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

Ginevra Giordani[1], Lorenzo Grassi[2,3], Silvia Onofri[4,*], Marco Pedicini[5]

[1] Università degli Studi dell'Aquila, L'Aquila (Italy)
[2] Ruhr University Bochum, Bochum (Germany)
[3] Ponos Technology, Zug (Switzerland)
[4] Scuola Normale Superiore, Pisa (Italy)
[5] Università degli Studi Roma Tre, Rome (Italy)
ginevra.giordani@graduate.univaq.it, Lorenzo.Grassi@ruhr-uni-bochum.de, silvia.onofri@sns.it, marco.pedicini@uniroma3.it

Abstract. The construction of invertible non-linear layers over $\mathbb{F}_p^n$ that minimize the multiplicative cost is crucial for the design of symmetric primitives targeting Multi Party Computation (MPC), Zero-Knowledge proofs (ZK), and Fully Homomorphic Encryption (FHE). At the current state of the art, only few non-linear functions are known to be invertible over $\mathbb{F}_p$, as the power maps $x \mapsto x^d$ for $\gcd(d, p-1) = 1$. When working over $\mathbb{F}_p^n$ for $n \geq 2$, a possible way to construct invertible non-linear layers $\mathcal{S}$ over $\mathbb{F}_p^n$ is by making use of a local map $F : \mathbb{F}_p^m \to \mathbb{F}_p$ for $m \leq n$, that is, $\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where $y_i = F(x_i, x_{i+1}, \ldots, x_{i+m-1})$. This possibility has been recently studied by Grassi, Onofri, Pedicini and Sozzi at FSE/ToSC 2022. Given a quadratic local map $F : \mathbb{F}_p^m \to \mathbb{F}_p$ for $m \in \{1, 2, 3\}$, they proved that the shift-invariant non-linear function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ defined as before is never invertible for any $n \geq 2 \cdot m - 1$.

In this paper, we face the problem by generalizing such construction. Instead of a single local map, we admit multiple local maps, and we study the creation of nonlinear layers that can be efficiently verified and implemented by a similar shift-invariant lifting. After formally defining the construction, we focus our analysis on the case $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ for $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ of degree at most 2. This is a generalization of the previous construction using two alternating functions F_0, F_1 instead of a single F. As main result, we prove that (i) if $n \geq 3$, then $\mathcal{S}_{F_0,F_1}$ is never invertible if both F_0 and F_1 are quadratic, and that (ii) if $n \geq 4$, then $\mathcal{S}_{F_0,F_1}$ is invertible if and only if it is a Type-II Feistel scheme.

Keywords: Invertible Quadratic Functions – Local Maps – Type-II Feistel

* Corresponding author

1 Introduction

The study of substitutive transformations in the Boolean case (the S-Boxes), $\mathcal{S} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ has led to the discovery of many families of functions with properties crucial to cryptography, including non-linearity [28], algebraic immunity [27], and arithmetic complexity. These properties play a significant role in cryptography, as they can be used to design cryptographic functions with desirable security properties. From the cryptographic point of view, important classes of non-linear functions include the (almost) perfect non-linear ((A)PN) ones [28, 29]. Given a function $\mathcal{F}$ over $\mathbb{F}_2^n$, let

$$\Delta_{\mathcal{F}} := \max_{a \neq 0, b \in \mathbb{F}_2^n} \left| \{x \in \mathbb{F}_2^n \mid \mathcal{F}(x+a) + \mathcal{F}(x) = b\} \right|.$$

$\mathcal{F}$ is said to be $\Delta_{\mathcal{F}}$-differentially uniform. In particular, $\mathcal{F}$ is perfect non-linear if $\Delta_{\mathcal{F}} = 1$, and almost perfect non-linear if $\Delta_{\mathcal{F}} = 2$.

Finding APN functions for n odd is easy. For example, APN functions include the Gold map [17] $x \mapsto x^{2^l+1}$ for $\gcd(l, n) = 1$, the inverse map [5] $x \mapsto x^{-1} \equiv x^{2l}$ for $n = 2l+1$, and many others. However, finding APN permutations for n even is less trivial. In fact, when $n \geq 8$ is even, this task is an open problem which has been nicknamed the *Big APN Problem*. Several works have been carried on in order to solve it, including [4, 8–12] among many others.

The research of APN functions is justified by the fact that, if used as S-Boxes, APN functions provide optimal resilience against differential attacks [6]. Given pairs of inputs with some fixed input differences, differential cryptanalysis considers the probability distribution of the corresponding output differences produced by the cryptographic primitive. Hence, it is natural to consider functions with low differential probability for preventing it. At the same time, it is well known that the security against differential (and more generally, statistical) attacks is achieved by a combination of the linear and the non-linear layers. As a concrete example, consider the case of the wide-trail design strategy [14], proposed by Daemen and Rijmen for designing the round transformation of key-alternating block ciphers that combines efficiency and resistance against linear and differential cryptanalysis. Instead of spending most of its resources for looking for large S-Boxes with "good" statistical properties, the wide-trail strategy aims at designing the round transformation(s) in order to maximize the minimum number of active S-Boxes over multiple rounds. Thus, in symmetric primitives designed by the wide trail strategy, the idea is to look for linear layers that guarantee a large number of active S-Boxes over several rounds. This fact together with the existence of 4-differentially uniform invertible functions for every $n \geq 3$ may imply that the big APN problem previously recalled could be considered a more theoretical rather than a practical open problem in symmetric cryptography.

At the opposite, the research of low-multiplicative[1] non-linear functions over prime fields $\mathbb{F}_p$ for $p \geq 3$ prime is currently very relevant for symmetric encryption schemes designed for applications like Multi Party Computation (MPC),

[1] In this paper, we use the term "$\mathbb{F}_p$-multiplication" – or simply, "multiplication" – to refer to a non-linear operation over $\mathbb{F}_p$.

Zero-Knowledge proofs (ZK), and Fully Homomorphic Encryption (FHE). MPC allows different users that do not necessarily trust each other to evaluate a function on a shared secret without revealing it. FHE allows a user to operate on encrypted data without decrypting them. Finally, ZK is a technique that allows to authenticate a secret information without disclosing it. The number of possible applications of these techniques is countless, including e.g. crypto-currency as probably the most well known one. In the recent years, several symmetric primitives over prime fields have been proposed for these applications, including MiMC [2], GMiMC [1], *Rescue* [3], HadesMiMC/Poseidon [22], Ciminion [15], Pasta [16], Reinforced Concrete [21], Neptune [24], Griffin [20], `Anemoi` [7], Hydra [25], among others.

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

- they are usually defined over prime fields $\mathbb{F}_p^t$ for a huge prime $p \approx 2^{128}$ (or even bigger), whereas classical schemes are defined over binary fields $\mathbb{F}_2^n$;
- they can be described via a simple algebraic expression over their natural field, whereas classical schemes usually admit a very complex algebraic structure.

In order to be efficient in MPC, FHE, and ZK protocols/applications, the number of multiplications or/and the multiplication depth necessary to evaluate/verify the considered symmetric primitive should be minimum. Moreover, besides that, unlike the case of traditional primitives, the size of the field over which the scheme is defined does not impact the cost of the performed operations. Apart from that, due to the large size of the field p, any sub-component (as the non-linear S-Boxes) that defines the symmetric primitive must be computed on the fly, that is, it cannot be pre-computed and stored as a look-up table. In both cases, a simple algebraic structure is in general the most convenient choice for achieving the best possible performances.

At the current state of the art, only few invertible non-linear functions over prime fields are known, recalled in the following section. In this paper, we analyze the possibility to set up invertible quadratic functions over $\mathbb{F}_p^n$ for MPC-/FHE-/ZK-friendly symmetric schemes via cyclic shift-invariant functions induced by multiple local maps.

1.1 Related Works: Shift-Invariant Lifting Functions induced by a Local Map

Well known examples of invertible non-linear functions over $\mathbb{F}_p$ for a prime integer $p \geq 3$ include (i) the power maps $x \mapsto x^d$, which are invertible if and only if $\gcd(d, p-1) = 1$, and (ii) the Dickson polynomials

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

which are invertible for $\gcd(d, p^2 - 1) = 1$. Other classes of invertible non-linear functions constructed via the Legendre symbol and/or the $x \mapsto (-1)^x$ function have been recently proposed in [23, 31], but it is currently not clear if they can be efficiently used for MPC, FHE, and ZK protocols/applications.

When working over $\mathbb{F}_p^n$ for $n \geq 2$, a possible way to set up non-linear invertible functions is by exploiting the Feistel and/or the Lai-Massey [19, 26, 32] approach. Another approach has been recently considered by Grassi et al. [24] at FSE/ToSC 2022, and it is inspired by the chi-function, which was introduced in the setting of cellular automata cryptography in [33] and studied by Joan Daemen in his PhD thesis "Cipher and Hash Function Design Strategies based on linear and differential cryptanalysis" [13]. The chi-function over $\mathbb{F}_2^n$ is a nonlinear shift-invariant transformation (i.e., a transformation which does not change its output when the input is shifted) that can be defined in terms of the local map $\chi(x_0, x_1, x_2) = x_0 \oplus (x_1 \oplus 1) \cdot x_2$. The *shift-invariant* chi-transformation is then applied to a binary sequence by taking triplets of the input sequence, with bits from the beginning of the sequence being used when the end of the input sequence is reached.

The general scheme with a single local map $F : \mathbb{F}_p^m \to \mathbb{F}_p$ is specified as the substitutive transformation over $\mathbb{F}_p^n$ such that for each $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_p^n$, we have

$$\mathcal{S}_F(x_0, x_1, \ldots, x_{n-1}) := y_0 \| y_1 \| \ldots \| y_{n-1} \quad \text{where} \quad y_i = F(x_0, x_1, \ldots, x_{m-1}) \,.$$

In [24], authors proved that, given any quadratic function $F : \mathbb{F}_p^2 \to \mathbb{F}_p$, the corresponding function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ for $n \geq 3$ as defined in Definition 3 is never invertible. An equivalent similar result holds when considering quadratic functions $F : \mathbb{F}_p^3 \to \mathbb{F}_p$ and the corresponding function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ for $n \geq 5$.

Later on, Grassi considered the possibility to exploit non-invertible non-linear functions as building blocks for MPC-/FHE-/ZK-friendly schemes *in which the internal state is obfuscated by a secret (e.g., a secret key).* In [18], he proved that the function $\mathcal{S}_F$ induced by $F : \mathbb{F}_p^2 \to \mathbb{F}_p$ defined as $F(x_0, x_1) = x_0^2 + x_1$ (or equivalent) minimizes the probability that a collision occurs among all $\mathcal{S}_F$ over $\mathbb{F}_p^n$ induced by any quadratic function $F : \mathbb{F}_p^m \to \mathbb{F}_p$ for $m \in \{1, 2\}$. Such probability is upper bounded by p^{-n}.

1.2 Our Contribution

The just mentioned recent results by Grassi concerning non-invertible non-linear functions cannot be used for setting up symmetric primitives in which the internal state is *not* obfuscated by a secret, as the case of a sponge hash function. Indeed, the absence of a secret key could potentially allow the attacker to control the inputs in order to ensure that they trigger a collision. Hence, the problem of constructing invertible non-linear functions with minimal multiplicative complexity remains crucial.

In this paper we adopt the same design to extend the construction: *instead of a single local map, we admit multiple local maps, and we study the creation*

of nonlinear layers that can be efficiently verified and implemented by a similar shift-invariant lifting. The general scheme with multiple local maps is specified as

$$\mathcal{S}_{F_0,F_1,\ldots,F_{n-1}}(x_0,x_1,\ldots,x_{n-1}) := y_0\|y_1\|\ldots\|y_{n-1}$$

where

$$y_i = F_i(x_0,x_1,\ldots,x_{m-1}) \qquad \text{for each } i \in \{0,\ldots,n-1\}$$

and $F_i : \mathbb{F}_p^m \to \mathbb{F}_p$ are possibly distinct functions. Instead of working with a generic function $\mathcal{S}$, in this paper we limit ourselves to consider the case in which each value y_i is specified by cyclically using h fixed local maps $F_0, F_1, \ldots, F_h : \mathbb{F}_p^m \to \mathbb{F}_p$ which depend on m components of the domain vector $x_0, x_1, \ldots, x_{n-1}$ for $m \leq n$, also these variables are taken by shifting the components, namely:

$$y_i = F_{i \bmod h}(x_i, x_{i+1}, \ldots x_{i+m-1}),$$

where indices of variables x_i are taken modulo n. We distinguish the case $h = 2$ that we call the *alternating shift-invariant lifting* (ASI-liftings), from the case $h > 2$ that we call *cyclic shift-invariant lifting* (CSI-liftings), see Definition 3 in Section 2. In there, we give a notion of similarity between families of local maps for which invertibility holds for the entire equivalent class, which allows us to simplify the proof of invertibility of ASI-liftings to a representative function of the equivalence class.

