Generalizations of the Lai-Massey Scheme: the Blooming of Amaryllises

Lorenzo Grassi

Digital Security Group, Radboud University, The Netherlands
l.grassi@science.ru.nl

Abstract. In this paper, we re-investigate the Lai-Massey scheme, originally proposed in the cipher IDEA. Due to the similarity with the Feistel schemes, 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 (affine) equivalent to any generalized Feistel scheme proposed in the literature so far. Then, inspired by the recent `Horst` construction, we propose the generalized `Amaryllises` construction as a generalization of the Lai-Massey scheme, in which the linear combination in the Lai-Massey scheme is replaced by a non-linear one. Besides proposing concrete examples of the `Amaryllises` construction, we discuss its (possible) advantages and disadvantages with respect to other existing schemes/constructions published in the literature, with particular attention on the Lai-Massey one and on the `Horst` one.

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

Contents

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 (for our goals, we do not make a 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 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 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,

$$[x_0, x_1] \mapsto [x_1 + F(x_0), x_0] \,.$$

With respect to the SPN case, FNs are invertible by construction independently of the details of the 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, computing a Feistel scheme in the forward or in the backward direction is very similar (even identical in some cases), since the same F-function is computed in the two processes. Due to these facts:

- a large proportion of schemes is based on the Feistel design approach, including DES, Blowfish [Sch93], MISTY [Mat97], CAST-128/-256 [Ada97], among many others;
- several generalizations have been proposed in the literature, including Type-I/-II/-III Feistel schemes [ZMI90, Nyb96], contracting and expanding Feistel schemes [SK96, HR10], among others;
- the indistinguishability and the indifferentiability of r rounds generalized Feistel schemes instantiated with a Pseudo-Random Function/Permutation (PRF/PRP) have been extensively analyzed – see [Pat98, Pat01, MP03, CPS08, DS16].

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]. Similar to Feistel, the input is first split into two halves, but in this case a function F is applied on their difference, and the result of such function is then added to each input, that is,

$$[x_0, x_1] \mapsto [x_0 + F(x_0 - x_1), x_1 + F(x_0 - x_1)] \,.$$

As in the case of Feistel schemes, the invertibility of Lai-Massey schemes follows from its construction, that is, it is independent of details of the function F. However, compared to the Feistel schemes, 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 schemes, 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 scheme 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 F and the halves that composed the input is replaced by a non-linear combination.

Our Contribution

Relation between Generalized Feistel and Lai-Massey Schemes

The simplest generalization of a Lai-Massey scheme recently proposed in [GØSW22] and recalled in Sect. 3 works as following:

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

In Sect. 4, we prove that any Lai-Massey scheme of that form is *affine equivalent* to a generalized Feistel scheme, that is, a Lai-Massey scheme of this form is equal to a generalized Feistel scheme pre- and post-processed with affine invertible transformations. In particular, we show that r Lai-Massey consecutive rounds are equivalent to r generalized Feistel consecutive rounds in which no swapping of the components takes place (besides an initial and a final invertible affine transformation). As a direct consequence, this fact implies the existence of invariant subspaces in Lai-Massey schemes, already found in [Vau99].

Keeping in mind that Feistel schemes are much better studied than Lai-Massey ones, it could be potentially possible to transfer for "free" the known results on generalized Feistel schemes to the Lai-Massey ones by exploiting the existence of the affine equivalence relation between such two schemes. Besides indistinguishability and indifferentiability previously recalled, this could e.g. also include the post-quantum security of Lai-Massey schemes and their variants [MGWH22, CS22, BCFN22], allowing the community to treat generalized Feistel schemes and the Lai-Massey ones as a single construction.

New Generalizations of the Lai-Massey Schemes

As next step, in Sect. 5, we propose two new generalizations of the Lai-Massey scheme introduced in [GØSW22] and just recalled. In these two new generalizations, our goal is to capture the essence of the Lai-Massey scheme:

generalized Lai-Massey schemes: instead of limiting ourselves to consider a fixed function for each input/output, we allow for *different functions that take linear combinations of the sub-blocks with the zero-sum condition on the coefficients as inputs and for which the entire construction is invertible*;

redundant Lai-Massey schemes: instead of limiting ourselves to consider a function which takes as inputs linear combinations of the sub-blocks with the zero-sum condition on the coefficients, we allow for *any fixed function F for which the entire construction is invertible*.

Formal definitions are given in Sect. 5, respectively Def. 6 and Def. 7.

With these new definitions in our hands, our goal is to set up variants of the Lai-Massey scheme that are not extended affine equivalent to any generalized Feistel scheme. This would potentially allow us to *construct new schemes with better properties than the generalized Feistel ones*, e.g., from the indifferentiability and/or indistinguishability and/or post-quantum security point of view.

In there, we propose 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 scheme. E.g., working over a prime field $\mathbb{F}_p^2$ for $p \geq 3$, the simplest example of an invertible redundant Lai-Massey scheme in which the function F depends on linear combinations of the sub-blocks for which the sum of the coefficients of such linear combination is *non*-zero is given by

$$[x_0, x_1] \mapsto \left[\alpha_0 \cdot \left(x_0 \underbrace{- \frac{\psi}{2} \cdot (x_0 - x_1)^2 \cdot (x_0 + x_1)}_{=F(x_0,x_1)}\right), \alpha_1 \cdot \left(x_1 \underbrace{- \frac{\psi}{2} \cdot (x_0 - x_1)^2 \cdot (x_0 + x_1)}_{=F(x_0,x_1)}\right)\right],$$

where $\alpha_0, \alpha_1 \in \mathbb{F}_p \setminus \{0\}$, with the condition that $\psi \in \mathbb{F}_p$ is a quadratic non-residue modulo p (that is, $\psi \neq z^2$ for each $z \in \mathbb{F}_p$). In such a case, the function F depends on $x_0 - x_1$ (whose coefficients $1, -1$ sum to zero) and on $x_0 + x_1$ (whose coefficients $1, 1$ do not sum to zero). We prove that the obtained invertible generalized Lai-Massey scheme is *not* extended affine equivalent to any generalized Feistel scheme. We refer to Sect. 5 for other examples.

The Generalized `Amaryllises` Construction

The new generalizations of the Lai-Massey scheme share several properties with the original Lai-Massey scheme, including the facts that

- a non-linear mixing among the inputs takes place on each round (this potentially imply that a linear layer is not necessary anymore for achieving full diffusion);
- the *same* non-linear function is used in the encryption/forward direction and in the decryption/backward one.

While this last property can have some concrete advantages from the e.g. implementation point of view, it may not be desirable from the security point of view. E.g., consider a Lai-Massey scheme for which the degree in encryption/forward direction is equal to the one in the decryption/backward direction. Compared to a scheme in which each round function has small degree in the encryption/forward direction and high (almost maximum) degree in the decryption/backward one (as in the case of power maps), the designer has to (almost) double the number of rounds in order to guarantee its security against Meet-in-the-Middle algebraic attacks. Based on these considerations (discussed in details in Sect. 6), our next goal is to construct a cryptographic scheme with the following properties:

1. it provides (full) non-linear mixing among the inputs;
2. the degree of the scheme in the decryption/backward direction is much higher than the degree and in the encryption/forward direction (or vice-versa).

We reached such goal by replacing the linear combinations in the Lai-Massey schemes with non-invertible ones. The starting points are

- the redundant Lai-Massey scheme $[x_0, x_1, \dots, x_{n-1}] \mapsto [y_0, y_1, \dots, y_{n-1}]$ defined as

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

  for a certain function $F : \mathbb{F}_q^n \to \mathbb{F}_q$;

- the `Horst` construction recently introduced by Grassi et al. [GHR+22], and defined over $\mathbb{F}_q^2$ as

$$[x_0, x_1] \mapsto [x_1 \cdot G(x_0) + F(x_0), x_0] \, .$$

The invertibility of this last scheme holds under the condition that G never returns zero. Moreover, generalizations of such construction over $\mathbb{F}_q^n$ for $n \geq 3$ are also possible.

Intuitively, by applying the same approach to the function proposed in (1), we get something of the form

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

for two functions $F, H : \mathbb{F}_q^n \to \mathbb{F}_q$. We call this new construction as the "generalized `Amaryllises`" scheme.[1] A formal definition is given in Def. 8 – see Sect. 6.2.

In Sect. 7, we show how to concretely set up generalized `Amaryllises` schemes by providing a list of (non-trivial) conditions that the functions F and H must satisfy in order to guarantee that the scheme is invertible. In particular, we show how to construct functions F, H with *low-multiplicative complexity* that satisfy such conditions. As we are going to show in there, when working over a small field $\mathbb{F}_q$ (e.g., q equal to $2^4, 2^8$ or similar), it is always possible to find functions F, H that satisfy the required conditions by using an exhaustive approach. However, this strategy immediately fails when q is very large, e.g.,

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

$q \geq 2^{64}$, as in the case of symmetric primitives used for Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge (ZK) proofs. In such a case, the ability to construct F, H that satisfy the required conditions and that are easy/cheap to compute (hence, with a simple algebraic expression) becomes crucial.

The obtained schemes satisfy the main objectives that we previously set ourselves. In order to better understand them, in Sect. 8 we discuss the advantages (and the possible disadvantages) of the generalized `Amaryllises` scheme with respect to the schemes already present/known in the literature in terms of efficiency and security, with particular attention to the generalized/redundant Lai-Massey schemes. As a final result, *the schemes proposed in this paper could may constitute a natural and useful building block for the designing of new symmetric primitives*, particularly for the ones targeting efficiency in MPC/FHE/ZK applications/protocols, whose cost metric is related to the number of non-linear operations necessary to evaluate and/or verify the symmetric scheme itself.

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 either parameters/indexes or variables, and greek letters to denote fixed elements in $\mathbb{F}_q$. We use capital letter or the calligraphic font to denote functions. We use the fraktur font (e.g., $\mathfrak{X}$) to denote sets of elements. 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 $s^{(0)}, s^{(1)}, \ldots, s^{(t-1)} \in \mathbb{F}_q^n$. We denote by $\mathrm{circ}(\mu_0, \mu_1, \ldots, \mu_{n-1}) \in \mathbb{F}_p^{n \times n}$ a circulant matrix

$$\mathrm{circ}(\mu_0, \mu_1, \ldots, \mu_{n-1}) \coloneqq \begin{bmatrix} \mu_0 & \mu_1 & \ldots & \mu_{n-2} & \mu_{n-1} \\ \mu_{n-1} & \mu_0 & \ldots & \mu_{n-3} & \mu_{n-2} \\ \vdots & & & & \vdots \\ \mu_1 & \mu_2 & \ldots & \mu_{n-1} & \mu_0 \end{bmatrix} .$$

EA-Equivalence. Two functions F and G are EA-equivalent if they satisfy the following requirement.

Definition 1 (EA-Equivalence)**.** Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer. Let $n, m \geq 1$, and let $F, G : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be two functions. F and 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

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

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

Generalized Feistel Schemes. Regarding the definition of generalized Feistel schemes, we propose the following:

Definition 2 (Generalized Feistel Schemes)**.** Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n \geq 2$. For each $i \in \{1, 2, \ldots, n-1\}$, let $F_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be a function. The generalized Feistel scheme $\mathcal{F}_{\mathrm{G}}$ over $\mathbb{F}_q^n$ is defined as

$$\mathcal{F}_{\mathrm{G}}(x_0, x_1, \ldots, x_{n-1}) \coloneqq y_0 \| y_1 \| \ldots \| y_{n-1}$$

where

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

The invertibility of the entire construction is independent of the details of $F_0, \ldots, F_{n-2}$. Indeed, we have that (i) $x_0 = y_{n-1}$, and (ii) for each $i \geq 1$, $x_i = y_{i-1} - F_i(x_0, x_1, \ldots, x_{i-1})$ where y_{i-1} and $x_0, x_1, \ldots, x_{i-1}$ are given.

In App. A.1, we show that any generalized Feistel scheme proposed in the literature including [ZMI90, Nyb96, SK96, SS04, HR10, SM10, YI13, BS13, BMT13, AGP+19] is *EA-equivalent* to the generalized Feistel scheme just proposed.

Known Permutations over $\mathbb{F}_q$. Well known examples of invertible functions over $\mathbb{F}_q$ include the power maps and the Dickson polynomials (recalled in App. E).

Theorem 1 ([MP13])**.** *Let $d \geq 1$ be a positive integer, and let $q = p^s$, where $p \geq 2$ is a prime and s is a positive integer. The power map $x \mapsto x^d$ over $\mathbb{F}_q$ is invertible if and only if* $\gcd(d, q-1) = 1$.

The Legendre Symbol. Next, we recall the Legendre symbol used in the following.

Definition 3. Let $p \geq 3$ be a prime number. An integer α is a quadratic residue modulo p if it is congruent to a perfect square modulo p, and it is a quadratic non–residue modulo p otherwise.

Definition 4 (Legendre Symbol)**.** The Legendre symbol $L_p(\cdot)$ is a function $L_p : \mathbb{F}_p \to \{-1, 0, 1\}$ defined as $L_p(x) \coloneqq x^{\frac{p-1}{2}} \mod p$, or equivalently $L_p(0) = 0$ and

$$L_p(x) \coloneqq \begin{cases} 1 & \text{if } x \text{ is a non-zero quadratic residue modulo } p, \\ -1 & \text{if } x \text{ is a quadratic non-residue modulo } p \end{cases}.$$

Proposition 1 ([MP13])**.** *The Legendre symbol has the following properties:*

1. *if $x = y \mod p$, then $L_p(x) = L_p(y)$;*
2. *$L_p(x \cdot y) = L_p(x) \cdot L_p(y)$.*

3 Related Work about Lai-Massey Schemes

Let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$. Given a function F over $\mathbb{F}_q$, the Lai-Massey construction over $\mathbb{F}_q^2$ introduced in [LM90] is defined as

$$[x_0, x_1] \mapsto [y_0, y_1] \coloneqq [x_0 + F(x_0 - x_1), x_1 + F(x_0 - x_1)]\,. \tag{2}$$

Its invertibility follows from the fact that $y_0 - y_1 = x_0 - x_1$, and so $x_j = y_j - F(y_0 - y_1)$ for each $j \in \{0, 1\}$.

3.1 Lai-Massey Schemes over $\mathbb{F}_q^{\geq 2}$ from [GØSW22]

A possible generalization of the Lai-Massey construction over $\mathbb{F}_q^n$ for $n \geq 2$ has been recently proposed in [GØSW22].[2]

Proposition 2 (Prop. 1, [GØSW22]). *Let $n \geq 2$ be an integer, and let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_p \setminus \{0\}$. Let $l \in \{1, 2, \ldots, n-1\}$. Let $F : \mathbb{F}_q^l \to \mathbb{F}_q$ be any function. For each $i \in \{0, 1, \ldots, l-1\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)} \in \mathbb{F}_q$ be such that (i) $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$, (ii) $[\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)}] \neq [0, 0, \ldots, 0]$, and (iii) the vectors $[\lambda_0^{(0)}, \lambda_1^{(0)}, \ldots, \lambda_{n-1}^{(0)}], [\lambda_0^{(1)}, \lambda_1^{(1)}, \ldots, \lambda_{n-1}^{(1)}], \ldots, [\lambda_0^{(l-1)}, \lambda_1^{(l-1)}, \ldots, \lambda_{n-1}^{(l-1)}]$ to be linearly independent.*

The Lai-Massey function $\mathcal{LM}$ over $\mathbb{F}_q^n$ defined as $\mathcal{LM}(x_0, x_1, \ldots, x_{n-1}) \coloneqq y_0 \| y_1 \| \ldots \| y_{n-1}$ where

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

is invertible.

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

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

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

3.2 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 construction proposed in Prop. 2. We refer to [GRR16] for a formal definition of (invariant) subspace trails. We limit ourselves to recall the following definition.[3]

Definition 5 ([GRR16]). Let $n \geq 2$ be an integer, and let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$. Let $\mathfrak{U}_0, \ldots, \mathfrak{U}_r \subseteq \mathbb{F}_q^n$ be $r+1$ subspaces such that $\dim(\mathfrak{U}_i) \leq \dim(\mathfrak{U}_{i+1}) < n$ for each $i \in \{0, 1, \ldots, r-1\}$. $(\mathfrak{U}_0, \ldots, \mathfrak{U}_r)$ is a subspace trail of length $r \geq 1$ for a function F over $\mathbb{F}_q^n$ if for each $i \in \{0, \ldots, r-1\}$ and for each $\varphi_i \in \mathbb{F}_q^n$, there exists $\varphi_{i+1} \in \mathbb{F}_q^n$ such that $F(\mathfrak{U}_i + \varphi_i) \coloneqq \{F(x) \mid \forall x \in \mathfrak{U}_i + \varphi_i\} \subseteq \mathfrak{U}_i + \varphi_{i+1}$. We say that it is an *invariant* subspace trail if $\mathfrak{U}_i = \mathfrak{U}_j$ for each $i, j \in \{0, 1, \ldots, r\}$.

Based on this, let's analyze the Lai-Massey construction $\mathcal{LM}$ defined as in Prop. 2 over $\mathbb{F}_q^n$ and instantiated by $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$. In such a case, it admits

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

[2] To be precise, the following proposition is a slightly modified version of the result proposed in [GØSW22]. In there, authors assume $\alpha_i = 1$ for each $i \in \{0, 1, \ldots, n-1\}$.

[3] We point out that the following definition is different from the one proposed in [LAAZ11, LMR15]. In such cases, the function F depends on a secret key k, and it is required that the equality $F_k(\mathfrak{U} + \varphi) = \mathfrak{U} + \varphi'$ hold for some $\varphi, \varphi' \in \mathbb{F}_q^n$, whose value usually depend on the value of the key. The existence of such invariant subspaces is in general strongly related to the existence of weak keys. In contrast, our discussion here is independent of the value of the key, making the definition proposed in [GRR16] more suitable for our purpose.

as *invariant* subspace. Indeed, it is easy to check that, for each $\varphi \in \mathbb{F}_q^n$, there exists $\psi \in \mathbb{F}_q^n$ such that

$$\mathcal{LM}(\mathfrak{X}+\varphi) \coloneqq \{\mathcal{LM}(x+\varphi) \in \mathbb{F}_q^n \mid \forall x \in \mathfrak{X}\} = \mathfrak{X} + \psi\,,$$

since

$$\forall i \in \{0,1,\dots,n-1\}: \qquad y_i = x_i + \underbrace{F\left(\sum_{j=0}^{n-1}\lambda_j^{(0)}\cdot\varphi_j, \sum_{j=0}^{n-1}\lambda_j^{(1)}\cdot\varphi_j, \dots, \sum_{j=0}^{n-1}\lambda_j^{(l-1)}\cdot\varphi_j\right)}_{=\psi_i \text{ (constant)}}$$

for each $x \in \mathfrak{X}+\varphi$.

