On Generalizations of the Lai–Massey Scheme: the Birth 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 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 `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 Lai–Massey · 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 or/and of 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 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. The motivations of this fact can be multiple, but they certainly include 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 `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 Generalized 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 this form is (extended) *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-computed with an affine invertible transformation. In particular, we show that $r \geq 2$ Lai–Massey consecutive rounds are equal to r generalized Feistel consecutive rounds in which no swapping of the components takes place (besides an initial and a final affine transformation). This fact implies the existence of invariant subspaces in Lai–Massey schemes, already found in [Vau99].

As next step, in Sect. 5, we generalize the Lai–Massey scheme just discussed. Instead of limiting ourselves to consider a function which takes linear combinations of the sub-blocks with the zero-sum condition on the coefficients as inputs, we allow for *any function F for which the entire construction is invertible.* (A formal definition is given in Def. 6.) Working over a prime field $\mathbb{F}_p^n$ for $p \geq 3$, we show concrete examples of invertible generalized Lai–Massey schemes 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 *not* zero. The simplest example of this is given by

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

over $\mathbb{F}_p^2$ for $p \geq 3$ 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 that the obtained invertible generalized Lai–Massey scheme is *not* affine

equivalence to any generalized Feistel scheme. To the best of our knowledge, this is the first example in the literature of a generalized Lai–Massey scheme that cannot be reduced to a generalized Feistel scheme.

The `Amaryllises` Construction

Let $\mathbb{F}_q$ be a field. Based on our (informal) definition just given, a function $\mathcal{LM}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ (where $\cdot\|\cdot$ denotes concatenation) is a generalized Lai–Massey scheme if

- there exists a certain function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ such that

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

- it is invertible.

Natural question arise: why should we limit ourselves to define each output y_i as a linear combination of the input x_i and of the output of the function $F(x_0, x_1, \ldots, x_{n-1})$? Is it possible to consider non-linear combinations without loosing the invertibility condition?

Grassi et al. [GHR+22] recently faced a similar challenge in the case of Feistel schemes. The result of their analysis is the `Horst` construction, 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 such scheme holds under the condition that G never returns zero. 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

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

for two functions $G, F : \mathbb{F}_q^n \to \mathbb{F}_q$. We call this new construction as (generalized) `Amaryllises`.[1] In Sect. 6 and in Sect. 7, we formalize it by showing that such construction can be invertible in the case in which the functions G and F satisfy some particular (non-trivial) conditions. Besides that, in there:

- we show how to construct functions F, G with *low-multiplicative complexity* that satisfy such conditions. 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, G that satisfy the required conditions by using an exhaustive approach. However, this strategy immediately fails when q is very large, e.g., $q \geq 2^{64}$, 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, G that satisfy the required conditions and that are easy to compute (hence, with a simple algebraic expression) becomes crucial;
- we discuss the advantages (and the possible disadvantages) of this new `Amaryllises` construction with respect to the ones already present in the literature in terms of efficiency and security, with particular attention with the Lai–Massey scheme and with the `Horst` one.

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.

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

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

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

Power Maps and Dickson Polynomial. Well known examples of invertible functions over $\mathbb{F}_q$ include the power maps and the Dickson polynomials:

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 $x \mapsto x^d$ is invertible if and only if $\gcd(d, q-1) = 1$;*
- *given $\alpha \in \mathbb{F}_q$, the Dickson polynomial $\mathcal{D}_{d,\alpha}$ defined as*

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

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

The Legendre Symbol. Here we recall some properties of the Legendre symbol used in the following.

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

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

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

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

Particular identities include:

- $L_p(-1) = 1$ if $p = 1 \mod 4$, while $L_p(-1) = -1$ if $p = 3 \mod 4$;
- $L_p(-3) = 1$ if $p = 1 \mod 3$, while $L_p(-3) = -1$ if $p = 2 \mod 3$;
- $L_p(2) = 1$ if $p = 1, 7 \mod 8$, while $L_p(2) = -1$ if $p = 3, 5 \mod 8$.

3 Related Works 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

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

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 $j \in \{0, 1\}$.

Lai–Massey Schemes over $\mathbb{F}_q^{\geq 2}$ from [GØSW22]. The most natural generalization of the Lai–Massey construction over $\mathbb{F}_q^n$ for $n \geq 2$ has been recently proposed in [GØSW22].

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 $l \in \{1, 2, \ldots, n-1\}$. 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 such that $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$ and $[\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)}] \neq [0, 0, \ldots, 0]$. Let $F : \mathbb{F}_q^l \to \mathbb{F}_q$ be any function. The Lai–Massey function $\mathcal{LM}$ over $\mathbb{F}_q^n$ defined as $\mathcal{LM}(x_0, x_1, \ldots, x_{n-1}) := y_0 \| y_1 \| \ldots \| y_{n-1}$ where*

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

is invertible.

As for the case of the Lai–Massey scheme over $\mathbb{F}_q^2$, the invertibility follows from the fact that

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

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. In particular, even if not strictly necessary, it makes sense to choose 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.

Invariant Subspace Trails. As already pointed out by Vaudenay in [Vau99] for the $\mathbb{F}_q^2$ case, there exists an invariant subspace for the Lai–Massey construction proposed in Prop. 2. We refer to [LAAZ11, LMR15, GRR16] for a formal definition of (invariant) subspace trails. We limit ourselves to recall the following definition.

Definition 3 ([GRR16])**.** Given q, n as before, let $\mathfrak{U}_0, \ldots, \mathfrak{U}_r \subseteq \mathbb{F}_q^n$ be $r+1$ subspace. $(\mathfrak{U}_0, \ldots, \mathfrak{U}_r)$ is a subspace trail of length $r \geq 1$ for a function F over $\mathbb{F}_q^n$ if (1st) $\dim(\mathfrak{U}_i) \leq \dim(\mathfrak{U}_{i+1}) < n$ for each $i \in \{0, 1, \ldots, r-1\}$ and (2nd) 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 $F(\mathfrak{U}_i + \varphi_i) := \{F(x) \mid \forall x \in \mathfrak{U}_i + \varphi_i\} \subseteq \mathfrak{U}_i + \varphi_{i+1}$. We say that it is an *invariant* subspace trail if $\mathfrak{U}_i = \mathfrak{U}_j$ for each $i, j \in \{0, 1, \ldots, r\}$.

The Lai–Massey construction $\mathcal{LM}$ defined as in Prop. 2 over $\mathbb{F}_q^n$ admits

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

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

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

Indeed, given $x \in \mathfrak{X} + \varphi$, we have that

$$\forall i \in \{0,1,\dots,n-1\} : \qquad y_i = x_i + \underbrace{F(0,0,\dots,0)}_{\text{constant}},$$

which means that only the coset is changed, while the subspace itself is not affected.

Independently of the values of $\lambda_j^{(i)}$, the subspace $\mathfrak{X}$ for the Lai–Massey construction proposed in Prop. 2 is never an empty set.

Lemma 1. $\langle [1,1,\dots,1] \rangle \subseteq \mathfrak{X}$. *Hence,* $\dim(\mathfrak{X}) \geq 1$.