In this paper, we limit ourselves to consider the case $h = 2$ with $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ both quadratic, or one linear and one quadratic. In such a case, we prove that the Feistel Type-II functions [30, 34] are the *only* ones in which the scheme we called alternating shift-invariant lifting functions is invertible over $\mathbb{F}_p^n$. More formally, our main result can be summarized as following:

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

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

Then:

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

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

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

Note that we focus on the case $n \geq 3$, since there exist *invertible* SI-lifting functions $\mathcal{S}_F(x_0, x_1)$ over $\mathbb{F}_p^2$ induced by quadratic local maps $F : \mathbb{F}_p^2 \to \mathbb{F}_p$, as $F(x_0, x_1) = \gamma_2 \cdot (x_0 - x_1)^2 + \gamma_1 \cdot x_1 + \gamma_0 \cdot x_0$, with $\gamma_0 \neq \pm\gamma_1$ and $\gamma_2 \neq 0$ – see [24] for details.

The proof of the previous Theorem is divided in two parts:

- in Section 4, we study the case where both F_0, F_1 are quadratic;
- in Section 5, we study the mixed case, where one function is linear and the other one is quadratic.

The problem of setting up a substitutive transformation quadratic and invertible over $\mathbb{F}_p^n$ for generic prime $p \geq 3$ and n remains open. Potential ideas for solving this problem are discussed in Section 6.

2 Preliminary: Notation and Related Works

2.1 Notation

From now on, let $p \geq 3$ be a prime number. Let $\mathbb{F}_p$ denote the field of integer numbers modulo p. We use small letters to denote either parameters/indexes or variables and greek letters to denote fixed elements in $\mathbb{F}_p$. Given $x \in \mathbb{F}_p^n$, we denote by x_i its i-th component for each $i \in \{0, 1, \ldots, n-1\}$, that is, $x = (x_0, x_1, \ldots, x_{n-1})$. We use capital letters to denote functions from $\mathbb{F}_p^m$ to $\mathbb{F}_p$ for $m \geq 1$, e.g., $F : \mathbb{F}_p^m \to \mathbb{F}_p$ and the calligraphic font to denote functions over $\mathbb{F}_p^n$ for $n \geq 1$, e.g., $\mathcal{S} : \mathbb{F}_p^n \to \mathbb{F}_p^n$. Given a matrix $M \in \mathbb{F}_p^{r \times c}$, we denote by $M^T \in^{c \times r}$ its transpose. We formally define the term "collision" as:

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

2.2 Related Works: Invertibility of $\mathcal{S}_F$ over $\mathbb{F}_p^n$ via a Quadratic Local Map $F : \mathbb{F}_p^m \to \mathbb{F}_p$

As already mentioned in the introduction, Grassi et al. [24] studied the invertibility of *shift-invariant lifting functions*:

Definition 2 (Shift-Invariant lifting). *Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Let $F : \mathbb{F}_p^m \to \mathbb{F}_p$ be a local map. The* shift-invariant lifting *(SI–lifting) function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ induced by the local map F is defined as*

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

where indexes i of x_i are taken modulo n.

In particular, they considered shift-invariant lifting functions $\mathcal{S}_F$ induced over $\mathbb{F}_p^n$ by a *quadratic* local map $F : \mathbb{F}_p^m \to \mathbb{F}_p$ for $m \in \{2, 3\}$. As a main result, they proved the following theorem regarding the impossibility to set up permutations for (i) $m = 2$ and $n \geq 3$ and (ii) $m = 3$ and $n \geq 5$. More formally,

Theorem 2 ([24, Theorems 2 & 3]). *Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$. Given $F : \mathbb{F}_p^m \to \mathbb{F}_p$ a quadratic local map, then the SI–lifting function $\mathcal{S}_F$ induced by F over $\mathbb{F}_p^n$ is not invertible neither if $m = 2$ and $n \geq 3$ nor if $m = 3$ and $n \geq 5$.*

For the cases $(m, n) \in \{(2, 2), (3, 3), (3, 4)\}$ they presented some local quadratic maps F for which $\mathcal{S}_F$ over $\mathbb{F}_p^n$ is invertible. In particular, in the case $(m, n) = (2, 2)$, invertibility can be achieved *only* with the shift-invariant lifting induced by a local map having the Lai–Massey structure:

Lemma 1 ([24, Proposition 8]). *Let $G : \mathbb{F}_p^2 \to \mathbb{F}_p$ a quadratic local map. Let $\gamma_0, \gamma_1 \in \mathbb{F}_p$ be such that $\gamma_0 \neq \pm\gamma_1$. The shift-invariant lifting function $\mathcal{S}_G$ induced by G over $\mathbb{F}_p^n$ is invertible if and only if*

$$G(x_0, x_1) = \gamma_0 \cdot x_0 + \gamma_1 \cdot x_1 + \gamma_2 \cdot (x_0 - x_1)^2 .$$

3 Alternating/Cyclic Shift-Invariant Lifting Functions via Multiple Local Maps

In this section, we introduce the concept of shift-invariant functions induced by *multiple* local maps, which generalizes the shift-invariant lifting functions recalled before.

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

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

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

For the follow-up, we use a notation similar to the one introduced in [24], that is, we denote the d-degree local map F_j as

$$F_j(x_0, x_1, \ldots, x_{m-1}) := \sum_{\substack{0 \leq i_0, \ldots, i_{m-1} \leq d \text{ s.t.} \\ i_0 + \ldots + i_{m-1} \leq d}} \alpha_{i_0,\ldots,i_{m-1};j} \cdot x_0^{i_0} \cdot \cdots \cdot x_{m-1}^{i_{m-1}} \qquad (1)$$

for each $j \in \{0, 1, \ldots, h-1\}$.

The previous definition corresponds to the one proposed in [24] for the case $h = 1$. In there, it was pointed out that the function $\mathcal{S}_F$ is shift-invariant in the sense that $\mathcal{S}_F \circ \Pi = \Pi \circ \mathcal{S}_F$ for each *translation permutation* Π over $\mathbb{F}_p^n$, that is, a map Π over $\mathbb{F}_p^n$ defined as

$$\begin{aligned} \Pi(x_0, x_1, \ldots, x_{n-1}) := x_{\pi(0)} \| x_{\pi(1)} \| \ldots \| x_{\pi(n-1)} \qquad & \text{where} \\ \forall j \in \{0, 1, \ldots, n-1\} : \qquad \pi(j) := j + i \mod n & \end{aligned}$$

for a certain $i \in \{0, 1, \ldots, n-1\}$. Here, a similar property holds. The function $\mathcal{S}_{F_0,F_1,\ldots F_{h-1}}$ is "cyclic shift-invariant" in the sense that

$$\Pi \circ \mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}(x) = \mathcal{S}_{F_{\pi(0)},F_{\pi(1)},\ldots,F_{\pi(h-1)}} \circ \Pi(x)$$

where the sub-indexes of F are computed modulo h. Hence, note that the π in the sub-index of F is useless if i is a multiple of h (as for the case $h = 1$).

In the rest of the paper, we mainly focus on the case $h = 2$, i.e., functions $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$ where

$$y_i = \begin{cases} F_0(x_i, x_{i+1}, \ldots, x_{i+m-1}) & \text{if } i \text{ is even} \\ F_1(x_i, x_{i+1}, \ldots, x_{i+m-1}) & \text{otherwise (if } i \text{ is odd)} \end{cases} \tag{2}$$

for each $i \in \{0, 1, \ldots, n-1\}$, where the sub-indexes of x_i are taken modulo n. We refer to the alternating shift-invariant function $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ defined via the local maps $F_0 : \mathbb{F}_p^m \to \mathbb{F}_p$ and $F_1 : \mathbb{F}_p^m \to \mathbb{F}_p$ as the *"alternating shift-invariant (m, n)-lifting $\mathcal{S}_{F_0,F_1}$ induced by the pair (F_0, F_1)"* (for simplicity, we usually make use of the abbreviation "ASI-lifting function $\mathcal{S}_{F_0,F_1}$").

3.1 Balanced Functions and Class of Equivalence

First, we recall the definition of balanced functions in order to prove a necessary condition for $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}$ to be invertible. As first thing, we recall a necessary condition that the functions $F_0, F_1, \ldots, F_{h-1}$ must satisfy for $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}$ being invertible.

Definition 4 (Balanced Function). *Let $p \geq 3$ be a prime integer and let $F : \mathbb{F}_p^m \to \mathbb{F}_p$. We say that F is* **balanced** *if and only if*

$$\forall y \in \mathbb{F}_p : \qquad |\{x \in \mathbb{F}_p^m \mid F(x) = y\}| = p^{m-1} .$$

Proposition 1. *Let $p \geq 3$ be a prime integer, and let $1 \leq m, h \leq n$. Let $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}} : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be the cyclic shift-invariant lifting function induced by $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^m \to \mathbb{F}_p$ over $\mathbb{F}_p^n$. If at least one function among $F_0, \ldots, F_{h-1}$ is not balanced, then $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}$ is not invertible.*

This is a well known result, and its proof is a simple generalization of the one provided in [24, Proposition 3].

Next, we introduce an equivalence relation for classifying families of local maps with similar properties that generalizes the one given in [24].

Definition 5 (Class of Equivalence). *Let $p \geq 3$ be a prime integer, and let $1 \leq m, h \leq n$. Let $\{F_i : \mathbb{F}_p^m \to \mathbb{F}_p\}_{1 \leq i < h}$ and $\{F'_i : \mathbb{F}_p^m \to \mathbb{F}_p\}_{1 \leq i < h}$ two indexed sets of functions. We say that the two indexed sets of functions are* similar *– denoted as $(F_0, F_1, \ldots, F_{h-1}) \sim (F'_0, F'_1, \ldots, F'_{h-1})$ – if and only if there exist*

- *a factor $\mu \in \mathbb{F}_p \setminus \{0\}$;*
- *a vector $\bar{\nu} = \nu || \nu || \ldots || \nu \in \mathbb{F}_p^m$;*

– *h values $\omega_i \in \mathbb{F}_p \setminus \{0\}$ and h values $\psi_i \in \mathbb{F}_p$ for $i \in \{0, 1, \ldots, h-1\}$;*

such that we have

$$F'_i(x) = \omega_i \cdot F_i(\mu \cdot x + \bar{\nu}) + \psi_i \qquad \text{for all } x \in \mathbb{F}_p^m \text{ and for any integer } 0 \leq i < h.$$

The following holds:

Lemma 2. *The relation $\sim$ introduced in Definition 5 is an equivalence relation, i.e., it satisfies the following properties: reflexivity, symmetry, and transitivity.*

The proof of this Lemma is equivalent to the one given in [24], where similarity relation is shown to be an equivalence relation.

We show that in the case of cyclic shift-invariant lifting functions, invertibility is an invariant by similarity of the two families of functions which induce the lifting:

Proposition 2. *Let $p \geq 3$ be a prime integer, and let $1 \leq m, h \leq n$. Let $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^m \to \mathbb{F}_p$ and $F'_0, F'_1, \ldots, F'_{h-1} : \mathbb{F}_p^m \to \mathbb{F}_p$ be two similar families of functions. Let*

$$\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}} : F_p^n \to \mathbb{F}_p^n, \qquad \textit{(resp., } \mathcal{S}_{F'_0,F'_1,\ldots,F'_{h-1}} : \mathbb{F}_p^n \to \mathbb{F}_p^n\textit{)}$$

be the cyclic SI-lifting function induced by $(F_0, \ldots, F_{h-1})$ (resp., $(F'_0, \ldots, F'_{h-1})$). Then, $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}$ is invertible if and only if $\mathcal{S}_{F'_0,F'_1,\ldots,F'_{h-1}}$ is invertible.