Independently of the values of $\lambda_j^{(i)}$, the subspace $\mathfrak{X}$ just defined for the Lai-Massey construction proposed in Prop. 2 and instantiated with $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$ is never an empty set.

Lemma 1. $\langle[1,1,\dots,1]\rangle \subseteq \mathfrak{X}$. *Moreover,*

$$\dim(\mathfrak{X}) = n - \dim(\langle[\lambda_0^{(0)},\lambda_1^{(0)},\dots,\lambda_{n-1}^{(0)}],\dots,[\lambda_0^{(l-1)},\lambda_1^{(l-1)},\dots,\lambda_{n-1}^{(l-1)}]\rangle) \geq 1\,.$$

Proof. It is sufficient to note that (i) $\langle[1,1,\dots,1]\rangle \equiv \{[x,x,\dots,x] \in \mathbb{F}_q^n \mid \forall x \in \mathbb{F}_q\}$ and that (ii) $\sum_{j=0}^{n-1}\lambda_j^{(i)}\cdot x = x\cdot\sum_{j=0}^{n-1}\lambda_j^{(i)} = x\cdot 0 = 0$ for each $i \in \{0,1,\dots,l-1\}$, due to the assumption on $\lambda_j^{(i)}$. □

In order to break such an invariant subspace, in [GØSW22], the authors proposed to apply an invertible linear layer defined via the multiplication with an invertible matrix $M \in \mathbb{F}_q^{n\times n}$ after each $\mathcal{LM}$ round. In such a case, an invariant subspace must be invariant both for the $\mathcal{LM}$ round and for the matrix M as well. By choosing a matrix M that does not admit any invariant subspace (i.e., such that no subspace $\mathfrak{Z} \subseteq \mathbb{F}_q^n$ satisfies $M \times \mathfrak{Z} = \mathfrak{Z}$), then no invariant subspace exists for the overall construction as well. Based on [GRS21, Prop. 12], a matrix in $\mathbb{F}_q^{n\times n}$ does not admit any invariant subspace if its minimal polynomial has (i) maximum degree n and it is (ii) irreducible. For completeness, we point out that it is possible to break the subspace trail of $\mathcal{LM}$ even if (i) the matrix M admits invariant subspaces (e.g., in the case in which the invariant subspaces of M are incompatible with the ones of $\mathcal{LM}$ – see [GØSW22, GRS21] for examples) and/or (ii) the rounds are instantiated by difference matrices. (see e.g. [GSW+21] for more details).

By exploiting a similar approach, it is also possible to defeat other analogous attacks, e.g., it is possible to guarantee that no iterative subspace trail exists (that is, a subspace trail that cyclically repeats itself after $r \geq 2$ rounds). We refer to [GØSW22, GRS21] for more details.

About the Coefficients α_i in Prop. 2. If $l = n-1$ (hence, F depends on all possible linear combinations of the inputs x_i – up to affine equivalence – that are (i) linearly independents and (ii) whose coefficients sum to zero), then the simplest matrix that can break the invariant subspaces of the previous Lai-Massey scheme is a diagonal matrix $M = \mathrm{diag}(\alpha_0,\alpha_1,\dots,\alpha_{n-1}) \in \mathbb{F}_q^{n\times n}$ for which (at least(two entries are different, that is, there exist $i,j \in \{0,1,\dots,n-1\}$ such that $\alpha_i \neq \alpha_j$. This is equivalent to remove the matrix multiplication, and to impose that at least two coefficients α_i, α_j in the Lai-Massey construction proposed in Prop. 2 are different.

About the Solution proposed in [Vau99]. For completeness, in App. B, we briefly discuss the solution proposed in [Vau99] for breaking the invariant subspace trail of the Lai-Massey construction over $\mathbb{F}_q^2$, showing that it is analogous to the one just described for the generic case $\mathbb{F}_q^n$.

4 Relation between Feistel and Lai-Massey Schemes

In this section, we prove that the Lai-Massey scheme over $\mathbb{F}_q^n$ proposed in Prop. 2 is affine equivalent to a generalized Feistel scheme. More formally:

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

In particular, we prove the following.

Theorem 3. *Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n \geq 2$ be an integer. For each $r \geq 1$, r rounds of a Lai-Massey scheme defined as in Prop. 2 are equivalent to r rounds of a generalized Feistel scheme in which no swapping/shuffle takes place (besides an initial and a final linear combination).*

The proof is proposed in the following. We study separately the case $n = 2$ from the one $n \geq 3$. 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 $\mathbb{F}_q^{n \times n}$.

4.1 Initial Remarks

About Invariant Subspaces for the Lai-Massey Scheme. As we already pointed out, a Lai-Massey scheme $\mathcal{LM}$ over $\mathbb{F}_q^n$ defined as in Prop. 2 must be combined with a proper invertible linear layer in order to destroy its invariant subspaces. Assuming Theorem 2 is true, here we point out that the combination of a Lai-Massey scheme and of an invertible linear layer (i.e., $M \circ \mathcal{LM}$ for a proper invertible linear layer M) is still EA-equivalent to a generalized Feistel scheme $\mathcal{F}_{\mathrm{G}}$ defined in Def. 2. Indeed:

$$\mathcal{LM} = B \circ \mathcal{F}_{\mathrm{G}} \circ A + C \qquad \longrightarrow \qquad M \circ \mathcal{LM} = \underbrace{B'}_{:= M \circ B} \circ \mathcal{F}_{\mathrm{G}} \circ A + \underbrace{C'}_{:= M \circ C},$$

where the first equality follows from Theorem 2, and where B' is invertible. For this reason, in the following we limit ourselves to prove Theorem 2 – 3 only for a Lai-Massey scheme $\mathcal{LM}$ over $\mathbb{F}_q^n$ defined as in Prop. 2 and instantiated with $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$.

About "Quasi-Feistel" Schemes. For completeness, we point out that the result proposed in Prop. 2 is not new in the literature. E.g., in [YPL11], Yun et al. introduced the concept of "quasi-Feistel" schemes, a generic class of primitives over finite quasi-groups that includes as special cases both the Feistel ones and the Lai-Massey ones. We recall it in details in App. A.2.

Our proof proposed in the following pointed out the relation between Feistel and Lai-Massey schemes in a much easier and clearer way, by directly showing that they are affine equivalent (without introducing any new function/construction).

4.2 Proof and Considerations for the Case $n = 2$

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

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

and $C = 0$. Indeed,

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

which is the Lai-Massey construction. That is, the Lai-Massey construction is a Feistel construction pre- and post-processed with two invertible linear functions. This obviously implies the result of Prop. 3 for the case $r = 1$.

Let's now define $\mathcal{F}' : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ as the Feistel scheme without the swapping, that is,

$$\mathcal{F}'(x_0, x_1) = [x_0, x_1 + F(x_0)] = \text{circ}(0, 1) \times \mathcal{F}(x_0, x_1)\,.$$

By considering two consecutive rounds of the Lai-Massey construction (analogous for $r \geq 2$ rounds), we get the following

$$\mathcal{LM} \circ \mathcal{LM}(x) = (B \times \mathcal{F} \circ A) \times (B \times \mathcal{F} \circ A) \times x = B' \times \mathcal{F}' \circ \hat{M} \times \mathcal{F}' \circ A \times x\,,$$

where $B' = B \times \text{circ}(0, 1)$ and where

$$\hat{M} \coloneqq A \times (B \times \text{circ}(0, 1))\,.$$

In the Lai-Massey case, we have that

$$\hat{M} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \times \left(\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is the identity matrix. That is, for each $r \geq 2$, *r Lai-Massey rounds are equivalent to r Feistel rounds in which no swapping takes place*, besides an initial and a final linear combination. This implies the existence of an invariant subspace for the Lai-Massey construction (which corresponds to the subspace that does not activate the function F in the Feistel construction $\mathcal{F}'$), as already pointed out in the previous section.

4.3 Proof and Considerations for the Case $n \geq 3$

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

1. the case $l = 1$ in which the function F in the Lai-Massey scheme over $\mathbb{F}_q^n$ as proposed in Prop. 2 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.

4.3.1 1st Case: A-Equivalent to a Type-I Feistel Scheme

Let's start by considering a Lai-Massey scheme over $\mathbb{F}_q^n$ as proposed in Prop. 2 for $l = 1$, that is, $x_i \mapsto y_i = x_i + F\left(\sum_{j=0}^{n-1} \lambda_j \cdot x_j\right)$ for each $i \in \{0, 1, \ldots, n-1\}$, where $F : \mathbb{F}_q \to \mathbb{F}_q$ 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 $\lambda_0 \neq 0$.[4] The analyzed Lai-Massey scheme is affine equivalent to a Type-I Feistel scheme $\mathcal{F}_I$ over $\mathbb{F}_q^n$ defined as $[x_0, x_1, x_2 \ldots, x_{n-1}] \mapsto [x_1 +$

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

$F(x_0), x_2, \ldots, x_{n-1}, x_0]$ via the invertible linear transformations

$$A = \begin{bmatrix} \lambda_0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-1} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & -1 & 1 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & -1 & 0 & \ldots & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & -\frac{\lambda_2}{\lambda_0} & \ldots & -\frac{\lambda_{n-1}}{\lambda_0} & \frac{1}{\lambda_0} \\ 1 & 0 & \ldots & 0 & 0 \\ 1 & 1 & \ldots & 0 & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 1 & 0 & \ldots & 1 & 0 \end{bmatrix}, \tag{3}$$

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

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

As before, r Lai-Massey rounds are equivalent to r Type-I Feistel rounds in which no swapping takes place, besides an initial and a final linear combination. Let's focus on $r \geq 2$ (the case $r = 1$ follows from the previous result immediately). This follows from the fact that

$$\begin{aligned} & A \times (B \times \mathrm{circ}(0, 1, 0, \ldots, 0)) \\ &= \begin{bmatrix} \lambda_0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-1} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & -1 & 1 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & -1 & 0 & \ldots & 1 \end{bmatrix} \times \begin{bmatrix} \frac{1}{\lambda_0} & 1 & -\frac{\lambda_2}{\lambda_0} & \ldots & -\frac{\lambda_{n-1}}{\lambda_0} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 1 & 1 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 1 & 0 & \ldots & 1 \end{bmatrix} = I \end{aligned}$$

is again the identity matrix. This implies the existence of invariant subspaces, as pointed out before.

4.3.2 2nd Case: A-Equivalent to a Contracting Feistel Scheme

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

In order to show that the analyzed Lai-Massey scheme is affine equivalent to a contracting Feistel scheme $\mathcal{F}_C$ defined over $\mathbb{F}_q^n$ as $[x_0, x_1, x_2, \dots, x_{n-1}] = [x_1, x_2, \dots, x_{n-1}, x_0 + F(x_1, x_2, \dots, x_{n-1})]$, we introduce the values $\mu_{i,0}, \dots, \mu_{i,n-2} \in \mathbb{F}_q$ for each $i \in \{1, \dots, n-1\}$ defined as the ones that satisfy the following equality:

$$\forall i \in \{1, \dots, n-1\} : \quad \begin{bmatrix} \lambda_0^{(0)} & \lambda_0^{(1)} & \dots & \lambda_0^{(n-2)} \\ \lambda_1^{(0)} & \lambda_1^{(1)} & \dots & \lambda_1^{(n-2)} \\ \vdots & & \ddots & \vdots \\ \lambda_{n-1}^{(0)} & \lambda_{n-1}^{(1)} & \dots & \lambda_{n-1}^{(n-2)} \end{bmatrix} \times \begin{bmatrix} \mu_{i,0} \\ \mu_{i,1} \\ \vdots \\ \mu_{i,n-2} \end{bmatrix} = \begin{bmatrix} -1 \\ \delta_{i,1} \\ \vdots \\ \delta_{i,n-2} \\ \delta_{i,n-1} \end{bmatrix}, \quad (4)$$

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

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

where the l.h.s. matrix is invertible due to the fact that the vectors $\hat{\lambda}^{(0)}, \hat{\lambda}^{(1)}, \dots, \hat{\lambda}^{(n-2)}$ 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 scheme $\mathcal{F}_C$ defined over $\mathbb{F}_q^n$ via the invertible linear transformations

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

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

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

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

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

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

Not surprisingly, r Lai-Massey rounds are equivalent to r contracting Feistel rounds in which no swapping takes place, besides an initial and a final linear combination. As proved in App. C, for $r \geq 2$, this follows from the fact that

$$A \times (B \times \mathrm{circ}(0, 1, 0, \ldots, 0)) = I\,.$$

(This also implies that both A and B are invertible, since $\det(A \times (B \times \mathrm{circ}(0, 1, 0, \ldots, 0))) = \det(I) = 1$ implies that $\det(A) \cdot \det(B) \neq 0$, and so $\det(A), \det(B) \neq 0$.) As before, invariant subspaces exist for the Lai-Massey scheme.

5 New Generalizations of the Lai-Massey Construction

As next step, we discuss possible generalization of the Lai-Massey construction. Our goal is to set up a scheme that (i) captures the main idea of the Lai-Massey construction, and that (ii) it is not EA-equivalent to any Feistel scheme. (In the following, we denote the "EA-equivalence class" (or"EA-class" for brevity) of generalized Feistel schemes as "Feistel EA-class".)

Let's start by recalling the generalization proposed in [RS22].[5]

Proposition 3 (Def. 12, [RS22]). *Let $n \geq 3$ be an integer, and let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$. Let $2 \leq m \leq n-1$, and let $1 \leq l \leq m-1$. For each $i \in \{0, 1, \ldots, l-1\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{m-1}^{(i)} \in \mathbb{F}_q$ be as in Prop. 2 (in particular, such that $\sum_{j=0}^{m-1} \lambda_j^{(i)} = 0$). Let $F : \mathbb{F}_q^{l+n-m} \to \mathbb{F}_q$ be any function.*

The Feistel+Lai-Massey function $\mathcal{FLM}$ over $\mathbb{F}_q^n$ defined as $\mathcal{FLM}(x_0, x_1, \ldots, x_{n-1}) \coloneqq y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i = \begin{cases} x_i + F\left(\sum_{j=0}^{m-1} \lambda_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{m-1} \lambda_j^{(l-1)} \cdot x_j, x_m, \ldots, x_{n-1}\right) & \text{if } i \in \{0, \ldots, m-1\}\,, \\ x_i & \text{otherwise} \end{cases}$$

is invertible.

[5] To be precise, the result proposed in Prop. 3 is not completely equal to the one proposed by Roy and Steiner in [RS22]. In particular, the following differences hold:

- in [RS22], l is fixed and equal to 1, that is, the function F depends on a single combination of the first m inputs, and on the remaining $n - m$ inputs;
- invertible S-Boxes S_i over $\mathbb{F}_q$ are applied on each input i, that is, each x_i in Prop. 3 is actually $S_i(x_i)$ in [RS22, Def. 12]. Since this corresponds to apply a S-Box layer before the Feistel+Lai-Massey scheme, we decided to omit it for simplicity;
- finally, such scheme is presented as "generalized Lai-Massey" in [RS22]. However, it combines both the Feistel and the Lai-Massey scheme. For this reason, we think that the nomenclature "Feistel+Lai-Massey" scheme highlights in a better way its main feature.

Note that the function F behaves as the Lai-Massey scheme defined in Prop. 2 for the first l inputs, while it corresponds to a (generalized) Feistel scheme defined as in Def. 2 for the last $n-m$ inputs. The invertibility follows immediately (without assumptions on F).

Even if such scheme generalized the Lai-Massey one by combining it with the Feistel one, it is (obviously) EA-equivalent to a Feistel scheme due to the results proposed in the previous section. For this reason, in the following we propose and discuss two new possible generalizations in order to reach our goal.The starting point is the result proposed in Prop. 2.

5.1 Generalized and Redundant Lai-Massey Schemes

5.1.1 Generalized Lai-Massey Scheme

One main feature of the Lai-Massey scheme proposed in Prop. 2 regards the fact that the inputs of the function F are linear combinations of the inputs x_i defined via coefficients $\lambda_i^{(j)}$ that sum to zero (that is, $\sum_{i=0}^{n-1} \lambda_i^{(j)} = 0$ for each $j \in \{0, 1, \dots, l-1\}$). A possible generalization of such result could consist in allowing for different functions $F_0, F_1, \dots, F_{n-1}$, under the restriction that their inputs are linear combinations of x_i as before.

More formally:

Definition 6 (Generalized Lai-Massey)**.** Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n \geq 2$ be an integer. Let $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Let $l \in \{1, 2, \dots, n-1\}$. For each $i \in \{0, 1, \dots, l-1\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \dots, \lambda_{n-1}^{(i)} \in \mathbb{F}_q$ be as in Prop. 2 (in particular, such that $\sum_{j=0}^{m-1} \lambda_j^{(i)} = 0$). Given n function $F^{(0)}, F^{(1)}, \dots, F^{(n-1)} : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$, let $\mathcal{LM}_{\mathrm{G}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be defined as $\mathcal{LM}_{\mathrm{G}}(x_0, x_1, \dots, x_{n-1}) = y_0 \| y_1 \| y_2 \| \dots \| y_{n-1}$ where

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

We say that $\mathcal{LM}_{\mathrm{G}}$ is a generalized Lai-Massey construction *if* it is invertible.

Obviously, the Lai-Massey scheme defined in Prop. 2 satisfies this definition.

Keeping in mind the generalized Feistel schemes proposed in the literature and recalled in App. A.1, examples of generalized Lai-Massey constructions over $\mathbb{F}_q^4$ (analogous over $\mathbb{F}_q^n$ for $n \geq 2$) include e.g. Type-I Lai-Massey schemes

$$[x_0, x_1, x_2, x_3] \mapsto [x_0 + F(x_0 - x_1), x_1 + F(x_0 - x_1), x_2, x_3]$$

and Type-II Lai-Massey schemes

$$[x_0, x_1, x_2, x_3] \mapsto [x_0 + F(x_0 - x_1), x_1 + F(x_0 - x_1), x_2 + F'(x_2 - x_3), x_3 + F'(x_2 - x_3)]$$

where $F, F' : \mathbb{F}_q \to \mathbb{F}_q$. Due to the results proposed before, it is trivial to check that such two constructions are invertible, and that they are A-equivalent to a generalized Feistel scheme defined over $\mathbb{F}_q^4$. We point out that the two previous generalized Lai-Massey round functions must be combined with a mixing layer (as a shuffle or a multiplication with an invertible matrix) in order to get full diffusion after a certain number of iterations.