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 particular: $\dim(\mathfrak{X}) = n - \dim(\langle [\lambda_0^{(0)}, \lambda_1^{(0)}, \dots, \lambda_{n-1}^{(0)}], \dots, [\lambda_0^{(l-1)}, \lambda_1^{(l-1)}, \dots, \lambda_{n-1}^{(l-1)}] \rangle)$, which is equal to $n-l$ if the previous vectors are linearly independent.

In order to break such invariant subspace, in [GØSW22], 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 maximum degree n and if it is irreducible. By making used of a similar approach, it is also possible to defeat other similar 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.

Before going on, we point out that it is possible to break the subspace trail of $\mathcal{LM}$ even if 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). Moreover, we note that it is not necessary to instantiate all the rounds with the same matrix M in order to break a subspace trail (see e.g. [GSW+21] for more details). Finally, in App. A, we briefly discuss the solution proposed in [Vau99] for breaking the 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 show that the Lai–Massey scheme over $\mathbb{F}_q^n$ proposed in Prop. 2 is extended-affine equivalent to a generalized Feistel scheme.

4.1 Preliminary: EA-Equivalence and Generalized Feistel Schemes

First, we introduce the definition of extended-affine equivalence and the one of generalized Feistel scheme.

EA-Equivalence. Two functions F and G are EA-equivalent if they are equivalent pre- and post-computed with affine transformations (besides the addition with an affine function).

Definition 4 (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

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

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

Definition 5 (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

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

where

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

The inveritiblity of the entire construction is independent of the details of $F_0, F_1, \ldots, F_{n-2}$. Indeed, $x_0 = y_{n-1}$, and for each $i \geq 1$, given y_{i-1} and given $x_0, x_1, \ldots, x_{i-1}$, we have that $x_i = y_{i-1} - F_i(x_0, x_1, \ldots, x_{i-1})$.

We highlight that any generalized Feistel scheme proposed in the literature is EA-equivalent to the generalized Feistel scheme just proposed. In particular:

- a Type-I Feistel [ZMI90, Nyb96] is defined via $F_i(x_0, x_1, \ldots, x_i) = 0$ 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 $G_0, G_2, \ldots, G_{\lfloor n/2 \rfloor}$ over $\mathbb{F}_q$, a Type-II Feistel [ZMI90,Nyb96] is defined via

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

  The EA-equivalence holds via the affine functions $A, B = I$ equal to the identity function, and $C = 0$;
- given functions $G_0, G_1, \ldots, G_{n-2}$ over $\mathbb{F}_q$, a Type-III Feistel [ZMI90,Nyb96] is defined via $F_i(x_0, x_1, \ldots, x_i) = G_i(x_i)$ for each $i \in \{0, 1, 2, \ldots, n-2\}$. 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
$$F_i(x_0, x_1, \dots, x_i) = \begin{cases} G(x_0, x_1, \dots, x_{n-2}) & \text{if } i = n-2 \\ 0 & \text{otherwise} \end{cases}.$$
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
$$F_i(x_0, x_1, \dots, x_i) = \begin{cases} 0 & \text{if } i < n/2 \\ G_i(x_0, x_1, \dots, x_{n/2-1}) & \text{otherwise} \end{cases}$$
for particular functions $G_{n/2}, \dots, G_{n-1}$ over $\mathbb{F}_q^{n/2}$ corresponding to a SPN construction. Moreover, the shuffle is of the form $[x_0, \dots, x_{n'-1}, x_{n'}, \dots, x_{n-1}] \mapsto [x_{n'}, \dots, x_{n-1}, x_0, \dots, x_{n'-1}]$ instead of $[x_0, x_1, \dots, x_{n-1}] \mapsto [x_1, \dots, x_{n-1}, x_0]$. The EA equivalence holds via the affine function $A = I$ equal to the identity function, an invertible shuffle permutation B, and $C = 0$.

4.2 EA-Equivalence between the Lai–Massey Schemes and the Generalized Feistel Ones

Here, we prove the EA-equivalence between the Lai–Massey scheme over $\mathbb{F}_q^n$ proposed in Prop. 2 and the generalized Feistel scheme.

Proposition 3. *Let $q = p^s$ where $p \geq 2$ is a prime and $s \geq 1$ is a positive integer, and let $n \geq 2$. The Lai–Massey scheme over $\mathbb{F}_q^n$ defined as in Prop. 2 is EA-equivalent to the generalized Feistel scheme defined in Def. 5.*

In particular, we prove the following.

Proposition 4. *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 $r \geq 2$, r Lai–Massey rounds defined as in Prop. 2 are equal to r Feistel rounds in which no swapping/shuffle takes place (besides an initial and a final linear combination).*

The proof is proposed in the following. We study the case $n = 2$ from the case $n \geq 2$ separately. The proof reduces to find the affine transformations A, B, C for which the EA-equivalence holds. Since we only deal with linear (invertible) transformations for $A, B : \mathbb{F}_q^n \to \mathbb{F}_q^n$, we simply identify them with the corresponding matrices in $\mathbb{F}_q^{n \times n}$. Moreover, C is always equal to 0 in the following.

4.2.1 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 EA-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 basically a Feistel construction pre-composed and post-composed with two invertible linear functions.

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

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

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

$$\hat{M} := A \times (B \times \mathrm{circ}(0, 1))\,.$$

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 equal 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 active the function F in the Feistel construction $\mathcal{F}'$), as already pointed out in the previous section.

About "Quasi-Feistel" Schemes. For completeness, we point out that this result 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. The result just proposed pointed out the relation between Feistel and Lai–Massey schemes in a much easier and clearer way, by showing that they are EA-equivalent.

4.2.2 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, (1st) 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, and (2nd) 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.

1st Case: EA-Equivalent to Type-I Feistel. Let's start by considering a Lai–Massey scheme over $\mathbb{F}_q^n$ as proposed in Prop. 2 for $l = 1$ instantiated with $F : \mathbb{F}_q \to \mathbb{F}_q$, that is, $x_i \mapsto y_i = x_i + F\left(\sum_{j=0}^{n-1} \lambda_j \cdot x_j\right)$ for each $i \in \{0, 1, \dots, n-1\}$, where $\lambda_0, \lambda_1, \dots, \lambda_{n-1} \in \mathbb{F}_q$ satisfy $\sum_{i=0}^{n-1} \lambda_i = 0$. W.l.o.g., let's assume $\lambda_0 \neq 0$.[2]

The analyzed Lai–Massey scheme is EA-equivalent to a Type-I Feistel scheme $\mathcal{F}_I$ over $\mathbb{F}_q^n$ defined as $[x_0, x_1, x_2 \dots, x_{n-1}] \mapsto [x_1 + F(x_0), x_2, \dots, x_{n-1}, x_0]$ via the invertible linear transformations

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

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 equal to r Type-I Feistel rounds in which no swapping takes place, besides an initial and a final linear combination. This follows from the fact that

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

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

2nd Case: EA-Equivalent to Contracting Feistel. 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, $x_i \mapsto y_i = x_i + F\big(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \dots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\big)$ for each $i \in \{0, 1, \dots, n-1\}$, 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 $i \in \{0, 1, \dots, n-2\}$;

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

First of all, we point out the following.

