Box has a degree that is much higher than the S-Box itself (as for the case of $x \mapsto x^d$ versus $x \mapsto x^{1/d}$), few rounds are required to reach the maximum degree (or a sufficiently high degree) in the backward direction.

Regarding Feistel networks, Lai-Massey schemes, and `Horst` constructions, several scenarios are possible. For Feistel networks and Lai-Massey schemes, there are cases in which the growth of the degree is the same in both the forward and the backward direction, and others in which the degree growths faster in the backward direction than in the forward one (or vice-versa). As concrete examples, in a Type-II Feistel network $[x_0, x_1, \ldots, x_{2n-1}] \mapsto [y_0, y_1, \ldots, y_{2n-1}]$, the growth of the degree is equal in the two directions, since for each $i \in \{0, 1, \ldots, 2n-1\}$:

$$y_i := \begin{cases} x_{i+1} + \mathcal{F}(x_i) & \text{if } i \bmod 2 = 0\,, \\ x_{i+1} & \text{otherwise}\,, \end{cases} \qquad \textit{versus} \qquad x_i = \begin{cases} y_{i-1} & \text{if } i \bmod 2 = 0\,, \\ y_{i-1} - \mathcal{F}(y_{i-2}) & \text{otherwise}\,. \end{cases}$$

A similar result/conclusion holds for e.g. the Lai-Massey scheme defined in Prop. 1. In all these cases, the same number of rounds is necessary to reach the same (maximum) degree in both the forward and the backward direction.

For comparison, given a Type-III Feistel network defined as

$$[x_0, \ldots, x_{n-2}, x_{n-1}] \mapsto [y_0, \ldots, y_{n-2}, y_{n-1}] := [x_1 + \mathcal{F}(x_0), \ldots, x_{n-1} + \mathcal{F}(x_{n-2}), x_0]\,,$$

its inverse is defined as

$$x_0 = y_{n-1}\,, \quad x_1 = y_0 - \mathcal{F}(y_{n-1})\,, \quad x_2 = y_1 - \mathcal{F}(y_0 - \mathcal{F}(y_{n-1}))\,, \quad \ldots\,.$$

In such a case, the degree of the inverse in the i-th $\mathbb{F}_q$-word is upper bounded by $(\deg(\mathcal{F}))^{i-1} \leq (\deg(\mathcal{F}))^{n-1}$, which is higher than the degree of the corresponding forward function (that is, $\deg(\mathcal{F})$). A similar result/conclusion holds for e.g. the generalized Lai-Massey schemes $\texttt{GLM}_n$ proposed in Prop. 3 – 4. In these cases, a smaller number of rounds is potentially sufficient in order to achieve the maximum degree (or a sufficiently high degree – see before) in the backward direction with respect to the one necessarily in the forward direction.

Regarding the `Horst` construction, the main difference between the forward and the backward direction relies on the fact that a division takes places instead of a multiplication:

$$y_i = x_i \cdot \mathcal{G}_i(x_0, \ldots, x_{i-1}) + \mathcal{F}_i(x_0, \ldots, x_{i-1}) \qquad \textit{versus} \qquad x_i = \frac{y_i - \mathcal{F}_i(x_0, \ldots, x_{i-1})}{\mathcal{G}_i(x_0, \ldots, x_{i-1})}\,,$$

for given $x_0, x_1, \ldots, x_{i-1}$. In such a case, the growth of the degree in the backward direction depends both on the "representation" and on the details of the functions $\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_{n-2}$. Regarding the representation, the attacker can work with the fraction representation, as originally proposed by Jakobsen and Knudsen in the interpolation attack against modified versions of SHARK instantiated with $x \mapsto x^{-1}$ (see [JK97, Sect. 3.4] for more details). In such a case, the degree of each fraction is at most $\max\{1, \deg(\mathcal{F}_i), \deg(\mathcal{G}_i)\}$. However, if all the functions $\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_{n-2}$ are different, and if one has to combine such fractions, the degree of the lowest common denominator could be much larger than the maximum degree of each function $\mathcal{G}_i$ (this is obviously not the case if all the functions $\mathcal{G}_i$ are equal). Finally, if the fraction representation is not considered, then the degree of the polynomial corresponding to $1/\mathcal{G}_i$ could be very large (as a simple example, the degree of $x \mapsto 1/x$ over $\mathbb{F}_p$ is $p-2$).

7.3.2 Specific Algebraic Attacks: an Open Problem related to Gröbner Basis

As pointed out before, the degree is not the only ingredient that influences the cost of an algebraic attack. Other factors such as the density of the interpolation polynomial, the number of equations and variables, among others, play a crucial role as well. However, all these factors strictly depend on the details of the functions that instantiate each scheme. Hence, making claim about the security against generic algebraic attacks for generic constructions is quite hard (and probably meaningless).

For this reason, we limit ourselves to point out an interesting open problem for future work regarding the Gröbner basis attack [Buc76]. Gröbner basis is a strategy that allows to find solution(s) – if they exist – of a given system of non-linear equations that describe the analyzed scheme (depending on the scheme, the variable could be either the key for a cipher or a pre-image/collision for an hash function). The cost of such attack depends on many factors, including (i) the number of (non-linear) equations that composed the system of equations to solve, (ii) the number of variables, among other factors. In [GHR+23, Sect. 6.3], Griffin's designers noticed that the `Horst` construction provides concrete advantages in defeating the Gröbner basis attack with respect to a Feistel scheme due to the non-linear combination between x_i and the function $\mathcal{G}_i(x_0, \ldots, x_{i-1})$. (We emphasize that *a formal theoretical argument that supports this observation is still missing*, and open for future research.) As a result, even if a single round of `Horst` is clearly more expensive than a Feistel round (from the multiplicative point of view), the `Horst` construction has concrete advantages both in terms of security and performances over multiple rounds. The problem of studying if the non-linear mixing in `Amaryllises` can provide similar concrete advantages in the case of Gröbner basis attacks is left open for future work.

8 Summary and Future Directions

In this paper, we re-considered the Lai-Massey scheme originally proposed in [LM90, Vau99], and we presented new generalizations that are not (extended) affine equivalent to any generalized Feistel network. Inspired by the recent `Horst` construction, we also introduce the `Amaryllises` construction, in which the linear combination that takes place in the

Lai-Massey scheme can be replaced by a non-linear one An initial analysis of its statistical and algebraic properties is provided, showing its possible advantages when used in the context of MPC-/FHE-/ZK-friendly primitives.

The initial results proposed in this paper may open up *new interesting scenarios regarding the construction of new non-linear layers for future MPC-/FHE-/ZK-friendly designs*. For this reason, we propose some open problems that could be interesting to analyze for future works:

- given the variants of the Lai-Massey schemes proposed in this paper that are not EA-equivalent to any Feistel network, is it possible to identify the ones with better statistical properties than the Feistel networks (for a similar cost)?
- check if the CCZ equivalence[12] [CCZ98, CP19] holds or not among (some of) the networks/schemes presented in this paper;
- propose new generalizations of the Lai-Massey schemes and of the `Amaryllises` constructions, and/or propose new concrete efficient instantiations of the schemes/constructions presented in this paper. As a concrete example, in App. D, we propose a variant of the `Amaryllises` construction called Contracting-`Amaryllises`. At the current state, it is not clear how to efficiently instantiate it;
- better understand the advantages and the disadvantages of the `Horst` and of the `Amaryllises` constructions when used to instantiate a MPC-/FHE-/ZK-friendly primitive, with particular attention to the case of Gröbner Basis attacks.

