Generalized Triangular Dynamical System: An Algebraic System for Constructing Cryptographic Permutations over Finite Fields

Arnab Roy[1] and Matthias Johann Steiner[2]

[1] Universität Innsbruck, Austria
arnab.roy@uibk.ac.at
[2] Alpen-Adria-Universität Klagenfurt, Universitätsstraße 65-67, 9020 Klagenfurt am Wörthersee, Austria
matthias.steiner@aau.at

Abstract. In recent years a new class of symmetric-key primitives over $\mathbb{F}_p$ that are essential to Multi-Party Computation and Zero-Knowledge Proofs based protocols, has emerged. Towards improving the efficiency of such primitives, a number of new block ciphers and hash functions over $\mathbb{F}_p$ were proposed. These new primitives also showed that following alternative design strategies to the classical Substitution-Permutation Network (SPN) and Feistel Networks leads to more efficient cipher and hash function designs over $\mathbb{F}_p$ specifically for large odd primes p.
In view of these efforts, in this work we build an *algebraic framework* that allows the systematic exploration of viable and efficient design strategies for constructing symmetric-key (iterative) permutations over $\mathbb{F}_p$. We first identify iterative polynomial dynamical systems over finite fields as the central building block of almost all block cipher design strategies. We propose a generalized triangular polynomial dynamical system (GTDS), and based on the GTDS we provide a generic definition of an iterative (keyed) permutation over $\mathbb{F}_p^n$.
Our GTDS-based generic definition is able to describe the three most well-known design strategies, namely SPNs, Feistel networks (FN) and Lai–Massey (LM). Consequently, the block ciphers that are constructed following these design strategies can also be instantiated from our generic definition. Moreover, we find that the recently proposed `Griffin` design, which neither follows the Feistel nor the SPN design, can be described using the generic GTDS-based definition. We also show that a new generalized Lai–Massey construction can be instantiated from the GTDS-based definition. The latter results confirm that our GTDS-based definition is able to instantiate cryptographic permutations that are beyond SPN, FN and LM based.
We further provide generic (security) analysis of the GTDS including an upper bound on the differential uniformity and the correlation.

1 Introduction

Constructing (keyed and unkeyed) permutations is at the center of designing some of the most broadly used cryptographic primitives like block ciphers and hash

functions. After half a century of research, Feistel and Substitution-Permutation Networks (SPN) have emerged as the two dominant iterative design strategies for constructing unkeyed permutations or block ciphers. Another notable, although not much used design strategy is the Lai–Massey construction. Altogether, SPN, Feistel and Lai–Massey are at the core of some of the most well-known block ciphers such as AES [25,19], DES [21], CLEFIA [47], IDEA [38], etc.

In the past few years, a new class of symmetric-key cryptographic functions (block ciphers, hash functions and stream ciphers) that are essential in privacy preserving cryptographic protocols such as Multi-Party Computation and Zero-Knowledge Proofs and Homomorphic Encryption, has emerged. For efficiency reasons these primitives are designed over $\mathbb{F}_p$ (for large primes $p > 2$). This is in contrast with the classical symmetric primitives that use functions defined over $\mathbb{F}_{2^n}$ (typically for small n e.g. $n \leq 8$).[3] By utilizing the classical SPN or Feistel design principles, a number of such symmetric-key functions (over $\mathbb{F}_p$) were proposed. However, current research suggests that these traditional strategies are not the best choices for efficient primitives over $\mathbb{F}_p$. For example, the partial SPN-based hash function Poseidon [32] performs more efficiently in R1CS or Plonk prover circuits than the generalized unbalanced Feistel-based construction `GMiMCHash` [3]. Recently proposed designs - Griffin [30] and Arion [46] follow neither SPN nor Feistel, and is more efficient in circuits than `GMiMCHash` and Poseidon. In the literature these new primitives are often called Arithmetization-Oriented (AO) primitives.

An important and relevant question here is thus: *What is the space of possible design strategies for constructing (efficient) symmetric-key cryptographic permutations/functions over $\mathbb{F}_p$? And how to explore the possible design strategies systematically?*

Moreover, given that such new cryptographic functions are inherently algebraic by design, their security is dictated by algebraic cryptanalytic techniques. For example, algebraic attacks (interpolation, Gröbner basis, GCD, etc.) [26,2,4,45] are the main attack vectors in determining the security of `GMiMC`, Poseidon, `MiMC` [4], etc.