[2] 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 $j = i$).

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

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

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

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

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

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

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

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

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 the sum of its rows is equal to the zero vector (due to the condition on $\lambda_i^{(j)}$), or equivalently, the sum of each column is equal to zero. Since the right-hand side (r.h.s.) vector satisfies the same zero sum, the previous system of linear equations reduces to

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

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

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

transformations

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

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

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

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

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

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

Not surprisingly, r Lai–Massey rounds are equal to r contracting Feistel rounds in which no swapping takes place, besides an initial and a final linear combination. As proved in App. B, this follows from the fact that

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

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

5 A New Generalization of the Lai–Massey Construction

The main feature of a Lai–Massey construction $[x_0, x_1, \dots, x_{n-1}] \mapsto [y_0, y_1, \dots, y_{n-1}]$ regards the fact that the difference of two outputs $y_i - y_j$ is always equal to the difference of two inputs $x_h - x_l$ for each $i, j, h, l \in \{0, 1, \dots, n-1\}$, that is, $y_i - y_j = x_h - x_l$ (with the only condition that $h = l$ if and only if $i = j$ – note that $(i, j) = (h, l)$ is *not* required). This is related to the fact that each output y_i is defined as the sum of the corresponding input x_i and of a certain element $z = F(x_0, x_1, \dots, x_{n-1})$, that is, $y_i = x_i + z$ where z is fixed for each $i \in \{0, 1, \dots, n-1\}$. However, in the original Lai–Massey construction, the element z (and so the function F) must be of a particular form in order to guarantee the inveritibility.

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

Definition 6. Let $q = p^s$ for $p \geq 2$ being a prime and $s \geq 1$ an integer, and let $n \geq 2$. Given a function $F : \mathbb{F}_q^n \to \mathbb{F}_q$, let $\mathcal{LM}_{\mathrm{G}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be defined as $\mathcal{LM}_{\mathrm{G}}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| y_2 \| \ldots \| y_{n-1}$ where

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

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.

The crucial point is that there exist generalized 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 $x_0, x_1, \ldots, x_{n-1}$ so that the sum of the coefficients that define the linear combination is zero), as the one given in the next example.

Lemma 3. *Let $q = p^s$ for $p \geq 2$ being a prime and $s \geq 1$ an integer, and let $n \geq 2$. Let $\mu_0, \mu_1, \ldots, \mu_{n-1} \in \mathbb{F}_q$ be such that $\sum_{i=0}^{n-1} \mu_i \neq 0$. Let $H : \mathbb{F}_q \to \mathbb{F}_q$ be a permutation. The generalized Lai–Massey scheme over $\mathbb{F}_q^n$ defined as $[x_0, x_1, \ldots, x_{n-1}] \mapsto [y_0, y_1, \ldots, y_{n-1}]$ where*

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

is invertible.

Proof. By simple computation:

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

since H is invertible. Hence:

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

The proposed scheme is EA-equivalent to a contracting Feistel scheme, due to the same argument proposed in Sect. 4.2.2. In particular, assuming $\mu_0 \neq 0$, 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 $C_{0,1} = -(\sum_{j=0}^{n-1} \mu_j)/\mu_0$.

Examples of generalized Lai–Massey Schemes that are not EA-equivalent to any generalized Feistel scheme are given in the following. We denote the "EA-equivalent class" (or"EA-class" for brevity) of generalized Feistel schemes as "Feistel EA-class".

5.1 A (Small) Zoo of Generalized Lai–Massey Schemes *Not* Belonging to the "Feistel EA-Class"

Here, we propose other examples of generalized Lai–Massey constructions based on Definition 6 just given. With respect to the Lai–Massey scheme proposed in Prop. 2, one of the n inputs of the function F depends on a linear combination whose coefficients do not necessarily sum to zero. Due to this fact, in the next subsection we prove that the following constructions are *not* EA-equivalent to any generalized Feistel scheme published in the literature so far.

Proposition 5. *Let $p \geq 3$ be a prime integer, and let $n \geq 2$. For each $i \in \{0, 1, \dots, n-2\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \dots, \lambda_{n-1}^{(i)} \in \mathbb{F}_p$ be such that $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$.[3] Let $\psi_0, \psi_1, \dots, \psi_{n-1} \in \mathbb{F}_p$ (**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 generalized Lai–Massey scheme over $\mathbb{F}_p^n$ defined as $[x_0, x_1, \dots, x_{n-1}] \mapsto [y_0, y_1, \dots, y_{n-1}]$ where

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

and where

$$z = G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \dots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\right)$$

is invertible.

We point out that, if $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$, then the vector $[\psi_0, \psi_1, \dots, \psi_{n-1}] \in \mathbb{F}_p^n$ and the vectors $[\lambda_0^{(0)}, \lambda_1^{(0)}, \dots, \lambda_{n-1}^{(0)}], \dots, [\lambda_0^{(n-2)}, \lambda_1^{(n-2)}, \dots, \lambda_{n-1}^{(n-2)}] \in \mathbb{F}_p^n$ 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 $y_0, y_1, \dots, y_{n-1}$ as before, we have

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

for each $j \in \{0, 1, \dots, n-2\}$, where $\sum_{i=0}^{n-1} \lambda_i^{(j)} = 0$ by assumption. It follows that

$$z = G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot y_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot y_j, \dots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot y_j\right)\,.$$

[3] As before, we point out that there are at most $n-1$ $\mathbb{F}_q^n$-vectors whose elements sum to zero and that are linearly independent. We also allow the case $\gamma_0^{(j)} = \gamma_1^{(j)} = \gamma_{n-1}^{(j)} = 0$ in order to make the function G dependent on only $l < n-1$ inputs without introducing the parameter l as done in Prop. 2.

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

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

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

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

Indeed, in such a case, 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 $i \in \{0, 1, \ldots, n-1\}$:

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

□

By combining the two examples just given, we obtain the following generalized Lai–Massey scheme.

Lemma 4. *Let $p \geq 3$ be a prime integer, and let $n \geq 2$. For each $i \in \{0, 1, \ldots, n-2\}$, let $\lambda_0^{(i)}, \lambda_1^{(i)}, \ldots, \lambda_{n-1}^{(i)} \in \mathbb{F}_p$ be such that $\sum_{j=0}^{n-1} \lambda_j^{(i)} = 0$. 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 $\alpha \in \mathbb{F}_p$ be such that $L_p(\alpha) = -1$. 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 generalized Lai–Massey scheme over $\mathbb{F}_p^n$ defined as $[x_0, x_1, \ldots, x_{n-1}] \mapsto [y_0, y_1, \ldots, y_{n-1}]$ where*

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

and where

$$z = G \left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j \right)$$

is invertible.

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

Similar to before, we have that $\sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j = \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot y_j$ for each $i \in \{0, 1, \dots, n-2\}$, which implies that

$$z = G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot y_j, \sum_{j=0}^{n-1} \lambda_j^{(1)} \cdot y_j, \dots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot y_j\right) .$$

It follows that

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

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

5.2 Considerations about the Generalized Lai–Massey Schemes Proposed in Sect. 5.1

Next, we make some considerations about the generalized Lai–Massey schemes just proposed. We also propose and leave two open problems for future work.