Acknowledgments. The author thanks the FSE/ToSC'22 Reviewers for their valuable suggestions and comments. This work was supported by the German Research Foundation (DFG) within the framework of the Excellence Strategy of the Federal Government and the States – EXC 2092 CaSa – 39078197.

References

[AC21] Riccardo Aragona and Roberto Civino. On Invariant Subspaces in the Lai–Massey Scheme and a Primitivity Reduction. *Mediterr. J. Math.*, 18(165), 2021.

[ACG+19] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC. In *ASIACRYPT 2019 - Part III*, volume 11923 of *LNCS*, pages 371–397, 2019.

[Bar23] Augustin Bariant. Algebraic Cryptanalysis of Full Ciminion. Cryptology ePrint Archive, Paper 2023/1283, 2023. https://eprint.iacr.org/2023/1283.

[BBC+23] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems. New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode. In *CRYPTO 2023 - Part III*, volume 14083 of *LNCS*, pages 507–539, 2023.

[12] Let $q = p^s$ where $p \geq 2$ is a prime and s is a positive integer, and let $n, m \geq 1$. Let $\mathcal{F}, \mathcal{G} : \mathbb{F}_q^n \to \mathbb{F}_q^m$. The functions $\mathcal{F}$ and $\mathcal{G}$ are CCZ-equivalent if there exists an affine transformation A over $\mathbb{F}_q^n \times \mathbb{F}_q^m$ such that $\{(x, \mathcal{F}(x)) \mid x \in \mathbb{F}_q^n\} = A(\{(x, \mathcal{G}(x)) \mid x \in \mathbb{F}_q^n\})$.

[BBLP22] Augustin Bariant, Clémence Bouvier, Gaëtan Leurent, and Léo Perrin. Algebraic Attacks against Some Arithmetization-Oriented Primitives. *IACR Trans. Symmetric Cryptol.*, 2022(3):73–101, 2022.

[BCD+20] Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, and Friedrich Wiemer. Out of Oddity - New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems. In *CRYPTO 2020 - Part III*, volume 12172 of *LNCS*, pages 299–328, 2020.

[BDH+17] Guido Bertoni, Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. Farfalle: parallel permutation-based cryptography. *IACR Trans. Symmetric Cryptol.*, 2017(4):1–38, 2017.

[BDPA08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the Indifferentiability of the Sponge Construction. In *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 181–197, 2008.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In *CHES 2007*, volume 4727 of *LNCS*, pages 450–466, 2007.

[BS90] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *CRYPTO 1990*, volume 537 of *LNCS*, pages 2–21, 1990.

[BS93] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993.

[BS13] Andrey Bogdanov and Kyoji Shibutani. Generalized Feistel networks revisited. *Des. Codes Cryptogr.*, 66(1-3):75–97, 2013.

[Buc76] Bruno Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.*, 10(3):19–29, 1976.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[CP19] Anne Canteaut and Léo Perrin. On CCZ-equivalence, extended-affine equivalence, and function twisting. *Finite Fields Their Appl.*, 56:209–246, 2019.

[DGGK21] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters. Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields. In *EUROCRYPT 2021 - Part II*, volume 12697 of *LNCS*, pages 3–34, 2021.

[DR00] Joan Daemen and Vincent Rijmen. Rijndael for AES. In *The Third Advanced Encryption Standard Candidate Conference, April 13-14, 2000, New York, New York, USA*, pages 343–348. National Institute of Standards and Technology,, 2000.

[DR01] Joan Daemen and Vincent Rijmen. The wide trail design strategy. In *Cryptography and Coding - IMA 2001*, volume 2260 of *LNCS*, pages 222–238, 2001.

[DR02] Joan Daemen and Vincent Rijmen. Security of a Wide Trail Design. In *Progress in Cryptology - INDOCRYPT 2002*, volume 2551 of *LNCS*, pages 1–11, 2002.

[DR20] Joan Daemen and Vincent Rijmen. *The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition.* Information Security and Cryptography. Springer, 2020.

[GHR+23] Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang. Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications. In *CRYPTO 2023 – Part III*, volume 14083 of *LNCS*, pages 573–606, 2023.

[GKRS22] Lorenzo Grassi, Dmitry Khovratovich, Sondre Rønjom, and Markus Schofnegger. The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over $\mathbb{F}_p^n$ Preimage Attack on Full Grendel. *IACR Trans. Symmetric Cryptol.*, 2022(1):5–37, 2022.

[GLR+20] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy. In *EUROCRYPT 2020 – Part II*, volume 12106 of *LNCS*, pages 674–704, 2020.

[GØSW23] Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, and Roman Walch. From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications. In *EUROCRYPT 2023 – Part IV*, volume 14007 of *LNCS*, pages 255–286, 2023.

[Gra23] Lorenzo Grassi. Bounded Surjective Quadratic Functions over $\mathbb{F}_p^n$ for MPC-/ZK-/FHE-Friendly Symmetric Primitives. *IACR Trans. Symmetric Cryptol.*, 2023(2):94–131, 2023.

[GRR16] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace Trail Cryptanalysis and its Applications to AES. *IACR Trans. Symmetric Cryptol.*, 2016(2):192–225, 2016.

[GRS21] Lorenzo Grassi, Christian Rechberger, and Markus Schofnegger. Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer. *IACR Trans. Symmetric Cryptol.*, 2021(2):314–352, 2021.

[GSW+21] Chun Guo, François-Xavier Standaert, Weijia Wang, Xiao Wang, and Yu Yu. Provable Security of SP Networks with Partial Non-Linear Layers. *IACR Trans. Symmetric Cryptol.*, 2021(2):353–388, 2021.

[HR10] Viet Tung Hoang and Phillip Rogaway. On Generalized Feistel Networks. In *CRYPTO 2010*, volume 6223 of *LNCS*, pages 613–630, 2010.

[JK97] Thomas Jakobsen and Lars R. Knudsen. The Interpolation Attack on Block Ciphers. In *FSE 1997*, volume 1267 of *LNCS*, pages 28–40, 1997.

[Knu94] Lars R. Knudsen. Truncated and Higher Order Differentials. In *FSE 1994*, volume 1008 of *LNCS*, pages 196–211, 1994.

[KR21] Nathan Keller and Asaf Rosemarin. Mind the Middle Layer: The HADES Design Strategy Revisited. In *EUROCRYPT 2021 - Part II*, volume 12697 of *LNCS*, pages 35–63, 2021.

[LAAZ11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In *CRYPTO 2011*, volume 6841 of *LNCS*, pages 206–221, 2011.

[LM90] Xuejia Lai and James L. Massey. A Proposal for a New Block Encryption Standard. In *EUROCRYPT 1990*, volume 473 of *LNCS*, pages 389–404, 1990.

[LMR15] Gregor Leander, Brice Minaud, and Sondre Rønjom. A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In *EUROCRYPT 2015 – Part I*, volume 9056 of *LNCS*, pages 254–283, 2015.

[LTW18] Gregor Leander, Cihangir Tezcan, and Friedrich Wiemer. Searching for Subspace Trails and Truncated Differentials. *IACR Trans. Symmetric Cryptol.*, 2018(1):74–100, 2018.

[Mat93] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In *EUROCRYPT 1993*, volume 765 of *LNCS*, pages 386–397, 1993.