Proof. By definition of F'_i and $\mathcal{S}_{F'_i}$, we have that

$$[\mathcal{S}_{F'_i}(x_0, \ldots, x_{n-1})]_i = F'_i(x_i, \ldots, x_{i+m-1}),$$

where the sub-indexes are taken modulo n. Since $F'_i(x) = \omega_i \cdot F_i(\mu \cdot x + \bar{\nu}) + \psi_i$ for each $x \in \mathbb{F}_p^m$, it follows that

$$\mathcal{S}_{F'_i}(x) = \omega_{i \bmod h} \cdot \mathcal{S}_{F_i}(\mu \cdot x + \bar{\nu}) + \bar{\psi}$$

where $\bar{\psi} \in \mathbb{F}_q^n$ such that $\bar{\psi}_i = \psi_{i \bmod h}$. That is, $\mathcal{S}_{F'_i}$ is equal to $\mathcal{S}_{F_i}$ pre-composed and post-composed with two invertible affine functions. This implies that $\mathcal{S}_{F'_i}$ is invertible if and only if $\mathcal{S}_{F_i}$ is invertible. □

3.2 Necessary Conditions for Quadratic Functions $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \to \mathbb{F}_p$

As next step, we introduce some necessary conditions that the quadratic functions $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \to \mathbb{F}_p$ should satisfy in order to build an invertible alternating or cyclic shift-invariant lifting $\mathcal{S}_{F_0,F_1,\ldots,F_{h-1}}$.

Lemma 3. *Let $p \geq 3$ be a prime integer, and let $n \geq 2$ be an integer. Let $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \to \mathbb{F}_p$ be $1 \leq h \leq n$ be quadratic functions. For each $j \in \{0, 1, \ldots, h-1\}$ and for each $i \in \{0, 1, 2\}$, let*

$$\alpha_j^{(i)} := \sum_{\substack{0 \leq i_0, i_1, \ldots, i_{h-1} \leq i \text{ s.t.} \\ i_0 + i_1 + \ldots + i_{h-1} = i}} \alpha_{i_0, i_1, \ldots, i_{h-1}; j} \tag{3}$$

be the sum of the coefficients of the monomials of degree i of the function F_j.

Let $\mathfrak{I} \subseteq \{0, 1, \ldots, h-1\}$ be the set of indices such that, for each $i \in \mathfrak{I}$, $\alpha_i^{(1)} = \alpha_i^{(2)} = 0$. If

$$\forall i, j \in \{0, 1, \ldots, h-1\} \setminus \mathfrak{I} : \qquad \alpha_j^{(1)} \cdot \alpha_i^{(2)} = \alpha_j^{(2)} \cdot \alpha_i^{(1)} ,$$

*then the cyclic SI-lifting $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ over $\mathbb{F}_p^n$ for $n \geq 3$ is **not** invertible.*

Proof. We prove such result by proposing collisions via inputs of the form $(x, x, \ldots, x)$ and $(y, y, \ldots, y)$ for $x \neq y$. A collision occurs if $F_j(x, x) = F_j(y, y)$ for each $j \in \{0, 1, \ldots, h-1\}$. By denoting $d = x - y \neq 0$ and $s = x + y$, these conditions hold if

$$\forall j \in \{0, 1, \ldots, h-1\} : \qquad s \cdot \alpha_j^{(2)} + \alpha_j^{(1)} = 0 .$$

It follows that

- if $\alpha_i^{(1)} = \alpha_i^{(2)} = 0$ for a certain $i \in \{0, 1, \ldots, h-1\}$, then such condition is always satisfied independently of s;
- otherwise, if for each $i, j \in \{0, 1, \ldots, h-1\} \setminus \{\mathfrak{I}\}$, there exists $\gamma_{i,j} \in \mathbb{F}_p \setminus \{0\}$ such that (i) $\alpha_j^{(1)} = \gamma_{i,j} \cdot \alpha_i^{(1)}$ and simultaneously (ii) $\alpha_i^{(2)} = \gamma_{i,j} \cdot \alpha_j^{(2)} \neq 0$, then the system reduces to a single equation, and a collision can be found.

Note that the existence of $\gamma_{i,j}$ is equivalent to the condition $\alpha_j^{(1)} \cdot \alpha_i^{(2)} = \alpha_j^{(2)} \cdot \alpha_i^{(1)}$ to hold. □

Another important requirement is that the quadratic functions $F_0, \ldots, F_{h-1}$ should not depend on a single variable, otherwise the alternating or cyclic shift-invariant lifting $\mathcal{S}_{F_0, \ldots, F_{h-1}}$ is not invertible.

Lemma 4. *Let $p \geq 3$ be a prime integer, and let $n \geq 2$ be an integer. Let $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^2 \to \mathbb{F}_p$ be $1 \leq h \leq n$ quadratic functions. If there exists $l \leq h$ such that the quadratic function F_l depends on a single variable, i.e.,*

$$F_l(x_0, x_1) = \alpha_{2 \cdot (1-i), 2i; l} \cdot x_i^2 + \alpha_{1-i, i; l} \cdot x_i + \alpha_{0,0; l} ,$$

*for $i \in \{0, 1\}$ and where $\alpha_{2 \cdot (1-i), i; l} \neq 0$, then the cyclic SI-lifting $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ defined over $\mathbb{F}_p^n$ for $n \geq 3$ is **not** invertible.*

Proof. As it is well known, a function of the form $x \mapsto \gamma_2 \cdot x^2 + \gamma_1 \cdot x + \gamma_0$ for $\gamma_2 \neq 0$ is not invertible and not balanced (indeed, there are $(p-1)/2$ $\mathbb{F}_p$ elements with two pre-images, $(p-1)/2$ $\mathbb{F}_p$ elements with zero pre-image, and 1 $\mathbb{F}_p$ element with one pre-image). Since this implies that $F_l(x_0, x_1)$ is not balanced as well, we can immediately conclude that $\mathcal{S}_{F_0, F_1, \ldots, F_{h-1}}$ is not invertible due to Proposition 1. □

4 Invertible Functions $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ via Quadratic $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$

In this section, we show an impossibility result: given two quadratic local maps $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$, we prove that it is not possible to build an invertible ASI-lifting $\mathcal{S}_{F_0,F_1} : \mathbb{F}_p^n \to \mathbb{F}_p^n$ for $n \geq 3$. We recall that for $n = 2$ there exist quadratic functions for which $\mathcal{S}$ is invertible, e.g., $F_0(x_0, x_1) = F_1(x_0, x_1) = x_0 + (x_0 - x_1)^2$.

The following proposition represents the main result of this section.

Proposition 3. *Let $p \geq 3$ be a prime integer. Let $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ be two quadratic functions. Then the ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ for $n \geq 3$ is **not** invertible.*

We divide the proof of the proposition in two parts:

- the case $n \geq 4$ even in Section 4.1;
- the case $n \geq 3$ odd in Section 4.2.

We study the case $n \geq 4$ even and the case $n \geq 3$ odd separately since the numbers of repetitions of F_0 and F_1 in $\mathcal{S}_{F_0,F_1}$ is different if n is odd. Then, collisions we find in order to prove the non-invertibility of $\mathcal{S}_{F_0,F_1}$ are slightly different.

4.1 Proof of Proposition 3 for the Case n Even

We separate the proof for the case n even in three lemmas:

- Lemma 5: $\alpha_{1,1;0} \neq 0, \alpha_{1,1;1} \neq 0$;
- Lemma 6: $\alpha_{1,1;0} = 0, \alpha_{1,1;1} \neq 0$ (or $\alpha_{1,1;0} \neq 0, \alpha_{1,1;1} = 0$);
- Lemma 7: $\alpha_{1,1;0} = \alpha_{1,1;1} = 0$.

Together, these lemmas show collisions for each possible ASI-lifting $\mathcal{S}_{F_0,F_1}$ where $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ are quadratic and $n \geq 4$ is even, proving Proposition 3.

Lemma 5. *Let $p \geq 3$ be a prime integer, and let $n \geq 4$ be an even number. Let F_0, F_1 be two quadratic functions such that $\alpha_{1,1;0} \neq 0, \alpha_{1,1;1} \neq 0$. Then, the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.*

Proof. Consider inputs $(x_0, x_1, x_2, x_3, \ldots, x_{n-1})$ and $(y_0, y_1, y_2, y_3, \ldots, y_{n-1}) = (x_0, x_1, y_2, x_3, \ldots, x_{n-1})$, i.e., *two inputs that differ only for the values of x_2, y_2, while the others are equal.* Then, the system $\mathcal{S}_{F_0,F_1}(x_0, x_1, x_2, x_3, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(x_0, x_1, y_2, x_3, \ldots, x_{n-1})$ reduces to the two equations

$$F_1(x_1, x_2) = F_1(x_1, y_2) \quad \text{and} \quad F_0(x_2, x_3) = F_0(y_2, x_3),$$

while the other equations are obviously satisfied (since the inputs are equal). Such two equations are equal to

$$\alpha_{0,2;1} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;1}}{2} \cdot d_2 \cdot s_1 + \alpha_{0,1;1} \cdot d_2 = 0\,,$$
$$\alpha_{2,0;0} \cdot d_2 \cdot s_2 + \frac{\alpha_{1,1;0}}{2} \cdot d_2 \cdot s_3 + \alpha_{1,0;0} \cdot d_2 = 0\,,$$

via the change of variables

$$d_i = x_i - y_i \qquad \text{and} \qquad s_i = x_i + y_i \,. \tag{4}$$

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

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

The determinant of the left hand side (*l.h.s.*, for short) matrix $\frac{\alpha_{1,1;1} \cdot \alpha_{1,1;0}}{4}$ is always different from zero, given that $\alpha_{1,1;0} \neq 0, \alpha_{1,1;1} \neq 0$. Then, the system is compatible and the solution provides a collision for $\mathcal{S}_{F_0,F_1}$. □

Lemma 6. *Let $p \geq 3$ be a prime integer, and let $n \geq 4$ be an even number. Let F_0, F_1 be two quadratic functions such that $\alpha_{1,1;0} = 0, \alpha_{1,1;1} \neq 0$ (or viceversa). Then, the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.*

Proof. First, note that, since $\alpha_{1,1;0} = 0$, at least one between $\alpha_{2,0;0}, \alpha_{0,2;0}$ is non-zero, otherwise F_0 would be linear. Let's first consider the case where $\alpha_{2,0;0} \neq 0$, and let's consider again inputs of the form $(x_0, x_1, x_2, x_3, \ldots, x_{n-1})$ and $(y_0, y_1, y_2, y_3, \ldots, y_{n-1}) = (x_0, x_1, y_2, x_3, \ldots, x_{n-1})$, with $x_2 \neq y_2$. Using the change of variables (4) and considering that $d_2 \neq 0$, the system can be written as

$$\begin{bmatrix} \frac{\alpha_{1,1;1}}{2} & \alpha_{0,2;1} \\ 0 & \alpha_{2,0;0} \end{bmatrix} \times \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = \begin{bmatrix} -\alpha_{0,1;1} \\ -\alpha_{1,0;0} \end{bmatrix},$$

The determinant of the l.h.s. matrix is $\frac{\alpha_{1,1;1}}{2} \cdot \alpha_{2,0;0} \neq 0$, then the system is compatible, i.e., it has a solution that is a collision for $\mathcal{S}_{F_0,F_1}$.

On the other side, if $\alpha_{0,2;0} \neq 0$, we set up a collision by considering the inputs $(x_0, x_1, x_2, \ldots, x_{n-1})$ and $(y_0, y_1, y_2, \ldots, y_{n-1}) = (x_0, y_1, x_2, \ldots, x_{n-1})$, where $x_1 \neq y_1$ and $d_i = 0$ for all $i \neq 1$. The system $\mathcal{S}_{F_0,F_1}(x_0, x_1, x_2, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(x_0, y_1, x_2, \ldots, x_{n-1})$ reduces to the equations $F_0(x_0, x_1) = F_0(x_0, y_1)$ and $F_1(x_1, x_2) = F_0(y_1, x_2)$, while the other equations are obviously satisfied. Using that $d_1 \neq 0$, it corresponds to

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

Since the determinant of the l.h.s. matrix is $\alpha_{0,2;0} \cdot \frac{\alpha_{1,1;1}}{2} \neq 0$, then the system has a solution, i.e., the ASI-lifting has a collision.