5.2.1 About the *Non* EA-Equivalence with Generalized Feistel Schemes

If $\sum_{j=0}^{n-1} \psi_j \neq 0 \mod p$ and if G depends on $n-1$ non-trivial inputs[4], then the schemes just proposed in Prop. 5 and in Lemma 4 are *not* EA-equivalent to any generalized Feistel scheme. This follows from the fact that

- the functions F_i in Def. 5 takes at most $i \leq n-1$ independent inputs;
- both the function $F(x_0, \dots, x_{n-1}) = \beta \cdot z^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j \cdot x_j\right)$ in Prop. 5 and the function $F(x_0, \dots, x_{n-1}) = \frac{(z^2-\alpha)}{\sum_{j=0}^{n-1} \psi_j} \cdot H\left(\sum_{j=0}^{n-1} \psi_j \cdot x_j\right) - \frac{\sum_{j=0}^{n-1} \psi_j \cdot x_j}{\sum_{j=0}^{n-1} \psi_j}$ in Lemma 4 (where $z := G\left(\sum_{j=0}^{n-1} \lambda_j^{(0)} \cdot x_j, \dots, \sum_{j=0}^{n-1} \lambda_j^{(n-2)} \cdot x_j\right)$ in both cases) depend on n independent inputs.

As a concrete example, based on the result given in Prop. 5, 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, 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, let's 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

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

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

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 happens only if both $a_{0,1} - a_{1,1} = 0$ and $a_{0,1} + a_{1,1} = 0$, which can only occur if $a_{0,1} = a_{1,1} = 0$. 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.

Open Problem. As a future open problem, it could be interesting to understand if there exists any non-trivial relation that links the generalized Lai–Massey schemes proposed in this section and the generalized Feistel scheme, as the CZZ one [CCZ98, CP19].[5]

5.2.2 About the Existence of Invariant Subspaces

Having said that, the subspace $\langle [1, 1, \ldots, 1] \equiv \{[x, x, \ldots, x] \mid \forall x \in \mathbb{F}_p\} \rangle \subseteq \mathbb{F}_p^n$ is still invariant for the generalized Lai–Massey constructions just proposed in Prop. 5 and in Lemma 4.

Let's start with the one given in Prop. 5. Given an input $[x, x, \ldots, x] \subseteq \mathbb{F}_p^n$, we have that

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

that is, $y_i = y_j$ for each $i, j \in \{0, 1, \ldots, n-1\}$. Since $-\beta \cdot (G(0, 0, \ldots, 0))^2 \cdot \left(\sum_{j=0}^{n-1} \psi_j\right) \neq 1$ due to the invertibility condition $L_p\left(-\beta \cdot \left(\sum_{j=0}^{n-1} \psi_j\right)\right) = -1$, the subspace $\langle [1, 1, \ldots, 1] \rangle$ remains invariant.

In the case of the scheme given in Lemma 4, given an input $[x, x, \ldots, x] \subseteq \mathbb{F}_p^n$, we have that

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

that is, $y_i = y_j$ for each $i, j \in \{0, 1, \ldots, n-1\}$. Since F is a permutation, the subspace $\langle [1, 1, \ldots, 1] \rangle$ remains invariant.

Open Problem. We leave the problem to find (if exists) a generalized Lai–Massey scheme that (i) it is not EA-equivalent to any generalized Feistel scheme and (ii) it does not admit any invariant subspace trail as future open problem.

[5] 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 $\{(x, F(x)) \mid \forall x \in \mathbb{F}_q^n\} = A(\{(x, G(x)) \mid \forall x \in \mathbb{F}_q^n\})$.

6 The Amaryllises Scheme

In this section, we present a more generalized version of the Lai–Massey scheme, inspired by the Horst construction recently proposed by Grassi et al. [GHR+22], a generalized Feistel scheme in which the linear combination in $(x, y) \mapsto (y + F(x), x)$ is replaced by a non-linear one, that is, $(x, y) \mapsto (y \times G(x), x)$. More formally:

Theorem 2 (The Horst Scheme [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 functions such that $G_i(x_0, x_1, \ldots, x_{i-1}) \neq 0$ 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 $\mathcal{H}(x_0, x_1, \ldots, x_{n-1}) := y_0 \| y_1 \| \ldots \| y_{n-1}$ where*

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

is invertible.

Due to the similarity between Feistel and Lai–Massey schemes, we propose a new variant of the Lai–Massey construction in which the sum operation in the Lai–Massey scheme is replaced by a multiplication/product. We call the obtained invertible scheme as Amaryllises.

Theorem 3 (The Amaryllises Scheme). *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*

1. *$F : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that (1st) $F(0) \neq 0$ and (2nd) $G(x) := x \cdot F(x)$ is invertible over $\mathbb{F}_q$;*

2. *$H : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ be any function;*

3. *$\beta_0, \beta_1, \ldots, \beta_{n-1} \in \mathbb{F}_q \setminus \{0\}$ 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 $z \in \mathbb{F}_q$);*

4. *for each $j \in \{0, 1, \ldots, n-2\}$, let $\{\gamma_i^{(j)}\}_{i \in \{0,1,\ldots,n-1\}}$ be such that $\gamma_i^{(j)} \in \mathbb{F}_q$ and $\sum_{i=0}^{n-1} \gamma_i^{(j)} = 0$.*

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

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

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

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

where G is invertible by definition. Note that the condition $\sum_{i=0}^{n-1} \beta_i = 0$ is *not* necessary if $H(x) = 0$ for each $x \in \mathbb{F}_q$.

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

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

where $z := F\left(G^{-1}\left(\sum_{i=0}^{n-1} \beta_i \cdot y_i\right)\right)$ and where $z \neq 0$ due to the fact that F never returns zero by assumption.

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

$$x_i = z^{-1} \cdot \left(y_i - H\left(\frac{\sum_{j=0}^{n-1} \gamma_j^{(0)} \cdot y_j}{z}, \ldots, \frac{\sum_{j=0}^{n-1} \gamma_j^{(n-2)} \cdot y_j}{z}\right)\right).$$

□

We remark that the Lai–Massey scheme is a particular case of the `Amaryllises` scheme in which F always returns one, as for case of Feistel and `Horst` schemes.

6.1 Constructing F as in Theorem 3

The previous construction would be meaningless if it would not be possible to construct functions F that satisfy the required assumptions of the previous Theorem 3. Here, we face this problem.

Lemma 5. *Let $q = p^s$, where $p \geq 2$ is a prime and s is a positive integer. Let G be a permutation over $\mathbb{F}_q$. Let $\psi \in \mathbb{F}_q \setminus \{0\}$. The function F over $\mathbb{F}_q$ defined as*

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

satisfies the requirements of Theorem 3.