Another example is given by

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} \mapsto \begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix} = \text{GLM-1}_3(x) = \begin{bmatrix} \alpha_0 \cdot (x_0 + F_1(x_0 - x_1) + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2)) \\ \alpha_1 \cdot (x_1 + F_1(x_0 - x_1) + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2)) \\ \alpha_2 \cdot (x_2 + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2)) \end{bmatrix}$$

where $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{F}_q \setminus \{0\}$, and where $F_i : \mathbb{F}_q^i \to \mathbb{F}_q$ for each $i \in \{1, 2\}$. The invertibility follows from the fact that

$$x_0 - x_1 = \frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1},$$
$$x_0 + x_1 - 2 \cdot x_2 = \frac{y_0}{\alpha_0} + \frac{y_1}{\alpha_1} - 2 \cdot \frac{y_2}{\alpha_2} - 2 \cdot F_1(x_0 - x_1) = \frac{y_0}{\alpha_0} + \frac{y_1}{\alpha_1} - 2 \cdot \frac{y_2}{\alpha_2} - 2 \cdot F_1\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}\right).$$

Also such scheme is EA-equivalent to a generalized Feistel scheme over $\mathbb{F}_q^3$, that is, there exist invertible linear layers A, B and a linear layer C over $\mathbb{F}_q^3$ such that

$$\text{GLM-1}_3(x) = B \circ \mathcal{F}_{\text{G}} \circ A(x) + C(x)$$

where $\mathcal{F}_{\text{G}}$ is defined in Def. 2. The linear layer $A, B, C \in \mathbb{F}_q^{3\times 3}$ are given by

$$A = \begin{bmatrix} 1 & -1 & 0 \\ 1 & 1 & -2 \\ 1 & 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} \alpha_0 & \alpha_0 & 1 \\ \alpha_1 & \alpha_1 & 0 \\ 0 & \alpha_2 & 0 \end{bmatrix}, \qquad C = \begin{bmatrix} -2 \cdot \alpha_0 & 0 & 2 \cdot \alpha_0 \\ -2 \cdot \alpha_1 & 0 & 2 \cdot \alpha_1 \\ -\alpha_2 & \alpha_2 & 0 \end{bmatrix}.$$

Indeed:

$$\begin{aligned}
\text{GLM-1}_3(x) = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} &\xrightarrow{A\times\cdot} \begin{bmatrix} x_0 - x_1 \\ x_0 + x_1 - 2 \cdot x_2 \\ x_0 \end{bmatrix} \xrightarrow{\mathcal{F}_{\text{G}}(\cdot)} \begin{bmatrix} x_0 + x_1 - 2 \cdot x_2 + F_1(x_0 - x_1) \\ x_0 + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2) \\ x_0 - x_1 \end{bmatrix} \xrightarrow{B\times\cdot} \\
&\begin{bmatrix} \alpha_0 \cdot (3 \cdot x_0 - 2 \cdot x_2 + F_1(x_0 - x_1) + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2) \\ \alpha_1 \cdot (2 \cdot x_0 + x_1 - 2 \cdot x_2 + F_1(x_0 - x_1) + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2)) \\ \alpha_2 \cdot (x_0 + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2)) \end{bmatrix} \xrightarrow{+C\times x} \\
&\begin{bmatrix} \alpha_0 \cdot (x_0 + F_1(x_0 - x_1) + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2) \\ \alpha_1 \cdot (x_1 + F_1(x_0 - x_1) + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2)) \\ \alpha_2 \cdot (x_2 + F_2(x_0 - x_1, x_0 + x_1 - 2 \cdot x_2)) \end{bmatrix}.
\end{aligned}$$

5.1.2 Redundant Lai-Massey Schemes

Focusing on the result proposed in Prop. 2, another main feature of such Lai-Massey construction $[x_0, x_1, \ldots, x_{n-1}] \mapsto [y_0, y_1, \ldots, y_{n-1}]$ regards the fact that the differences of two outputs $y_i - y_j$ are always equal to the differences of two inputs $x_h - x_l$ for each $i, j, h, l \in \{0, 1, \ldots, n-1\}$ with $i \neq j$ and $h \neq l$, that is, $y_i - y_j = x_h - x_l$ (where the condition $(i, j) = (h, l)$ is *not* required). This is a consequence of the fact that each output y_i is defined as the sum of the corresponding input x_i and of a certain element $z = F(x_0, x_1, \ldots, x_{n-1})$, that is, $y_i = x_i + z$ where z is fixed for each $i \in \{0, 1, \ldots, n-1\}$.

Here, we propose the following definition that aims to generalize the Lai-Massey construction by capturing the observation just pointed out.

Definition 7 (Redundant Lai-Massey)**.** Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, 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 $F : \mathbb{F}_q^n \to \mathbb{F}_q$, let $\mathcal{LM}_{\text{R}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be defined as $\mathcal{LM}_{\text{R}}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| y_2 \| \ldots \| y_{n-1}$ where

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

We say that $\mathcal{LM}_{\text{R}}$ is a redundant[6] Lai-Massey construction *if* it is invertible.

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

Obviously, the Lai-Massey scheme defined in Prop. 2 satisfies this definition. At the same time, there exist redundant Lai-Massey constructions that are not of the same form given in Prop. 2 (where the function F only takes as inputs linear combinations of $x_0, x_1, \dots, x_{n-1}$ so that the sum of the coefficients that define the linear combination is zero), as the one given in the next example.

Lemma 3 (RLM-0)**.** *Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n \geq 2$ be an integer. Let $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Let $\mu_0, \mu_1, \dots, \mu_{n-1} \in \mathbb{F}_q$ be such that $\sum_{i=0}^{n-1} \mu_i \neq 0$. Let $H : \mathbb{F}_q \to \mathbb{F}_q$ be a permutation.*

The redundant Lai-Massey scheme RLM-0$(x_0, x_1, \dots, x_{n-1}) = y_0 \| y_1 \| \dots \| y_{n-1}$ over $\mathbb{F}_q^n$ defined as

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

is invertible.

Proof. By simple computation:

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

since H is invertible. Hence:

$$\forall i \in \{0, 1, \dots, n-1\} : \qquad x_i = \frac{y_i}{\alpha_i} + \frac{H^{-1}\left(\sum_{j=0}^{n-1} \mu_j \cdot y_j/\alpha_j \right)}{\sum_{j=0}^{n-1} \mu_j} - \frac{\sum_{j=0}^{n-1} \mu_j \cdot y_j/\alpha_j}{\sum_{j=0}^{n-1} \mu_j} . \quad \square$$

The proposed scheme is EA-equivalent to a contracting Feistel scheme, due to the same argument proposed in Sect. 4.3. In particular, assuming $\mu_0 \neq 0$ and $\alpha_0 = \alpha_1 = \dots = \alpha_{n-1} = 1$ (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 (3), while the linear transformation C is defined via the matrix $C \in \mathbb{F}_q^{n \times n}$ identically equal to zero except for $C_{0,1} = -(\sum_{j=0}^{n-1} \mu_j)/\mu_0$.

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

As next step, we propose a concrete example of a generalized Lai-Massey scheme over $\mathbb{F}_q^n$ that is *not* EA-equivalent to any generalized Feistel scheme. We construct such scheme iteratively, that is:

1. we first propose it over $\mathbb{F}_q^4$ in Prop. 4;

2. given the scheme over $\mathbb{F}_q^n$ for n *even*, we construct it over $\mathbb{F}_q^{n+2}$ in Prop. 5 and over $\mathbb{F}_q^{n+1}$ in Prop. 6.

Proposition 4 (GLM-1_4)**.** *Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer. Let $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q \setminus \{0\}$. For each $i \in \{1, 2, 3\}$, let $F_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be a function.*

The generalized Lai-Massey construction GLM-$1_4(x_0, x_1, x_2, x_3) = y_0 \| y_1 \| y_2 \| y_3$ over $\mathbb{F}_q^4$ defined as

$$\begin{aligned}
y_0 &\coloneqq \alpha_0 \cdot (x_0 + F_1(x_0 - x_1) + F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \,, \\
y_1 &\coloneqq \alpha_1 \cdot (x_1 + F_1(x_0 - x_1) + F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \,, \\
y_2 &\coloneqq \alpha_2 \cdot (x_2 + F_2(x_0 - x_1, x_2 - x_3) + F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \,, \\
y_3 &\coloneqq \alpha_3 \cdot (x_3 + F_2(x_0 - x_1, x_2 - x_3) + F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \,;
\end{aligned}$$

is invertible.

Proof. The invertibility follows from the following

$$\begin{aligned}
x_0 - x_1 &= \frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1} \,, \\
x_2 - x_3 &= \frac{y_2}{\alpha_2} - \frac{y_3}{\alpha_3} \,, \\
x_1 - x_2 &= \frac{y_1}{\alpha_1} - \frac{y_2}{\alpha_2} - F_1\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}\right) - F_2\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}, \frac{y_2}{\alpha_2} - \frac{y_3}{\alpha_3}\right) \,.
\end{aligned}$$

By making use of the same strategy exploited for the Lai-Massey scheme e.g. in Prop. 2, these information are sufficient for recovering x_0, x_1, x_2, x_3. E.g.,

$$x_0 = \frac{y_0}{\alpha_0} - F_1\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}\right) - F_3\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}, \frac{y_2}{\alpha_2} - \frac{y_3}{\alpha_3}, \frac{y_1}{\alpha_1} - \frac{y_2}{\alpha_2} - F_1\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}\right) - F_2\left(\frac{y_0}{\alpha_0} - \frac{y_1}{\alpha_1}, \frac{y_2}{\alpha_2} - \frac{y_3}{\alpha_3}\right)\right) \,.$$

□

Proposition 5 (GLM-1_n)**.** *Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n = 2 \cdot n' \geq 6$ be an even integer. 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 $F_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be a function.*

The generalized Lai-Massey construction GLM-$1_n(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ over $\mathbb{F}_q^n$ defined as

$$y_i \coloneqq \begin{cases} z_i + \alpha_i \cdot F_{n-1}\left(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w_{n-2}\right) & \text{if } i \in \{0, 1, \ldots, n-3\} \,, \\ \alpha_i \cdot \big(x_i + F_{n-2}(w_0, w_1, \ldots, w_{n-4}, w_{n-2}) & \text{otherwise } (i \in \{n-2, n-1\}) \\ \qquad + F_{n-1}(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w_{n-2})\big) & \end{cases}$$

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

- $[z_0, z_1, \ldots, z_{n-3}] \coloneqq$ *GLM-$1_{n-2}(x_0, x_1, \ldots, x_{n-3})$ is the output of the generalized Lai-Massey construction GLM-1_{n-2} over $\mathbb{F}_q^{n-2}$, and*
- *for each $i \in \{0, 1, \ldots, n-1\}$: $w_i \coloneqq x_i - x_{i+1}$,*

is invertible.

Proof. We prove the invertibility by working iteratively, keeping in mind that GLM-1_4 is invertible. Let's assume that GLM-1_{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 $F_{n-1}(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w_{n-2})$ in such a way that the difference $\frac{y_i}{\alpha_i} - \frac{y_j}{\alpha_j}$ is independent of $F_{n-1}(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w_{n-2})$ – note that z_i is a multiple of 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:

$$x_{n-2} - x_{n-1} = \frac{y_{n-2}}{\alpha_{n-2}} - \frac{y_{n-1}}{\alpha_{n-1}},$$
$$x_{n-3} - x_{n-2} = \frac{y_{n-3}}{\alpha_{n-3}} - \frac{y_{n-2}}{\alpha_{n-2}} - \sum_{i=1}^{n-3} F_i(w_0, w_1, \ldots, w_{i-1}) - F_{n-2}(w_0, w_1, \ldots, w_{n-4}, w_{n-2}),$$

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 $x_0, x_1, \ldots, x_{n-1}$. □

Proposition 6 (GLM-2_n)**.** *Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n = 2 \cdot n' + 1 \geq 5$ be an odd integer. 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 $F_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be a function. Let $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in \mathbb{F}_q$ be such that $\sum_{i=0}^{n-1} \lambda_i = 0$.*

The generalized Lai-Massey construction GLM-$2_n(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ over $\mathbb{F}_q^n$ defined as

$$y_i \coloneqq \begin{cases} z_i + \alpha_i \cdot F_{n-1}\left(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w'_{n-2}\right) & \text{if } i \in \{0, 1, \ldots, n-2\}, \\ \alpha_i \cdot \left(x_i + F_{n-1}\left(w_0, w_1, \ldots, w_{n-4}, w_{n-3}, w'_{n-2}\right)\right) & \text{otherwise } (i = n-1) \end{cases}$$

where

- $[z_0, z_1, \ldots, z_{n-2}] \coloneqq$ GLM-$1_{n-1}(x_0, x_1, \ldots, x_{n-2})$ *is the output of the generalized Lai-Massey construction GLM-1_{n-1} over $\mathbb{F}_q^{n-1}$ defined as in Prop. 4 – 5;*
- $w_i \coloneqq x_i - x_{i+1}$ *if $i \in \{0, 1, \ldots, n-2\}$, and $w'_{n-2} \coloneqq \sum_{i=0}^{n-1} \lambda_i \cdot x_i$;*

is invertible.

The proof is equivalent to the one given for the even case.

About Invariant Subspaces. As before, each input in the subspace $\langle [1, 1, \ldots, 1] \rangle \equiv \{[x, x, \ldots, x] \mid \forall x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ does not active any function F_i of the generalized Lai-Massey schemes defined in Prop. 4 – 5 – Prop. 6, since their inputs are just zero. Such subspace can be broken by imposing that at least two coefficients α_i and α_j for $i, j \in \{0, 1, \ldots, n-1\}$ are different.

About the EA-Equivalence. Next, we show that the generalized Lai-Massey schemes defined in Prop. 4 – 5 – 6 are not equivalent to any generalized Feistel scheme.

Theorem 4. *Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n \geq 4$. The generalized Lai-Massey constructions GLM-1_n and GLM-2_n proposed in Prop. 4 – 5 – 6 are **not** extended affine equivalent to any generalized Feistel scheme.*

Proof. Let's start to analyze 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

$$\text{GLM-}1_4(x) = B \circ \mathcal{F}_{\text{G}} \circ A(x) + C(x)$$

where $\mathcal{F}_{\mathrm{G}}$ is defined in Def. 2. Let's first consider the case in which A, B, C are linear. Since GLM-1_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 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

$$\mathcal{F}_{\mathrm{G}} \circ A(x) = \begin{bmatrix} x_2 - x_3 + F_1(x_0 - x_1) \\ x_1 - x_2 + F_2(x_0 - x_1, x_2 - x_3) \\ \psi_0 \cdot x_0 + \psi_1 \cdot x_1 + \psi_2 \cdot x_2 + \psi_3 \cdot x_3 + F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3) \\ x_0 - x_1 \end{bmatrix}.$$

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

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

for $\varphi_0, \varphi_1, \ldots, \varphi_6 \in \mathbb{F}_q$. This is due to the distribution of the functions F_i in GLM-$1^{(4)}$:

$$B \circ \mathcal{F}_{\mathrm{G}} \circ A(x) = \begin{bmatrix} L^{(0)}(x_0, x_1, x_2, x_3) + \alpha_0 \cdot (\varphi_0 \cdot F_1(x_0 - x_1) + \varphi_2 \cdot F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \\ L^{(1)}(x_0, x_1, x_2, x_3) + \alpha_1 \cdot (\varphi_0 \cdot F_1(x_0 - x_1) + \varphi_2 \cdot F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \\ L^{(2)}(x_0, x_1, x_2, x_3) + \alpha_2 \cdot (\varphi_1 \cdot F_2(x_0 - x_1, x_2 - x_3) + \varphi_2 \cdot F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \\ L^{(3)}(x_0, x_1, x_2, x_3) + \alpha_3 \cdot (\varphi_1 \cdot F_2(x_0 - x_1, x_2 - x_3) + \varphi_2 \cdot F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \end{bmatrix},$$

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, due to a linear dependence that holds between the first three columns:

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

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

$$B^{(4)} = \begin{bmatrix} \alpha_0 \cdot \varphi_0 & 0 & \alpha_0 \cdot \varphi_2 \\ \alpha_1 \cdot \varphi_0 & 0 & \alpha_1 \cdot \varphi_2 \\ 0 & \alpha_3 \cdot \varphi_1 & \alpha_2 \cdot \varphi_2 \\ 0 & \alpha_3 \cdot \varphi_1 & \alpha_3 \cdot \varphi_2 \end{bmatrix} \in \mathbb{F}_q^{4 \times 3}\,.$$

For each $n = 2 \cdot n' \geq 6$, we define $B^{(n)} \in \mathbb{F}_q^{n \times (n-1)}$ as

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

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. Given $B^{(n)}$, $B \in \mathbb{F}_q^{n\times n}$ is defined as

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

in order to realize the EA-equivalent with the generalized Feistel scheme. As before, B is never invertible since the columns of $B^{(n)}$ are linearly dependent.

Finally, an analogous proof holds for the case $n = 2 \cdot n' + 1 \geq 5$ odd. As before, it is possible to construct an invertible matrix $A \in \mathbb{F}_q^{n\times n}$ that returns both $\sum_{i=0}^{n-1} \lambda_i \cdot x_i$ and all differences $x_i - x_{i+1}$ for each $i \in \{0, 1, \ldots, n-3\}$. Given $B^{(n-1)} \in \mathbb{F}_q^{(n-1)\times(n-2)}$ as before (note that $n-1$ is even), $B \in \mathbb{F}_q^{n\times n}$ is defined as

$$B = \left[\begin{array}{ccccc|cc} & & & & & \alpha_0 \cdot \varphi_{n-2} & \varphi_{n-1} \\ & & & & & \alpha_1 \varphi_{n-2} & \varphi_n \\ & & B^{(n-1)} & & & \vdots & \vdots \\ & & & & & \alpha_{n-3} \cdot \varphi_{n-2} & \varphi_{2n-3} \\ & & & & & \alpha_{n-2} \cdot \varphi_{n-2} & \varphi_{2n-2} \\ \hline 0 & 0 & \cdots & 0 & 0 & \alpha_{n-1} \cdot \varphi_{n-2} & \varphi_{2n-1} \end{array}\right]$$

in order to realize the EA-equivalent with the Feistel scheme. As before, B is never invertible since the columns of $B^{(n-1)}$ are linearly dependent. □

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

Next, we propose an example of a redundant Lai-Massey construction that is *not* EA-equivalent to any generalized Feistel scheme published in the literature so far. We achieve this result by imposing that one of the n inputs of the function F depends on a linear combination whose coefficients do not necessarily sum to zero. Another analogous example is proposed in App. D.2.