The case where $\alpha_{1,1;0} \neq 0, \alpha_{1,1;1} = 0$ is equivalent: we can find the collisions for $\mathcal{S}_{F_0,F_1}$ starting from inputs $(x_0, x_1, x_2, \ldots, x_{n-1}), (y_0, y_1, y_2, y_3, \ldots, y_{n-1}) = (x_0, y_1, x_2, \ldots, x_{n-1})$ if $\alpha_{2,0;1} \neq 0$, while if $\alpha_{0,2;1} \neq 0$ we work with inputs $(x_0, x_1, x_2, x_3, \ldots, x_{n-1})$, $(y_0, y_1, y_2, y_3, \ldots, y_{n-1}) = (x_0, x_1, y_2, x_3, \ldots, x_{n-1})$.

□

Lemma 7. *Let $p \geq 3$ be a prime integer, and let $n \geq 4$ be an even number. Let F_0, F_1 be two quadratic functions such that $\alpha_{1,1;0} = \alpha_{1,1;1} = 0$. Then, the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.*

Proof. In order to prove the lemma, we set up a collision by working with the system $\mathcal{S}_{F_0,F_1}(x_0,\ldots,x_{n-1}) = \mathcal{S}_{F_0,F_1}(y_0,\ldots,y_{n-1})$, that is,

$$\begin{bmatrix} \alpha_{2,0;0}\cdot d_0 & \alpha_{0,2;0}\cdot d_1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \alpha_{2,0;1}\cdot d_1 & \alpha_{0,2;1}\cdot d_2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \alpha_{2,0;0}\cdot d_2 & \alpha_{0,2;0}\cdot d_3 & \ldots & 0 & 0 \\ \vdots & & & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & \alpha_{2,0;1}\cdot d_{n-2} & \alpha_{0,2;1}\cdot d_{n-1} \\ \alpha_{0,2;1}\cdot d_0 & 0 & 0 & 0 & \ldots & 0 & \alpha_{2,0;1}\cdot d_{n-1} \end{bmatrix} \times \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ \vdots \\ s_{n-2} \\ s_{n-1} \end{bmatrix}$$

$$= - \begin{bmatrix} \alpha_{1,0;0}\cdot d_0 + \alpha_{0,1;0}\cdot d_1 \\ \alpha_{1,0;1}\cdot d_1 + \alpha_{0,1;1}\cdot d_2 \\ \alpha_{1,0;0}\cdot d_2 + \alpha_{0,1;0}\cdot d_3 \\ \vdots \\ \alpha_{1,0;0}\cdot d_{n-2} + \alpha_{0,1;0}\cdot d_{n-1} \\ \alpha_{1,0;1}\cdot d_{n-1} + \alpha_{0,1;1}\cdot d_0 \end{bmatrix} \tag{5}$$

where d_i and s_i are defined as in Equation (4). The determinant of the l.h.s. matrix is $\left(\alpha_{2,0;0}^{\frac{n}{2}}\cdot\alpha_{2,0;1}^{\frac{n}{2}} - \alpha_{0,2;0}^{\frac{n}{2}}\cdot\alpha_{0,2;1}^{\frac{n}{2}}\right)\cdot\prod_{i=0}^{n-1} d_i$. Then, by taking $d_i \neq 0$ for all i, the determinant is different from zero if $\alpha_{2,0;0}^{\frac{n}{2}}\cdot\alpha_{2,0;1}^{\frac{n}{2}} - \alpha_{0,2;0}^{\frac{n}{2}}\cdot\alpha_{0,2;1}^{\frac{n}{2}} \neq 0$. Otherwise, if $\alpha_{2,0;0}^{\frac{n}{2}}\cdot\alpha_{2,0;1}^{\frac{n}{2}} = \alpha_{0,2;0}^{\frac{n}{2}}\cdot\alpha_{0,2;1}^{\frac{n}{2}}$, the rows of the matrix are linearly dependent, i.e., there exists a linear combination among the rows that is equal to zero. This means that the same linear combination holds for the rows of the right hand side (*r.h.s.*, for short) vector, i.e., there exist $\{\lambda_i\}_{i\in\{0,\ldots,n-1\}} \in \mathbb{F}_p \setminus \{0\}$ such that

$$\sum_{i=0}^{n-1} \lambda_i \cdot (\alpha_{1,0;i \bmod 2}\cdot d_i + \alpha_{0,1;i \bmod 2}\cdot d_{i+1}) = 0.$$

Let d_0 be the variable that satisfies such combination. Then, we can rewrite the system as

$$\begin{bmatrix} \alpha_{2,0;1}\cdot d_1 & \alpha_{0,2;1}\cdot d_2 & 0 & \ldots & 0 & 0 \\ 0 & \alpha_{2,0;0}\cdot d_2 & \alpha_{0,2;0}\cdot d_3 & \ldots & 0 & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \alpha_{2,0;0}\cdot d_{n-2} & \alpha_{0,2;0}\cdot d_{n-1} \\ 0 & 0 & 0 & \ldots & 0 & \alpha_{2,0;1}\cdot d_{n-1} \end{bmatrix} \times \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{n-2} \\ s_{n-1} \end{bmatrix}$$

$$= - \begin{bmatrix} \alpha_{1,0;1}\cdot d_1 + \alpha_{0,1;1}\cdot d_2 \\ \alpha_{1,0;0}\cdot d_2 + \alpha_{0,1;0}\cdot d_3 \\ \vdots \\ \alpha_{1,0;0}\cdot d_{n-2} + \alpha_{0,1;0}\cdot d_{n-1} \\ \alpha_{1,0;1}\cdot d_{n-1} + d_0\cdot(\alpha_{0,1;1} + \alpha_{0,2;1}\cdot s_0) \end{bmatrix},$$

where s_0 is a free variable. The determinant of the l.h.s. matrix is $\left(\alpha_{2,0;1}^{\frac{n}{2}}\cdot\alpha_{2,0;0}^{\frac{n}{2}-1}\right)\cdot\prod_{i=1}^{n-1} d_i$, which is non-null if and only if $\alpha_{2,0;0} \neq 0$ and $\alpha_{2,0;1} \neq 0$. In such a

case, a collision exists.

SubCase: $\alpha_{2,0;1} = 0$ *and* $\alpha_{2,0;0} \neq 0$. In such a case, the linear system (5) is equal to

$$\begin{bmatrix} \alpha_{2,0;0} \cdot d_0 & \alpha_{0,2;0} \cdot d_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \alpha_{0,2;1} \cdot d_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & \alpha_{2,0;0} \cdot d_2 & \alpha_{0,2;0} \cdot d_3 & \dots & 0 & 0 \\ \vdots & & & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \alpha_{2,0;0} \cdot d_{n-2} & \alpha_{0,2;0} \cdot d_{n-1} \\ \alpha_{0,2;1} \cdot d_0 & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \times \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ \vdots \\ s_{n-2} \\ s_{n-1} \end{bmatrix}$$

$$= - \begin{bmatrix} \alpha_{1,0;0} \cdot d_0 + \alpha_{0,1;0} \cdot d_1 \\ \alpha_{1,0;1} \cdot d_1 + \alpha_{0,1;1} \cdot d_2 \\ \alpha_{1,0;0} \cdot d_2 + \alpha_{0,1;0} \cdot d_3 \\ \vdots \\ \alpha_{1,0;0} \cdot d_{n-2} + \alpha_{0,1;0} \cdot d_{n-1} \\ \alpha_{1,0;1} \cdot d_{n-1} + \alpha_{0,1;1} \cdot d_0 \end{bmatrix}.$$

The determinant of the l.h.s. matrix is $-\left(\alpha_{0,2;0}^{\frac{n}{2}} \cdot \alpha_{0,2;1}^{\frac{n}{2}}\right) \cdot \prod_{i=0}^{n-1} d_i$. Since $\alpha_{0,2;1} \neq 0$, otherwise F_1 would be linear, the determinant is not null unless $\alpha_{0,2;0} = 0$. In such a case, consider $\mathcal{S}_{F_0,F_1}(x_0, x_1, \dots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(y_0, y_1, \dots, y_{n-1})$, that is

$$\begin{bmatrix} \alpha_{2,0;0} \cdot d_0 & \alpha_{0,1;0} & 0 & \dots & 0 & 0 \\ 0 & \alpha_{1,0;1} & \alpha_{0,2;1} \cdot d_2 & \dots & 0 & 0 \\ \vdots & & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \alpha_{2,0;0} \cdot d_{n-2} & \alpha_{0,1;0} \\ \alpha_{0,2;1} \cdot d_0 & 0 & 0 & \dots & 0 & \alpha_{1,0;1} \end{bmatrix} \times \begin{bmatrix} s_0 \\ d_1 \\ \vdots \\ s_{n-2} \\ d_{n-1} \end{bmatrix} = - \begin{bmatrix} \alpha_{1,0;0} \cdot d_0 \\ \alpha_{0,1;1} \cdot d_2 \\ \vdots \\ \alpha_{1,0;0} \cdot d_{n-2} \\ \alpha_{0,1;1} \cdot d_0 \end{bmatrix}.$$

We solve this system of n equations with respect to the variables s_i for even i and d_i for odd i, that gives the set of variables $\{s_0, d_1, s_2, d_3 \dots, s_{n-2}, d_{n-1}\}$. We leave the other d_i's as free variables.

The determinant of the l.h.s. matrix is

$$\prod_{i \text{ even}} d_i \cdot \left(\alpha_{2,0;0}^{\frac{n}{2}} \cdot \alpha_{1,0;1}^{\frac{n}{2}} + \alpha_{0,2;1}^{\frac{n}{2}} \cdot \alpha_{0,1;0}^{\frac{n}{2}}\right).$$

If $\left(\alpha_{2,0;0}^{\frac{n}{2}} \cdot \alpha_{1,0;1}^{\frac{n}{2}} + \alpha_{0,2;1}^{\frac{n}{2}} \cdot \alpha_{0,1;0}^{\frac{n}{2}}\right) \neq 0$ and if we choose $d_i \neq 0$ for all i, the system is compatible and there is a collision for the ASI-lifting. Otherwise, there is a linear combination among the rows of the matrix that is equal to zero, i.e., there exist $\{\lambda_i\}_{i \in \{0,\dots,n-1\}} \in \mathbb{F}_p \setminus \{0\}$ such that

$$\sum_{i \text{ even}} (\lambda_i \cdot \alpha_{1,0;0} \cdot d_i + \lambda_{i+1} \cdot \alpha_{0,1;1} \cdot d_{i+2}) = 0.$$

Then, suppose that d_1 satisfies this combination. We can rewrite the system as

$$\begin{bmatrix} \alpha_{2,0;0} \cdot d_0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & \alpha_{2,0;0} \cdot d_2 & \alpha_{0,1;0} & 0 & \dots & 0 & 0 \\ 0 & 0 & \alpha_{1,0;1} & \alpha_{0,2;1} \cdot d_4 & \dots & 0 & 0 \\ \vdots & & & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \alpha_{2,0;0} \cdot d_{n-2} & \alpha_{0,1;0} \\ \alpha_{0,2;1} \cdot d_0 & 0 & 0 & 0 & \dots & 0 & \alpha_{1,0;1} \end{bmatrix} \times \begin{bmatrix} s_0 \\ s_2 \\ d_3 \\ \vdots \\ s_{n-2} \\ d_{n-1} \end{bmatrix} =$$

$$- \left[\alpha_{1,0;0} \cdot d_0; \alpha_{0,1;1} \cdot d_2 + \alpha_{1,0;1} \cdot d_1; \alpha_{1,0;0} \cdot d_2; \dots; \alpha_{1,0;0} \cdot d_{n-2}; \alpha_{0,1;1} \cdot d_0\right]^T .$$

The determinant of the l.h.s. matrix is $\prod_{i \text{ even}} d_i \cdot \left(\alpha_{2,0;0}^{\frac{n}{2}} \cdot \alpha_{1,0;1}^{\frac{n}{2}-1}\right)$. Since $\alpha_{2,0;0} \neq 0$ (otherwise F_0 would be linear), this determinant is non-zero if $\alpha_{1,0;1} \neq 0$. If $\alpha_{1,0;1} = 0$, F_1 is non-balanced due to Lemma 4, then $\mathcal{S}_{F_0,F_1}$ is always non-invertible. The case where $\alpha_{2,0;1} \neq 0$ and $\alpha_{2,0;0} = 0$ is analogous.