Proof. It is sufficient to show that (i) $F(0) \neq 0$ and that (ii) $x \mapsto x \cdot F(x)$ is a permutation. First of all, $F(0) = \psi \neq 0$. Secondly,

$$F(x) \cdot x = \begin{cases} G(x) - G(0) & \text{if } x \neq 0 \\ x \cdot \psi = 0 & \text{otherwise } (x = 0) \end{cases} = G(x) - G(0)\,,$$

which is a permutation since G is a permutation. □

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

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

Indeed:

- if $x \neq 0$, then $\prod_{i \in \mathbb{F}_q \setminus \{0\}} (i - x) = 0$, which implies $F(x) = H(x) = \frac{G(x)-G(0)}{x}$;
- 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 $F(0) = H(0) + (\psi - H(0)) = \psi$.

Constructing F via Power Maps and Dickson Polynomials. If the given function have a very complex algebraic structure, a problem can arise in scenarios in which (i) q is very large (e.g., $q \geq 2^{64}$) and (ii) one is forced to use such an algebraic expression for computing/evaluating the function (e.g., the MPC/FHE/ZK applications recalled in the introduction). For this reason, as next step, we provide concrete examples of functions F that satisfy the assumptions of Theorem 3 and that are cheap to compute, e.g., from the point of view of the *multiplicative complexity*.

Lemma 6. *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*

$$F(x) = \frac{(x \pm \alpha)^d \mp \alpha^d}{x} = \sum_{i=1}^{d} \binom{d}{i} x^{i-1} \cdot (\pm\alpha)^{d-i} \tag{6}$$

satisfies the requirements of Theorem 3.

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. □

Lemma 7. *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*

$$F(x) = \frac{\mathcal{D}_{d,\alpha}(x)}{x} := \sum_{j=0}^{\lfloor d/2 \rfloor} \frac{d}{d-j} \cdot \binom{d-j}{j} \cdot (-\alpha)^j \cdot x^{d-2j-1} \tag{7}$$

satisfies the requirements of Theorem 3.

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. □

Regarding the multiplicative cost of the two functions just proposed, the function defined in (7) via the Dickson polynomial costs $(d-1)/2$ multiplications (since it contains only monomials of the form x^{2i} for $i \in \{0, 1, \ldots, (d-1)/2\}$) versus $d - 1$ multiplications for the function defined in (6) via the power map.

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

Lemma 8. *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*

$$G^{(n)}(x_0, x_1, \ldots, x_{n-1}) := G^{(1)} \circ H^{(n)}(x_0, x_1, \ldots, x_{n-1})$$

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 $G^{(1)}$.

6.2 Generic Observations on the `Amaryllises` Construction

Next, we compare the advantages and disadvantages of `Amaryllises` construction with respect to other schemes/constructions proposed in the literature, focusing on the case of the `Horst` scheme and on the Lai–Massey one.

Remark 1. 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 point out possible high-level relations among the analyzed schemes.

6.2.1 Relation with `Horst` Schemes

About the Full Non-Linear Diffusion. Both in a `Horst` scheme as well as in a generalized Feistel one, there exists (at least) one output $\mathbb{F}_q$–element that is equal to one input $\mathbb{F}_q$–element. This scenario never happens in the `Amaryllises` case, since every output $\mathbb{F}_q$–element is defined via a non-linear function that depends on all input $\mathbb{F}_q$–elements. To be more precise, in the `Amaryllises` case, there is *no linear combination* of the output $\mathbb{F}_q$–elements that is the result of a linear function of the input $\mathbb{F}_q$–elements. E.g., given $[x_0, x_1, \ldots, x_{n-1}] \in \mathbb{F}_q^n$, let $[y_0, y_1, \ldots, y_{n-1}] \in \mathbb{F}_q^n$ be the outputs of a `Amaryllises` scheme, as in (5). The smallest degree of any relation among the inputs and the outputs is at least two:

$$\forall i, j, k, l \in \{0, 1, \ldots, n-1\} : \qquad (x_i - x_j) \cdot (y_k - y_l) = (y_i - y_j) \cdot (x_k - x_l)\,.$$

As a result, one round of the `Amaryllises` case is sufficient for achieving full non-linear diffusion, while at least two rounds are necessary in the `Horst`/Feistel case.

This advantage comes at the price of strongest assumptions on the components of the `Amaryllises` scheme in order to guarantee that the overall scheme is invertible. In particular, while the only assumption in the case of `Horst` regards the fact that each function G_i never returns zero, the function F in a `Amaryllises` scheme must satisfy the further condition that $x \mapsto x \cdot F(x)$ is a permutation. As a direct consequence, the number of possible choices for G_i is much larger than the corresponding number of possible choices for F. This could represent a significant advantage for `Horst` in the design phase, since the designer can e.g. choose functions G_i that are cheaper to evaluate/implement with respect to the `Amaryllises` case, without sacrificing the invertibility (and potentially the security) of the resulting primitive.

About the Inverse. As a direct consequence of the previous fact:

- as in the Feistel/Lai–Massey case, computing `Horst` has almost the same cost of computing its inverse. The only main difference regards the fact that a division takes places instead of a multiplication, i.e.,

$$y_i = x_i \cdot G_i(x_0, \dots, x_{i-1}) + F_{i-1}(x_0, \dots, x_{i-1}) \quad \textit{versus} \quad x_i = \frac{y_i - F_{i-1}(x_0, \dots, x_{i-1})}{G_i(x_0, \dots, x_{i-1})},$$

  where $x_0, x_1, \dots, x_{i-1}$ are given. In particular, both in the "regular/forward" and in the "inverse/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);

- in the case of a SPN scheme, one has to compute the inverse of each S-Box in order to compute its inverse. Similarly, in the case of `Amaryllises`, one has to compute the inverse of $x \mapsto x \cdot F(x)$ in order to compute its inverse – see the proof of Theorem 3 for more details.

As a result of this, computing the inverse of a `Amaryllises` scheme could be much more expensive than computing it, as it happens in the case in which F is instantiated via one of the low-degree functions proposed in Sect. 6.1. E.g., if $F(x) \cdot x = G(x) = x^d$, then $G^{-1} = x^{1/d} \equiv x^{\hat{d}}$ 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). Since $q \gg d$, then $\hat{d}$ is of the same order of q. Similarly, the inverse of $F(x) \cdot x = G(x) = \mathcal{D}_{d,\alpha}(x)$ is $G^{-1}(x) = \mathcal{D}_{\hat{d},\alpha}(x)$ where $\hat{d} \cdot d = 1 \mod (q^2 - 1)$.

While this could represent a disadvantage if the user has to compute the inverse of `Amaryllises` in order to e.g. decrypt, this fact represents an advantage in order to prevent/frustrate backward and/or Meet-in-the-Middle (MitM) algebraic attacks. In such a case, the idea of the attack is to exploit 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 as the interpolation one [JK97] or the higher-order differential one [Knu94] would be defeated after few rounds. For comparison, the inverse of a `Horst` scheme can be potentially described by low degree functions by making used 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). In such a scenario, a `Horst` scheme would require a larger number of rounds than a `Amaryllises` one for preventing backward and/or Meet-in-the-Middle algebraic attacks, with a potential negative impact on the overall cost of the designed primitive.

Besides that, we point out that, in many applications, computing the inverse of the `Amaryllises` construction is not required. 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 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 considerations hold for the Farfalle mode of operation [BDH+17] instantiated with permutations.