A well-defined generic algebraic design framework will prescribe a systematic approach towards exploring viable and efficient design strategies over $\mathbb{F}_p$. Such a generic framework will allow the design of new symmetric-key primitives and will shed new light into the algebraic properties of SPN- and Feistel-based designs, among others, over $\mathbb{F}_p$. A "good" generic framework should ultimately allow instantiation of primitives over $\mathbb{F}_q$ where $q = p^n$ for arbitrary primes p and naturally encompass existing classical design strategies, such as SPN, Feistel and Lai–Massey.

The primary aim of this work is to find such a general framework which describes iterative algebraic systems for constructing AO (keyed or unkeyed) permutations.

[3] There are symmetric primitives that (additionally) use functions defined over the ring $\mathbb{Z}_{2^n}$ for $n \geq 1$

Study of generic frameworks and our work. The study of generic frameworks for cryptographic constructions and their generic security analysis is a topic of high impact. It allows designers to validate their design strategies and gives recipes for possible design and analysis optimization advancements. Examples of research on generic design frameworks include the studies on Even-Mansour (EM) design variants [24,17,18,23,27], Sponge construction and variants thereof [7,12,29,28], etc. However, a generic understanding and study of AO design strategy is not possible following this line of works. The main idea behind AO designs are efficient polynomial evaluation and/or efficient representation of an iterative function with minimal multiplicative complexity over a finite field. Thus, a generic AO design requires a focus on the polynomial structure and naturally, a polynomial-based approach.

The EM construction or general SPN or Feistel constructions considered in (above-mentioned) previous works are much more generic in comparison to our proposed framework. They only consider functions or permutations without focusing on their algebraic structure. The generic framework and its analysis in our work take polynomial structure into account and are based on the properties of polynomials over finite fields $\mathbb{F}_q$. For the cryptographic analysis in this work we only exploit the statistical (e.g. correlation, differential) and algebraic (polynomial degree) properties. This approach is comparable (up to the considered properties) to the (statistical) security analysis [41] of the generic SPN.

In mathematics literature, properties of polynomial dynamical system or iterative polynomial system are studied over finite fields. In [44], Ostafe and Shparlinski studied the degree growth of a class of iterative polynomial system namely triangular polynomial dynamical system. They also prove a bound on the discrepancy which is a well-accepted measure (in mathematics literature) to quantify the uniformity of a sequence, of this dynamical system when viewed as pseudo-random number generator.

1.1 Our Results

In this paper we lay out a generic strategy for constructing cryptographic (keyed and unkeyed) permutations combined with security analysis against differential cryptanalysis.

We first discuss (Section 2) that so-called orthogonal systems are the only polynomial systems suitable to represent (keyed) permutations and henceforth block ciphers over finite fields.

We then propose a novel algebraic system (in Section 3) that is the foundation for constructing generic iterative permutations. More specifically, we construct a polynomial dynamical system over a finite field $\mathbb{F}_q$ (where $q = p^n$ with p a prime and $n \geq 1$) that we call Generalized Triangular Dynamical System (GTDS). We then provide a generic definition of iterative (keyed) permutations using the GTDS and a linear/affine permutation. We show (in Section 4) that our GTDS-based definition of iterative permutations is able to describe the SPN, different types of Feistel networks and the Lai–Massey construction. Consequently,

different block ciphers that are instantiations of these design strategies can also be instantiated from the GTDS-based permutation.

Beyond encompassing these well-known design strategies, our framework provides a systematic way to study different algebraic design strategies and security of permutations (with or without key). This is extremely useful in connection with the recent design efforts for constructing block ciphers and hash function over $\mathbb{F}_p$ where p is a large prime. For example, GTDS already covers the recently proposed partial SPN design strategy [33] used in designing block ciphers and hash functions [32].

Our GTDS-based definition of iterative permutations allows for instantiations of new (keyed) permutations. For example, the recently proposed construction Griffin can also be instantiated from our generic definition of an iterative permutation. Moreover, using our generic definition we propose a generalization (Section 4.3) of the Lai–Massey design strategy. A new efficient and secure cryptographic permutation (and hash function) [46] with low multiplicative complexity is also instantiated from our generic definition.

In Section 5 we perform a generic analysis to bound the differential uniformity as well as the correlation of the GTDS.