[Mat97] Mitsuru Matsui. New Block Encryption Algorithm MISTY. In *FSE 1997*, volume 1267 of *LNCS*, pages 54–68, 1997.

[Nyb96] Kaisa Nyberg. Generalized Feistel Networks. In *ASIACRYPT 1996*, volume 1163 of *LNCS*, pages 91–104, 1996.

[RS22] Arnab Roy and Matthias Steiner. An Algebraic System for Constructing Cryptographic Permutations over Finite Fields. *CoRR*, abs/2204.01802, 2022.

[RST23] Arnab Roy, Matthias Johann Steiner, and Stefano Trevisani. Arion: Arithmetization-Oriented Permutation and Hashing from Generalized Triangular Dynamical Systems. *CoRR*, abs/2303.04639, 2023.

[Sch93] Bruce Schneier. Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). In *FSE 1993*, volume 809 of *LNCS*, pages 191–204, 1993.

[Vau99] Serge Vaudenay. On the Lai-Massey Scheme. In *ASIACRYPT 1999*, volume 1716 of *LNCS*, pages 8–19, 1999.

[YPL11] Aaram Yun, Je Hong Park, and Jooyoung Lee. On Lai-Massey and quasi-Feistel ciphers. *Des. Codes Cryptogr.*, 58(1):45–72, 2011.

[ZMI90] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In *CRYPTO 1989*, volume 435 of *LNCS*, pages 461–480, 1990.

SUPPLEMENTARY MATERIAL

A About the Generalized Triangular Dynamical System

In this section, we show that the Generalized Triangular Dynamical System (GTDS) is a combination of a SPN' S-Box layer and of a `Horst` construction as defined in Theorem 1.

Let $q = p^s$ for a prime $p \geq 2$ and a positive integer $s \geq 1$, and let $n \geq 1$. For each $i \in \{0, 1, \ldots, n-1\}$, let $\mathcal{S}_i : \mathbb{F}_q \to \mathbb{F}_q$ be n permutation. Moreover, for each $i \in \{1, 2, \ldots, n-2\}$, let $\mathcal{F}_i, \mathcal{G}_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be $2 \cdot (n-1)$ functions such that $\mathcal{G}_i(x_0, x_1, \ldots, x_{i-1}) \neq 0$ for each $x_0, x_1, \ldots, x_{i-1} \in \mathbb{F}_q$. Following [RS22], a GTDS over $\mathbb{F}_q^n$ is defined as $\texttt{GTDS}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i := \begin{cases} \mathcal{S}_{i+1}(x_{i+1}) \cdot \mathcal{G}_{i+1}(x_0, x_1, \ldots, x_{i-1}) + \mathcal{F}_{i+1}(x_0, x_1, \ldots, x_{i-1}) & \text{if } i \in \{0, 1, \ldots, n-2\} \\ \mathcal{S}_0(x_0) & \text{otherwise } (i = n-1) \end{cases} .$$

In order to prove our statement, let

$$\forall i \in \{0,1,\ldots,n-1\}: \qquad z_i := \mathcal{S}_i(x_i)\,.$$

By simple computation, we have $y_{n-1} = z_0$ and

$$\forall i \in \{0,1,\ldots,n-2\}: \qquad y_i = z_{i+1} \cdot \mathcal{G}'_{i+1}(z_0, z_1, \ldots, z_{i-1}) + \mathcal{F}'_{i+1}(z_0, z_1, \ldots, z_{i-1})$$

where

$$\mathcal{G}'_i(w_0, w_1, \ldots, w_{i-1}) := \mathcal{G}_i\left(\mathcal{S}_0^{-1}(w_0), \mathcal{S}_1^{-1}(w_1), \ldots, \mathcal{S}_{i-1}^{-1}(w_{i-1})\right)\,,$$
$$\mathcal{F}'_i(w_0, w_1, \ldots, w_{i-1}) := \mathcal{F}_i\left(\mathcal{S}_0^{-1}(w_0), \mathcal{S}_1^{-1}(w_1), \ldots, \mathcal{S}_{i-1}^{-1}(w_{i-1})\right)\,.$$

Note that $\mathcal{G}'_i$ never returns zero due to the definition of $\mathcal{G}_i$.

Our claim follows immediately.

B Proof of Prop. 2 for the Case $n \geq 3$

We limit ourselves to prove the results for the two extremes and most commonly used cases, that is,

1. the case $l = 1$ in which the function $\mathcal{F}$ in the Lai-Massey scheme over $\mathbb{F}_q^n$ as proposed in Prop. 1 depends only on a single linear combinations of the inputs
2. the case $l = n-1$ in which it depends on $n-1$ independent linear combinations of the inputs.

The other "intermediate" cases can be easily proved by combining the two strategies proposed for these two extreme cases.

Moreover, we limit ourselves to prove the results for the case of a Lai-Massey scheme $\texttt{LM}$ over $\mathbb{F}_q^n$ defined as in Prop. 1 instantiated with $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$. It is simple to observe that, if such scheme is affine equivalent to a Feistel network, then the most generic Lai-Massey scheme $\texttt{LM}$ over $\mathbb{F}_q^n$ defined as in Prop. 1 (which corresponds to the combination of a Lai-Massey scheme and of an invertible linear layer, i.e., $M \circ \texttt{LM}$ for a proper invertible linear layer M) is affine equivalent as well. Indeed, $\texttt{LM} = B \circ \texttt{F}_{\text{G}} \circ A + C$ implies $M \circ \texttt{LM} = B' \circ \texttt{F}_{\text{G}} \circ A + C'$ for $B' := M \circ B$ and $C' := M \circ C$, where B' is obviously invertible.

B.1 1st Case: A-Equivalent to a Type-I Feistel Network

Let's start by considering a Lai-Massey scheme over $\mathbb{F}_q^n$ as proposed in Prop. 1 for $l = 1$, that is, $x_i \mapsto y_i = x_i + \mathcal{F}\left(\sum_{j=0}^{n-1} \lambda_j \cdot x_j\right)$ for each $i \in \{0,1,\ldots,n-1\}$, where $\mathcal{F} : \mathbb{F}_q \to \mathbb{F}_q$ and where $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in \mathbb{F}_q$ satisfy $\sum_{i=0}^{n-1} \lambda_i = 0$.

W.l.o.g., let's assume $\lambda_0 \neq 0$.[13] The analyzed Lai-Massey scheme is affine equivalent to a Type-I Feistel network $\texttt{F}_{\text{T.-I}}$ over $\mathbb{F}_q^n$ defined as

$$[x_0, x_1, x_2 \ldots, x_{n-1}] \mapsto [x_1 + \mathcal{F}(x_0), x_2, \ldots, x_{n-1}, x_0]$$

via the invertible linear transformations

$$A = \begin{bmatrix} \lambda_0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-1} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & -1 & 1 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & -1 & 0 & \ldots & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & -\frac{\lambda_2}{\lambda_0} & \ldots & -\frac{\lambda_{n-1}}{\lambda_0} & \frac{1}{\lambda_0} \\ 1 & 0 & \ldots & 0 & 0 \\ 1 & 1 & \ldots & 0 & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 1 & 0 & \ldots & 1 & 0 \end{bmatrix}, \qquad (6)$$

[13] If $\lambda_0 = 0$, then the following argument works by considering another equivalent Type-I Feistel network (e.g., if $\lambda_i \neq 0$, then it is sufficient to work with $y_i = x_{i+1} + \mathcal{F}(x_{i+2})$ a part from $y_j = x_{j+1}$ for $j = i$).