Proposition 7 (RLM-1)**.** *Let $p \geq 3$ be a prime integer, and let $n \geq 2$. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Let $l \in \{1, 2, \ldots, n-1\}$. For each $i \in \{0, 1, \ldots, l-1\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)} \in \mathbb{F}_q$ be as in Prop. 2 (in particular, such that $\sum_{j=0}^{m-1} \lambda_j^{(i)} = 0$). Let $\psi_0, \psi_1, \ldots, \psi_{n-1} \in \mathbb{F}_p$ (**no** condition on $\sum_{j=0}^{n-1} \psi_j$). Let $G : \mathbb{F}_p^{n-1} \to \mathbb{F}_p$ be any function. Let $\beta \in \mathbb{F}_p \setminus \{0\}$ be such that*

$$L_p\left(-\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j\right)\right) = -1\,.$$

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

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

and where

$$z \coloneqq G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot x_j\right)$$

is invertible.

We point out that, if $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$, then the vector $[\psi_0, \psi_1, \ldots, \psi_{n-1}] \in \mathbb{F}_p^n$ and the vectors $[\lambda_0^{(0)}, \lambda_1^{(0)}, \ldots, \lambda_{n-1}^{(0)}], \ldots, [\lambda_0^{(l-1)}, \lambda_1^{(l-1)}, \ldots, \lambda_{n-1}^{(l-1)}] \in \mathbb{F}_p^n$ are linearly independent. Otherwise, if the sum is equal to zero, they are linearly dependent.

Proof. If $\sum_{j=0}^{n-1} \psi_j = 0 \mod p$, then the invertibility follows from Prop. 2. Hence, let's assume $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$. 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

$$z = G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot \frac{y_j}{\alpha_j}, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot \frac{y_j}{\alpha_j}, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot \frac{y_j}{\alpha_j} \right).$$

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

$$\begin{aligned} \sum_{j=0}^{n-1} \psi_j \cdot \frac{y_j}{\alpha_j} &= \sum_{j=0}^{n-1} \psi_j \cdot \left(x_j + \beta \cdot z^2 \cdot \left(\sum_{l=0}^{n-1} \psi_l \cdot x_l \right) \right) \\ &= \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j \right) + \beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \right) \cdot \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j \right) \\ &= \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j \right) \cdot \left(1 + \beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \right) \right). \end{aligned}$$

Such equality is invertible if

$$\forall z \in \mathbb{F}_p : \qquad 1 \neq -\beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \right).$$

Such condition is always satisfied for each $z \in \mathbb{F}_p$ by choosing $\beta \neq 0$ such that

$$L_p\left(-\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j \right) \right) = -1 .$$

In such a way, one term of the equality is a quadratic residue (that is, $L_p(1) = 1$), while the other one is a quadratic non-residue (that is, $L_p\left(-\beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j\right)\right) = L_p(z^2) \cdot L_p\left(-\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j\right)\right) = L_p\left(-\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j\right)\right) = -1$ by definition of β).

As a result, for each $i \in \{0, 1, \ldots, n-1\}$:

$$x_i = \frac{y_i}{\alpha_i} - \frac{\beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \cdot y_j/\alpha_j \right)}{1 + \beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \right)} . \qquad \square$$

About Invariant Subspaces. As before, the inputs in the subspace $\langle [1,1,\ldots,1] \rangle \equiv \{[x,x,\ldots,x] \mid \forall x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ do not active any non-linear function, since:

$$\forall i \in \{0,1,\ldots,n-1\}: \qquad y_i = \alpha_i \cdot \Bigg(\underbrace{1 + \beta \cdot (G(0,0,\ldots,0))^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \right)}_{\neq 0 \text{ (constant)}} \Bigg) \cdot x \,,$$

where $-\beta \cdot (G(0,0,\ldots,0))^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j\right) \neq 1$ since $L_p\left(-\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j\right)\right) = -1$. Such subspace can be easily broken by imposing that at least two coefficients α_i and α_j for $i,j \in \{0,1,\ldots,n-1\}$ are different.

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

Theorem 5. *Let $p \geq 3$ be a prime integer, and let $n \geq 2$. The redundant Lai-Massey scheme defined in Prop. 7 for which*

- $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$
- $l = n-1$ *(that is, G depends on $n-1$ non-trivial inputs[7])*

is not EA-equivalent to any generalized Feistel scheme.

Proof. The proof follows from the fact that

- the functions F_i in any generalized Feistel scheme as in Def. 2 depend on at most $i \leq n-1$ independent inputs;
- the function $F(x_0,\ldots,x_{n-1}) := \beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j\right)$ in Prop. 7 (where $z := G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\right)$) depend on n independent inputs.

As a result, the equivalence

$$\forall x \in \mathbb{F}_p^n: \qquad \text{RLM-1}(x) = B \circ \mathcal{F}_{\text{G}} \circ A(x) + C(x)$$

is never realized for any invertible affine layer A, B and for any affine layer C. □

As a concrete example, we prove this fact in details for the case $\mathbb{F}_p^2$ in App. D.1.

6 The Blooming of the `Amaryllises` Scheme

In this section, we discuss the advantages and the disadvantages of the possible invertible non-linear functions over $\mathbb{F}_q^n$ proposed in the literature, focusing on the special case in which q is of huge size (e.g., $q \geq 2^{64}$). We point out that this is not only of theoretical interest, since the size q of the field $\mathbb{F}_q^n$ considered in many recent applications/protocols like MPC/FHE/ZK is of that size. Based on such analyse, we propose a new invertible non-linear function – called `Amaryllises` – which aims to combine the advantages of the different constructions proposed in the literature so far.

[7] The "trivial inputs" case occurs either if $\gamma_0^{(j)} = \gamma_1^{(j)} = \ldots = \gamma_{n-1}^{(j)} = 0$ for a certain $j \in \{0,1,\ldots,n-2\}$ or if the vectors $[\lambda_0^{(0)}, \lambda_1^{(0)}, \ldots, \lambda_{n-1}^{(0)}], \ldots, [\lambda_0^{(n-2)}, \lambda_1^{(n-2)}, \ldots, \lambda_{n-1}^{(n-2)}] \in \mathbb{F}_p^n$ are linearly independent.

6.1 Invertible Non-Linear Functions over $\mathbb{F}_q^n$

Several strategies are possible in order to construct invertible non-linear functions over $\mathbb{F}_q^n$(we refer to [Gra22] for an analysis of schemes instantiated with *non-invertible* non-linear functions). The following analysis does not aim to be exhaustive. Rather, our goal is to study the advantages and the disadvantages of some of the most common invertible non-linear functions over $\mathbb{F}_q^n$ proposed in the literature. For this reason, we focus on the following cases: (1st) SPN (parallel S-Boxes), (2nd) Feistel/Lai-Massey schemes, and (3rd) `Horst` schemes.

6.1.1 SPN (Parallel S-Boxes)

Let $S^{(0)}, S^{(1)}, \ldots, S^{(n-1)} : \mathbb{F}_q \to \mathbb{F}_q$ be n invertible non-linear functions. In the case of SPN schemes, the non-linear layer over $\mathbb{F}_q^n$ is simply defined as

$$[x_0, x_1, \ldots, x_{n-1}] \mapsto [S^{(0)}(x_0), S^{(1)}(x_1), \ldots, S^{(n-1)}(x_{n-1})] .$$

Obviously, such layer is invertible if and only if each S-Box $S^{(i)}$ is invertible. This restricts the possible range of options for the function $S^{(i)}$ itself. In the case in which q is relatively small (e.g., $q \leq 2^8$), a designer can potentially brute force many possible invertible S-Boxes until one with the desired statistical and algebraic properties is found (see [LP07] for the case $q = 2^4$). This is obviously not possible when q is very large, as e.g. $q \geq 2^{64}$. In such a case, the S-Box must also have a very simple algebraic structure, since it must be computed on the fly (due to the huge size of q, the S-Box cannot be pre-computed and stored as a look-up table). At the current state of the art, only few functions are known to be invertible over $\mathbb{F}_q$ for a generic q, including the power maps $x \mapsto x^d$ and the Dickson polynomials (recalled in Theorem 7). E.g., most of the MPC-/FHE-/ZK-friendly schemes as MiMC [AGR+16], HadesMiMC/Poseidon [GLR+20, GKR+21], *Rescue* [AAB+20], Neptune [GOPS22], Griffin [GHR+22], Hydra [GØSW22], Anemoi [BBC+22] are instantiated with power maps.

Disadvantageous: Importance of the Linear Layer & Cost of Decryption. Obviously, no mixing takes place among the variables. Hence, the details of the affine layer are crucial in order to reach full diffusion after a finite number of rounds.

In order to decrypt a SPN scheme, one has to compute the inverse of each S-Box $S^{(i)}$ (let's assume for simplicity that $S \equiv S^{(0)} = S^{(1)} = \ldots = S^{(n-1)}$). In the case in which $\deg(S^{-1}) \gg \deg(S)$, computing the inverse of a SPN scheme could be much more *expensive* than computing it. E.g., consider the case in which the S-Box is instantiated by a power map $S(x) = x^d$. The inverse of $x \mapsto x^d$ is $S^{-1}(x) = x^{1/d} \equiv x^{\hat{d}}$ 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 in which $q \gg d$, then $\hat{d}$ is of the same order of q. Similarly, the inverse of the degree-d Dickson polynomial $\mathcal{D}_{d,\alpha}(x)$ has degree $\hat{d}$ where $\hat{d} \cdot d = 1 \mod (q^2 - 1)$.

Advantageous: Frustrating Meet-in-the-Middle Algebraic Attacks. Having said that, computing the inverse of a construction is not required in many applications. Just to give some concrete examples:

- stream ciphers instantiated via a cipher $E_k(\cdot)$ used in a mode of operation as the counter-mode, that is, $x \mapsto x + E_k(N)$ for a nonce N and a key k. In such a case, both the encryption and the decryption require the computation of $E_k(\cdot)$ only (never its inverse). As a concrete example, this is exactly what MiMC's and HadesMiMC's designers [AGR+16, GLR+20] proposed for their schemes: "*[...] decryption is much more expensive than encryption. Using modes where the inverse is not needed is thus advisable.*" (see [AGR+16, Sect. 1]);

- sponge hash functions [BDPA08] instantiated with permutations (in order to avoid internal collisions). In such a case, no inverse computation of the permutation is performed for computing the hash value. Same consideration holds for the Farfalle and for the MEGAFONO modes of operation [BDH+17, GØSW22] instantiated with permutations.

As a result, the fact that computing the inverse is more expensive than computing it in the forward direction does not represent a disadvantage in many practical use cases.

Moreover, the previous disadvantageous about the cost of the inverse turns out to be an advantage in the case in which one aims to frustrate Meet-in-the-Middle (MitM) algebraic attacks. In such a case, the attack exploits the low degree of the inverse of the attacked scheme in order to break it. However, in the case in which such inverse is of high (close to maximum) degree, attack approaches such as the interpolation one [JK97] or the higher-order differential one [Knu94] would be defeated after few rounds.

6.1.2 Feistel and Lai-Massey Schemes

Since Feistel and Lai-Massey schemes have been already discussed in this paper, we directly focus on their advantages and disadvantageous.

Advantageous: Non-Linear Mixing & More Freedom for the Designer & Cost of Decryption. One of the main differences between Feistel/Lai-Massey schemes and SPN scheme regards the fact that a non-linear mixing takes place in the first case. Hence, several rounds of Feistel/Lai-Massey schemes are potentially sufficient by themselves for reaching full diffusion without any additional linear layer.

The other main feature of (generalized) Feistel and Lai-Massey schemes regards the fact that their invertibility is generally independent of the details of the functions that instantiate them.[8] As a direct consequence, the number of possible choices for such functions is much larger than the corresponding number for SPN schemes. This could represent a significant advantage for Feistel and Lai-Massey schemes, 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.

As a direct consequence of the previous fact, both in the Feistel and in the Lai-Massey case, the same functions are computed both in the forward/encryption direction and in the backward/decryption direction (note that such functions are not invertible in general), which implies the *same cost in term of number of function evaluations* for the two processes.

Disadvantageous: Security against Meet-in-the-Middle Algebraic Attacks. The previous fact may turn out to be a disadvantage when considering the security of such schemes against e.g. MitM algebraic attacks. In the case in which the degree of the encryption/forward direction and in the decryption/backward direction are equal, then a larger number of rounds (almost double, when comparing to the SPN scenario) could be necessary for preventing such attacks. A concrete example of this is the Type-II Feistel case $[x_0, x_1, \ldots, x_{2n-1}] \mapsto [y_0, y_1, \ldots, y_{2n-1}]$, for which the degree is the same in the two directions:

$$y_i \coloneqq \begin{cases} x_{i+1} + F(x_i) & \text{if } i \mod 2 = 0\,, \\ x_{i+1} & \text{otherwise}\,, \end{cases} \quad \text{and} \quad x_i = \begin{cases} y_{i-1} & \text{if } i \mod 2 = 0\,, \\ y_{i-1} - F(y_{i-2}) & \text{otherwise}\,, \end{cases}$$

(analogous for e.g. a Type-II Lai-Massey scheme). In other cases, the degree in the decryption/backward direction could be actually higher than the degree in the encryption/forward

[8] We remark that this is not true for all the generalized/redundant Lai-Massey schemes. However, there is no doubt that more freedom is possible in the choices of the functions that instantiate such Lai-Massey schemes without affecting their invertibility.

direction. A concrete example of this is the Type-III Feistel case

$$[x_0, x_1, \ldots, x_{n-2}, x_{n-1}] \mapsto [y_0, y_1, \ldots, y_{n-2}, y_{n-1}] = [x_1 + F(x_0), x_2 + F(x_1), \ldots, x_{n-1} + F(x_{n-2}), x_0]\,,$$

whose inverse is given by

$$x_0 = y_{n-1}\,, \quad x_1 = y_0 - F(y_{n-1})\,, \quad x_2 = y_1 - F(y_0 - F(y_{n-1}))\,, \quad x_3 = y_2 - F(y_1 - F(y_0 - F(y_{n-1})))\,,$$

and so on. In such a case, the inverse of the i-th $\mathbb{F}_q$-word has degree $\deg(F)^{i-1} \leq \deg(F)^{n-1}$, which is higher than the degree of the corresponding forward function (that is, $\deg(F)$). Still, in the case in which $\deg(F)^{n-1} \ll q$ (which could happen e.g. in MPC-/FHE-/ZK-friendly schemes), such schemes would require more rounds in order to reach maximum degree than a SPN scheme instantiated as before with e.g. power maps. A similar result/conclusion holds for e.g. the generalized Lai–Massey schemes GLM-1_n and GLM-2_n proposed in Prop. 4 – 5 – 6.

6.1.3 The `Horst` Scheme

The `Horst` construction recently proposed by Grassi et al. [GHR+22] is a generalization of the Feistel schemes in which the linear combination in $(x_0, x_1) \mapsto (x_1 + F(x_0), x_0)$ is replaced by a non-linear one, that is, $(x_0, x_1) \mapsto (x_1 \times G(x_0) + F(x_0), x_0)$. More formally:

Theorem 6 (`Horst` [GHR+22])**.** *Let $q = p^s$, where $p \geq 2$ is a prime and s is a positive integer, and let $n \geq 2$ be an integer. For each $i \in \{1, 2, \ldots, n-2\}$, let $F_i, G_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be $2 \cdot (n-1)$ functions, where $G_i(x_0, x_1, \ldots, x_{i-1}) \neq 0$ for each $x_0, x_1, \ldots, x_{i-1} \in \mathbb{F}_q$. The `Horst` construction $\mathcal{H}$ over $\mathbb{F}_q^n$ defined as $\mathcal{H}(x_0, x_1, \ldots, x_{n-1}) \coloneqq y_0 \| y_1 \| \ldots \| y_{n-1}$ where*

$$y_i \coloneqq \begin{cases} x_i \cdot G_i(x_0, x_1, \ldots, x_{i-1}) + F_i(x_0, x_1, \ldots, x_{i-1}) & \text{if } i \in \{0, 1, \ldots, n-2\} \\ x_0 & \text{otherwise } (i = n-1) \end{cases}$$

is invertible.

The advantages and disadvantages of the `Horst` Scheme are equivalent to the ones just listed for the case of Feistel and Lai-Massey schemes. E.g., both in the forward and in the backward computation of a `Horst` scheme, one never computes the inverse of G_i and/or of F_i (which do not exist in general). The only main difference regards the fact that a division takes places instead of a multiplication in the decryption/backward computation, i.e.,

$$y_i = x_i \cdot G_i(x_0, \ldots, x_{i-1}) + F_i(x_0, \ldots, x_{i-1}) \qquad \textit{versus} \qquad x_i = \frac{y_i - F_i(x_0, \ldots, x_{i-1})}{G_i(x_0, \ldots, x_{i-1})}\,,$$

for given $x_0, x_1, \ldots, x_{i-1}$. We point out that such difference is not sufficient by its own to affect the previous argument proposed for the MitM algebraic attacks. Indeed, the inverse of a `Horst` scheme can be potentially described by low degree functions by making use of 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).

6.2 The Generalized `Amaryllises` Scheme

Having said that, our goal is to set up an invertible scheme with the following properties:

- similar to SPN schemes, its degree is small in the forward/encryption direction, and very high (close to maximum) in the backward/decryption direction (or vice-versa);
- similar to Feistel/Lai-Massey/`Horst` schemes, a "full" non-linear mixing takes place among the inputs.

As we are going to show, a possible way to achieve it is by applying the `Horst` approach to the redundant Lai-Massey scheme defined before in Def. 7. That is, we propose a new variant of the redundant Lai-Massey construction – called generalized `Amaryllises` – in which the linear combination between the inputs x_i and the function $F(x_0, x_1, \dots, x_{n-1})$ is replaced by a non-linear one. More formally:

Definition 8 (Generalized `Amaryllises`)**.** Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n \geq 2$ be an integer. Let $e \geq 1$ be a positive integer, and let $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Given two functions $F, H : \mathbb{F}_q^n \to \mathbb{F}_q$, let $\mathcal{A}_G : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be defined as $\mathcal{A}_G(x_0, x_1, \dots, x_{n-1}) = y_0 \| y_1 \| y_2 \| \dots \| y_{n-1}$ where

$$\forall i \in \{0, 1, \dots, n-1\} : \qquad y_i \coloneqq \alpha_i \cdot (x_i^e \cdot F(x_0, x_1, \dots, x_{n-1}) + H(x_0, x_1, \dots, x_{n-1})) \ .$$

We say that $\mathcal{A}_G$ is a generalized `Amaryllises` construction *if* it is invertible.

In the next section, we propose concrete examples of the generalized `Amaryllises` construction just proposed, showing that we are able to reach the goals we fixed before. Moreover, we compare the advantages and the disadvantages of such construction compared to the Lai-Massey ones.