Our generic constructions, definitions and results holds for arbitrary p. However, our main aim is to propose an algebraic framework for constructing primitives and provide generic (security) analysis over $\mathbb{F}_p$ for (large) $p > 2$. The security analysis given in this paper can be refined and improved for $p = 2$. Our (security) analysis is not aimed for binary extension field and should be viewed as generic analysis for $p > 2$. However, the GTDS-based construction(s) proposed in this paper can be applied over $\mathbb{F}_q$ (where $q = p^n$ with p a prime and $n \geq 1$).

2 Block Ciphers and Permutation Polynomials

In general a block cipher can be described as a pair of (keyed) mappings

$$F : \mathcal{M} \times \mathcal{K} \to \mathcal{C}, \qquad F^{-1} : \mathcal{C} \times \mathcal{K} \to \mathcal{M}, \tag{1}$$

where $\mathcal{M}$, $\mathcal{K}$ and $\mathcal{C}$ denoting the plaintext, key and ciphertext space respectively, are finite. For any $\mathbf{k} \in \mathcal{K}$, $F_{\mathbf{k}}$ is a permutation and $F^{-1}(\_, \mathbf{k}) \circ F(\_, \mathbf{k}) = \mathrm{id}_{\mathcal{M}}$. In this work we will assume that $\mathcal{M} = \mathcal{C} = \mathbb{F}_q^n$ and $\mathcal{K} = \mathbb{F}_q^{n \times r}$, where $r, n \geq 1$, and $\mathbb{F}_q$ is a finite field with $q = p^n$ for prime p.

For any function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ we can find a unique polynomial $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ (via interpolation) with degree less than q in each variable such that $F(\mathbf{x}) = P(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_q^n$. Hence, all ciphers can be viewed as vectors of polynomials. We recall the following algebraic notion in this context.

Definition 1 ([40, 7.34., 7.35. Definition]). *Let $\mathbb{F}_q$ be a finite field.*

(1) A polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is called a permutation polynomial if the equation $f(x_1, \ldots, x_n) = \alpha$ has q^{n-1} solutions in $\mathbb{F}_q^n$ for each $\alpha \in \mathbb{F}_q$.

(2) A system of polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, where $1 \leq m \leq n$, is said to be orthogonal if the system of equations $f_1(x_1, \ldots, x_n) = \alpha_1, \ldots, f_m(x_1, \ldots, x_n) = \alpha_m$ has exactly q^{n-m} solutions in $\mathbb{F}_q^n$ for each $(\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_q^m$.

The permutation polynomials over $\mathbb{F}_2$, are known as balanced functions [15] in the cryptography/computer science literature.
Since one of our main interests is in keyed permutations let us extend the definition of orthogonal systems. In general, we will denote with x the plaintext variables and with y the key variables.

Definition 2. *Let $\mathbb{F}_q$ be a finite field.*

(1) Let $F : \mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2} \to \mathbb{F}_q^{n_1}$ be a function. We call F a keyed permutation, if for any fixed $\mathbf{y} \in \mathbb{F}_q^{n_2}$ the function $F(\_, \mathbf{y}) : \mathbb{F}_q^{n_1} \to \mathbb{F}_q^{n_1}$ induces a permutation.
(2) Let $f_1, \ldots, f_m \in \mathbb{F}_q^n[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$, where $1 \leq m \leq n_1$ be polynomials. We call $f_1, \ldots, f_m$ a keyed orthogonal system, if for any fixed $(y_1, \ldots, y_{n_2}) \in \mathbb{F}_q^{n_2}$ the system $f_1, \ldots, f_m$ is an orthogonal system.

Remark 3. (1) Note that in our definition we allow for trivial keyed permutations, i.e., permutations that are constant in the key variable. In particular, every permutation $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ induces a keyed permutation $\hat{F} : \mathbb{F}_q^n \times \mathbb{F}_q^m \to \mathbb{F}_q^n$ via $\hat{F}(\mathbf{x}, \mathbf{y}) = F(\mathbf{x})$ for any $m \in \mathbb{Z}_{\geq 1}$.
(2) A keyed orthogonal system is also an orthogonal system in $\mathbb{F}_q[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$. Suppose we are given a keyed orthogonal system $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$ and equations $f_i(\mathbf{x}, \mathbf{y}) = \alpha_i$, where $\alpha_i \in \mathbb{F}_q$. If we fix $\mathbf{y}$ then we have $q^{n_1 - m}$ many solutions for $\mathbf{x}$. There are q^{n_2} possible choices for $\mathbf{y}$, so the system has $q^{n_1 + n_2 - m}$ solutions. Hence, our definition of keyed orthogonal systems does not induce any essentially new structure, it is merely semantic.