and $C = 0$. Indeed, we have that

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{bmatrix} \xrightarrow{A\times\cdot} \begin{bmatrix} \sum_{i=0}^{n-1} \lambda_i \cdot x_i \\ x_1 \\ x_2 - x_1 \\ \vdots \\ x_{n-1} - x_1 \end{bmatrix} \xrightarrow{\texttt{F}_{\text{T.-I}}} \begin{bmatrix} x_1 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i \cdot x_i\right) \\ x_2 - x_1 \\ \vdots \\ x_{n-1} - x_1 \\ \sum_{i=0}^{n-1} \lambda_i \cdot x_i \end{bmatrix} \xrightarrow{B\times\cdot} \begin{bmatrix} x_0 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i \cdot x_i\right) \\ x_1 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i \cdot x_i\right) \\ x_2 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i \cdot x_i\right) \\ \vdots \\ x_{n-1} + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i \cdot x_i\right) \end{bmatrix}.$$

B.2 2nd Case: A-Equivalent to a Contracting Feistel Network

Next, we consider the case of a Lai-Massey scheme over $\mathbb{F}_q^n$ as proposed in Prop. 1 for $l = n-1$ instantiated with $\mathcal{F} : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$, that is, $x_i \mapsto y_i = x_i + \mathcal{F}\big(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\big)$ for each $i \in \{0, 1, \ldots, n-1\}$, where we assume that $\lambda_i^{(j)} \in \mathbb{F}_q$ satisfy the following conditions:

i. $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$ for each $i \in \{0, 1, \ldots, n-2\}$;

ii. the vectors $\bar{\lambda}^{(0)} = [\lambda_0^{(0)}, \lambda_1^{(0)}, \ldots, \lambda_{n-1}^{(0)}], \bar{\lambda}^{(1)} = [\lambda_0^{(1)}, \lambda_1^{(1)}, \ldots, \lambda_{n-1}^{(1)}], \ldots, \bar{\lambda}^{(n-2)} = [\lambda_0^{(n-2)}, \lambda_1^{(n-2)}, \ldots, \lambda_{n-1}^{(n-2)}] \in \mathbb{F}_q^n \setminus \{0\}$ are linearly independent.

First of all, we point out the following.

Lemma 4. *Given q and n as before, let $\bar{\lambda}^{(0)}, \bar{\lambda}^{(1)}, \ldots, \bar{\lambda}^{(n-2)} \in \mathbb{F}_q^n$ be $n-1$ vectors that satisfy the previous two conditions just given. Then, the vectors $\hat{\lambda}^{(0)} = [\lambda_0^{(0)}, \lambda_1^{(0)}, \ldots, \lambda_{n-2}^{(0)}]$, $\hat{\lambda}^{(1)} = [\lambda_0^{(1)}, \lambda_1^{(1)}, \ldots, \lambda_{n-2}^{(1)}], \ldots, \hat{\lambda}^{(n-2)} = [\lambda_0^{(n-2)}, \lambda_1^{(n-2)}, \ldots, \lambda_{n-2}^{(n-2)}] \in \mathbb{F}_q^{n-1}$ (i.e., the previous vectors without the final component) are linearly independent as well.*

Proof. Assume *by contradiction* that there exist (non-trivial) $\psi_0, \psi_1, \ldots, \psi_{n-2} \in \mathbb{F}_q$ such that $\sum_{j=0}^{n-2} \psi_j \cdot \hat{\lambda}^{(j)} = 0 \in \mathbb{F}_q^{n-1}$. This also implies that $\sum_{j=0}^{n-2} \psi_j \cdot \bar{\lambda}^{(j)} = 0 \in \mathbb{F}_q^n$ as well, since

- for each $i \in \{0, 1, \ldots, n-2\}$: $\sum_{j=0}^{n-2} \psi_j \cdot \lambda_i^{(j)} = 0 \in \mathbb{F}_q$, due to the fact that $\sum_{j=0}^{n-2} \psi_j \cdot \hat{\lambda}^{(j)} = 0 \in \mathbb{F}_q^{n-1}$;
- about the last component:

$$\sum_{j=0}^{n-2} \psi_j \cdot \lambda_{n-1}^{(j)} = \sum_{j=0}^{n-2} \psi_j \cdot \left(-\sum_{i=0}^{n-2} \lambda_i^{(j)}\right) = -\sum_{i=0}^{n-2} \left(\sum_{j=0}^{n-2} \psi_j \cdot \lambda_i^{(j)}\right) = \sum_{i=0}^{n-2} 0 = 0 \in \mathbb{F}_q\,,$$

where the first equality is due to the first condition $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0 \in \mathbb{F}_q$ for each $i \in \{0, 1, \ldots, n-2\}$, while the third one is due to $\sum_{j=0}^{n-2} \psi_j \cdot \hat{\lambda}^{(j)} = 0 \in \mathbb{F}_q^{n-1}$.

This contradicts the second condition of linear independence among $\bar{\lambda}^{(0)}, \bar{\lambda}^{(1)}, \ldots, \bar{\lambda}^{(n-2)}$. □

In order to show that the analyzed Lai-Massey scheme is affine equivalent to a contracting Feistel network $\texttt{F}_C$ defined over $\mathbb{F}_q^n$ as

$$[x_0, x_1, x_2, \ldots, x_{n-1}] \mapsto [x_1, x_2, \ldots, x_{n-1}, x_0 + \mathcal{F}(x_1, x_2, \ldots, x_{n-1})]\,,$$

we introduce the values $\mu_{i,0}, \ldots, \mu_{i,n-2} \in \mathbb{F}_q$ for each $i \in \{1, \ldots, n-1\}$ defined as the ones that satisfy the following equality:

$$\forall i \in \{1, \ldots, n-1\} : \quad \begin{bmatrix} \lambda_0^{(0)} & \lambda_0^{(1)} & \ldots & \lambda_0^{(n-2)} \\ \lambda_1^{(0)} & \lambda_1^{(1)} & \ldots & \lambda_1^{(n-2)} \\ \vdots & & \ddots & \vdots \\ \lambda_{n-1}^{(0)} & \lambda_{n-1}^{(1)} & \ldots & \lambda_{n-1}^{(n-2)} \end{bmatrix} \times \begin{bmatrix} \mu_{i,0} \\ \mu_{i,1} \\ \vdots \\ \mu_{i,n-2} \end{bmatrix} = \begin{bmatrix} -1 \\ \delta_{i,1} \\ \vdots \\ \delta_{i,n-2} \\ \delta_{i,n-1} \end{bmatrix}, \quad (7)$$

where $\delta_{i,j}$ is the Kronecker delta (that is, $\delta_{i,j} = 1$ if $i = j$, and 0 otherwise). The left-hand side (l.h.s.) matrix has $n-1$ columns and n rows. However, its rows are not linearly independent, since their sum is equal to the zero vector (due to the condition on $\lambda_i^{(j)}$), or equivalently, the sum of each column is equal to zero. Since the right-hand side (r.h.s.) vector satisfies the same zero sum, the previous system of linear equations reduces to

$$\forall i \in \{1, \ldots, n-1\} : \quad \begin{bmatrix} \lambda_0^{(0)} & \lambda_0^{(1)} & \ldots & \lambda_0^{(n-2)} \\ \lambda_1^{(0)} & \lambda_1^{(1)} & \ldots & \lambda_1^{(n-2)} \\ \vdots & & \ddots & \vdots \\ \lambda_{n-2}^{(0)} & \lambda_{n-2}^{(1)} & \ldots & \lambda_{n-2}^{(n-2)} \end{bmatrix} \times \begin{bmatrix} \mu_{i,0} \\ \mu_{i,1} \\ \vdots \\ \mu_{i,n-2} \end{bmatrix} = \begin{bmatrix} -1 \\ \delta_{i,1} \\ \vdots \\ \delta_{i,n-2} \end{bmatrix},$$

where the l.h.s. matrix is invertible due to the fact that the vectors $\hat{\lambda}^{(0)}, \hat{\lambda}^{(1)}, \ldots, \hat{\lambda}^{(n-2)}$ are linearly independent, as proved before.