SubCase: $\alpha_{2,0;1} = \alpha_{2,0;0} = 0$. In such a case, the linear system (5) reduces to

$$\begin{aligned} \forall i \in \{1, 3, \dots, n-1\} : &\quad \alpha_{0,2;0} \cdot d_i \cdot s_i = -\alpha_{1,0;0} \cdot d_{i-1} - \alpha_{0,1;0} \cdot d_i \\ \forall i \in \{0, 2, \dots, n-2\} : &\quad \alpha_{0,2;1} \cdot d_i \cdot s_i = -\alpha_{1,0;1} \cdot d_{i-1} - \alpha_{0,1;1} \cdot d_i \,. \end{aligned}$$

Note that $\alpha_{0,2;1} \neq 0$ and $\alpha_{0,2;0} \neq 0$, otherwise F_0, F_1 would be linear. By taking $d_i \neq 0$ for all i, a solution of such system of equations is given by

$$\begin{aligned} \forall i \in \{1, 3, \dots, n-1\} : &\quad s_i = -\frac{\alpha_{1,0;0} \cdot d_{i-1} + \alpha_{0,1;0} \cdot d_i}{\alpha_{0,2;0} \cdot d_i} \\ \forall i \in \{0, 2, \dots, n-2\} : &\quad s_i = \frac{\alpha_{1,0;1} \cdot d_{i-1} + \alpha_{0,1;1} \cdot d_i}{\alpha_{0,2;1} \cdot d_i} \,, \end{aligned}$$

which corresponds to a collision for the analyzed ASI-lifting function. □

4.2 Proof of Proposition 3 for the Case n Odd

In order to prove Proposition 3 in the case n odd, we separate the proof again in three lemmas:

- Lemma 8: $\alpha_{1,1;0} \neq 0$;
- Lemma 9: $\alpha_{1,1;0} = 0, \alpha_{1,1;1} \neq 0$;
- Lemma 10: $\alpha_{1,1;0} = \alpha_{1,1;1} = 0$.

As before, these lemmas analyze each possible $\mathcal{S}_{F_0,F_1}$ for $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ are quadratic functions and n is odd, showing the non-invertibility of the ASI-lifting.

Lemma 8. *Let $p \geq 3$ be a prime integer, and let $n \geq 3$ be an odd number. Let F_0, F_1 be two quadratic functions such that $\alpha_{1,1;0} \neq 0$. Then, the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.*

Proof. Consider inputs of the form $(x_0, x_1, \ldots, x_{n-1})$ and $(y_0, y_1, \ldots, y_{n-1}) = (y_0, x_1, \ldots, x_{n-1})$, i.e., inputs that differ just in the first element. Referring to the change of variables in Equation (4), we suppose $d_0 \neq 0$, while $d_i = 0$ for all $i \in \{1, 2, \ldots, n-1\}$. Then, the system $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(y_0, x_1, \ldots, x_{n-1})$ can be represented as

$$\begin{bmatrix} \frac{\alpha_{1,1;0}}{2} & 0 \\ 0 & \frac{\alpha_{1,1;0}}{2} \end{bmatrix} \times \begin{bmatrix} s_1 \\ s_{n-1} \end{bmatrix} = - \begin{bmatrix} \alpha_{2,0;0} \cdot s_0 + \alpha_{1,0;0} \\ \alpha_{0,2;0} \cdot s_0 + \alpha_{0,1;0} \end{bmatrix}.$$

Since the determinant of the l.h.s. matrix is $\left(\frac{\alpha_{1,1;0}}{2}\right)^2 \neq 0$, the system is compatible, i.e., it is always possible to find a collision for the ASI-lifting. □

Lemma 9. *Let $p \geq 3$ be a prime integer, and let $n \geq 3$ be an odd number. Let F_0, F_1 be two quadratic functions such that $\alpha_{1,1;0} = 0, \alpha_{1,1;1} \neq 0$. Then, the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.*

Proof. Let start from inputs $(x_0, x_1, x_2, \ldots, x_{n-1})$ and $(y_0, y_1, y_2, \ldots, y_{n-1}) = (x_0, y_1, x_2, \ldots, x_{n-1})$, where only $x_1 \neq y_1$, while the others are equal. In such a case, by using the change of variables defined in Equation (4) and the fact that $d_1 \neq 0$, the system $\mathcal{S}_{F_0,F_1}(x_0, x_1, x_2, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(x_0, y_1, x_2, \ldots, x_{n-1})$ can be written as

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

Since the determinant of the l.h.s. matrix is $\alpha_{0,2;0} \cdot \frac{\alpha_{1,1;1}}{2}$ and $\alpha_{1,1;1} \neq 0$, the system is compatible if and only if $\alpha_{0,2;0} \neq 0$. Otherwise, we can find a collision for $\mathcal{S}_{F_0,F_1}$ using inputs $(x_0, x_1, x_2, x_3, \ldots, x_{n-1})$ and $(y_0, y_1, y_2, y_3, \ldots, y_{n-1}) = (x_0, x_1, y_2, x_3, \ldots, x_{n-1})$, i.e., with $d_2 \neq 0$ and $d_i = 0$ for $i \neq 2$. Then, the system is

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

The determinant of the l.h.s. matrix is $\alpha_{2,0;0} \cdot \frac{\alpha_{1,1;1}}{2} \neq 0$, since $\alpha_{2,0;0} \neq 0$, otherwise F_0 would be a linear function. □

Lemma 10. *Let $p \geq 3$ be a prime integer, and let $n \geq 3$ be an odd number. Let F_0, F_1 be two quadratic functions such that $\alpha_{1,1;0} = \alpha_{1,1;1} = 0$. Then, the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is not invertible.*

Proof. The proof is analogous to the one provided to prove Lemma 7. □

5 Invertible Functions $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ via Linear F_0 and Quadratic F_1 (or Vice-Versa)

In this section, we analyse the ASI-lifting functions $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ induced by a linear local map $F_0 : \mathbb{F}_p^2 \to \mathbb{F}_p$ and a quadratic one $F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$, or vice-versa. The main result is given in the following proposition.

Proposition 4. *Let $p \geq 3$ be a prime integer, and let $n \geq 3$. Let $F_0 : \mathbb{F}_p^2 \to \mathbb{F}_p$ be a linear function and $F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ a quadratic function, or vice-versa. If $n > 3$, then $\mathcal{S}_{F_0,F_1}$ is invertible if and only if it is a Type-II Feistel scheme, that is,*

- *F_0 (resp., F_1) depends on one variable only, and*
- *$F_1(x_0, x_1) = \alpha_{1-i,i;1} \cdot x_i + H(x_{1-i})$ for $i \in \{0, 1\}$, where $H : \mathbb{F}_p \to \mathbb{F}_p$ is a quadratic function (resp., $F_0(x_0, x_1) = \alpha_{1-i,i;0} \cdot x_i + H(x_{1-i})$).*

If $n = 3$, then $\mathcal{S}_{F_0,F_1}$ is invertible if and only if

- *it is a Type-II Feistel scheme (as before), or*
- *$F_0(x_0, x_1) = \alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1$, $\alpha_{1,0;0}, \alpha_{0,1;0} \neq 0$, and $F_1(x_0, x_1) = \gamma \cdot \left(\frac{\alpha_{0,1;0}}{\alpha_{1,0;0}} \cdot x_0 - \frac{\alpha_{1,0;0}}{\alpha_{0,1;0}} \cdot x_1\right)^2 + \alpha_{1,0;1} \cdot x_0 + \alpha_{0,1;1} \cdot x_1$, with $\gamma \in \mathbb{F}_p$ and $\alpha_{1,0;1} \cdot \alpha_{1,0;0}^2 \neq -\alpha_{0,1;1} \cdot \alpha_{0,1;0}^2$.*

The proof is organized as follows:

- first, for $n \geq 4$, we show that if one of the two functions is linear and depends on a single variable only, then the only invertible ASI-liftings are the Type-II Feistel schemes;
- in Section 5.1, we study the case $n \geq 4$ even, showing that no ASI-lifting $\mathcal{S}_{F_0,F_1}$ is invertible besides the Type-II Feistel one;
- in Section 5.2, we study the case $n \geq 3$ odd. We divide the proof in two subcases: Lemma 13 deals with the case where F_0 is quadratic and F_1 linear, while Lemma 14 proves the proposition for F_0 linear and F_1 quadratic, including the special result for the case $n = 3$.

As we did in the previous section, we study the cases n even and n odd separately, since the numbers of repetitions of F_0 and F_1 in $\mathcal{S}_{F_0,F_1}$ is different if n is odd. Moreover, due to Definition 5, we assume $\alpha_{0,0;0} = \alpha_{0,0;1} = 0$, and we usually work with a linear function of the form $F_l(x_0, x_1) = x_0 + \alpha \cdot x_1$ or $F_l(x_0, x_1) = x_1 + \alpha \cdot x_0$ for $\alpha \in \mathbb{F}_p$ and $l \in \{0, 1\}$.

Type-II Feistel Schemes for $n \geq 4$. First of all, we consider the case in which one function is linear and depends on a single variable only. In the next lemma, we prove that the only functions $\mathcal{S}_F$ of this form that are invertible are the Type-II Feistel schemes [30, 34].

Lemma 11. *Let $p \geq 3$ be a prime integer, and let $n \geq 4$. Let $F_j(x_0, x_1) = x_i$ for $i, j \in \{0, 1\}$ be a linear function over $\mathbb{F}_p$ that depends on one variable only. The corresponding ASI-lifting function $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ for $n \geq 4$ is invertible if and only if F_{1-j} is linear in one of the two variables, that is, $F_{1-j}(x_0, x_1) = x_l + H(x_{1-l})$ for $l \in \{0, 1\}$.*

We point out that the previous scheme corresponds to a Type-II Feistel scheme. We emphasize that for $n = 3$ there exist ASI-lifting functions $\mathcal{S}_{F_0,F_1}$ that are invertible even if (i) F_0 (resp., F_1) is linear and does not depend on a single variable and (ii) $\mathcal{S}_{F_0,F_1}$ is not a Type-II Feistel scheme – see Lemma 14.

Proof. We limit ourselves to propose the proof for the case $n \geq 4$ even only. The proof for the case $n \geq 5$ odd is analogous, independently of the fact that F_0 or F_1 is linear.

W.l.o.g., let $F_0(x_0, x_1) = x_0$ (i.e., $\alpha_{0,1;0} = 0$) – the other cases are analogous since n is even. Then, given a generic quadratic function F_1, we have that $y = \mathcal{S}_{F_0,F_1}(x)$ corresponds to

$$\begin{aligned} y_i &= \alpha_{2,0;1} \cdot x_i^2 + \alpha_{1,1;1} \cdot x_i \cdot x_{i+1} + \alpha_{0,2;1} \cdot x_{i+1}^2 + \alpha_{1,0;1} \cdot x_i + \alpha_{0,1;1} \cdot x_{i+1} \,, \\ y_{i+1} &= x_{i+1} \,, \end{aligned}$$

for each $i \in \{1, 3, \ldots, n-1\}$. By replacing the second equation in the first one, we get

$$\alpha_{2,0;1} \cdot x_i^2 + (\alpha_{1,1;1} \cdot y_{i+1} + \alpha_{1,0;1}) \cdot x_i + (\alpha_{0,2;1} \cdot y_{i+1}^2 + \alpha_{0,1;1} \cdot y_{i+1} - y_i) = 0$$

for each $i \in \{1, 3, \ldots, n-1\}$. Note that each equation depends on a different variable x_i. By working independently on each one of such equations, it follows that the ASI-lifting function $\mathcal{S}_{F_0,F_1}$ is always invertible if and only if

- the coefficient of the monomial x_i^2 is zero, that is, $\alpha_{2,0;1} = 0$;
- the coefficient of the monomial x_i is non-null, that is, $\alpha_{1,1;1} \cdot y_{i+1} + \alpha_{1,0;1} \neq 0$.