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

Conclusion. To summarize, the advantages and the disadvantages of `Amaryllises` versus `Horst` are (surprisingly) similar to the ones that one encounter when comparing an invertible SPN scheme with a Feistel and/or a Lai–Massey scheme:

1. both in `Horst` and in Feistel/Lai–Massey schemes, the invertibility of the entire construction is (almost) independent of the details of the internal components. This implies (almost) the same cost for computing the scheme in the regular/forward and in the inverse/backward direction, as well as the fact that algebraic attacks are (almost) equally efficient in the forward and in the backward direction;

2. in the case of `Amaryllises` and of a SPN schemes, the invertibility of each subcomponent is crucial in order to guarantee the invertibility of the entire construction. Moreover, the cost of computing the inverse of such schemes could be (very) different than computing the schemes in the regular/forward direction, with potential negative effects on the implementation cost in the cases in which decryption is required. At the same time, this could represent an advantage in order to prevent backward and/or Meet-in-the-Middle algebraic attacks, as previously discussed.

6.2.2 Relation with Lai–Massey Schemes

Next, we compare the `Amaryllises` scheme and the Lai–Massey one, focusing on the security aspects. Our goal is to understand the impact of the multiplication with F in the `Amaryllises` scheme from a security point of view.

Invariant Subspaces. As recalled in Sect. 3, the Lai–Massey schemes proposed in Prop. 2 admit an invariant subspace of the form $\mathfrak{X} = \{x \in \mathbb{F}_q^n \mid \forall i \in \{0, 1, \ldots, n-2\} : \sum_{j=0}^{n-1} \lambda_j^{(i)} \cdot x_j = 0\}$. The multiplication with F in `Amaryllises` is *not* sufficient by itself to destroy it, that is, the `Amaryllises` scheme admits an invariant subspace as well. Indeed

- if H is not identically equal to zero, then $\sum_{i=0}^{n-1} \beta_i = \sum_{i=0}^{n-1} \gamma_i^{(0)} = \sum_{i=0}^{n-1} \gamma_i^{(1)} = \ldots = \sum_{i=0}^{n-1} \gamma_i^{(n-2)} = 0$ 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 in the case of the Lai–Massey schemes previously analyzed, this implies that a linear layer is crucial in order to destroy the invariant subspace trails of the `Amaryllises` schemes.

Statistical Attacks. Regarding other statistical attacks, the impact of the multiplication with F in `Amaryllises` 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 function F 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

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

In the generalized Lai–Massey case as in Def. 6, we have that

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

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

$$0 \leq \text{Prob}(\delta \neq 0 \to \Delta) \leq \begin{cases} 0 & \text{if } \exists i, j \in \{0, 1, \dots, n-1\} \text{ such that } \Delta_i - \delta_i \neq \Delta_j - \delta_j \\ q^{-1} & \text{otherwise} \end{cases} ,$$

that is, the system of equations reduces to a single non-linear equation, and the DP is never bigger than q^{-1}.

For comparison, in the case of a `Amaryllises` scheme, we have that

$$\begin{aligned} \Delta_i =& (x_i + \delta_i) \cdot F\left(\sum_{j=0}^{n-1} \beta_j \cdot (x_j + \delta_j)\right) - x_i \cdot F\left(\sum_{j=0}^{n-1} \beta_j \cdot x_j\right) \\ &+ H\left(\sum_{j=0}^{n-1} \gamma_j^{(0)} \cdot (x_j + \delta_j), \dots, \sum_{j=0}^{n-1} \gamma_j^{(n-2)} \cdot (x_j + \delta_j)\right) - H\left(\sum_{j=0}^{n-1} \gamma_j^{(0)} \cdot x_j, \dots, \sum_{j=0}^{n-1} \gamma_j^{(n-2)} \cdot x_j\right) \end{aligned}$$

for each $i \in \{0, 1, \dots, n-1\}$.[6] As a result, the probability is – in general – proportional to $\mathcal{O}(q^{-n})$, since such system of equations cannot be reduced to a single equation as in the Lai–Massey case. A similar conclusion holds for linear attacks [Mat93] as well.

Algebraic Attacks. Similar conclusion holds for the case of algebraic attacks. As already pointed out, the degree of the Lai–Massey scheme evaluated in the regular/forward direction and in the inverse/backward direction are equal. Instead, the degree of `Amaryllises` scheme in the inverse/backward direction can be much higher than the one in the regular/forward direction. This fact could make a big difference when preventing backward or/and MitM algebraic attacks.

This is not the only advantage of the multiplication with F in `Amaryllises` schemes. Consider e.g. the security against a Gröbner basis attack [Buc76], in which the goal is factorize and 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 `Amaryllises` scheme or of a Lai–Massey one. When comparing such two schemes, we face the following scenario:

[6] Given $z := \sum_{j=0}^{n-1} \beta_j \cdot x_j$, note that one of the equations of such system can be replaced by

$$\left(z + \sum_{j=0}^{n-1} \beta_j \cdot \delta_j\right) \cdot F\left(z + \sum_{j=0}^{n-1} \beta_j \cdot \delta_j\right) - z \cdot F(z) = \sum_{j=0}^{n-1} \beta_j \cdot \Delta_j ,$$

which is independent of H.

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

$$\begin{cases} y_0 = x_0 + F(x_0, x_1, \ldots, x_{n-1}) \,, \\ y_i - y_0 = x_i - x_0 & \forall i \in \{1, 2, \ldots, n-1\} \,, \end{cases}$$

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

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

$$\begin{cases} y_0 = x_0 \cdot F\left(\sum_{j=0}^{n-1} \beta_j \cdot x_j\right) + H\left(\sum_{j=0}^{n-1} \gamma_j^{(0)} \cdot x_j, \ldots, \sum_{j=0}^{n-1} \gamma_j^{(n-2)} \cdot x_j\right) \,, \\ y_1 - y_0 = (x_1 - x_0) \cdot F\left(\sum_{j=0}^{n-1} \beta_j \cdot x_j\right) \,, \\ (x_i - x_0) \cdot (y_1 - y_0) = (y_i - y_0) \cdot (x_1 - x_0) & \forall i \in \{2, 3, \ldots, n-1\} \,, \end{cases}$$

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

  If H is identically equal to zero, the `Amaryllises` scheme can be described by the following system of equations:

$$\begin{cases} y_0 = x_0 \cdot F\left(\sum_{j=0}^{n-1} \beta_j \cdot x_j\right) \,, \\ y_i \cdot x_0 = x_i \cdot y_0 & \forall i \in \{1, 2, \ldots, n-1\} \,, \end{cases}$$

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

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

7 The Contracting–`Amaryllises` Construction

In this section, we introduce the Contracting–`Amaryllises` construction, as a variant of the `Amaryllises` just proposed. Similar to what happens in the case of contracting Feistel schemes, 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 in 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 also the name "contracting" suggests).