Given $\mu_{i,j}$ as before, we can now show that the analyzed Lai-Massey scheme is EA-equivalent to a contracting Feistel network $\mathtt{F}_C$ defined over $\mathbb{F}_q^n$ via the invertible linear transformations

$$A = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ \lambda_0^{(0)} & \lambda_1^{(0)} & \lambda_2^{(0)} & \ldots & \lambda_{n-1}^{(0)} \\ \lambda_0^{(1)} & \lambda_1^{(1)} & \lambda_2^{(1)} & \ldots & \lambda_{n-1}^{(1)} \\ \vdots & \vdots & & \ddots & \vdots \\ \lambda_0^{(n-2)} & \lambda_1^{(n-2)} & \lambda_2^{(n-2)} & \ldots & \lambda_{n-1}^{(n-2)} \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 0 & \ldots & 0 & 1 \\ \mu_{1,0} & \mu_{1,1} & \ldots & \mu_{1,n-2} & 1 \\ \mu_{2,0} & \mu_{2,1} & \ldots & \mu_{2,n-2} & 1 \\ \vdots & & \ddots & \vdots & \vdots \\ \mu_{n-1,0} & \mu_{n-1,1} & \ldots & \mu_{n-1,n-2} & 1 \end{bmatrix},$$

and $C = 0$. Indeed, we have that

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix} \xrightarrow{A\times\cdot} \begin{bmatrix} x_0 \\ \sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i \\ \vdots \\ \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i \end{bmatrix} \xrightarrow{\mathtt{F}_C(\cdot)} \begin{bmatrix} \sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i \\ \vdots \\ \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i \\ x_0 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i\right) \end{bmatrix}$$

$$\xrightarrow{B\times\cdot} \begin{bmatrix} x_0 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i\right) \\ \sum_{j=0}^{n-2} \mu_{1,j} \cdot \left(\sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot x_i\right) + x_0 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i\right) \\ \vdots \\ \sum_{j=0}^{n-2} \mu_{n-1,j} \cdot \left(\sum_{i=0}^{n-1} \lambda_i^{(j)} \cdot x_i\right) + x_0 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i\right) \end{bmatrix}$$

$$= \begin{bmatrix} x_0 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i\right) \\ x_1 + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i\right) \\ \vdots \\ x_{n-1} + \mathcal{F}\left(\sum_{i=0}^{n-1} \lambda_i^{(0)} \cdot x_i, \ldots, \sum_{i=0}^{n-1} \lambda_i^{(n-2)} \cdot x_i\right) \end{bmatrix},$$

where the last equality holds due to the definition of $\mu_{i,j}$.

Details about $\boldsymbol{A} \times (\boldsymbol{B} \times \text{circ}(\mathbf{0}, \mathbf{1}, \mathbf{0}, \dots, \mathbf{0})) = \boldsymbol{I}$

Here we show that

$$\begin{aligned} &A \times (B \times \text{circ}(0,1,0,\dots,0)) \\ &= \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ \lambda_0^{(0)} & \lambda_1^{(0)} & \lambda_2^{(0)} & \dots & \lambda_{n-1}^{(0)} \\ \lambda_0^{(1)} & \lambda_1^{(1)} & \lambda_2^{(1)} & \dots & \lambda_{n-1}^{(1)} \\ \vdots & \vdots & & \ddots & \vdots \\ \lambda_0^{(n-2)} & \lambda_1^{(n-2)} & \lambda_2^{(n-2)} & \dots & \lambda_{n-1}^{(n-2)} \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & \mu_{1,0} & \mu_{1,1} & \dots & \mu_{1,n-2} \\ 1 & \mu_{2,0} & \mu_{2,1} & \dots & \mu_{2,n-2} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & \mu_{n-1,0} & \mu_{n-1,1} & \dots & \mu_{n-1,n-2} \end{bmatrix} = I \end{aligned}$$

is again the identity matrix. Indeed, by re-writing Eq. (7), we get

$$\begin{bmatrix} \lambda_0^{(0)} & \lambda_0^{(1)} & \dots & \lambda_0^{(n-2)} \\ \lambda_1^{(0)} & \lambda_1^{(1)} & \dots & \lambda_1^{(n-2)} \\ \lambda_2^{(0)} & \lambda_2^{(1)} & \dots & \lambda_2^{(n-2)} \\ \vdots & & \ddots & \vdots \\ \lambda_{n-1}^{(0)} & \lambda_{n-1}^{(1)} & \dots & \lambda_{n-1}^{(n-2)} \end{bmatrix} \times \begin{bmatrix} \mu_{1,0} & \mu_{2,0} & \dots & \mu_{n-1,0} \\ \mu_{1,1} & \mu_{2,1} & & \mu_{n-1,0} \\ \vdots & & \ddots & \vdots \\ \mu_{1,n-2} & \mu_{2,n-1} & & \mu_{n-1,n-1} \end{bmatrix} = \begin{bmatrix} -1 & -1 & \dots & -1 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix},$$

that is,

$$\underbrace{\begin{bmatrix} \lambda_1^{(0)} & \lambda_1^{(1)} & \dots & \lambda_1^{(n-2)} \\ \lambda_2^{(0)} & \lambda_2^{(1)} & \dots & \lambda_2^{(n-2)} \\ \vdots & & \ddots & \vdots \\ \lambda_{n-1}^{(0)} & \lambda_{n-1}^{(1)} & \dots & \lambda_{n-1}^{(n-2)} \end{bmatrix}}_{\equiv \hat{A}} \times \underbrace{\begin{bmatrix} \mu_{1,0} & \mu_{2,0} & \dots & \mu_{n-1,0} \\ \mu_{1,1} & \mu_{2,1} & & \mu_{n-1,0} \\ \vdots & & \ddots & \vdots \\ \mu_{1,n-2} & \mu_{2,n-1} & & \mu_{n-1,n-1} \end{bmatrix}}_{\equiv \hat{B}} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Hence, given $\hat{A}, \hat{B} \in \mathbb{F}_q^{(t-1)\times(t-1)}$ such that $\hat{A} \times \hat{B} = I$, we also have that $\hat{B} \times \hat{A} = I$ and that $(\hat{B} \times \hat{A})^T = \hat{A}^T \times \hat{B}^T = I^T = I$, that is,

$$\begin{bmatrix} \lambda_1^{(0)} & \lambda_2^{(0)} & \dots & \lambda_{n-1}^{(0)} \\ \lambda_1^{(1)} & \lambda_2^{(1)} & \dots & \lambda_{n-1}^{(1)} \\ \vdots & & \ddots & \vdots \\ \lambda_1^{(n-2)} & \lambda_2^{(n-2)} & \dots & \lambda_{n-1}^{(n-2)} \end{bmatrix} \times \begin{bmatrix} \mu_{1,0} & \mu_{1,1} & \dots & \mu_{1,n-2} \\ \mu_{2,0} & \mu_{2,1} & \dots & \mu_{2,n-2} \\ \vdots & & \ddots & \vdots \\ \mu_{n-1,0} & \mu_{n-1,1} & \dots & \mu_{n-1,n-2} \end{bmatrix} = I\,.$$

The result $A \times (B \times \text{circ}(0,1,0,\dots,0)) = I$ follows immediately.