Since y_{i+1} can take any possible value, then the second condition is satisfied only by $\alpha_{1,1;1} = 0$ and $\alpha_{1,0;1} \neq 0$. This concludes the proof.

□

5.1 Proof of Proposition 4 for the Case n Even

In this subsection, we only consider the case F_0 linear and F_1 quadratic. We emphasize that the case F_0 quadratic and F_1 linear is equivalent, since n is even.

Lemma 12. *Let $p \geq 3$ be a prime integer, and let $n \geq 4$ be an even number. Let $F_0(x_0, x_1) = \alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1$ be a linear function over $\mathbb{F}_p$, while let $F_1(x_0, x_1)$ be a quadratic function over $\mathbb{F}_p$. Then, the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is invertible if and only if*

1. *$\alpha_{1,0;0} = 0$ or $\alpha_{0,1;0} = 0$;*
2. *$F_1(x_0, x_1) = \alpha_{1-i,i;1} \cdot x_i + H(x_{1-i})$ for $i \in \{0, 1\}$, where $H : \mathbb{F}_p \to \mathbb{F}_p$ is a quadratic function.*

Proof. We already proved in Lemma 11 that, if $\alpha_{1,0;0} = 0$ or $\alpha_{0,1;0} = 0$, Type-II Feistel are the only invertible ASI-liftings. For this reason, we consider the case $F_0(x_0, x_1) = x_0 + \alpha_{0,1;0} \cdot x_1$ with $\alpha_{0,1;0} \neq 0$. Here, we prove that the corresponding $\mathcal{S}_{F_0,F_1}$ is never invertible by constructing a collision. Let $y = \mathcal{S}_{F_0,F_1}(x)$, then

$$\begin{aligned} y_i &= \alpha_{2,0;1} \cdot x_i^2 + \alpha_{1,1;1} \cdot x_i \cdot x_{i+1} + \alpha_{0,2;1} \cdot x_{i+1}^2 + \alpha_{1,0;1} \cdot x_i + \alpha_{0,1;1} \cdot x_{i+1}, \\ y_{i+1} &= x_{i+1} + \alpha_{0,1;0} \cdot x_{i+2} \end{aligned}$$

for each $i \in \{1, 3, 5, \ldots, n-1\}$. By replacing $x_{i+1} = y_{i+1} - \alpha_{0,1;0} \cdot x_{i+2}$, we get equations of the form

$$\begin{aligned}&\alpha_{2,0;1} \cdot x_i^2 - \alpha_{1,1;1} \cdot \alpha_{0,1;0} \cdot x_i \cdot x_{i+2} + \alpha_{0,2;1} \cdot \alpha_{0,1;0}^2 \cdot x_{i+2}^2 \\ &+x_i \cdot (\alpha_{1,1;1} \cdot y_{i+1} + \alpha_{1,0;1}) + x_{i+2} \cdot (-2 \cdot \alpha_{0,2;1} \cdot \alpha_{0,1;0} \cdot y_{i+1} - \alpha_{0,1;1} \cdot \alpha_{0,1;0}) \\ &+\alpha_{0,2;1} \cdot y_{i+1}^2 + \alpha_{0,1;1} \cdot y_{i+1} - y_i = 0.\end{aligned}$$

Note that each equation can be interpreted as a local map on the variables x_i, x_{i+2}. Hence, let's fix the values of $y_0, y_2, \ldots, y_{2j}, \ldots, y_{n-2} \in \mathbb{F}_p$ such that

$$y' = y_0 = y_2 = \ldots = y_{2j} = \ldots = y_{n-2}$$

for a certain $y' \in \mathbb{F}_p$, and let's introduce the function $G_{y'} : \mathbb{F}_p^2 \to \mathbb{F}_p$ defined as

$$G_{y'}(x_0, x_1) = \beta_{2,0} \cdot x_0^2 + \beta_{1,1} \cdot x_0 \cdot x_1 + \beta_{0,2} \cdot x_1^2 + \beta_{1,0} \cdot x_0 + \beta_{0,1} \cdot x_1,$$

where

$$\begin{aligned}&\beta_{2,0} = \alpha_{2,0;1}\,, \qquad \beta_{1,1} = -\alpha_{1,1;1} \cdot \alpha_{0,1;0}\,, \qquad \beta_{0,2} = \alpha_{0,2;1} \cdot \alpha_{0,1;0}^2\,, \\ &\beta_{1,0} = \alpha_{1,1;1} \cdot y' + \alpha_{1,0;1}\,, \qquad \beta_{0,1} = -2 \cdot \alpha_{0,2;1} \cdot \alpha_{0,1;0} \cdot y' - \alpha_{0,1;1} \cdot \alpha_{0,1;0}.\end{aligned}$$

Let's now consider the SI-lifting $\mathcal{S}_{G_{y'}}$ over $\mathbb{F}_p^{n/2}$ defined via the local map $G_{y'}$. Note that a collision for $\mathcal{S}_{G_{y'}}$ implies a collision on $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ as well, i.e., $\mathcal{S}_{G_{y'}}(x_0, x_1, \ldots, x_{n/2-1}) = \mathcal{S}_{G_{y'}}(x'_0, x'_1, \ldots, x'_{n/2-1})$ implies

$$\begin{aligned}&\mathcal{S}_{F_0,F_1}(y' - \alpha_{0,1;0} \cdot x_0, x_0, y' - \alpha_{0,1;0} \cdot x_1, x_1, \ldots, y' - \alpha_{0,1;0} \cdot x_{n/2-1}, x_{n/2-1}) \\ =&\mathcal{S}_{F_0,F_1}(y' - \alpha_{0,1;0} \cdot x'_0, x'_0, y' - \alpha_{0,1;0} \cdot x'_1, x'_1, \ldots, y' - \alpha_{0,1;0} \cdot x'_{n/2-1}, x'_{n/2-1})\,.\end{aligned}$$

Hence, in order to prove our result, it is sufficient to show that $\mathcal{S}_{G_{y'}}$ is *not* invertible over $\mathbb{F}_p^{n/2}$: this immediately implies that $\mathcal{S}_{F_0,F_1}$ cannot be invertible.

Due to Theorem 2, such S-Box $\mathcal{S}_{G_{y'}}$ is not invertible for $\frac{n}{2} \geq 3$, i.e., $n \geq 6$. In the case $n/2 = 2$, the S-Box $\mathcal{S}_{G_{y'}}$ is invertible if

$$G_{y'}(x_0, x_1) = \gamma_0 \cdot x_0 + \gamma_1 \cdot x_1 + \gamma_2 \cdot (x_0 - x_1)^2$$

with $\gamma_0 \neq \pm\gamma_1$, as proved in Lemma 1.

Then, by the definition of our local map, the SI-lifting is invertible if

1. $\beta_{2,0} = \beta_{0,2}$, that is, $\alpha_{2,0;1} = \alpha_{0,2;1} \cdot \alpha_{0,1;0}^2$;
2. $\beta_{1,1} = -2 \cdot \beta_{2,0}$, that is, $\alpha_{1,1;1} = \frac{2 \cdot \alpha_{2,0;1}}{\alpha_{0,1;0}} = 2 \cdot \alpha_{0,2;1} \cdot \alpha_{0,1;0}$;
3. $\beta_{1,0} \neq \pm\beta_{0,1}$, that is, $y' \cdot (\alpha_{1,1;1} \pm 2 \cdot \alpha_{0,2;1} \cdot \alpha_{0,1;0}) \neq -\alpha_{1,0;1} \mp \alpha_{0,1;1} \cdot \alpha_{0,1;0}$,

where the third condition is satisfied if

3.a $\pm 2 \cdot \alpha_{0,2;1} \cdot \alpha_{0,1;0} = -\alpha_{1,1;1}$ (note that y' can take any possible value);
3.b $\pm\alpha_{0,1;1} \cdot \alpha_{0,1;0} \neq -\alpha_{1,0;1}$.

By replacing the second condition in (3.a) and since $\alpha_{0,1;0} \neq 0$, we get the condition $\pm 2 \cdot \alpha_{0,2;1} = -2 \cdot \alpha_{0,2;1}$, which is satisfied if and only if $\alpha_{0,2;1} = 0$. By the first condition, we also have $\alpha_{2,0;1} = 0$. By the second condition, it follows that $\alpha_{1,1;1} = 0$. Since $\alpha_{2,0;1} = \alpha_{1,1;1} = \alpha_{0,2;1} = 0$, we have that F_1 must be linear in order to get invertibility for n even. Hence, the ASI-lifting $\mathcal{S}_{F_0,F_1}$ is never invertible for $n \geq 4$ if F_1 is quadratic and if $\alpha_{1,0;0}, \alpha_{0,1;0} \neq 0$. □

5.2 Proof of Proposition 4 for the Case $n \geq 3$ Odd

We are going to consider separately the following two cases: Lemma 13 covers the case where F_0 is a quadratic function and F_1 is linear, while Lemma 14 deals with F_0 linear and F_1 quadratic. In the case $n \geq 5$, the only invertible non-linear functions $\mathcal{S}_{F_0,F_1}$ are the ones with a Feistel structure. Note that in the case $n = 3$ there is an extra case in which the function $\mathcal{S}_{F_0,F_1}$ is invertible without being a Type-II Feistel scheme – see Lemma 14.

Lemma 13. *Let $p \geq 3$ be a prime integer, and let $n \geq 3$ be an odd number. Let F_0 be a quadratic function over $\mathbb{F}_p$, while let $F_1(x_0, x_1) = \alpha_{1,0;1} \cdot x_0 + \alpha_{0,1;1} \cdot x_1$ be a linear function over $\mathbb{F}_p$. Then, the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ is invertible if and only if it is a Type-II Feistel Scheme, that is,*

- *$\alpha_{1,0;1} = 0$ or $\alpha_{0,1;1} = 0$;*
- *$F_0(x_0, x_1) = \alpha_{i,1-i;0} \cdot x_i + H(x_i)$ for $i \in \{0, 1\}$, where $H : \mathbb{F}_p \to \mathbb{F}_p$ is a quadratic function.*

Proof. Since the invertibility of Type-II Feistel schemes in the case $F_1(x_0, x_1) = x_0$ or $F_1(x_0, x_1) = x_1$ is treated in Lemma 11, we focus on $F_1(x_0, x_1) = \alpha_{1,0;1} \cdot x_0 + \alpha_{0,1;1} \cdot x_1$, with $\alpha_{1,0;1}, \alpha_{0,1;1} \neq 0$. We show that, in such a case, a collision always occurs for $\mathcal{S}_{F_0,F_1}$.

In order to find the collision, let consider the inputs $(x_0, x_1, \ldots, x_{n-1})$ and $(y_0, y_1, \ldots, y_{n-1}) = (y_0, x_1, \ldots, x_{n-1})$, where $y_0 \neq x_0$. Then, the system representing $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(y_0, x_1, \ldots, x_{n-1})$ reduces to

$$\alpha_{2,0;0} \cdot d_0 \cdot s_0 + \frac{\alpha_{1,1;0}}{2} \cdot d_0 \cdot s_1 + \alpha_{1,0;0} \cdot d_0 = 0\,,$$
$$\alpha_{0,2;0} \cdot d_0 \cdot s_0 + \frac{\alpha_{1,1;0}}{2} \cdot d_0 \cdot s_{n-1} + \alpha_{0,1;0} \cdot d_0 = 0\,,$$

via the variables d_i, s_i introduced in (4). If $\alpha_{1,1;0} \neq 0$, the system admits the solution

$$s_1 = -2\frac{\alpha_{1,0;0} + \alpha_{2,0;0} \cdot s_0}{\alpha_{1,1;0}} \quad \text{and} \quad s_{n-1} = -2\frac{\alpha_{0,1;0} + \alpha_{0,2;0} \cdot s_0}{\alpha_{1,1;0}}$$

which corresponds to a collision for the analysed ASI-lifting function. If otherwise $\alpha_{1,1;0} = 0$, then one between $\alpha_{2,0;0}$ and $\alpha_{0,2;0}$ should be non-zero, otherwise F_0 would be linear. We study separately these two subcases.