As intuition suggests keyed orthogonal systems are well-behaved under iteration. We state the following theorem for completeness.

Theorem 4. *Let $\mathbb{F}_q$ be a finite field. The keyed polynomial system $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$ is keyed orthogonal if and only if the system $g_1(f_1, \ldots, f_m, y_1, \ldots, y_{n_2}), \ldots, g_m(f_1, \ldots, f_m, y_1, \ldots, y_{n_2}) \in \mathbb{F}_q[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$ is keyed orthogonal for every keyed orthogonal system $g_1, \ldots, g_m \in \mathbb{F}_q[x_1, \ldots, x_m, y_1, \ldots, y_{n_2}]$.*

The proof of this theorem is given in Appendix A.1.
In practice keyed orthogonal systems are usually derived from orthogonal systems by a simple addition of the key variables before or after an evaluation of a function.

Example 5. If $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a permutation, then

$$F(\mathbf{x} + \mathbf{y}) \qquad \text{and} \qquad F(\mathbf{x}) + \mathbf{y}$$

are keyed permutations.

3 Generalized Triangular Dynamical Systems

We propose the generalized triangular dynamical system (GTDS) as the main algebraic system in designing a block cipher. The GTDS is also the main ingredient in unifying different design principles proposed in the literature such as SPN and Feistel networks.

Definition 6 (Generalized triangular dynamical system). *Let $\mathbb{F}_q$ be a finite field, and let $n \geq 1$. For $1 \leq i \leq n$, let $p_i \in \mathbb{F}_q[x]$ be permutation polynomials, and for $1 \leq i \leq n-1$, let $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ be polynomials such that the polynomials g_i do not have zeros over $\mathbb{F}_q$. Then we define a generalized triangular dynamical system $\mathcal{F} = \{f_1, \ldots, f_n\}$ as follows*

$$\begin{aligned}
f_1(x_1, \ldots, x_n) &= p_1(x_1) \cdot g_1(x_2, \ldots, x_n) + h_1(x_2, \ldots, x_n),\\
f_2(x_1, \ldots, x_n) &= p_2(x_2) \cdot g_2(x_3, \ldots, x_n) + h_2(x_3, \ldots, x_n),\\
&\ldots\\
f_{n-1}(x_1, \ldots, x_n) &= p_{n-1}(x_{n-1}) \cdot g_{n-1}(x_n) + h_{n-1}(x_n),\\
f_n(x_1, \ldots, x_n) &= p_n(x_n).
\end{aligned}$$

Note that a GTDS $\mathcal{F} = \{f_1, \ldots, f_n\}$ must be considered as ordered tuple of polynomials since in general the order of the f_i's cannot be interchanged.

Proposition 7. *A generalized triangular dynamical system is an orthogonal system.*

The proof of the proposition is provided in Appendix A.2.

Corollary 8. *The inverse orthogonal system $\mathcal{F}^{-1} = \{\tilde{f}_1, \ldots, \tilde{f}_n\}$ to the generalized triangular dynamical system $\mathcal{F} = \{f_1, \ldots, f_n\}$ is given by*

$$\begin{aligned}
\tilde{f}_1(x_1, \ldots, x_n) &= p_1^{-1}\left(\left(x_1 - h_1(\tilde{f}_2, \ldots, \tilde{f}_n)\right) \cdot \left(g_1(\tilde{f}_2, \ldots, \tilde{f}_n)\right)^{q-2}\right)\\
\tilde{f}_2(x_1, \ldots, x_n) &= p_2^{-1}\left(\left(x_2 - h_2(\tilde{f}_3, \ldots, \tilde{f}_n)\right) \cdot \left(g_2(\tilde{f}_3, \ldots, \tilde{f}_n)\right)^{q-2}\right)\\
&\ldots\\
\tilde{f}_{n-1}(x_1, \ldots, x_n) &= p_{n-1}^{-1}\left(\left(x_{n-1} - h_{n-1}(\tilde{f}_n)\right) \cdot \left(g_{n-1}(\tilde{f}_n)\right)^{q-2}\right)\\
\tilde{f}_n(x_1, \ldots, x_n) &= p_n^{-1}(x_n).
\end{aligned}$$