C Details and Examples for Sect. 5

C.1 Proof of Lemma 1

Here, we prove that the construction proposed in Lemma 1 is invertible.

By simple computation:

$$\begin{aligned}
\sum_{i=0}^{n-1} \mu_i \cdot \frac{y_i}{\alpha_i} &= \sum_{i=0}^{n-1} \mu_i \cdot x_i + \sum_{i=0}^{n-1} \left(\mu_i \cdot \left(\frac{1}{\sum_{j=0}^{n-1} \mu_j} \cdot \mathcal{H}\left(\sum_{j=0}^{n-1} \mu_j \cdot x_j \right) - \frac{\sum_{j=0}^{n-1} \mu_j \cdot x_j}{\sum_{j=0}^{n-1} \mu_j} \right) \right) \\
&= \sum_{i=0}^{n-1} \mu_i \cdot x_i + \left(\frac{1}{\sum_{j=0}^{n-1} \mu_j} \cdot \mathcal{H}\left(\sum_{j=0}^{n-1} \mu_j \cdot x_j \right) - \frac{\sum_{j=0}^{n-1} \mu_j \cdot x_j}{\sum_{j=0}^{n-1} \mu_j} \right) \cdot \left(\sum_{i=0}^{n-1} \mu_i \right) \\
&= \sum_{i=0}^{n-1} \mu_i \cdot x_i + \mathcal{H}\left(\sum_{j=0}^{n-1} \mu_j \cdot x_j \right) - \sum_{j=0}^{n-1} \mu_j \cdot x_j \\
&= \mathcal{H}\left(\sum_{j=0}^{n-1} \mu_j \cdot x_j \right) \qquad \longrightarrow \qquad \sum_{j=0}^{n-1} \mu_j \cdot x_j = \mathcal{H}^{-1}\left(\sum_{j=0}^{n-1} \mu_j \cdot \frac{y_j}{\alpha_j} \right),
\end{aligned}$$

since $\mathcal{H}$ is invertible. As a result, for each $i \in \{0, 1, \ldots, n-1\}$:

$$x_i = \frac{y_i}{\alpha_i} + \frac{1}{\sum_{j=0}^{n-1} \mu_j} \cdot \left(\mathcal{H}^{-1}\left(\sum_{j=0}^{n-1} \mu_j \cdot y_j/\alpha_j \right) - \sum_{j=0}^{n-1} \mu_j \cdot y_j/\alpha_j \right).$$

About the EA-Equivalence

We point out that the proposed scheme is EA-equivalent to a contracting Feistel network, due to the same argument proposed in App. B. In particular, assuming $\mu_0 \neq 0$ and $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$ (analogous for the other cases), the affine equivalence holds via the invertible matrices $A, B \in \mathbb{F}_q^{n \times n}$ equal to the ones given in (6), while the linear transformation C is defined via the matrix $C \in \mathbb{F}_q^{n \times n}$ identically equal to zero except for $C_{0,1} = -(\sum_{j=0}^{n-1} \mu_j)/\mu_0$.

C.2 Proof of Prop. 4

Here, we prove that the construction proposed in Prop. 4 is invertible.

The invertibility is proven by working iteratively, keeping in mind that $\texttt{GLM}_4$ is invertible (see Prop. 3 for details). Let's assume that $\texttt{GLM}_{n-2}$ is invertible. It follows immediately that it is possible to recover $x_0 - x_1, x_1 - x_2, \ldots, x_{n-4} - x_{n-3}$ by $y_0, y_1, \ldots, y_{n-3}$, due to the fact that such differences are independent of the last two outputs. Indeed, by construction, for each $i \in \{0, 1, \ldots, n-3\}$, the output y_i depends only on $w_0, w_1, \ldots, w_{n-4}$ and on $\mathcal{F}_{n-1}(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w_{n-2})$ in such a way that the difference $\frac{y_i}{\alpha_i} - \frac{y_j}{\alpha_j}$ is independent of $\mathcal{F}_{n-1}(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w_{n-2})$ – note that every element in z_i is multiplied by α_i.

Next, given $w_0 = x_0 - x_1, w_1 = x_1 - x_2, \ldots, w_{n-4} = x_{n-4} - x_{n-3}$, we have to find $w_{n-3} = x_{n-3} - x_{n-2}$ and $w_{n-2} = x_{n-2} - x_{n-1}$ in order to invert the system. By simple computation:

$$\begin{aligned}
x_{n-2} - x_{n-1} &= \frac{y_{n-2}}{\alpha_{n-2}} - \frac{y_{n-1}}{\alpha_{n-1}}, \\
x_{n-3} - x_{n-2} &= \frac{y_{n-3}}{\alpha_{n-3}} - \frac{y_{n-2}}{\alpha_{n-2}} - \sum_{i=1}^{n-3} \mathcal{F}_i(w_0, w_1, \ldots, w_{i-1}) - \mathcal{F}_{n-2}(w_0, w_1, \ldots, w_{n-4}, w_{n-2}),
\end{aligned}$$

where the r.h.s. of this last equation is independent of w_{n-3} by construction. Working exactly as before, given w_i for each $i \in \{0, 1, \ldots, n-2\}$, it is possible to invert the system and recover $x_0, x_1, \ldots, x_{n-1}$. This concludes the proof.

D The Contracting-`Amaryllises` Construction

In this section, we introduce the contracting-`Amaryllises` constructions, in which the function $\mathcal{F}$ takes as input n $\mathbb{F}_q$-elements and returns a single $\mathbb{F}_q$-element (i.e., $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q$), as the name "contracting" suggests.

Proposition 7 (Contracting-`Amaryllises`)**.** *Let $q = p^s$ be as before, and let $n \geq 2$ be an integer. Let $e \geq 1$ be an integer such that $\gcd(e, q-1) = 1$. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function that never returns zero for any non-zero input, that is,*

$$\forall [x_0, x_1, \ldots, x_{n-1}] \in \mathbb{F}_q^n \setminus \{[0, 0, \ldots, 0]\} : \qquad \mathcal{F}(x_0, x_1, \ldots, x_{n-1}) \neq 0 \,.$$

If the function $\mathcal{G}_{\psi_0, \psi_1, \ldots, \psi_{n-1}}(x) : \mathbb{F}_q \to \mathbb{F}_q$ defined as

$$\mathcal{G}_{\psi_0, \psi_1, \ldots, \psi_{n-1}}(x) := x^e \cdot \mathcal{F}(\psi_0 \cdot x, \psi_1 \cdot x, \ldots, \psi_{n-1} \cdot x)$$

is invertible for each arbitrary fixed non-null $[\psi_0, \psi_1, \ldots, \psi_{n-1}] \in \mathbb{F}_q^n \setminus \{[0, 0, \ldots, 0]\}$, then the contracting-`Amaryllises` construction $\mathtt{A}_C$ over $\mathbb{F}_q^n$ defined as $\mathtt{A}_C(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i := \alpha_i \cdot x_i^e \cdot \mathcal{F}(x_0, x_1, \ldots, x_{n-1}) \tag{8}$$

is invertible.