Theorem 4. *Let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$, and let $n \geq 2$. Let $e \geq 1$ be an integer such that $\gcd(e, q-1) = 1$. Let $F : \mathbb{F}_q^n \to \mathbb{F}_q$ a function that never returns zero for any non-zero input, that is, such that*

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

If the function $G_{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}}(x) : \mathbb{F}_q \to \mathbb{F}_q$ defined as

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

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

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

is invertible.

Proof. We start by pointing out two observations:

- first of all, the following equality always holds:

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

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

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

Assume that $[y_0,y_1,\ldots,y_{n-1}] \neq [0,0,\ldots,0]$ (otherwise, the input is zero due to the previous observation). For each $i \in \{0,1,\ldots,n-1\}$ such that $y_i \neq 0$ (remember that $y_i = 0$ implies $x_i = 0$), then

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

due to (9), and where $x \mapsto x^e$ is invertible by assumption on e. By assumption, G is invertible (note that $\alpha_j = (y_j/y_i)^{1/e}$ is fixed for each $j \in \{0,1,\ldots,n-1\}$).

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

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

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

Relation with the `Amaryllises` Scheme. Almost all the considerations/observations made before for the `Amaryllises` schemes apply as well to Contracting–`Amaryllises` schemes just defined. The main differences can be summarized as following:

- the class of functions F that can instantiate a Contracting–`Amaryllises` scheme is much larger than the one for an `Amaryllises` scheme previously proposed;
- with respect to the `Amaryllises` constructions, the Contracting–`Amaryllises` scheme does *not* necessarily admit invariant subspaces, since the function F works directly on the inputs $x_0,x_1,\ldots,x_{n-1}$ and not on a single linear combination of them. However, the existence of such subspace obviously depends on the details of the function F itself;
- we are able to guarantee that the overall construction is invertible only in the case in which the function H in (5) is identically equal to zero. The open problem to set up an invertible Contracting–`Amaryllises` construction in which H is not identically equal to zero is left for future work.

Constructing Suitable Functions F. Having said that, the main problem to face regards the construction of a function F that satisfies the assumptions of Theorem 4. 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 Theorem 4 and that (ii) are efficient to compute from the multiplicative point of view (equivalently, of low degree). The proposed constructions are based on the following result.

Proposition 6. *Let $q = p^s$ where $p \geq 2$ is a prime integer and $s \geq 1$, and let $n \geq 2$. Let $d \geq 3$ be such that $\gcd(d, q-1) = 1$, and let $1 \leq e \leq d-2$ be an integer such that $\gcd(e, q-1) = 1$. Let $d' := d - e \in \{2, 3, \ldots, d-1\}$. Let $F : \mathbb{F}_q^n \to \mathbb{F}_q$ be a homogeneous function of degree d' (that is, a sum of monomials of degree d' only) of the form*

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

where $\mathfrak{I}_{d'} := \left\{ [i_0, i_1, \ldots, i_{n-1}] \in \mathbb{Z}_+^n \middle| \sum_{j=0}^{n-1} i_j = d' \right\}$ and where $\varphi_{i_0, i_1, \ldots, i_{n-1}} \in \mathbb{F}_q$. If

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

then the Contracting–`Amaryllises` construction $\mathcal{A}_C$ defined over $\mathbb{F}_q^n$ as in Theorem 4 (with $e = d - d'$) is invertible.

Proof. It is sufficient to prove that F satisfies the assumption of Theorem 4, that is, $G_{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}}(x) = x^{d-d'} \cdot F(\alpha_0 \cdot x, \alpha_1 \cdot x, \ldots, \alpha_{n-1} \cdot x)$ is invertible for each arbitrary fixed non-null $[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}] \in \mathbb{F}_q^n \setminus \{[0, 0, \ldots, 0]\}$. Since F contains only monomials of degree d', then

$$\begin{aligned}
G_{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}}(x) &= x^{d-d'} \cdot F(\alpha_0 \cdot x, \alpha_1 \cdot x, \ldots, \alpha_{n-1} \cdot x) \\
&= x^{d-d'} \cdot \sum_{\{i_0, i_1, \ldots, i_{n-1}\} \in \mathfrak{I}_{d'}} \varphi_{i_0, i_1, \ldots, i_{n-1}} \cdot (\alpha_0 \cdot x)^{i_0} \cdot (\alpha_1 \cdot x)^{i_1} \cdot \ldots \cdot (\alpha_{n-1} \cdot x)^{i_{n-1}} \\
&= x^d \cdot \sum_{\{i_0, i_1, \ldots, i_{n-1}\} \in \mathfrak{I}_{d'}} \varphi_{i_0, i_1, \ldots, i_{n-1}} \cdot \alpha_0^{i_0} \cdot \alpha_1^{i_1} \cdot \ldots \cdot \alpha_{n-1}^{i_{n-1}} \\
&= x^d \cdot F(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) .
\end{aligned}$$

Since (i) $x \mapsto x^d$ is invertible due to the assumption on d and since (ii) $F(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \neq 0$ for each non-null input by assumption, then function G is invertible:

$$G^{-1}_{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}}(y) = \left(\frac{y}{F(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})} \right)^{\frac{1}{d}} . \qquad \square$$

7.1 Examples of the Contracting–`Amaryllises` Construction over $\mathbb{F}_q^2$

In this subsection, we propose some concrete examples of the Contracting–`Amaryllises` scheme over $\mathbb{F}_q^2$ by making used of the result proposed in Prop. 6.

Lemma 9. *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 $d' = d - 1$ (and so $e = 1$). 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 assumptions of Prop. 6 (and so of Theorem 4).

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 $z := x_0/x_1$, 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 $[x_0, x_1] = [0, 0]$. □

Lemma 10. *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. 6 (and so of Theorem 4).

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 $[x_0, x_1] = [0, 0]$. □

Case: Prime Fields. Next, we propose two examples for prime fields only.

Lemma 11. *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. 6 (and so of Theorem 4).

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. □

Lemma 12. *Let $p \geq 3$ be a prime integer, and let $d' = 2$. Let $d \geq 3$ be such that $\gcd(d, p-1) = \gcd(d-2, p-1) = 1$. Let α, β be such that $\alpha^2 - 4 \cdot \beta$ is a quadratic non-residue modulo p, that is, $L_p(\alpha^2 - 4 \cdot \beta) = -1$. The function*

$$F(x_0, x_1) = x_0^2 + \alpha \cdot x_0 \cdot x_1 + \beta \cdot x_1^2$$

satisfies the assumptions of Prop. 6 (and so of Theorem 4).

Proof. Let $z := x_0/x_1$. The proof follows from the fact that $z^2 + \alpha z + \beta = 0$ does not admit any solution. Indeed, the only possible solutions would be

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

but $L_p(\alpha^2 - 4 \cdot \beta) = -1$ due to the choice of α, β, which implies that no square root of $\alpha^2 - 4 \cdot \beta$ exists. □

7.2 Examples of the Contracting–Amaryllises Construction over $\mathbb{F}_q^{\geq 3}$

As next step, 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. 6 (and so of Theorem 4) 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 7. *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 $n := \sum_{i=0}^{m-1} n_i$.*

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 same conditions given in Prop. 6, that is, (i) it is an homogeneous function of a certain degree $\deg(F^{(i)}) \geq 2$ 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 $[x_0, x_1, \ldots, x_{i-1}] \in \mathbb{F}_p^i \setminus \{[0, 0, \ldots, 0]\}$).