SubCase: $\alpha_{1,1;0} = 0$, $\alpha_{2,0;0} \neq 0$. In such a case, using the change of variables introduced in (4), the collision $\mathcal{S}_{F_0,F_1}(x_0, x_1, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(y_0, y_1, \ldots, y_{n-1})$

corresponds to the linear system

$$\begin{bmatrix} \alpha_{2,0;0}\cdot d_0 & \alpha_{0,2;0}\cdot s_1+\alpha_{0,1;0} & 0 & 0 & \dots & 0 & 0 \\ 0 & \alpha_{1,0;1} & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \alpha_{2,0;0}\cdot d_2 & \alpha_{0,1;0} & \dots & 0 & 0 \\ \vdots & & & \ddots & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & \alpha_{1,0;1} & 0 \\ \alpha_{0,2;0}\cdot d_0 & 0 & 0 & 0 & \dots & 0 & \alpha_{2,0;0}\cdot d_{n-1} \end{bmatrix} \times \begin{bmatrix} s_0 \\ d_1 \\ s_2 \\ d_3 \\ \vdots \\ d_{n-2} \\ s_{n-1} \end{bmatrix}$$

$$= - \begin{bmatrix} \alpha_{1,0;0}\cdot d_0 \\ \alpha_{0,1;1}\cdot d_2 \\ \alpha_{1,0;0}\cdot d_2 \\ \alpha_{0,1;1}\cdot d_3 \\ \vdots \\ \alpha_{0,1;1}\cdot d_{n-1} \\ \alpha_{1,0;0}\cdot d_{n-1}+\alpha_{0,1;0}\cdot d_0 \end{bmatrix}.$$

We solve this system of n equations with respect to the variables s_i for even i and d_i for odd i, that gives the set of variables $\{s_0, d_1, s_2, d_3 \dots, s_{n-1}\}$. We leave the others as free variables.

The determinant of the l.h.s. matrix is $\alpha_{2,0;0}^{\frac{n+1}{2}} \cdot \alpha_{1,0;1}^{\frac{n-1}{2}} \cdot \prod_{i \text{ even}} d_i$. Then, if we take $d_i \neq 0$ for all even i, the system is compatible and the ASI-lifting has a collision if $\alpha_{2,0;0} \neq 0$ (since $\alpha_{1,0;1} \neq 0$). The last case to analyse is when $\alpha_{2,0;0} = \alpha_{1,1;0} = 0$ (and so $\alpha_{0,2;0} \neq 0$).

SubCase: $\alpha_{1,1;0} = \alpha_{2,0;0} = 0$, $\alpha_{0,2;0} \neq 0$. Working as before, the system of equations corresponding to the collision is given by

$$\begin{bmatrix} \alpha_{0,2;0}\cdot d_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \alpha_{0,1;1} & 0 & \dots & 0 & 0 \\ 0 & \alpha_{1,0;0} & \alpha_{0,2;0}\cdot d_3 & \dots & 0 & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & \alpha_{0,1;1} & 0 \\ 0 & 0 & 0 & \dots & \alpha_{1,0;0} & \alpha_{0,2;0}\cdot d_0 \end{bmatrix} \times \begin{bmatrix} s_1 \\ d_2 \\ s_3 \\ \vdots \\ d_{n-1} \\ s_0 \end{bmatrix} = - \begin{bmatrix} \alpha_{1,0;0}\cdot d_0+\alpha_{0,1;0}\cdot d_1 \\ \alpha_{1,0;1}\cdot d_1 \\ \alpha_{0,1;0}\cdot d_3 \\ \vdots \\ \alpha_{1,0;1}\cdot d_{n-2} \\ \alpha_{0,1;0}\cdot d_0 \end{bmatrix}.$$

This time, we solve this system of n equations with respect to the variables $\{s_1, d_2, s_3 \dots, d_{n-1}, s_0\}$. We leave the others as free variables. In such a case, the determinant of the l.h.s. matrix is $\alpha_{0,2;0}^{\frac{n+1}{2}} \cdot \alpha_{0,1;1}^{\frac{n-1}{2}} \cdot d_0 \cdot \prod_{i \text{ odd}} d_i$. Then, by taking $d_i \neq 0$ for $i = 0$ and for each i odd, the determinant is always non-zero. As a result, the system is compatible and we can find a collision for the ASI-lifting.

□

Lemma 14. *Let $p \geq 3$ be a prime integer, and let $n \geq 3$ be an odd number. Let $F_0(x_0, x_1) = \alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1$ be a linear function over $\mathbb{F}_p$, while let F_1 be a quadratic function over $\mathbb{F}_p$.*

If $n \geq 5$, then the corresponding ASI-lifting $\mathcal{S}_{F_0,F_1}$ defined over $\mathbb{F}_p^n$ is invertible if and only if it is a Type-II Feistel Scheme, that is,

– $\alpha_{1,0;0} = 0$ *or* $\alpha_{0,1;0} = 0$*;*
– $F_1(x_0, x_1) = \alpha_{i,1-i;0} \cdot x_i + H(x_i)$ *for* $i \in \{0, 1\}$*, where* $H : \mathbb{F}_p \to \mathbb{F}_p$ *is a quadratic function.*

If $n = 3$*, then* $\mathcal{S}_{F_0,F_1}$ *is invertible if and only if either (i) the condition just given holds, or (ii)* $F_0(x_0, x_1) = \alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1$ *for* $\alpha_{1,0;0}, \alpha_{0,1;0} \neq 0$ *and*

$$F_1(x_0, x_1) = \gamma \cdot \left(\frac{\alpha_{0,1;0}}{\alpha_{1,0;0}} \cdot x_0 - \frac{\alpha_{1,0;0}}{\alpha_{0,1;0}} \cdot x_1 \right)^2 + \alpha_{1,0;1} \cdot x_0 + \alpha_{0,1;1} \cdot x_1$$

where $\gamma \in \mathbb{F}_p$ *and* $\alpha_{1,0;1} \cdot \alpha_{1,0;0}^2 \neq -\alpha_{0,1;1} \cdot \alpha_{0,1;0}^2$ *.*

Proof. Again, the case $F_0(x_0, x_1) = x_0$ or $F_0(x_0, x_1) = x_1$ follows from Lemma 11, so we limit ourselves to consider the case $F_0(x_0, x_1) = \alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1$ with $\alpha_{1,0;0}, \alpha_{0,1;0} \neq 0$. We start by showing that for $n \geq 5$ the ASI-lifting is never invertible, i.e., we can always find a collision.

In order to prove it, let's start by considering $(x_0, x_1, x_2, x_3, x_4, \ldots, x_{n-1})$ and $(y_0, y_1, y_2, y_3, y_4, \ldots, y_{n-1}) = (x_0, x_1, y_2, y_3, x_4, \ldots, x_{n-1})$, i.e., two inputs that differ just in $y_2 \neq x_2$ and $y_3 \neq x_3$. Using the change of variables of Equation (4), the system reduces to

$$\begin{aligned}
&d_2 \cdot \left(\alpha_{0,2;1} \cdot s_2 + \frac{\alpha_{1,1;1}}{2} \cdot s_1 + \alpha_{0,1;1} \right) = 0 \,, \\
&\alpha_{1,0;0} \cdot d_2 + \alpha_{0,1;0} \cdot d_3 = 0 \,, \\
&d_3 \cdot \left(\alpha_{2,0;1} \cdot s_3 + \frac{\alpha_{1,1;1}}{2} \cdot s_4 + \alpha_{1,0;1} \right) = 0 \,.
\end{aligned}$$

Since $\alpha_{1,0;0}, \alpha_{0,1;0} \neq 0$, the second equation is satisfied by $d_2 = -\frac{\alpha_{0,1;0}}{\alpha_{1,0;0}} \cdot d_3$. By taking $d_2, d_3 \neq 0$, the other equations reduce to

$$\begin{aligned}
\alpha_{0,2;1} \cdot s_2 + \frac{\alpha_{1,1;1}}{2} \cdot s_1 &= -\alpha_{0,1;1} \,, \\
\alpha_{2,0;1} \cdot s_3 + \frac{\alpha_{1,1;1}}{2} \cdot s_4 &= -\alpha_{1,0;1} \,.
\end{aligned}$$

If $\alpha_{1,1;1} \neq 0$, then the system admits a solution, which corresponds to a collision. Similar result holds for $\alpha_{1,1;1} = 0$ and $\alpha_{0,2;1}, \alpha_{2,0;1} \neq 0$. Hence, the only remaining cases to analyse are (i) $\alpha_{1,1;1} = \alpha_{0,2;1} = 0$ and $\alpha_{2,0;1} \neq 0$, or (ii) $\alpha_{1,1;1} = \alpha_{2,0;1} = 0$ and $\alpha_{0,2;1} \neq 0$. We limit ourselves to analyse the first case, since the other one is analogous.

SubCase: $\alpha_{1,1;1} = \alpha_{2,0;1} = 0$*,* $\alpha_{0,2;1} \neq 0$*.* By using the change of variables of Equation (4), the system $\mathcal{S}_{F_0,F_1}(x_0, \ldots, x_{n-1}) = \mathcal{S}_{F_0,F_1}(y_0, \ldots, y_{n-1})$ is equal to

$$\begin{bmatrix}
\alpha_{1,0;0} & \alpha_{0,1;0} & 0 & 0 & \ldots & 0 & 0 \\
0 & \alpha_{1,0;1} & \alpha_{0,2;1} \cdot d_2 & 0 & \ldots & 0 & 0 \\
0 & 0 & 0 & \alpha_{0,1;0} & \ldots & 0 & 0 \\
\vdots & & & \ddots & \ddots & & \vdots \\
0 & 0 & 0 & 0 & \ldots & \alpha_{1,0;1} & \alpha_{0,2;1} \cdot d_{n-1} \\
\alpha_{0,1;0} & 0 & 0 & 0 & \ldots & 0 & 0
\end{bmatrix} \times \begin{bmatrix} d_0 \\ d_1 \\ s_2 \\ d_3 \\ \vdots \\ d_{n-2} \\ s_{n-1} \end{bmatrix} = - \begin{bmatrix} 0 \\ \alpha_{0,1;1} \cdot d_2 \\ \alpha_{0,1;0} \cdot d_3 \\ \alpha_{1,0;0} \cdot d_2 \\ \vdots \\ \alpha_{0,1;1} \cdot d_{n-1} \\ \alpha_{1,0;0} \cdot d_{n-1} \end{bmatrix} .$$

We solve this system with respect to the variables $\{d_0, d_1, s_2, d_3 \ldots, d_{n-2}, s_{n-1}\}$, i.e., variables d_i for odd i and for d_0 and variables s_i for even $i \geq 2$. We leave the others as free variables.

Since the determinant of the l.h.s. matrix is $-\alpha_{0,1;0}^{\frac{n+1}{2}} \cdot \alpha_{0,2;1}^{\frac{n-1}{2}} \cdot \prod_{i \geq 2 \text{ even}} d_i$, if we choose each $d_i \neq 0$ for $i \geq 2$ even, then the system is compatible and the ASI-lifting is not invertible.