Proof. We start by pointing out two observations:

- first of all, the following equality always holds:

$$\forall i, j \in \{0, 1, \ldots, n-1\} : \qquad \frac{y_i \cdot x_j^e}{\alpha_i} = \frac{y_j \cdot x_i^e}{\alpha_j} = x_i^e \cdot x_j^e \cdot \mathcal{F}(x_0, x_1, \ldots, x_{n-1}) \,; \tag{9}$$

- secondly, $x_i = 0$ if and only if $y_i = 0$.

Regarding this second point, note that if $x_i = 0$, then $y_i = 0$. Vice-versa, if $y_i = 0$, then either $x_i^e = 0$ (and so $x_i = 0$) or $\mathcal{F}(x_0, x_1, \ldots, x_{n-1}) = 0$. However, $\mathcal{F}(x_0, x_1, \ldots, x_{n-1}) = 0$ if and only if $[x_0, x_1, \ldots, x_{n-1}] = [0, 0, \ldots, 0]$, which implies again $x_i = 0$.

W.l.o.g., assume that $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$ (other cases are analogous). For each $i \in \{0, 1, \ldots, n-1\}$ such that $y_i \neq 0$ (remember that $y_i = 0$ implies $x_i = 0$):

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

due to (9), and where $x \mapsto x^e$ is invertible by assumption on e. Since $\mathcal{G}$ is invertible by assumption (note that $\psi_j = (y_j/y_i)^{1/e}$ is fixed for each $j \in \{0, 1, \ldots, n-1\}$), it is always possible to recover x_i for each $i \in \{0, 1, \ldots, n-1\}$ as

$$x_i = \begin{cases} 0 & \text{if } y_i = 0 \,, \\ \mathcal{G}^{-1}_{\left(\frac{y_0}{y_i}\right)^{\frac{1}{e}}, \ldots, \left(\frac{y_{i-1}}{y_i}\right)^{\frac{1}{e}}, 1, \left(\frac{y_{i+1}}{y_i}\right)^{\frac{1}{e}}, \ldots, \left(\frac{y_{n-1}}{y_i}\right)^{\frac{1}{e}}}(y_i) & \text{otherwise} \,. \end{cases}$$

□

Regarding the contracting-`Amaryllises` construction, it does *not* admit invariant subspaces in general, since the inputs of the function $\mathcal{F}$ are $x_0, x_1, \ldots, x_{n-1}$ directly, and not linear combinations of them. However, such invariant subspace can exist depending on the details of the function $\mathcal{F}$ itself.

D.1 Homogeneous Functions for the contracting-`Amaryllises` Construction

The challenge we now have to face regards the construction of functions $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q$ that (i) satisfy the assumptions of Prop. 7, and that (ii) are efficient to compute from the multiplicative point of view.

In Prop. 8, we prove that homogeneous functions that never return zero satisfy such assumptions. Based on it, in the next subsection, we then provide some concrete examples of such functions.

Proposition 8. *Let $q = p^s$ be as before, and let $n \geq 1$. Let $d \geq 3$ be such that $\gcd(d, q-1) = 1$, and let $e \geq 1$ be an integer such that (i) $\gcd(e, q-1) = 1$ and such that (ii) $d' := d - e \geq 0$. Let $\mathfrak{I}_{d'} := \left\{[i_0, i_1, \ldots, i_{n-1}] \in \mathbb{Z}_+^n \mid \sum_{j=0}^{n-1} i_j = d'\right\}$.*

A function $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q$ satisfies the assumptions of Prop. 7 if the following conditions are satisfied:

1. *$\mathcal{F}$ is a homogeneous function of degree d' (that is, a sum of monomials of degree d' only) as*
$$\mathcal{F}(x_0, x_1, \ldots, x_{n-1}) = \sum_{\{i_0, i_1, \ldots, i_{n-1}\} \in \mathfrak{I}_{d'}} \varphi_{i_0, i_1, \ldots, i_{n-1}} \cdot x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{n-1}^{i_{n-1}} \,,$$
where $\varphi_{i_0, i_1, \ldots, i_{n-1}} \in \mathbb{F}_q$;
2. *$\mathcal{F}$ never returns zero for any non-zero input, that is, $\mathcal{F}(x_0, x_1, \ldots, x_{n-1}) \neq 0$ for each $[x_0, x_1, \ldots, x_{n-1}] \in \mathbb{F}_q^n \setminus \{[0, 0, \ldots, 0]\}$.*

Proof. It is sufficient to prove that $\mathcal{G}_{\psi_0, \psi_1, \ldots, \psi_{n-1}}(x) = x^{d-d'} \cdot \mathcal{F}(\psi_0 \cdot x, \psi_1 \cdot x, \ldots, \psi_{n-1} \cdot x)$ is invertible for each arbitrary fixed non-null $[\psi_0, \psi_1, \ldots, \psi_{n-1}] \in \mathbb{F}_q^n \setminus \{[0, 0, \ldots, 0]\}$.

Since $\mathcal{F}$ contains only monomials of degree d', then

$$\mathcal{G}_{\psi_0, \psi_1, \ldots, \psi_{n-1}}(x) = x^e \cdot \mathcal{F}(\psi_0 \cdot x, \psi_1 \cdot x, \ldots, \psi_{n-1} \cdot x) = x^d \cdot \mathcal{F}(\psi_0, \psi_1, \ldots, \psi_{n-1}) \,,$$

where $d = d' + e$ by definition, and since $\mathcal{F}$ is homogeneous of degree d. Since (i) $x \mapsto x^d$ is invertible due to the assumption on d and since (ii) $\mathcal{F}$ never returns zero for each non-null input by assumption, then the inverse of $y = \mathcal{G}_{\psi_0, \psi_1, \ldots, \psi_{n-1}}(x)$ is given by

$$x = \mathcal{G}^{-1}_{\psi_0, \psi_1, \ldots, \psi_{n-1}}(y) = \left(\frac{y}{\mathcal{F}(\psi_0, \psi_1, \ldots, \psi_{n-1})}\right)^{\frac{1}{d}} \,.$$

This concludes the proof. □

D.2 Suitable Functions for the contracting-`Amaryllises` Construction and Open Problems

D.2.1 Suitable Functions $\mathbb{F}_q^2 \to \mathbb{F}_q$

Here, we start by proposing some concrete examples of functions from $\mathbb{F}_q^2$ into $\mathbb{F}_q$ that satisfy the conditions just given in Prop. 8.

Lemma 5. *Given $q = p^s$ as before, let $d \geq 3$ be such that $\gcd(d, q-1) = 1$, and let $d' = d - 1$ (equivalently, $e = 1$). Let $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$. The function $\mathcal{F} : \mathbb{F}_q^2 \to \mathbb{F}_q$ defined as*

$$\mathcal{F}(x_0, x_1) = \sum_{i=1}^{d} \binom{d}{i} \cdot \alpha^i \cdot \beta^{d-i} \cdot x_0^{i-1} \cdot x_1^{d-i} = \begin{cases} \frac{(\alpha \cdot x_0 + \beta \cdot x_1)^d - (\beta \cdot x_1)^d}{x_0} & \text{if } x_0 \neq 0 \,, \\ d \cdot \alpha \cdot \beta^{d-1} \cdot x_1^{d-1} & \text{otherwise} \,, \end{cases}$$

satisfies the conditions given in Prop. 8.