Remark. Before going on, we point out that computing a generalized `Amaryllises` construction costs n additions, n multiplications, n e-powers (if $e \neq 1$), and the evaluation of the functions F and H. Even if it is possible to define a similar scheme by using the generalized Lai-Massey scheme defined in Def. 6 as starting point, we point out that such variant may be more expensive to compute in general (since $2 \cdot n$ different functions F_i and H_i must be computed, besides the other operations).

7 A Botanical Garden of Generalized `Amaryllises` Schemes

In this section, we present concrete examples of the generalized `Amaryllises` Schemes.

7.1 The `Amaryllises` Scheme

Probably, the simplest (non-trivial) example of a generalized `Amaryllises` scheme is the following.

Proposition 8 (`Amaryllises`)**.** *Let $q = p^s$, where $p \geq 2$ is a prime and s is a positive integer, and let $n \geq 2$ be an integer. Let $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that (1st) $F(0) \neq 0$ and (2nd) $G(x) \coloneqq x \cdot F(x)$ is invertible over $\mathbb{F}_q$. Let $H : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ be any function, and let $\beta_0, \beta_1, \dots, \beta_{n-1} \in \mathbb{F}_q \setminus \{0\}$ such that $\sum_{i=0}^{n-1} \beta_i = 0$ **if** H is not identically equal to zero (equivalently, no condition on $\sum_{i=0}^{n-1} \beta_i$ is imposed if $H(z) = 0$ for each $z \in \mathbb{F}_q$). For each $j \in \{0, 1, \dots, n-2\}$, let $\lambda_0^{(j)}, \lambda_1^{(j)}, \dots, \lambda_{n-1}^{(j)} \in \mathbb{F}_q$ be such that $\sum_{i=0}^{n-1} \lambda_i^{(j)} = 0$.*

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

$$y_i \coloneqq \alpha_i \cdot \left(x_i \cdot F\left(\sum_{j=0}^{n-1} \beta_j \cdot x_j \right) + H\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \dots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j \right) \right) \tag{5}$$

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

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

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:

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

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

In a similar way, it is possible to recover $\sum_{i=0}^{n-1} \gamma_i^{(j)} \cdot x_i$ for each $j \in \{0, 1, \ldots, n-2\}$:

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

where

$$z = F\left(G^{-1}\left(\sum_{i=0}^{n-1} \beta_i \cdot \frac{y_i}{\alpha_i}\right)\right) \neq 0$$

and where F never returns zero by assumption.

It follows that for each $i \in \{0, \ldots, n-1\}$:

$$x_i = \frac{1}{z} \cdot \left(\frac{y_i}{\alpha_i} - H\left(\frac{\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot y_j/\alpha_j}{z}, \ldots, \frac{\sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot y_j/\alpha_j}{z}\right)\right). \qquad \square$$

We remark that the Lai-Massey scheme is a particular case of the `Amaryllises` scheme in which F always returns one and $e = 1$. Moreover, we point out that such scheme realizes our goals, that is, (i) the degree of the inverse is in general higher degree than the degree of the scheme itself, and (ii) a non-linear mixing among the inputs takes place.

7.1.1 About Invariant Subspaces

As for the case of the redundant Lai-Massey scheme proposed before, the `Amaryllises` scheme can admit invariant subspaces. In particular, the multiplication with F in `Amaryllises` is *not* sufficient by itself to destroy the subspace $\mathfrak{X} = \{x \in \mathbb{F}_q^n \mid \forall i \in \{0, 1, \ldots, n-2\} : \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j = 0\}$. Indeed, assume that $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 1$:

- if H is not identically equal to zero, then $\sum_{i=0}^{n-1} \beta_i = \sum_{i=0}^{n-1} \lambda_i^{(0)} = \sum_{i=0}^{n-1} \lambda_i^{(1)} = \ldots = \sum_{i=0}^{n-1} \lambda_i^{(n-2)} = 0$ is required for guaranteeing the invertibility. In such a case, $\langle [1, 1, \ldots, 1]^T \rangle$ is an invariant subspace for the `Amaryllises` scheme $[x_0, \ldots, x_{n-1}] \mapsto [y_0, \ldots, y_{n-1}]$ as well. Indeed, given an input $[x, x, \ldots, x] \in \mathbb{F}_q^n$, we have that

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

  that is, $y_i = y_j$ for each $i, j \in \{0, 1, \ldots, n-1\}$;

- if H is identically equal to zero, then no condition is imposed on $\sum_{i=0}^{n-1} \beta_i$. Still, the subspace $\mathfrak{B} = \{x \in \mathbb{F}_q^n \mid \sum_{i=0}^{n-1} \beta_i \cdot x_i = 0\}$ is invariant for `Amaryllises`. Indeed, by applying `Amaryllises` on $\mathfrak{B}$, we have

  $$[x_0, x_1, \ldots, x_{n-1}] \mapsto [x_0 \cdot F(0), x_1 \cdot F(0), \ldots, x_{n-1} \cdot F(0)] \equiv F(0) \cdot [x_0, x_1, \ldots, x_{n-1}] \,.$$

  Since F never returns zero by assumption, the subspace $\mathfrak{B}$ is invariant.

As before, if H depends on all $n-1$ linearly independent combinations of the inputs x_i (for which the sum of the coefficients is zero), then the previous subspace can be destroyed by imposing that at least two coefficients α_i and α_j for $i, j \in \{0, 1, \ldots, n-1\}$ are different.

7.1.2 Constructing Suitable Functions for the `Amaryllises` Construction

A Generic Result. Next, we show how to construct functions F that satisfy the required assumptions of the previous Prop. 8.

Lemma 4. *Let $q = p^s$, where $p \geq 2$ is a prime and s is a positive integer. Let P be a permutation over $\mathbb{F}_q$. Let $\psi \in \mathbb{F}_q \setminus \{0\}$. The function F over $\mathbb{F}_q$ defined as*

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

satisfies the requirements of Prop. 8.

Proof. The proof trivially follows from the facts that (i) $F(0) = \psi \neq 0$ and (ii) $x \mapsto x \cdot F(x) = P(x) - P(0)$ is a permutation (since P is a permutation). □

Let $P'(x) \coloneqq \frac{P(x)-P(0)}{x}$, where note that the polynomial $P(x) - P(0)$ is divisible by x. The algebraic expression of the function F just given is

$$F(x) = P'(x) + \frac{\psi - P'(0)}{\prod_{i \in \mathbb{F}_q \setminus \{0\}} i} \cdot \prod_{i \in \mathbb{F}_q \setminus \{0\}} (i - x) \,.$$

Indeed, if $x \neq 0$, then $\prod_{i \in \mathbb{F}_q \setminus \{0\}} (i - x) = 0$, which implies $F(x) = P'(x) = \frac{P(x)-P(0)}{x}$. Otherwise, if $x = 0$, then $\prod_{i \in \mathbb{F}_q \setminus \{0\}} i = \prod_{i \in \mathbb{F}_q \setminus \{0\}} (i - x)$, which implies $F(0) = \psi$.

Constructing F via Power Maps and Dickson Polynomials. By exploiting this result, we present concrete examples of functions F that satisfy the assumptions of Theorem 8 and that are cheap to compute (e.g., from the point of view of the *multiplicative complexity*) especially for the case in which q is very large (e.g., $q \geq 2^{64}$).

Lemma 5. *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*

$$F(x) = \sum_{i=1}^{d} \binom{d}{i} x^{i-1} \cdot (\pm\alpha)^{d-i} = \begin{cases} \frac{(x \pm \alpha)^d \mp \alpha^d}{x} & \text{if } x \neq 0\,, \\ \pm d \cdot \alpha^{d-1} & \text{otherwise} \end{cases} \tag{6}$$

satisfies the requirements of Prop. 8.

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

Another example constructed via the Dickson polynomial is proposed in Lemma 10. We point out that the function defined in (15) via the Dickson polynomial (which contains only monomials of the form x^{2i} for $i \in \{0, 1, \ldots, (d-1)/2\}$) is cheaper to compute than the one just defined via power maps ($(d-1)/2$ versus $d-1$ multiplications).

About the Function G in the `Horst` Construction. Since the functions just listed never return zero, they can also be exploited to instantiate the functions G_i that satisfy the assumption of the `Horst` construction.

Lemma 6. *Let $q = p^s$ for a prime $p \geq 2$ and a positive integer s. Let $G_1 : \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}$ be a function that never returns zero. For each $n \geq 2$, let $H_n : \mathbb{F}_q^n \to \mathbb{F}_q$ be any function. The function $G_n : \mathbb{F}_q^n \to \mathbb{F}_q$ defined as $G_n(x_0, x_1, \ldots, x_{n-1}) \coloneqq G_1 \circ H_n(x_0, x_1, \ldots, x_{n-1})$ never returns zero.*

The proof is trivial. If there exists an input $[x_0, x_1, \ldots, x_{n-1}] \in \mathbb{F}_q^n$ for which G_n returns zero, then G_1 returns zero as well for the input $H_n(x_0, x_1, \ldots, x_{n-1})$, which contradicts the assumption on G_1.

7.2 The (Extended) Contracting–`Amaryllises` Construction

Next, we introduce the (extended) contracting–`Amaryllises` constructions, as variants of the `Amaryllises` just proposed. The main difference between contracting–`Amaryllises` and `Amaryllises` schemes relies on the details of the function F in (5): while the function F in the `Amaryllises` construction is defined over $\mathbb{F}_q$, it takes as input n $\mathbb{F}_q$-elements and returns a single $\mathbb{F}_q$-element in the contracting–`Amaryllises` construction, that is, it is of the form $F : \mathbb{F}_q^n \to \mathbb{F}_q$ (as the name "contracting" suggests).

Proposition 9 (Contracting–`Amaryllises`)**.** *Let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$, 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 $F : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function that never returns zero for any non-zero input, that is,*

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

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

$$G_{\psi_0, \psi_1, \ldots, \psi_{n-1}}(x) \coloneqq x^e \cdot F(\psi_0 \cdot x, \psi_1 \cdot x, \ldots, \psi_{n-1} \cdot x)$$

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

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad y_i \coloneqq \alpha_i \cdot x_i^e \cdot F(x_0, x_1, \ldots, x_{n-1}) \tag{7}$$

is invertible.

Proof. We start by pointing out two observations:

- first of all, the following equality always holds:

$$\forall i,j \in \{0,1,\dots,n-1\}: \qquad \frac{y_i \cdot x_j^e}{\alpha_i} = \frac{y_j \cdot x_i^e}{\alpha_j} = x_i^e \cdot x_j^e \cdot F(x_0,x_1,\dots,x_{n-1})\,; \quad (8)$$

- 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 $F(x_0,x_1,\dots,x_{n-1}) = 0$. However, $F(x_0,x_1,\dots,x_{n-1}) = 0$ if and only if $[x_0,x_1,\dots,x_{n-1}] = [0,0,\dots,0]$, 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). In the case in which $[y_0,y_1,\dots,y_{n-1}] \neq [0,0,\dots,0]$ (otherwise, the input is zero due to the previous observation), then for each $i \in \{0,1,\dots,n-1\}$ such that $y_i \neq 0$ (remember that $y_i = 0$ implies $x_i = 0$):

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

due to (8), and where $x \mapsto x^e$ is invertible by assumption on e. By assumption, G is invertible (note that $\psi_j = (y_j/y_i)^{1/e}$ is fixed for each $j \in \{0,1,\dots,n-1\}$).

As a result, the inverse of the contracting–`Amaryllises` scheme is defined as:

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

for each $i \in \{0,1,\dots,n-1\}$. □

Proposition 10 (Extended contracting–`Amaryllises`)**.** *Let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$, and let $n \geq 2$ be an integer. Let $\alpha_0,\alpha_1,\dots,\alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$. Let $l \in \{1,2,\dots,n-1\}$. For each $i \in \{0,1,\dots,l-1\}$, let $\lambda_0^{(i)},\lambda_1^{(i)},\dots,\lambda_{n-1}^{(i)} \in \mathbb{F}_q$ be as in Prop. 2 (in particular, such that $\sum_{j=0}^{m-1}\lambda_j^{(i)} = 0$). Let $H : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ be any function. Let $F : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ be a function that never returns zero for any non-zero input, that is,*

$$\forall [x_0,x_1,\dots,x_{n-2}] \in \mathbb{F}_q^{n-1} \setminus \{[0,0,\dots,0]\}: \qquad F(x_0,x_1,\dots,x_{n-2}) \neq 0\,.$$

If the function $G_{\psi_0,\psi_1,\dots,\psi_{n-2}}(x) : \mathbb{F}_q \to \mathbb{F}_q$ defined as

$$G_{\psi_0,\psi_1,\dots,\psi_{n-2}}(x) \coloneqq x \cdot F(\psi_0 \cdot x, \psi_1 \cdot x, \dots, \psi_{n-2} \cdot x)$$

is invertible for each arbitrary fixed non-null $[\psi_0,\psi_1,\dots,\psi_{n-2}] \in \mathbb{F}_q^{n-1} \setminus \{[0,0,\dots,0]\}$, then the extended contracting–`Amaryllises` scheme $\mathcal{A}_{EC}$ over $\mathbb{F}_q^n$ defined as $\mathcal{A}_{EC}(x_0,\dots,x_{n-1}) = y_0\|\dots\|y_{n-1}$ where for each $i \in \{0,1,\dots,n-1\}$:

$$y_i \coloneqq \alpha_i \cdot \left(x_i \cdot F\left(\sum_{j=0}^{n-1}\lambda_j^{(0)} \cdot x_j, \dots, \sum_{j=0}^{n-1}\lambda_j^{(l-1)} \cdot x_j\right) + H\left(\sum_{j=0}^{n-1}\lambda_j^{(0)} \cdot x_j, \dots, \sum_{j=0}^{n-1}\lambda_j^{(l-1)} \cdot x_j\right)\right) \quad (9)$$

is invertible.

Proof. The invertibility of the extended contracting–`Amaryllises` scheme follows from the invertibility of the contracting–`Amaryllises` construction. Indeed, note that for each $i \in \{0, 1, \ldots, l-1\}$:

$$\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot \frac{y_j}{\alpha_j} = \left(\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j \right) \cdot F \left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j \right) ,$$

since $\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot H \left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j \right) = 0$ due to the fact that $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$. The previous system of equations reduces to

$$\forall i \in \{0, 1, \ldots, n-2\} : \qquad w_i = z_i \cdot F(z_0, z_1, \ldots, z_{n-2}) ,$$

where

$$w_i \coloneqq \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot \frac{y_j}{\alpha_j} , \qquad z_i \coloneqq \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j$$

for each $i \in \{0, 1, \ldots, n-1\}$. This is exactly a contracting–`Amaryllises` scheme over $\mathbb{F}_q^{n-1}$, which is invertible due to Prop. 9. Hence, given $z_0, z_1, \ldots, z_{n-2} \in \mathbb{F}_q$, we have that

$$\forall i \in \{0, 1, \ldots, n-2\} : \qquad x_i = \frac{y_i/\alpha_i - H(z_0, z_1, \ldots, z_{n-2})}{F(z_0, z_1, \ldots, z_{n-2})} ,$$

where F never returns zero by assumption. □

As before, both the contracting–`Amaryllises` scheme and the extended contracting–`Amaryllises` scheme realize our goals, i.e., (i) their inverse have in general higher degree than the schemes themselves, and (ii) non-linear mixing takes place among the inputs.

About Invariant Subspaces. Similar to the `Amaryllises` scheme, each input in the subspace $\langle [1, 1, \ldots, 1]^T \rangle \equiv \{[x, x, \ldots, x] \mid \forall x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$ does not active any non-linear function of the extended contracting–`Amaryllises` scheme. In order to break it, it is sufficient to impose that at least two coefficients α_i and α_j for $i, j \in \{0, 1, \ldots, n-1\}$ are different.

Regarding the contracting–`Amaryllises` scheme, it does *not* admit invariant subspaces in general, since the inputs of the function F are $x_0, x_1, \ldots, x_{n-1}$ and not linear combinations of them. However, the existence of such subspace obviously depends on the details of the function F itself.

7.3 Constructing Suitable Functions for the (Extended) contracting–`Amaryllises` Construction

In the following, we show how to set up functions $F : \mathbb{F}_q^n \to \mathbb{F}_q$ that (i) satisfy the assumptions of Prop. 9 – 10 and that (ii) are efficient to compute from the multiplicative point of view (equivalently, of low degree).

First, in Prop. 11, we prove that homogeneous functions that never return zero satisfy such assumptions. Based on it, we then provide some concrete examples of such functions over $\mathbb{F}_q^n$ for $n \geq 2$.

Remark 1. The result proposed in Prop. 9 depends on a parameter e that must satisfy $\gcd(e, q-1) = 1$. In order to apply the following results both to Prop. 9 and to Prop. 10, from now on, we assume $e = 1$ for the result proposed in Prop. 10.

Proposition 11. *Let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$, 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) $d' \coloneqq d - e \geq 0$. Let $\mathfrak{I}_{d'} \coloneqq \left\{[i_0, i_1, \ldots, i_{n-1}] \in \mathbb{Z}_+^n \mid \sum_{j=0}^{n-1} i_j = d'\right\}$.*

A function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ satisfies the assumptions of Prop. 9 – 10 if the following conditions are satisfied:

1. *F is a homogeneous function of degree d' (that is, a sum of monomials of degree d' only), that is,*

$$F(x_0, x_1, \ldots, x_{n-1}) = \sum_{\{i_0,i_1,\ldots,i_{n-1}\} \in \mathfrak{I}_{d'}} \varphi_{i_0,i_1,\ldots,i_{n-1}} \cdot x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{n-1}^{i_{n-1}} ,$$

   where $\varphi_{i_0,i_1,\ldots,i_{n-1}} \in \mathbb{F}_q$;

2. *F never returns zero for any non-zero input, that is,*

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

Proof. We limit ourselves to prove the case $\omega = 1$ only (the other case is analogous).