SubCase: $n = 3$. Finally, we prove the result for $n = 3$. Given $F_0(x_0, x_1) = \alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1$ for $\alpha_{0,1;0}, \alpha_{1,0;0} \neq 0$, the system $y = \mathcal{S}_{F_0,F_1}(x)$ is

$$\begin{aligned}
&\alpha_{1,0;0} \cdot x_0 + \alpha_{0,1;0} \cdot x_1 = y_0 \,, \\
&\alpha_{2,0;1} \cdot x_1^2 + \alpha_{0,2;1} \cdot x_2^2 + \alpha_{1,1;1} \cdot x_1 \cdot x_2 + \alpha_{1,0;1} \cdot x_1 + \alpha_{0,1;1} \cdot x_2 = y_1 \,, \\
&\alpha_{1,0;0} \cdot x_2 + \alpha_{0,1;0} \cdot x_0 = y_2 \,.
\end{aligned}$$

By replacing $x_1 = \frac{y_0 - \alpha_{1,0;0} \cdot x_0}{\alpha_{0,1;0}}, x_2 = \frac{y_2 - \alpha_{0,1;0} \cdot x_0}{\alpha_{1,0;0}}$ in the second equation, we get

$$\begin{aligned}
&x_0^2 \cdot \left(\frac{\alpha_{2,0;1} \cdot \alpha_{1,0;0}^2}{\alpha_{0,1;0}^2} + \frac{\alpha_{0,2;1} \cdot \alpha_{0,1;0}^2}{\alpha_{1,0;0}^2} + \alpha_{1,1;1} \right) + x_0 \cdot \left(y_0 \cdot \left(-2 \cdot \frac{\alpha_{2,0;1} \cdot \alpha_{1,0;0}}{\alpha_{0,1;0}^2} - \frac{\alpha_{1,1;1}}{\alpha_{1,0;0}} \right) \right. \\
&\quad \left. + y_2 \cdot \left(-2 \cdot \frac{\alpha_{0,2;1} \cdot \alpha_{0,1;0}}{\alpha_{1,0;0}^2} - \frac{\alpha_{1,1;1}}{\alpha_{0,1;0}} \right) - \frac{\alpha_{1,0;1} \cdot \alpha_{1,0;0}}{\alpha_{0,1;0}} - \frac{\alpha_{0,1;1} \cdot \alpha_{0,1;0}}{\alpha_{1,0;0}} \right) \\
&\quad + \frac{\alpha_{2,0;1}}{\alpha_{0,1;0}^2} \cdot y_0^2 + \frac{\alpha_{0,2;1}}{\alpha_{1,0;0}^2} \cdot y_2^2 + \frac{\alpha_{1,1;1}}{\alpha_{0,1;0} \cdot \alpha_{1,0;0}} \cdot y_0 \cdot y_2 + \frac{\alpha_{1,0;1}}{\alpha_{0,1;0}} \cdot y_0 + \frac{\alpha_{0,1;1}}{\alpha_{1,0;0}} \cdot y_2 - y_1 = 0 \,.
\end{aligned}$$

Working as in the proof of Lemma 11, the ASI-lifting is always invertible if and only if

- the coefficient of the monomial x_0^2 is zero, that is, $\alpha_{2,0;1} \cdot \alpha_{1,0;0}^4 + \alpha_{0,2;1} \cdot \alpha_{0,1;0}^4 + \alpha_{1,1;1} \cdot \alpha_{1,0;0}^2 \cdot \alpha_{0,1;0}^2 = 0$;
- the coefficient of the monomial x_0 is non-null, that is,
  1. $-2 \cdot \alpha_{1,0;0}^2 \cdot \alpha_{2,0;1} - \alpha_{1,1;1} \cdot \alpha_{0,1;0}^2 = 0 \,,$
  2. $-2 \cdot \alpha_{0,2;1} \cdot \alpha_{0,1;0}^2 - \alpha_{1,1;1} \cdot \alpha_{1,0;0}^2 = 0 \,,$
  3. $\alpha_{1,0;1} \cdot \alpha_{1,0;0}^2 \neq -\alpha_{0,1;1} \cdot \alpha_{0,1;0}^2 \,.$

By combining these conditions, we get that the ASI-lifting is invertible if

$$F_1(x_0, x_1) = \gamma \cdot \left(\frac{\alpha_{0,1;0}}{\alpha_{1,0;0}} \cdot x_0 - \frac{\alpha_{1,0;0}}{\alpha_{0,1;0}} \cdot x_1 \right)^2 + \alpha_{1,0;1} \cdot x_0 + \alpha_{0,1;1} \cdot x_1$$

where $\gamma \in \mathbb{F}_p$ and $\alpha_{1,0;1} \cdot \alpha_{1,0;0}^2 \neq -\alpha_{0,1;1} \cdot \alpha_{0,1;0}^2 \,.$ □

6 Summary and Open Problems for Future Work

In this paper, we show that it is impossible to have invertibility of alternating shift-invariant lifting functions $\mathcal{S}_{F_0,F_1}$ over $\mathbb{F}_p^n$ induced by two local quadratic maps $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$. When we relax conditions and we take one of the two

local maps to be linear, we find some invertible functions. Unfortunately, for each $n \geq 4$, we get only the already known Type-II Feistel schemes.

Our findings provide some insights, though it leaves open for future research the problem of setting up invertible quadratic non-linear functions over $\mathbb{F}_p^n$ induced by local maps. An obvious possible way to solve it is to consider local maps $F_0, F_1, \ldots, F_{h-1} : \mathbb{F}_p^m \to \mathbb{F}_p$ defined over a larger input domain by taking $m \geq 3$. Another strategy may consist of generalizing the current construction. E.g., let's focus on the case of the SI-lifting function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ for $F : \mathbb{F}_p^m \to \mathbb{F}_p$. In the current definition, the function F takes in input consecutive elements $x_i, x_{i+1}, \ldots, x_{i+m-1}$. A possible way to generalize such definition consists of allowing for non-consecutive inputs, as formally given in the following definition.

Definition 6. *Let $p \geq 3$ be a prime integer, and let $1 \leq m \leq n$ be two positive integers. Let $F : \mathbb{F}_p^m \to \mathbb{F}_p$, and let $j_1, j_2, \ldots, j_{m-1} \in \{1, 2, \ldots, n-1\}$ be $m-1$ **distinct** integers. We define $\mathcal{S}_{F,[j_1,j_2,\ldots,j_{m-1}]}$ over $\mathbb{F}_p^n$ as*

$$\mathcal{S}_{F,[j_1,j_2,\ldots,j_{m-1}]}(x_0, x_1, \ldots, x_{n-1}) = y_0 \| y_1 \| \ldots \| y_{n-1}$$

where

$$y_i = F(x_i, x_{i+j_1}, x_{i+j_2}, \ldots, x_{i+j_{m-1}}) \qquad \text{for each } i \in \{0, 1, \ldots, n-1\}.$$

A similar construction can be proposed for cycling and alternating shift-invariant functions as well. We leave the problem to study their invertibility as future work.

Acknowledgement. Lorenzo Grassi was supported by the German Research Foundation (DFG) within the framework of the Excellence Strategy of the Federal Government and the States EXC 2092 CaSa 39078197.

References

1. Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schofnegger, M.: Feistel Structures for MPC, and More. In: ESORICS 2019. LNCS, vol. 11736, pp. 151–171 (2019)
2. Albrecht, M.R., Grassi, L., Rechberger, C., Roy, A., Tiessen, T.: MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity. In: Advances in Cryptology – ASIACRYPT 2016. LNCS, vol. 10031, pp. 191–219 (2016)
3. Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S., Szepieniec, A.: Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols. IACR Transactions on Symmetric Cryptology 2020(3), 1–45 (2020)
4. Beierle, C., Carlet, C., Leander, G., Perrin, L.: A further study of quadratic APN permutations in dimension nine. Finite Fields Their Appl. 81, 102049 (2022)
5. Beth, T., Ding, C.: On Almost Perfect Nonlinear Permutations. In: Advances in Cryptology - EUROCRYPT 1993. LNCS, vol. 765, pp. 65–76 (1993)
6. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Advances in Cryptology – CRYPTO 1990. LNCS, vol. 537, pp. 2–21 (1990)

7. Bouvier, C., Briaud, P., Chaidos, P., Perrin, L., Salen, R., Velichkov, V., Willems, D.: New Design Techniques for Efficient Arithmetization-Oriented Hash Functions:Anemoi Permutations and Jive Compression Mode. Cryptology ePrint Archive, Paper 2022/840 (2022), https://eprint.iacr.org/2022/840
8. Budaghyan, L., Calderini, M., Carlet, C., Davidova, D., Kaleyski, N.S.: On Two Fundamental Problems on APN Power Functions. IEEE Trans. Inf. Theory 68(5), 3389–3403 (2022)
9. Budaghyan, L., Carlet, C., Leander, G.: Constructing new APN functions from known ones. Finite Fields Their Appl. 15(2), 150–159 (2009)
10. Carlet, C.: Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Des. Codes Cryptogr. 59(1-3), 89–109 (2011)
11. Carlet, C.: Boolean functions. In: Handbook of Finite Fields, pp. 241–252. Discrete mathematics and its applications, CRC Press (2013)
12. Carlet, C.: On APN exponents, characterizations of differentially uniform functions by the Walsh transform, and related cyclic-difference-set-like structures. Des. Codes Cryptogr. 87(2-3), 203–224 (2019)
13. Daemen, J.: Cipher and hash function design, strategies based on linear and differential cryptanalysis, PhD Thesis. K.U.Leuven (1995), http://jda.noekeon.org/
14. Daemen, J., Rijmen, V.: The Wide Trail Design Strategy. In: Cryptography and Coding, 8th IMA International Conference 2001. LNCS, vol. 2260, pp. 222–238 (2001)
15. Dobraunig, C., Grassi, L., Guinet, A., Kuijsters, D.: Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields. In: Advances in Cryptology – EUROCRYPT 2021. LNCS, vol. 12697, pp. 3–34 (2021)
16. Dobraunig, C., Grassi, L., Helminger, L., Rechberger, C., Schofnegger, M., Walch, R.: Pasta: A Case for Hybrid Homomorphic Encryption. Cryptology ePrint Archive, Report 2021/731 (2021), https://ia.cr/2021/731 – accepted at TCHES 2023
17. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory 14, 154–156 (1968)
18. Grassi, L.: Bounded Surjective Quadratic Functions over $\mathbb{F}_p{}^n$ for MPC-/ZK-/HE-Friendly Symmetric Primitives. Cryptology ePrint Archive, Paper 2022/1313 (2022), https://eprint.iacr.org/2022/1313
19. Grassi, L.: On Generalizations of the Lai-Massey Scheme: the Blooming of Amaryllises. Cryptology ePrint Archive, Paper 2022/1245 (2022), https://eprint.iacr.org/2022/1245
20. Grassi, L., Hao, Y., Rechberger, C., Schofnegger, M., Walch, R., Wang, Q.: Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications. Cryptology ePrint Archive, Report 2022/403 (2022), https://ia.cr/2022/403
21. Grassi, L., Khovratovich, D., Lüftenegger, R., Rechberger, C., Schofnegger, M., Walch, R.: Reinforced Concrete: A Fast Hash Function for Verifiable Computation. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022. pp. 1323–1335. ACM (2022)
22. Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., Schofnegger, M.: Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. In: USENIX Security 2021. USENIX Association (2021)
23. Grassi, L., Khovratovich, D., Rønjom, S., Schofnegger, M.: The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over $(\mathbb{F}_p)^n$. IACR Trans. Symmetric Cryptol. 2022(1), 5–37 (2022)

24. Grassi, L., Onofri, S., Pedicini, M., Sozzi, L.: Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p{}^n$ – Application to Poseidon. IACR Trans. Symmetric Cryptol. 2022(3), 20–72 (2022)
25. Grassi, L., Øygarden, M., Schofnegger, M., Walch, R.: From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications. In: Advances in Cryptology - EUROCRYPT 2023. LNCS, vol. 14007, pp. 255–286 (2023)
26. Lai, X., Massey, J.L.: A Proposal for a New Block Encryption Standard. In: Advances in Cryptology – EUROCRYPT 1990. LNCS, vol. 473, pp. 389–404 (1990)
27. Meier, W., Pasalic, E., Carlet, C.: Algebraic Attacks and Decomposition of Boolean Functions. In: Advances in Cryptology - EUROCRYPT 2004. LNCS, vol. 3027, pp. 474–491 (2004)
28. Meier, W., Staffelbach, O.: Nonlinearity Criteria for Cryptographic Functions. In: Advances in Cryptology - EUROCRYPT 1989. LNCS, vol. 434, pp. 549–562 (1989)
29. Nyberg, K.: S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. In: Fast Software Encryption – FSE 1994. LNCS, vol. 1008, pp. 111–130 (1994)
30. Nyberg, K.: Generalized Feistel Networks. In: Advances in Cryptology - ASIACRYPT 1996. LNCS, vol. 1163, pp. 91–104 (1996)
31. Szepieniec, A.: On the Use of the Legendre Symbol in Symmetric Cipher Design. Cryptology ePrint Archive, Report 2021/984 (2021), `https://ia.cr/2021/984`
32. Vaudenay, S.: On the Lai-Massey Scheme. In: Advances in Cryptology – ASIACRYPT 1999. LNCS, vol. 1716, pp. 8–19 (1999)
33. Wolfram, S.: Cryptography with Cellular Automata. In: Advances in Cryptology - CRYPTO 1985. LNCS, vol. 218, pp. 429–432 (1985)
34. Zheng, Y., Matsumoto, T., Imai, H.: On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In: Advances in Cryptology - CRYPTO 1989. LNCS, vol. 435, pp. 461–480 (1989)