Proof. The proof is trivial. Indeed, it is obvious that the function $\mathcal{F}$ is homogeneous of degree $d' = d-1$. Moreover, it never returns zero for any non-zero input, since (i) $d \cdot \alpha \cdot \beta^{d-1} \cdot x_1^{d-1} = 0$ if and only if $x_0 = x_1 = 0$, and (ii) $\frac{(\alpha \cdot x_0 + \beta \cdot x_1)^d - (\beta \cdot x_1)^d}{x_0} = 0$ if and only if $(\alpha \cdot x_0 + \beta \cdot x_1)^d = (\beta \cdot x_1)^d$, that is, $x_0 = 0$, which is not possible by assumption. □

An example for the prime fields only is proposed in the following.

Lemma 6. *Let $p \geq 3$ be a prime integer, and let $d \geq 3$ be such that $\gcd(d, p-1) = 1$. Let $d' \in \{2, 4, \dots, d-1\}$ be an even integer smaller than d such that $\gcd(d - d', p-1) = 1$. Let $\alpha, \beta, \lambda, \lambda', \omega \in \mathbb{F}_p$ be such that (i) $\lambda \neq \lambda'$ and (ii) ω is a quadratic non-residue modulo p. The function*

$$\mathcal{F}(x_0, x_1) = \alpha^2 \cdot (x_0 + \lambda \cdot x_1)^{d'} - \omega \cdot \beta^2 \cdot (x_0 + \lambda' \cdot x_1)^{d'}$$

satisfies the assumptions of Prop. 8.

Proof. It is sufficient to show that $\mathcal{F}(x_0, x_1) \neq 0$ for each $[x_0, x_1] \neq [0, 0]$. Assume by contradiction that there exists $[x_0, x_1] \neq [0, 0]$ such that $\mathcal{F}(x_0, x_1) = 0$, that is, $\left(\alpha \cdot (x_0 + \lambda \cdot x_1)^{\frac{d'}{2}}\right)^2 = \omega \cdot \left(\beta \cdot (x_0 + \lambda' \cdot x_1)^{\frac{d'}{2}}\right)^2$. Such equality is satisfied only in the case where both sides are equal to zero, since the left-hand side of the equality is a quadratic residue modulo p, while the right-hand side is a quadratic non-residue modulo p, due to the choice of ω. However, note that $x_0 + \lambda \cdot x_1 = x_0 + \lambda' \cdot x_1 = 0$ occurs if and only if $x_0 = x_1 = 0$, since the vectors $[1, \lambda] \in \mathbb{F}_p^2$ and $[1, \lambda'] \in \mathbb{F}_p^2$ are linearly independent (since $\lambda \neq \lambda'$). Hence, if $x_0 \neq 0$ or/and $x_1 \neq 0$, such equality never holds. □

D.2.2 Suitable Functions $\mathbb{F}_q^{\geq 3} \to \mathbb{F}_q$

Next, we generalize the previous results for the case $\mathbb{F}_q^n \to \mathbb{F}_q$ with $n \geq 3$. Our strategy is to construct the functions $\mathcal{F}$ that satisfy Prop. 8 in an iterated way, that is, given a function $\mathcal{F}_m : \mathbb{F}_q^m \to \mathbb{F}_q$ for a certain $m \geq 2$ that satisfies the required properties, we show how to construct a function $\mathcal{F}_n : \mathbb{F}_q^n \to \mathbb{F}_q$ for $n > m$ that satisfies the required properties as well.

Proposition 9. *Given $q = p^s$ as before, let $m \geq 2$ and let $n_0, n_1, \dots, n_{m-1} \geq 1$ and let $n := \sum_{i=0}^{m-1} n_i$. For each $i \in \{n_0, n_1, \dots, n_{m-1}, m\}$, let $\mathcal{F}_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be a function that satisfy the assumptions of Prop. 8, that is, (i) it is an homogeneous function of a certain degree $\deg(\mathcal{F}_i) \geq 1$, and (ii) it never returns zero for any non-zero input (i.e., $\mathcal{F}_i(x_0, x_1, \dots, x_{i-1}) \neq 0$ for each $[x_0, x_1, \dots, x_{i-1}] \in \mathbb{F}_q^i \setminus \{[0, 0, \dots, 0]\}$).*

Let $d \geq 2$ be the least common multiple of $\deg(\mathcal{F}_{n_0}), \deg(\mathcal{F}_{n_1}), \dots, \deg(\mathcal{F}_{n_{m-1}})$, that is,

$$d := lcm\left(\deg(\mathcal{F}_{n_0}), \deg(\mathcal{F}_{n_1}), \dots, \deg(\mathcal{F}_{n_{m-1}})\right) .$$

The function $\mathcal{F}_n : \mathbb{F}_q^n \to \mathbb{F}_q$ defined as

$$\mathcal{F}_n(x_0, x_1, \dots, x_n) := \mathcal{F}_m\Bigg((\mathcal{F}_{n_0}(x_0, \dots, x_{n_0 - 1}))^{\frac{d}{\deg(\mathcal{F}_{n_0})}}, (\mathcal{F}_{n_1}(x_{n_0}, \dots, x_{n_0 + n_1 - 1}))^{\frac{d}{\deg(\mathcal{F}_{n_1})}}, \dots, (\mathcal{F}_{n_{m-1}}(x_{n-n_m}, \dots, x_{n-1}))^{\frac{d}{\deg(\mathcal{F}_{n_{m-1}})}} \Bigg)$$

satisfies the assumptions of Prop. 8, that is,

1. *it is homogeneous of degree $d \cdot \deg(\mathcal{F}_m)$;*
2. *$\mathcal{F}_n$ never returns zero for any non-zero input in $\mathbb{F}_q^n$.*

Proof. Regarding the first point, $\mathcal{F}_n$ is a homogeneous function of degree $d \cdot \deg(\mathcal{F}_m)$ since (i) $\mathcal{F}_m$ is a homogeneous function of degree $\deg(\mathcal{F}_m)$ and (ii) each input of $\mathcal{F}_m$ is a homogeneous function of degree d.

Regarding the second point, $\mathcal{F}_n$ returns zero if and only if all its inputs are equal to zero since (i) $\mathcal{F}_m$ returns zero if and only if all its inputs are equal to zero and (ii) each input of $\mathcal{F}_m$, that is, $\mathcal{F}_{n_i}(z_0, z_1, \dots, z_{n_i-1})$, returns zero if and only $z_0 = z_1 = \dots = z_{n_i-1} = 0$. □

By applying the previous result iteratively, it is possible to construct functions $\mathcal{F}_n : \mathbb{F}_q^n \to \mathbb{F}_q$ that satisfy the assumptions of Prop. 8 for each $n \geq 3$ as

$$\mathcal{F}_n(x_0, x_1, \dots, x_{n-1}) = \mathcal{F}_2\left(\mathcal{F}_{n-1}(x_0, x_1, \dots, x_{n-2}), x_{n-1}^{\deg(\mathcal{F}_{n-1})}\right)$$

by making use of the functions $\mathcal{F}_2 : \mathbb{F}_q^2 \to \mathbb{F}_q$ proposed before.

Open Problem. The main drawback of this strategy regards the fact that the degrees of the obtained functions are *strictly* bigger than the degrees of the input functions. We leave the problem to propose low-degree functions $\mathcal{F}_n$ that satisfy the required assumptions of Prop. 8 as an open problem for future work.