It is sufficient to prove that $G_{\psi_0,\psi_1,\ldots,\psi_{n-1}}(x) = x^{d-d'} \cdot F(\psi_0 \cdot x, \psi_1 \cdot x, \ldots, \psi_{n-1} \cdot x)$ 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 F contains only monomials of degree d', then

$$\begin{aligned}
G_{\psi_0,\psi_1,\ldots,\psi_{n-1}}(x) &= x^e \cdot F(\psi_0 \cdot x, \psi_1 \cdot x, \ldots, \psi_{n-1} \cdot x) \\
&= x^e \cdot \sum_{\{i_0,i_1,\ldots,i_{n-1}\} \in \mathfrak{I}_{d'}} \varphi_{i_0,i_1,\ldots,i_{n-1}} \cdot (\psi_0 \cdot x)^{i_0} \cdot (\psi_1 \cdot x)^{i_1} \cdot \ldots \cdot (\psi_{n-1} \cdot x)^{i_{n-1}} \\
&= x^d \cdot \sum_{\{i_0,i_1,\ldots,i_{n-1}\} \in \mathfrak{I}_{d'}} \varphi_{i_0,i_1,\ldots,i_{n-1}} \cdot \psi_0^{i_0} \cdot \psi_1^{i_1} \cdot \ldots \cdot \psi_{n-1}^{i_{n-1}} \\
&= x^d \cdot F(\psi_0, \psi_1, \ldots, \psi_{n-1}) ,
\end{aligned}$$

where $d = d' + e$ by definition. Since (i) $x \mapsto x^d$ is invertible due to the assumption on d and since (ii) $F(\psi_0, \psi_1, \ldots, \psi_{n-1}) \neq 0$ for each non-null input by assumption, then the inverse of $y = G_{\psi_0,\psi_1,\ldots,\psi_{n-1}}(x)$ is given by

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

An analogous result holds by assuming $d' \coloneqq e - d$ and by considering functions F of the form

$$F(x_0, x_1, \ldots, x_{n-1}) = \frac{1}{\sum_{\{i_0,i_1,\ldots,i_{n-1}\} \in \mathfrak{I}_{d'}} \varphi_{i_0,i_1,\ldots,i_{n-1}} \cdot x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{n-1}^{i_{n-1}}} ,$$

that never returns zero (where $1/0 \coloneqq 0$). The proof is equivalent to the one just given.

7.3.1 Suitable Functions over $\mathbb{F}_q^2$

In this subsection, we propose some concrete examples of functions over $\mathbb{F}_q^2$ that satisfy the conditions given in Prop. 11.

Lemma 7. *Let $q = p^s$ for a prime $p \geq 2$ and a positive integer $s \geq 1$. Let $d \geq 3$ be such that $\gcd(d, q-1) = 1$, and let $d' = d - 1$. Let $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$. The function $F : \mathbb{F}_q^2 \to \mathbb{F}_q$ defined as*

$$F(x_0, x_1) = \sum_{i=1}^{d} \binom{d}{i} \cdot \alpha^i \cdot \beta^{d-i} \cdot x_0^{i-1} \cdot x_1^{d-i}$$

satisfies the conditions given in Prop. 11.

Proof. It is sufficient to prove that F never returns zero for a non-zero input. This fact follows from the following observations:

- if $x_1 = 0$, then $F(x_0, 0) = \alpha^d \cdot x_0^{d-1}$, which is equal to zero if and only if $x_0 = 0$;
- if $x_1 \neq 0$, let $z \coloneqq x_0/x_1$, and note that

$$F(z, x_1) = x_1^{d-1} \cdot \frac{(\alpha \cdot z + \beta)^d - \beta^d}{z} .$$

  By simple observation, $F(z, x_1) = 0$ if and only if $(\alpha \cdot z + \beta)^d - \beta^d = 0$ and $z \neq 0$ (since the denominator is z). However, since $x \mapsto x^d$ is a permutation, $(\alpha \cdot z + \beta)^d = \beta^d$ occurs if and only if $z = 0$, which is excluded.

As a result, $F(x_0, x_1) = 0$ if and only if $[x_0, x_1] = [0, 0]$. □

A similar example constructed via the Dickson polynomial is proposed in Lemma 11.

Case: Prime Fields. Next, we propose an example for prime fields only.

Lemma 8. *Let $p \geq 3$ be a prime integer, and let $d \geq 3$ be such that $\gcd(d, p-1) = 1$. Let $d' \in \{2, 4, \ldots, d-1\}$ 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, that is, $L_p(\omega) = -1$. The function*

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

satisfies the assumptions of Prop. 11.

Proof. As before, it is sufficient to show that $F(x_0, x_1) \neq 0$ for each $[x_0, x_1] \neq [0, 0]$. Assume by contradiction that $F(x_0, x_1) = \alpha^2 \cdot (x_0 + \lambda \cdot x_1)^{d'} - \omega \cdot \beta^2 \cdot (x_0 + \lambda' \cdot x_1)^{d'} = 0$ for a certain $[x_0, x_1] \neq [0, 0]$:

$$\begin{aligned} & \alpha^2 \cdot (x_0 + \lambda \cdot x_1)^{d'} = \omega \cdot \beta^2 \cdot (x_0 + \lambda' \cdot x_1)^{d'} \\ \longrightarrow \quad & \left(\alpha \cdot (x_0 + \lambda \cdot x_1)^{\frac{d'}{2}}\right)^2 = \omega \cdot \left(\beta \cdot (x_0 + \lambda' \cdot x_1)^{\frac{d'}{2}}\right)^2 . \end{aligned}$$

Such equality is satisfied only in the case in which both sides are equal to zero. Indeed, note that 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. □

In the case $d' = 2$, the previous function reduces to

$$F(x_0, x_1) = \phi \cdot x_0^2 + \psi \cdot x_0 \cdot x_1 + \varphi \cdot x_1^2 ,$$

where $\phi, \psi, \gamma \in \mathbb{F}_p$ must satisfy the condition that $\phi^2 - 4 \cdot \psi \cdot \varphi$ is a quadratic non-residue modulo p, that is, $L_p(\psi^2 - 4 \cdot \phi \cdot \varphi) = -1$. Indeed:

$$\begin{aligned} & \alpha^2 \cdot (x_0 + \lambda \cdot x_1)^2 - \omega \cdot \beta^2 \cdot (x_0 + \lambda' \cdot x_1)^2 \\ = & x_0^2 \cdot \underbrace{(\alpha^2 - \omega \cdot \beta^2)}_{=\phi} + 2 \cdot x_0 \cdot x_1 \cdot \underbrace{(\alpha^2 \cdot \lambda - \omega \cdot \beta^2 \cdot \lambda')}_{=\psi/2} + x_1^2 \cdot \underbrace{(\alpha^2 \cdot \lambda^2 - \omega \cdot \beta^2 \cdot \lambda'^2)}_{=\varphi} \end{aligned}$$

where

$$\begin{aligned} L_p(\psi^2 - 4\cdot\phi\cdot\varphi) &= L_p\left(\left(2\cdot(\alpha^2\cdot\lambda - \omega\cdot\beta^2\cdot\lambda')\right)^2 - 4\cdot(\alpha^2-\omega\cdot\beta^2)\cdot(\alpha^2\cdot\lambda^2 - \omega\cdot\beta^2\cdot\lambda'^2)\right) \\ &= L_p\left((\alpha^2\cdot\lambda - \omega\cdot\beta^2\cdot\lambda')^2 - (\alpha^2-\omega\cdot\beta^2)\cdot(\alpha^2\cdot\lambda^2 - \omega\cdot\beta^2\cdot\lambda'^2)\right) \\ &= L_p\left(\omega\cdot\alpha^2\cdot\beta^2\cdot(\lambda+\lambda')^2\right) = L_p(\omega) = -1\,. \end{aligned}$$

Note that this fact is related to the (potential) solutions of the quadratic equation $\phi\cdot z^2 + \psi z + \varphi = 0$, which are

$$z_\pm = \left(-\psi \pm \sqrt{\psi^2 - 4\cdot\phi\cdot\varphi}\right)/(2\cdot\phi)\,.$$

Since $L_p(\psi^2 - 4\cdot\phi\cdot\varphi) = -1$ due to the assumption on ϕ, ψ, φ, no solution exists.

7.3.2 Suitable Functions over $\mathbb{F}_q^{\geq 3}$

Next, we generalize the previous $\mathbb{F}_q^2$-results for the case $\mathbb{F}_q^n$ with $n \geq 3$. Our strategy is to construct the functions F that satisfy Prop. 11 in an iterated way, that is, given a function $F_m : \mathbb{F}_q^m \to \mathbb{F}_q$ for a certain $m \geq 2$ that satisfies the required properties, we show how to construct a function $F_n : \mathbb{F}_q^n \to \mathbb{F}_q$ for $n > m$ that satisfies the required properties as well.

Proposition 12. *Let $q = p^s$ for a prime integer $p \geq 2$ and for a positive integer s. Let $m \geq 2$, let $n_0, n_1, \ldots, n_{m-1} \geq 1$ and let $n \coloneqq \sum_{i=0}^{m-1} n_i$.*

For each $i \in \{n_0, n_1, \ldots, n_{m-1}, m\}$, let $F_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be a function that satisfy the assumptions of Prop. 11, that is, (i) it is an homogeneous function of a certain degree $\deg(F_i) \geq 1$, and (ii) it never returns zero for any non-zero input (i.e., $F_i(x_0, x_1, \ldots, x_{i-1}) \neq 0$ for each $[x_0, x_1, \ldots, x_{i-1}] \in \mathbb{F}_q^i \setminus \{[0,0,\ldots,0]\}$).

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

$$d \coloneqq lcm\left(\deg(F_{n_0}), \deg(F_{n_1}), \ldots, \deg(F_{n_{m-1}})\right)\,.$$

The function $F_n : \mathbb{F}_q^n \to \mathbb{F}_q$ be defined as

$$\begin{aligned} F_n(x_0, x_1, \ldots, x_n) \coloneqq F_m\Big(&(F_{n_0}(x_0, \ldots, x_{n_0-1}))^{\frac{d}{\deg(F_{n_0})}}\,, \\ &(F_{n_1}(x_{n_0}, \ldots, x_{n_0+n_1-1}))^{\frac{d}{\deg(F_{n_1})}}, \ldots, \left(F_{n_{m-1}}(x_{n-n_m}, \ldots, x_{n-1})\right)^{\frac{d}{\deg(F_{n_{m-1}})}} \Big) \end{aligned}$$

satisfies the assumptions of Prop. 11, that is,

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

Proof. Regarding the first point, F_n is a homogeneous function of degree $d\cdot\deg(F_m)$ since

- F_m is a homogeneous function of degree $\deg(F_m)$;
- each input of F_m is a homogeneous function of degree d.

Regarding the second point, F_n returns zero if and only if all its inputs are equal to zero since:

- F_m returns zero if and only if all its inputs are equal to zero;
- each input of F_m, that is, $F_{n_i}(z_0, z_1, \ldots, z_{n_i-1})$, returns zero if and only $z_0 = z_1 = \ldots = z_{n_i-1} = 0$. □

By applying the previous result iteratively, it is possible to construct functions $F_n : \mathbb{F}_q^n \to \mathbb{F}_q$ that satisfy the assumptions of Prop. 11 for each $n \geq 3$, as

$$F_n(x_0, x_1, \ldots, x_{n-1}) = F_2\left(F_{n-1}(x_0, x_1, \ldots, x_{n-2}), x_{n-1}^{\deg(F_{n-1})}\right) .$$

Other concrete examples for $n = 4$ (analogous for $n \geq 5$) are given by

$$\begin{aligned} F_4(x_0, x_1, x_2, x_3) &= F_3\left(F_2(x_0, x_1), x_2^{\deg(F_2)}, x_3^{\deg(F_2)}\right) , \\ F_4(x_0, x_1, x_2, x_3) &= F_2\left(F_3(x_0, x_1, x_2), x_3^{\deg(F_3)}\right) , \\ F_4(x_0, x_1, x_2, x_3) &= F_2\left(F_2(x_0, x_1), F_2(x_2, x_3)\right) , \end{aligned}$$

and so on. The starting points are (i) the identity function $F_1(x) = x$, and (ii) the functions $F_2 : \mathbb{F}_q^2 \to \mathbb{F}_q$ proposed in the previous subsection.

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 F_n that satisfy the required assumptions of Prop. 11 as an open problem for future work.

8 Lai-Massey versus Generalized `Amaryllises` Schemes

In order to better understand the generalized `Amaryllises` schemes, we compare their security with the one of the Lai-Massey schemes. We refer to the analysis proposed in Sect. 6 for the comparison between the generalized `Amaryllises` and the SPN/Feistel/`Horst` schemes.

Remark 2. We emphasize that the following observations do not take into account the details of the sub-components of the considered schemes. Rather, our goal is to emphasize the impact of the multiplication with F on the security of a generalized `Amaryllises` scheme.

8.1 Statistical Attacks

Regarding the statistical attacks, we focus on invariant subspace attacks and (truncated) differential attacks. We point out that, due to the non-linear mixing that occurs among the $\mathbb{F}_q$-state, the statistical attacks that exploit the strong alignment of the attacked scheme [BDKA21, CGG+22] become – in general – quickly infeasible in the case of iterated Lai-Massey and generalized `Amaryllises` schemes.

Invariant Subspaces. Both Lai-Massey schemes and generalized `Amaryllises` schemes can admit invariant subspace trails. As already discussed before, we limit ourselves to recall that a proper choice of the constants $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_q \setminus \{0\}$ could be sufficient for preventing the existence of such invariant subspaces.

Differential (and Linear) Attacks. Regarding other statistical attacks, the impact of the multiplication with F in the generalized `Amaryllises` scheme could make a big difference on the security. Let's focus on the case of differential attacks [BS90, BS93], in which the attacker considers 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 through a permutation P over $\mathbb{F}_q^n$. The differential

probability (DP) of having a certain output difference Δ given a particular input difference δ is equal to

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

A variant of differential cryptanalysis is the truncated differential cryptanalysis [Knu94]. In the latter, the attacker does not fix the values of the differences, but either specifies conditions between the differences of the $\mathbb{F}_q$-state that should be satisfied, or fixes some differences to zero. We point out that the following analysis can be easily modified in order to cover linear attacks [Mat93] as well.

Lai-Massey Schemes. In the case of a redundant Lai-Massey scheme as in Def. 7, we have that

$$\alpha_i \cdot (x_i + \delta_i + F(x_0 + \delta_0, x_1 + \delta_1, \dots, x_{n-1} + \delta_{n-1})) - \alpha_i \cdot (x_i + F(x_0, x_1, \dots, x_{n-1})) = \Delta_i ,$$

that is,

$$F(x_0 + \delta_0, x_1 + \delta_1, \dots, x_{n-1} + \delta_{n-1}) - F(x_0, x_1, \dots, x_{n-1}) = \frac{\Delta_i}{\alpha_i} - \delta_i \tag{10}$$

for each $i \in \{0, 1, \dots, n-1\}$. Hence:

- if $\frac{\Delta_i}{\alpha_i} - \delta_i = \frac{\Delta_j}{\alpha_j} - \delta_j$ for each $i, j \in \{0, 1, \dots, n-1\}$, then the system of n equations reduces to a single equation;
- otherwise, the system does not admit any solution, and so the probability that the input difference δ is mapped into the output difference Δ is zero.

Let $\#_F(\delta_0, \delta_1, \dots, \delta_{n-1})$ be the number of solutions $[x_0, x_1, \dots, x_{n-1}] \in \mathbb{F}_q^n$ of Eq. (10). Then:

$$\text{Prob}(\delta \neq 0 \rightarrow \Delta) = \frac{\#_F(\delta_0, \delta_1, \dots, \delta_{n-1})}{q^n} .$$

Usually, for a generic function F and a generic $\delta_0, \dots, \delta_{n-1}$, the previous probability is of order $\mathcal{O}(q^{-1})$, since $\#_F(\delta_0, \delta_1, \dots, \delta_{n-1}) \leq (\deg(F) - 1) \cdot q^{n-1}$.

Besides that, the scheme admits a truncated differential with probability 1 of the form

$$(\delta, \delta, \dots, \delta) \in \mathbb{F}_q^n \longrightarrow (\Delta \cdot \alpha_0, \Delta \cdot \alpha_1, \dots, \Delta \cdot \alpha_{n-1}) \in \mathbb{F}_q^n$$

where $\Delta \in \mathbb{F}_q$ is *not* fixed. It is trivial to check that it is not possible such probability-1 truncated differential for more than one round if $\alpha_i \neq \alpha_j$ for a certain $i, j \in \{0, 1, \dots, n-1\}$.

In the case of a generalized Lai-Massey scheme as in Def. 7, we have that

$$\delta_i + F_i\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot (x_j + \delta_j), \dots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot (x_j + \delta_j)\right) - F_i\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \dots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\right) = \frac{\Delta_i}{\alpha_i} .$$

for each $i \in \{0, 1, \dots, n-1\}$. In the case $\delta_0 = \delta_1 = \dots = \delta_{n-1} \equiv \delta \in \mathbb{F}_q \setminus \{0\}$, then $\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot \delta = 0$ since $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$ for each $i \in \{0, 1, \dots, n-2\}$, and the previous equation reduces to

$$\forall i \in \{0, 1, \dots, n-1\} : \qquad \delta = \frac{\Delta_i}{\alpha_i} ,$$

which is always verified if $\alpha_i \cdot \Delta_j = \alpha_j \cdot \Delta_i$ for each $i, j \in \{0, 1, \dots, n-1\}$. Hence, for any fixed $\delta \in \mathbb{F}_q$, the differential characterestic

$$(\delta, \delta, \dots, \delta) \in \mathbb{F}_q^n \longrightarrow (\delta \cdot \alpha_0, \delta \cdot \alpha_1, \dots, \delta \cdot \alpha_{n-1}) \in \mathbb{F}_q^n$$

has probability 1 for the generalized Lai-Massey as well.

Generalized ***Amaryllises*** *Schemes.* In the case of a generalized `Amaryllises` scheme, we have that

$$(x_i + \delta_i) \cdot F(x_0 + \delta_0, x_1 + \delta_1, \ldots, x_{n-1} + \delta_{n-1}) - x_i \cdot F(x_0, x_1, \ldots, x_{n-1}) \\ + H(x_0 + \delta_0, x_1 + \delta_1, \ldots, x_{n-1} + \delta_{n-1}) - H(x_0, x_1, \ldots, x_{n-1}) = \frac{\Delta_i}{\alpha_i}$$

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

$$\forall i \in \{0, 1, \ldots, n-1\} : \qquad x_i \cdot z + w = \frac{\Delta_i}{\alpha_i}$$

where

$$z \coloneqq F(x_0 + \delta_0, x_1 + \delta_1, \ldots, x_{n-1} + \delta_{n-1}) - F(x_0, x_1, \ldots, x_{n-1}) \,, \tag{11}$$

$$w \coloneqq \delta_i \cdot F(x_0 + \delta_0, x_1 + \delta_1, \ldots, x_{n-1} + \delta_{n-1}) + H(x_0 + \delta_0, x_1 + \delta_1, \ldots, x_{n-1} + \delta_{n-1}) \\ - H(x_0, x_1, \ldots, x_{n-1}) \,. \tag{12}$$

Hence, for each value of $z, w \in \mathbb{F}_q$:

- if $z \neq 0$, then the value of x_i is given by $x_i = z^{-1} \cdot \left(\frac{\Delta_i}{\alpha_i} - w\right)$. Such values $x_0, x_1, \ldots, x_{n-1} \in \mathbb{F}_q$ are a solution for the differential characteristic if the equalities (11) – (12) are satisfied;
- if $z = 0$, then the equalities $x_i \cdot z + w = \frac{\Delta_i}{\alpha_i}$ are satisfied independently of z if and only if $w = \frac{\Delta_i}{\alpha_i}$ for each $i \in \{0, 1, \ldots, n-1\}$, and so $\frac{\Delta_j}{\alpha_j} = \frac{\Delta_i}{\alpha_i}$ for each $i, j \in \{0, 1, \ldots, n-1\}$.