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,

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

Let $F^{(n)} : \mathbb{F}_q^n \to \mathbb{F}_q$ be defined as

$$\begin{aligned} F^{(n)}(x_0, x_1, \ldots, x_n) := F^{(m)}\Bigg(& \left(F^{(n_0)}(x_0, \ldots, x_{n_0-1})\right)^{\frac{d}{\deg(F^{(n_0)})}}\,, \\ & \left(F^{(n_1)}(x_{n_0}, \ldots, x_{n_0+n_1-1})\right)^{\frac{d}{\deg(F^{(n_1)})}}\,, \ldots, \\ & \left(F^{(n_{m-1})}(x_{n-n_m}, \ldots, x_{n-1})\right)^{\frac{d}{\deg(F^{(n_{m-1})})}}\Bigg)\,. \end{aligned}$$

The function $F^{(n)}$ satisfies the assumptions of Prop. 6 (and so of Theorem 4), 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, note that

- $F^{(m)}$ is an homogeneous function of degree $\deg(F^{(m)})$;
- each input of $F^{(m)}$ is an homogeneous function of degree d.

It follows that $F^{(n)}$ is an homogeneous function of degree $d \cdot \deg(F^{(m)})$.

Regarding the second point, note that:

- $F^{(m)}$ 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 $z_0 = z_1 = \ldots = z_{n_i-1} = 0$.

It follows that $F^{(n)}$ returns zero if and only if all its inputs are equal to zero. □

By applying the previous result iteratively, it is possible to construct functions $F^{(n)} : \mathbb{F}_q^n \to \mathbb{F}_q$ for each $n \geq 2$ that satisfy the assumptions of Prop. 6, as

$$\begin{aligned}
F^{(3)}(x_0, x_1, x_2) &= F^{(2)}\left(F^{(2)}(x_0, x_1), x_2^{\deg(F^{(2)})}\right) , \\
F^{(4)}(x_0, x_1, x_2, x_3) &= F^{(3)}\left(F^{(2)}(x_0, x_1), x_2^{\deg(F^{(2)})}, x_3^{\deg(F^{(2)})}\right) , \\
F^{(4)}(x_0, x_1, x_2, x_3) &= F^{(2)}\left(F^{(3)}(x_0, x_1, x_2), x_3^{\deg(F^{(3)})}\right) , \\
F^{(4)}(x_0, x_1, x_2, x_3) &= F^{(2)}\left(F^{(2)}(x_0, x_1), F^{(2)}(x_2, x_3)\right) ,
\end{aligned}$$

and so on. In particular, for each $n \geq 3$, it is always possible to construct $F^{(n)}$ iteratively as:

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

Note that 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 degree of the obtained function is *strictly* higher 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. 6 and/or of Theorem 4 as an open problem for future work.

8 Future Directions

In this paper, we re–considered the Lai–Massey scheme originally proposed in [LM90,Vau99], proposing new generalizations that are not (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.

At the same time, the analysis of possible new generalizations of the `Amaryllises` scheme is far from being finished. Inspired by Def. 6 introduced for the case of generalized Lai–Massey schemes, we propose the following definition for the Generalized `Amaryllises` schemes.

Definition 7. Let $q = p^s$ for $p \geq 2$ being a prime and $s \geq 1$ an integer. Let $n \geq 2$. Given functions $F, G : \mathbb{F}_q^n \to \mathbb{F}_q$, let $\mathcal{A}_G : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be defined as $\mathcal{A}_G(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| y_2 \| \ldots \| y_{n-1}$ where

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

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

An open problem for future work regards the analysis and the construction of (non-trivial) generalized `Amaryllises` schemes.

Another possible line of research consists in the analysis of the advantages and disadvantages of a design instantiated with the `Amaryllises` scheme with respect to e.g. more traditional designs as the SPN/AES-like ones. To be more concrete, our initial analysis proposed in this paper does not take into account the details of the functions/sub-components that define the `Amaryllises` scheme, besides e.g. the effect of a linear layer applied before or after it. In particular, since the `Amaryllises` scheme provides full diffusion, it could make sense to ask (i) if a linear layer is still necessary (besides for the goal of destroying invariant subspace trails of the `Amaryllises` scheme itself) and/or (ii) how to design a linear layer that maximizes the advantages of such construction with respect to several parameters, including the diffusion, the security against statistical attacks, and so on.

In conclusion, the initial results proposed in this paper may open up *new interesting possibilities regarding the construction of non-linear layers for future designs.*

Acknowledgments. Lorenzo Grassi is supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA.

References

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

[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.

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

[BDPA08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the Indifferentiability of the Sponge Construction. In *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.

[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.

[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.

[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.

[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.

[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.

[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.

[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. Springer, 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.

[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 Invariant Subspaces: the Solution proposed in [Vau99]

Here, we briefly discuss the solution proposed in [Vau99] for breaking the subspace trail of the (generalized) Lai–Massey construction (recently re-considered in [AC21]). 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

$$[x_0, x_1] \to [y_0, y_1] = [S(x_0 + H(x_0 - x_1)), x_1 + H(x_0 - x_1)] \tag{10}$$

for a certain function $S : \mathbb{F}_q \to \mathbb{F}_q$. In particular, it is requested that S is an *orthomorphism* (a function S is an orthomorphism if and only if both S and $S'(x) := S(x) - x$ are permutations[7]). The reason behind this request is the following. The invariant subspace for the Lai–Massey construction over $\mathbb{F}_q^2$ is $\mathfrak{X} = \langle [1, 1] \rangle$. By applying (10), we get

$$[x + \varphi_0, x + \varphi_1] \mapsto [S(x + \varphi_0 + H(\varphi_0 - \varphi_1)), x + \varphi_1 + H(\varphi_0 - \varphi_1)] \,,$$

where $[S(x+\varphi_0+H(\varphi_0-\varphi_1)), x+\varphi_1+H(\varphi_0-\varphi_1)] \in \mathfrak{X} + [\psi_0, \psi_1]$ for certain $\psi_0, \psi_1 \in \mathbb{F}_q$ if and only if

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

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

that is,

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

where $S'(x) := S(x) - x$. Such a condition cannot be satisfied even when consider a linear function $S(x) = \sigma \cdot x$ for a certain $\sigma \in \mathbb{F}_q \setminus \{0, 1\}$, which 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 $[1; 1]$ as invariant subspace. In such a case, $S'(x) = \sigma \cdot x - x = (\sigma - 1) \cdot x$ is a permutation as well (since $\sigma \neq 1$), which implies that its output is uniformly distributed, a condition that is necessary for e.g. proving that 3-round Lai–Massey construction, within the birthday bound, is CPA-secure – see [Vau99, Sect. 3].

At the same time, we point out that the condition "S is an orthomorphism" is not strictly necessary *if* one only aims to destroy the invariant subspace trails, and that a similar result can be achieved when working with a non-linear function S (which is in general is not an orthomorphism).

B Details for Sect. 4.2.2 – Contracting Feistel

Here we show that

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

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