As before, let $\#_F(\delta_0, \delta_1, \ldots, \delta_{n-1})$ and $\#_{F,H}(\delta_0, \delta_1, \ldots, \delta_{n-1})$ be the number of solutions $[x_0, x_1, \ldots, x_{n-1}] \in \mathbb{F}_q^n$ of respectively Eq. (11) and Eq. (12). Based on the previous considerations, the differential characterestic has probability

$$\mathrm{Prob}(\delta \neq 0 \to \Delta) = \frac{\#_F(\delta_0, \delta_1, \ldots, \delta_{n-1}) \cdot \#_{F,H}(\delta_0, \delta_1, \ldots, \delta_{n-1})}{q^{2 \cdot n}} \,.$$

Usually, for generic function F, H and generic $\delta_0, \ldots, \delta_{n-1}$, the previous probability is of order $\mathcal{O}(q^{-2})$, since $\#_F(\delta_0, \delta_1, \ldots, \delta_{n-1}) \leq (\deg(F)-1) \cdot q^{n-1}$ and since $\#_{F,H}(\delta_0, \delta_1, \ldots, \delta_{n-1}) \leq \max\{\deg(H) - 1, \deg(F)\} \cdot q^{n-1}$. Note that this probability is in general *smaller* than the corresponding one previously given for the Lai-Massey schemes, due to the presence of the multiplication with F.

Besides that, the truncated differential corresponding to the case $z = 0$, that is,

$$(\delta_0, \delta_1, \ldots, \delta_{n-1}) \in \mathbb{F}_q^n \longrightarrow (\Delta \cdot \alpha_0, \Delta \cdot \alpha_1, \ldots, \Delta \cdot \alpha_{n-1}) \in \mathbb{F}_q^n$$

where $\Delta \in \mathbb{F}_q$ is *not* fixed, has probability

$$\mathrm{Prob}(\delta \neq 0 \to \Delta) = \frac{\#_F(\delta_0, \delta_1, \ldots, \delta_{n-1})}{q^n} \,.$$

Again, for a generic function F, this probability is of order $\mathcal{O}(q^{-1})$ (since $\#_F(\delta_0, \delta_1, \ldots, \delta_{n-1}) \leq (\deg(F) - 1)/q$), which is in general *smaller* than the corresponding one for Lai-Massey schemes. At the same time, there are some special cases, for which this probability could be close to 1. E.g., in the `Amaryllises` scheme proposed in Prop. 8, if $\delta_0 = \delta_1 = \ldots = \delta_{n-1} \in \mathbb{F}_q$, then the previous truncated differential has probability one (since $z = 0$ is always satisfied, as in the case of a generalized Lai-Massey scheme). As before, if $\alpha_i \neq \alpha_j$ for a certain $i, j \in \{0, 1, \ldots, n-1\}$, then it is not possible to extend such probability-1 truncated differential for more than a single round.

8.2 Algebraic Attacks

Similar conclusions proposed for the statistical attacks hold for the algebraic attacks as well. Here, we discuss two concrete advantages of the multiplication with the function F in the generalized `Amaryllises` schemes.

Meet-in-the-Middle Algebraic Attacks. As already pointed out, MitM algebraic attacks are not so efficient in the case in which the degree of the inverse scheme is much higher than the corresponding degree of the scheme itself (or vice-versa). All the proposed generalized `Amaryllises` schemes proposed in this paper satisfy this requirement. E.g., in the `Amaryllises` scheme proposed in Prop. 8, $x \mapsto x \cdot F(x)$ is evaluated in the forward direction versus $x \mapsto F(G^{-1}(x))$ in the backward one (where $G(x) \coloneqq x \cdot F(x)$). Similar scenario occurs for the (extended) contracting–`Amaryllises` scheme proposed in Prop. 9.

In the case of Lai-Massey schemes, the degree in inverse/backward direction could be either equal or bigger than the one in the forward direction (still, it is in general smaller than q for the usual value used in MPC/FHE/ZK protocols/applications – see Sect. 6 for more details about this). This fact could make a big difference when preventing backward or/and MitM algebraic attacks.

Gröbner Basis Attacks. This is not the only advantage of the multiplication with F in the generalized `Amaryllises` schemes. Consider e.g. the security against a Gröbner basis attack [Buc76], which allows to find solution(s) – if 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, and (iii) the degrees of the equations, besides other factors.

Let $[x_0, x_1, \dots, x_{n-1}] \mapsto [y_0, y_1, \dots, y_{n-1}]$ be the inputs and the outputs either of a generalized `Amaryllises` scheme or of a Lai-Massey one:

- a redundant Lai-Massey scheme can be described by the following system of equations:

$$\begin{cases} y_0 = \alpha_0 \cdot (x_0 + F(x_0, x_1, \dots, x_{n-1})) \ , \\ y_i \cdot \alpha_0 - y_0 \cdot \alpha_i = \alpha_0 \cdot \alpha_i \cdot (x_i - x_0) \qquad \forall i \in \{1, 2, \dots, n-1\} \, , \end{cases}$$

  that is, one non-linear equation of degree $\deg(F)$, and $n-1$ *linear* equations;

- the generalized `Amaryllises` scheme instantiated with $H = 0$ (that is, in the case in which H is identically equal to zero) can be described by the following system of equations:

$$\begin{cases} y_0 = \alpha_0 \cdot x_0 \cdot F\left(x_0, x_1, \dots, x_{n-1}\right) \ , \\ \alpha_0 \cdot y_i \cdot x_0 = \alpha_i \cdot x_i \cdot y_0 \qquad \forall i \in \{1, 2, \dots, n-1\} \, , \end{cases}$$

  that is, one non-linear equation of degree $1 + \deg(F)$, and $n-1$ *quadratic* ones;

- the generalized `Amaryllises` scheme can be described by the following system of equations:

$$\begin{cases} y_0 = \alpha_0 \cdot \left(x_0 \cdot F\left(x_0, x_1, \dots, x_{n-1}\right) + H\left(x_0, x_1, \dots, x_{n-1}\right)\right) \ , \\ \alpha_0 \cdot y_1 - \alpha_1 \cdot y_0 = \alpha_0 \cdot \alpha_1 \cdot (x_1 - x_0) \cdot F\left(x_0, x_1, \dots, x_{n-1}\right) \ , \\ \frac{(x_i - x_0) \cdot (\alpha_0 \cdot y_1 - \alpha_1 \cdot y_0)}{\alpha_1} = \frac{(\alpha_0 \cdot y_i - \alpha_i \cdot y_0) \cdot (x_1 - x_0)}{\alpha_i} \qquad \forall i \in \{2, 3, \dots, n-1\} \, , \end{cases}$$

  that is, two non-linear equations of degree $\max\{\deg(H), 1 + \deg(F)\}$ and $1 + \deg(F)$ respectively, and $n-2$ *quadratic* ones.

Since the number of variables is the same for the two schemes, it follows that the generalized `Amaryllises` scheme is naturally more resistant than the redundant Lai-Massey one with respect to Gröbner basis attacks.

A high-level comparison with the generalized Lai-Massey scheme is more difficult/complicated, since it is affected by the details of the functions $F^{(i)}$. Indeed, regarding the case of the generalized Lai-Massey scheme, it can be described by the following system of equations:

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

that is, *at most* n non-linear equations, each one of degree $\deg(F^{(i)})$. Hence, it could be potentially more resistant than the generalized `Amaryllises` scheme. However, by making use of the relation among the functions $F^{(i)}$, it is in general possible to heavily simplify such system of equations. E.g., the GLM-1_4 scheme proposed in Prop. 4 can be described by the following system of equations:

$$\begin{cases} y_0 = \alpha_0 \cdot (x_0 + F_1(x_0 - x_1) + F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \,, \\ \alpha_0 \cdot y_1 - \alpha_1 \cdot y_0 = \alpha_0 \cdot \alpha_1 \cdot (x_1 - x_0) \\ y_2 = \alpha_2 \cdot (x_2 + F_2(x_0 - x_1, x_2 - x_3) + F_3(x_0 - x_1, x_1 - x_2, x_2 - x_3)) \,, \\ \alpha_2 \cdot y_3 - \alpha_3 \cdot y_2 = \alpha_2 \cdot \alpha_3 \cdot (x_3 - x_2) \,, \end{cases}$$

that is, two non-linear equations and two linear equations, rather than four independent non-linear equations. Similar conclusion holds for GLM-1_n and GLM-2_n as well.

9 Summary and Future Directions

In this paper, we re-considered the Lai-Massey scheme originally proposed in [LM90, Vau99], proposing new generalizations that are not (extended) affine equivalent to any generalized Feistel scheme. Inspired by the recent `Horst` construction, we also present the `Amaryllises` scheme, in which the linear combination that takes place in the Lai-Massey construction is replaced by a non-linear one. In particular, we propose concrete instantiations of the `Amaryllises` scheme, and we discussed possible advantages and disadvantages with respect to other constructions proposed in the literature.

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

- check if the CCZ equivalence[9] [CCZ98, CP19] holds or not among (some of) the schemes presented in this paper;
- propose new generalizations of the Lai-Massey/`Amaryllises` scheme, and/or propose new concrete instantiations of the schemes presented in this paper;
- better understand the advantages and the disadvantages of a design instantiated with the non-linear invertible constructions proposed in this paper with respect to e.g. more traditional designs as the SPN/AES-like ones. (Note that our initial analysis proposed in this paper does not take into account the details of the functions/sub-components that instantiate the proposed constructions, besides e.g. the effect of a mixing linear/affine layer applied before or after them.)

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

Acknowledgments. The author thanks the FSE/ToSC'22 Reviewers for their valuable suggestions and comments. Lorenzo Grassi is supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA.

References

[AAB+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols. *IACR Trans. Symmetric Cryptol.*, 2020(3):1–45, 2020.

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

[Ada97] Carlisle M. Adams. Constructing Symmetric Ciphers Using the CAST Design Procedure. *Des. Codes Cryptogr.*, 12(3):283–316, 1997.

[AGP+19] Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. Feistel Structures for MPC, and More. In *Computer Security - ESORICS 2019*, volume 11736 of *LNCS*, pages 151–171, 2019.

[AGR+16] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity. In *Advances in Cryptology - ASIACRYPT 2016*, volume 10031 of *LNCS*, pages 191–219, 2016.

[AW21] Jack Allsop and Ian M. Wanless. Degree of orthomorphism polynomials over finite fields. *Finite Fields and Their Applications*, 75, 2021.

[BBC+22] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, and Vesselin Velichkov. Anemoi: Exploiting the Link between Arithmetization-Orientation and CCZ-Equivalence. Cryptology ePrint Archive, Paper 2022/840, 2022. https://eprint.iacr.org/2022/840.

[BCFN22] Ritam Bhaumik, André Chailloux, Paul Frixons, and María Naya-Plasencia. Safely Doubling your Block Ciphers for a Post-Quantum World. Cryptology ePrint Archive, Paper 2022/1342, 2022.

[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.

[BDKA21] Nicolas Bordes, Joan Daemen, Daniël Kuijsters, and Gilles Van Assche. Thinking Outside the Superbox. In *Advances in Cryptology - CRYPTO 2021*, volume 12827 of *LNCS*, pages 337–367, 2021.

[BDPA08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the Indifferentiability of the Sponge Construction. In *Advances in Cryptology - 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 *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *LNCS*, pages 450–466, 2007.

[BMT13] Thierry P. Berger, Marine Minier, and Gaël Thomas. Extended Generalized Feistel Networks Using Matrix Representation. In *Selected Areas in Cryptography - SAC 2013*, volume 8282 of *LNCS*, pages 289–305, 2013.

[BS90] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *Advances in Cryptology - 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.

[CGG+22] Carlos Cid, Lorenzo Grassi, Aldo Gunsing, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Influence of the Linear Layer on the Algebraic Degree in SP-Networks. *IACR Trans. Symmetric Cryptol.*, 2022(1):110–137, 2022.

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

[CPS08] Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin. The Random Oracle Model and the Ideal Cipher Model Are Equivalent. In *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *LNCS*, pages 1–20, 2008.

[CS22] Amit Kumar Chauhan and Somitra Sanadhya. Quantum Security of FOX Construction based on Lai-Massey Scheme. Cryptology ePrint Archive, Paper 2022/1001, 2022.

[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.

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

[DS16] Yuanxi Dai and John P. Steinberger. Indifferentiability of 8-Round Feistel Networks. In *Advances in Cryptology - CRYPTO 2016*, volume 9814 of *LNCS*, pages 95–120, 2016.

[GHR+22] Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang. A New Feistel Approach Meets Fluid-SPN: Griffin for Zero-Knowledge Applications. Cryptology ePrint Archive, Paper 2022/403, 2022. https://eprint.iacr.org/2022/403.

[GKR+21] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. In *USENIX Security 2021*. USENIX Association, 2021.

[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 *Advances in Cryptology - EUROCRYPT 2020*, volume 12106 of *LNCS*, pages 674–704, 2020.

[GOPS22] Lorenzo Grassi, Silvia Onofri, Marco Pedicini, and Luca Sozzi. Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$: Application to Poseidon. *IACR Transactions on Symmetric Cryptology*, 2022(3):20–72, 2022.

[GØSW22] Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, and Roman Walch. From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications. Cryptology ePrint Archive, Report 2022/342, 2022. https://ia.cr/2022/342.

[Gra22] Lorenzo Grassi. Weak Bijective Quadratic Functions over $\mathbb{F}_p^n$. Cryptology ePrint Archive, Paper 2022/1313, 2022. https://eprint.iacr.org/2022/1313.

[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 *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 613–630, 2010.

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

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

[LAAZ11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In *Advances in Cryptology - 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 *Advances in Cryptology – 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 *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 254–283, 2015.

[LP07] Gregor Leander and Axel Poschmann. On the Classification of 4 Bit S-Boxes. In *Arithmetic of Finite Fields – WAIFI 2007*, volume 4547 of *LNCS*, pages 159–176, 2007.

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

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

[MGWH22] Shuping Mao, Tingting Guo, Peng Wang, and Lei Hu. Quantum Attacks on Lai-Massey Structure. In *Post-Quantum Cryptography – PQCrypto 2022*, volume 13512 of *LNCS*, pages 205–229, 2022.

[MP03] Ueli M. Maurer and Krzysztof Pietrzak. The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations. In *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 544–561, 2003.

[MP13] Gary L. Mullen and Daniel Panario. *Handbook of Finite Fields*. Chapman & Hall/CRC, 1st edition, 2013.

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

[Pat98] Jacques Patarin. About Feistel Schemes with Six (or More) Rounds. In *Fast Software Encryption – FSE 1998*, volume 1372 of *LNCS*, pages 103–121, 1998.

[Pat01] Jacques Patarin. Generic Attacks on Feistel Schemes. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 222–238, 2001.

[RS22] Arnab Roy and Matthias Steiner. Generalized Triangular Dynamical System: An Algebraic System for Constructing Cryptographic Permutations over Finite Fields, 2022.

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

[SK96] Bruce Schneier and John Kelsey. Unbalanced Feistel Networks and Block Cipher Design. In *Fast Software Encryption – FSE 1996*, volume 1039 of *LNCS*, pages 121–144, 1996.

[SM10] Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the generalized feistel. In Seokhie Hong and Tetsu Iwata, editors, *Fast Software Encryption – FSE 2010*, volume 6147 of *LNCS*, pages 19–39, 2010.

[SS04] Taizo Shirai and Kyoji Shibutani. Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by Using Multiple MDS Matrices. In *Fast Software Encryption – FSE 2004*, volume 3017 of *LNCS*, pages 260–278, 2004.

[SSA+07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Blockcipher CLEFIA. In *Fast Software Encryption – FSE 2007*, volume 4593 of *LNCS*, pages 181–195, 2007.

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

[YI13] Shingo Yanagihara and Tetsu Iwata. Improving the Permutation Layer of Type 1, Type 3, Source-Heavy, and Target-Heavy Generalized Feistel Structures. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 96-A(1):2–14, 2013.

[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 *Advances in Cryptology – CRYPTO 1989*, volume 435 of *LNCS*, pages 461–480, 1990.

A About Generalized Feistel and Quasi–Feistel Schemes

A.1 Generalized Feistel Schemes

In this section, we show that any generalized Feistel scheme proposed in the literature is EA-equivalent to the generalized Feistel scheme proposed in Def. 2. In particular:

- a Type-I Feistel [ZMI90, Nyb96] is defined via $F_i(x_0, x_1, \dots, x_i) = 0$ for each $i \geq 1$ (while no condition on F_0). The EA-equivalence holds via the affine functions $A, B = I$ equal to the identity function, and $C = 0$;

- given functions $G_0, G_2, \dots, G_{\lfloor n/2 \rfloor}$ over $\mathbb{F}_q$, a Type-II Feistel [ZMI90,Nyb96] is defined via

$$F_i(x_0, x_1, \dots, x_i) = \begin{cases} G_i(x_i) & \text{if } i \text{ even (hence, } i \in \{0, 2, \dots, \lfloor n/2 \rfloor\}) \\ 0 & \text{otherwise} \end{cases} .$$

  The EA-equivalence holds via the affine functions $A, B = I$ equal to the identity function, and $C = 0$;

- given functions $G_0, G_1, \dots, G_{n-2}$ over $\mathbb{F}_q$, a Type-III Feistel [ZMI90,Nyb96] is defined via $F_i(x_0, x_1, \dots, x_i) = G_i(x_i)$ for each $i \in \{0, 1, 2, \dots, n-2\}$. The EA-equivalence holds via the affine functions $A, B = I$ equal to the identity function, and $C = 0$;

- the Feistel schemes analyzed and proposed in [SM10, YI13, AGP+19] are Type–II/–III Feistel schemes in which a final shuffle is applied. In such a case, the EA equivalence holds via the affine function $A = I$ equal to the identity function, an invertible shuffle permutation B, and $C = 0$;

- the Feistel schemes proposed by Bogdanov et al. [BS13] and by Berger et al. [BMT13] are generalizations of Type–II/–III Feistel schemes where (i) the functions F_i are of the form

$$F_i(x_0, x_1, \dots, x_i) = \sum_{j=0}^{i} G_{i,j}(x_j)$$

  for functions $G_{i,j}$ defined over $\mathbb{F}_q$, and where (ii) a final shuffle is applied. As before, the EA equivalence holds via the affine function $A = I$ equal to the identity function, an invertible shuffle permutation B, and $C = 0$;

- given a function G over $\mathbb{F}_q$, an expanding Feistel [SK96, HR10] is defined via $F_i(x_0, x_1, \dots, x_i) = G(x_0)$ for each $i \geq 1$. The EA-equivalence holds via the affine functions $A, B = I$ equal to the identity function, and $C = 0$;

- given $G : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$, a contracting Feistel [SK96, HR10] is defined via

$$F_i(x_0, x_1, \ldots, x_i) = \begin{cases} G(x_0, x_1, \ldots, x_{n-2}) & \text{if } i = n-2 \\ 0 & \text{otherwise} \end{cases}.$$

  The EA-equivalence holds via the affine functions $A, B = I$ equal to the identity function, and $C = 0$;

- in a SP–type Feistel [SS04, BS13], the round function of the Feistel scheme is instantiated via a SPN construction, as e.g. in the case of the block cipher CLEFIA [SSA+07]. Let $n = 2 \cdot n'$ be an even integer. In such a case, the functions F_i are of the form

$$F_i(x_0, x_1, \ldots, x_i) = \begin{cases} 0 & \text{if } i < n/2 \\ G_i(x_0, x_1, \ldots, x_{n/2-1}) & \text{otherwise} \end{cases}$$

  for particular functions $G_{n/2}, \ldots, G_{n-1}$ over $\mathbb{F}_q^{n/2}$ corresponding to a SPN construction. Moreover, the shuffle is of the form $[x_0, \ldots, x_{n'-1}, x_{n'}, \ldots, x_{n-1}] \mapsto [x_{n'}, \ldots, x_{n-1}, x_0, \ldots, x_{n'-1}]$ instead of $[x_0, x_1, \ldots, x_{n-1}] \mapsto [x_1, \ldots, x_{n-1}, x_0]$. The EA equivalence holds via the affine function $A = I$ equal to the identity function, an invertible shuffle permutation B, and $C = 0$.

A.2 Quasi-Feistel Schemes

Let $q = p^s$ for a prime $p \geq 2$ and for a positive integer $s \geq 1$, and let $n \geq 2$. Let $\Gamma : \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ be a combiner function. When both the last $\mathbb{F}_q^{n-1}$-input and one of the first two $\mathbb{F}_q$–inputs are fixed, such function is assumed to be a permutation over $\mathbb{F}_q$. Let P, P' be two permutations over $\mathbb{F}_q^n$. Let $F_0, F_1, \ldots, F_{r-1} : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ be $r \geq 1$ generic functions. Following [YPL11, Def. 2], a scheme $\mathcal{QF}$ is a Quasi-Feistel scheme over $\mathbb{F}_q^n$ if and only if it is defined as $\mathcal{QF}(x_0, x_1, \ldots, x_{n-1}) \coloneqq y_r \| y_{r+1} \| \ldots \| y_{r+n-1}$, where

- $P(x_0, x_1, \ldots, x_{n-1}) = x'_0 \| x'_1 \| \ldots \| x'_{n-1}$;
- for each $0 \leq i \leq n + r - 1$:

$$y'_i \coloneqq \begin{cases} x'_i & \text{if } i \leq n-1\,, \\ \Gamma\left(y'_{i-1}, F_{i-n}(y'_{i-n}, y'_{i+1-n}, \ldots, y'_{i-2}), [y'_{i-n}, y'_{i+1-n}, \ldots, y'_{i-2}]\right) & \text{otherwise}\ ; \end{cases}$$

- $P'(y'_0, y'_1, \ldots, y'_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$.

(We point out that the "combiner" definition can be actually simplified by removing the second input.)

A quasi-Feistel scheme reduces to a Feistel scheme or to a Lai-Massey scheme for a proper choice of Γ, P and P'.

B Invariant Subspaces: the Solution proposed in [Vau99]

Here, we briefly discuss the solution proposed in [Vau99] (and recently re-considered in [AC21]) for breaking the invariant subspace trail of the Lai-Massey construction. For simplicity, we focus on the case $\mathbb{F}_q^2$ only. Instead of working with a linear map that mixes the entire state, Vaudenay proposed to apply a partial non-linear layer, that is, to work with

$$[x_0, x_1] \to [y_0, y_1] \coloneqq [S(x_0 + H(x_0 - x_1)), x_1 + H(x_0 - x_1)] \tag{13}$$

for a certain function $S : \mathbb{F}_q \to \mathbb{F}_q$. In such a case, the invariant subspace is always broken if S is an *orthomorphism* (a function S is an orthomorphism if and only if both S and $S'(x) \coloneqq S(x) - x$ are permutations[10]).

This follows from the following fact. The invariant subspace for the Lai-Massey construction over $\mathbb{F}_q^2$ is $\mathfrak{X} = \langle [1,1] \rangle$. By applying (13), we get $[x + \varphi_0, x + \varphi_1] \mapsto [S(x + \varphi_0 + H(\varphi_0 - \varphi_1)), x + \varphi_1 + H(\varphi_0 - \varphi_1)]$, for some constants $\varphi_0, \varphi_1 \in \mathbb{F}_q$. The condition

$$[S(x + \varphi_0 + H(\varphi_0 - \varphi_1)), x + \varphi_1 + H(\varphi_0 - \varphi_1)] \in \mathfrak{X} + [\psi_0, \psi_1]$$

for certain $\psi_0, \psi_1 \in \mathbb{F}_q$ is satisfied if and only if

$$\forall x \in \mathbb{F}_q : \qquad S(x + \varphi_0 + H(\varphi_0 - \varphi_1)) = x + \varphi_1 + H(\varphi_0 - \varphi_1) + \psi_1 - \psi_0 \,,$$

that is,

$$\forall x \in \mathbb{F}_q : \qquad S'(x + \varphi_0 + H(\varphi_0 - \varphi_1)) = \varphi_1 - \varphi_0 + \psi_1 - \psi_0 \tag{14}$$

where $S'(x) \coloneqq S(x) - x$. If S is an orthomorphism (which implies that S' is a permutation), then the previous condition is never satisfied.

As a concrete example, the equality (14) is never satisfied when choosing the linear function $S(x) = \sigma \cdot x$ for a certain $\sigma \in \mathbb{F}_q \setminus \{0, 1\}$. This corresponds to apply a multiplication after (2) with the matrix

$$\mathrm{diag}(\sigma, 1) \equiv \begin{bmatrix} \sigma & 0 \\ 0 & 1 \end{bmatrix} ,$$

which does not admit $\langle [1,1] \rangle$ as invariant subspace.

We conclude by pointing out that the condition "S is an orthomorphism" is not strictly necessary *if* one only aims to destroy the invariant subspace trails, in the sense that a weaker assumption on S is usually sufficient for such a goal. E.g., such a result can be usually achieved by working with a non-linear invertible function S (which is not an orthomorphism in general).

EA-Equivalence between the Lai-Massey Scheme defined in [Vau99] and a 2-round Feistel Scheme. As last thing, we prove that the Lai-Massey scheme defined in (13) is EA-equivalent to 2-round Feistel instantiated with H and S over $\mathbb{F}_q$ as round functions, that is,

$$[x_0, x_1] \mapsto [x_0 + H(x_1), x_1 + S(x_0 + H(x_1))] \,.$$

The EA-equivalent is defined by the following linear matrices $A, B, C \in \mathbb{F}_q^{2\times 2}$:

$$A = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} , \qquad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} , \qquad C = \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} ,$$

where A and B are invertible. Indeed:

$$\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \xrightarrow{A\times\cdot} \begin{bmatrix} x_0 \\ x_0 - x_1 \end{bmatrix} \xrightarrow{\text{2-round Feistel} \circ} \begin{bmatrix} x_0 + H(x_0 - x_1)) \\ x_0 - x_1 + S(x_0 + H(x_0 - x_1)) \end{bmatrix}$$
$$\xrightarrow{B\times\cdot} \begin{bmatrix} x_0 - x_1 + S(x_0 + H(x_0 - x_1)) \\ x_0 + H(x_0 - x_1)) \end{bmatrix} \xrightarrow{+C\times x} \begin{bmatrix} S(x_0 + H(x_0 - x_1)) \\ x_1 + H(x_0 - x_1)) \end{bmatrix} .$$

[10] Obviously, the identity map is never an orthomorphism. We point out that a non-linear orthomorphism has usually high (e.g., almost maximum) degree – see e.g. [AW21].

C Details for Sect. 4.3 – Contracting Feistel

Here we show that

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

is again the identity matrix. Indeed, by re-writing Eq. (4), we get

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

that is,

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

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,

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

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

D Details and Example for Sect. 5.3

D.1 Proof of Theorem 5 for the Case $\mathbb{F}_p^2$

In this section, we prove Theorem 5 in details for the case $\mathbb{F}_p^2$. Based on the result given in Prop. 7, consider the generalized Lai-Massey scheme

$$[x_0, x_1] \mapsto [y_0, y_1] = \left[x_0 + \beta \cdot (x_0 - x_1)^2 \cdot (x_0 + x_1), x_1 + \beta \cdot (x_0 - x_1)^2 \cdot (x_0 + x_1)\right]$$

over $\mathbb{F}_p^2$ for $p \geq 3$, where $L_p(-2 \cdot \beta) = -1$, where $G(x) = x$ is the identity function (the following argument holds for any function G), and where $\lambda_0 = \psi_0 = \psi_1 = 1$ and $\lambda_1 = -1$. There are *no* affine transformations A, B, C over $\mathbb{F}_p^2$ (with the conditions

that A, B are invertible) for which such generalized Lai-Massey scheme is EA-equivalent to any generalized Feistel scheme over $\mathbb{F}_p^2$. In order to prove this result, we try to construct the affine transformations A, B, C (where A and B are invertible) for which the previous generalized Lai-Massey scheme would be EA-equivalent to the Feistel scheme $[x_1 + F(x_0), x_0]$. Let $A, B : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ be defined as

$$A(x_0, x_1) = \begin{bmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} a'_0 \\ a'_1 \end{bmatrix}, \qquad B(x_0, x_1) = \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} b'_0 \\ b'_1 \end{bmatrix}.$$

If the EA-equivalence holds, the following equality must be satisfied:

$$\begin{aligned} x_1 + F(x_0) = x_0 \cdot (b_{0,0} \cdot a_{0,0} + b_{0,1} \cdot a_{1,0} + c_{0,0}) + x_1 \cdot (b_{0,0} \cdot a_{0,1} + b_{0,1} \cdot a_{1,1} + c_{0,1}) + (b_{0,0} + b_{0,1}) \\ \cdot \beta \cdot ((a_{0,0} - a_{1,0}) \cdot x_0 + (a_{0,1} - a_{1,1}) \cdot x_1)^2 \cdot ((a_{0,0} + a_{1,0}) \cdot x_0 + (a_{0,1} + a_{1,1}) \cdot x_1), \\ x_0 = x_0 \cdot (b_{1,0} \cdot a_{0,0} + b_{1,1} \cdot a_{1,0} + c_{1,0}) + x_1 \cdot (b_{1,0} \cdot a_{0,1} + b_{1,1} \cdot a_{1,1} + c_{1,1}) + (b_{1,0} + b_{1,1}) \\ \cdot \beta \cdot ((a_{0,0} - a_{1,0}) \cdot x_0 + (a_{0,1} - a_{1,1}) \cdot x_1)^2 \cdot ((a_{0,0} + a_{1,0}) \cdot x_0 + (a_{0,1} + a_{1,1}) \cdot x_1). \end{aligned}$$

The first equality holds only in the case in which the non-linear part in the r.h.s. depends only on x_0. This fact occurs only if $a_{0,1} - a_{1,1} = a_{0,1} + a_{1,1} = 0$, which obviously imply $a_{0,1} = a_{1,1} = 0$. However, in such a case, A is not invertible anymore.

Note that the components a'_0, a'_1, b'_0, b'_1 would not change the result just given. Moreover, C does not play any role, since it would only impact the linear part. This implies that the EA-equivalence does *not* hold, as stated before.

D.2 Another Redundant Lai-Massey Scheme *Not* Belonging into the "Feistel EA-Class"

Here we propose another example of a redundant Lai-Massey scheme that is not EA-equivalent to any generalized Feistel scheme.

Lemma 9 (RLM-2)**.** *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 $l \in \{1, 2, \ldots, n-1\}$. For each $i \in \{0, 1, \ldots, l-1\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)} \in \mathbb{F}_q$ be as in Prop. 2 (in particular, such that $\sum_{j=0}^{m-1} \lambda_j^{(i)} = 0$). Let $\psi_0, \psi_1, \ldots, \psi_{n-1} \in \mathbb{F}_p$ be such that $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$. Let $\beta \in \mathbb{F}_p$ be such that $L_p(\beta) = -1$. Let $G : \mathbb{F}_p^{n-1} \to \mathbb{F}_p$ be any function, and let $H : \mathbb{F}_p \to \mathbb{F}_p$ be a permutation.*

The redundant Lai-Massey scheme over $\mathbb{F}_p^n$ defined as RLM-2$(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where

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

and where

$$z \coloneqq G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot x_j \right)$$

is invertible.

Proof. First of all, note that $z^2 = \beta$ is never possible, since $L_p(z^2) = 1$ while $L_p(\beta) = -1$ by assumption.

Similar to before, we have that $\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j = \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot y_j / \alpha_j$ for each $i \in \{0, 1, \ldots, l-1\}$, which implies that

$$z = G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot \frac{y_j}{\alpha_j}, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot \frac{y_j}{\alpha_j}, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(l-1)} \cdot \frac{y_j}{\alpha_j} \right).$$

It follows that

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

noting that (i) $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$, $z^2 \neq \beta$ by assumption, and that (ii) H is invertible. As a result, the entire scheme is invertible. □

The fact that such scheme is not EA-equivalent to any generalized Feistel scheme follows from Theorem 5 as before.

E Examples via Dickson Polynomial

In this section, we recall the Dickson polynomials, and we exploit them to construct some examples for the functions proposed in this paper.

Theorem 7 ([MP13]). *Let $d \geq 1$ be a positive integer, and let $q = p^s$, where $p \geq 2$ is a prime and s is a positive integer. Given $\alpha \in \mathbb{F}_q$, the Dickson polynomial $\mathcal{D}_{d,\alpha}$ defined as*

$$\mathcal{D}_{d,\alpha}(x) \coloneqq \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i}\binom{d-i}{i}(-\alpha)^i x^{d-2i}$$

is invertible if and only if $\gcd(d, q^2 - 1) = 1$.

We recall that $\mathcal{D}_{d,0}(x) = x^d$, and $\mathcal{D}_{1,\alpha}(x) = x$, $\mathcal{D}_{2,\alpha}(x) = x^2 - 2 \cdot \alpha$, and $\mathcal{D}_{d+1,\alpha}(x) \coloneqq x \cdot \mathcal{D}_{d,\alpha}(x) - \alpha \cdot \mathcal{D}_{d-1,\alpha}(x)$ for all $d \geq 2$. Note that $\mathcal{D}_{d,\alpha}$ only contains monomials of even degree if d is even, and only monomials of odd degree if d is odd.

Lemma 10. *Let $q = p^s$, where $p \geq 2$ is a prime and $s \geq 1$. Let $\alpha \in \mathbb{F}_q \setminus \{0\}$, and let $d = 2d' + 1 \geq 3$ be an odd integer such that* $\gcd(d, q^2 - 1) = 1$. *The function F defined as*

$$F(x) = \sum_{j=0}^{\lfloor d/2 \rfloor} \frac{d}{d-j} \cdot \binom{d-j}{j} \cdot (-\alpha)^j \cdot x^{d-2j-1} = \begin{cases} \frac{\mathcal{D}_{d,\alpha}(x)}{x} & \text{if } x \neq 0\,, \\ d \cdot (-\alpha)^{\lfloor d/2 \rfloor} & \text{otherwise} \end{cases} \tag{15}$$

satisfies the requirements of Prop. 8.

Proof. Since d is an odd integer, then $\mathcal{D}_{d,\alpha}(x)$ is defined as a sum of monomials of odd degrees (hence, each monomial is divisible for x, that is, $\mathcal{D}_{d,\alpha}(x)$ does not contain any monomial of degree 0). In order to prove the result, it is sufficient to note that (i) $F(0) = \frac{d}{\lceil d/2 \rceil} \cdot \binom{\lceil d/2 \rceil}{\lfloor d/2 \rfloor} \cdot (-\alpha)^{\lfloor d/2 \rfloor} = d \cdot (-\alpha)^{\lfloor d/2 \rfloor} \neq 0$ (since $\alpha \neq 0$) and that (ii) $x \mapsto x \cdot F(x) = \mathcal{D}_{d,\alpha}(x)$ is invertible by assumption. □

Lemma 11. *Let $q = p^s$ for a prime $p \geq 2$ and a positive integer $s \geq 1$. Let $d \geq 3$ be an odd integer such that* $\gcd(d, q^2 - 1) = 1$, *let $d' = d - 1$ (and so $e = 1$), and let $\alpha \neq 0$. The function $F : \mathbb{F}_q^2 \to \mathbb{F}_q$ defined as*

$$F(x_0, x_1) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i}\binom{d-i}{i}(-\alpha)^i \cdot x_0^{d-2i-1} \cdot x_1^i$$

satisfies the assumptions of Prop. 11.

Proof. Similar to before:

- if $x_1 = 0$, then $F(x_0, 0) = x_0^{d-1}$, which is equal to zero if and only if $x_0 = 0$;
- if $x_1 \neq 0$, let $z := x_0/x_1$, and note that

$$F(z, x_1) = x_1^{d-1} \cdot \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-\alpha)^i \cdot z^{d-2i-1} = x_1^{d-1} \cdot \frac{\mathcal{D}_{d,\alpha}(z)}{z} \,,$$

  where $\mathcal{D}_{d,\alpha}$ is the Dickson polynomial. The equality $F(z, x_1) = 0$ holds if and only if $\mathcal{D}_{d,\alpha}(z) = 0$ and $z \neq 0$. By assumption on d, the Dickson polynomial $D_{d,\alpha}$ is a permutation, and it is equal to zero if and only if $z = 0$ (since d is odd), which is however excluded.

As a result, $F(x_0, x_1) = 0$ if and only if $[x_0, x_1] = [0, 0]$. □