Proof. If we consider $\mathcal{F}$ and $\mathcal{F}^{-1}$ in $\mathbb{F}_q[x_1, \ldots, x_n]/\left(x_1^q - x_1, \ldots, x_n^q - x_n\right)$, then it is easy to see that $\mathcal{F}^{-1} \circ \mathcal{F} = \mathcal{F} \circ \mathcal{F}^{-1} = \mathrm{id}$. □

Note that the Triangular Dynamical System introduced by Ostafe and Shparlinski [44] is a special case of our GTDS up to permutation. Moreover, one can drop the conditions on p_i and g_i (given in definition 6) to obtain a generalized dynamical system beyond permutation (which is not the focus of this work). In particular,

if we choose $p_i(x_i) = x_i$ for all i and impose the condition that each polynomial g_i has a unique leading monomial of maximal degree, i.e.,

$$g_i(x_{i+1}, \ldots, x_n) = x_{i+1}^{s_{i,i+1}} \cdots x_n^{s_{i,n}} + \tilde{g}_i(x_{i+1}, \ldots, x_n), \tag{2}$$

where

$$\deg(\tilde{g}_i) < s_{i,i+1} + \ldots + s_{i,n}, \text{ and} \tag{3}$$
$$\deg(h_i) \leq \deg(g_i) \tag{4}$$

for $i = 1, \ldots, n-1$, then we obtain the triangular dynamical system in [44]. Notice that under iteration these systems exhibit a property highly uncommon for general polynomial dynamical systems: polynomial degree growth (see [44, §2.2]).

Since the triangular dynamical system of [44] as a special case of GTDS has $p_i(x_i) = x_i$, it can not be used to instantiate many (cryptographic) permutations. More specifically, permutations where polynomials p_i are such that $\deg(p_i) \geq 2$, can not be instantiated. Examples of such permutation include well-known SPN, recently proposed Reinforced Concrete permutation [31] and Arion. In this work we will use our generalized definition 6 to describe cryptographic permutations.

3.1 GTDS and (Keyed) Permutations

In practice, every keyed permutation or block cipher (in cryptography) is constructed using an iterative structure where round functions are iterated a fixed number of times. Using the GTDS we first define such a round function. In this section $n \in \mathbb{N}$ denotes the number of field elements constituting a block and $r \in \mathbb{N}$ denotes the number of rounds of an iterative permutation.

Definition 9 (Round function). *Let $\mathbb{F}_q$ be a finite field, $n \geq 1$ be an integer, $\mathbf{A} \in \mathbb{F}_q^{n \times n}$ be an invertible matrix, and $\mathbf{b} \in \mathbb{F}_q^n$ be a vector. Then, the affine mixing layer is described by the map*

$$\mathcal{L} : \mathbb{F}_q^n \to \mathbb{F}_q^n, \qquad \mathbf{x} \mapsto \mathbf{A} \cdot \mathbf{x} + \mathbf{b},$$

and the key addition is described by the map

$$\mathcal{K} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n, \qquad (\mathbf{x}, \mathbf{k}) \mapsto \mathbf{x} + \mathbf{k}.$$

We abbreviate $\mathcal{K}_\mathbf{k} = \mathcal{K}(\_, \mathbf{k})$. Let $\mathcal{F} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a GTDS or a composition of two or more GTDS and affine permutations. Then the round function of a block cipher is defined as the following composition

$$\mathcal{R} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n, \qquad (\mathbf{x}, \mathbf{k}) \mapsto \mathcal{K}_\mathbf{k} \circ \mathcal{L} \circ \mathcal{F}(\mathbf{x}).$$

We also abbreviate $\mathcal{R}_\mathbf{k} = \mathcal{R}(\_, \mathbf{k})$.

It is obvious that $\mathcal{R}$ is a keyed permutation, hence it also is a keyed orthogonal system of polynomials in the sense of Definition 2. Now we can introduce our generalized notion of block ciphers which encompasses almost all existing block ciphers.

Definition 10 (An algebraic description of keyed permutations). *Let $\mathbb{F}_q$ be a finite field, let $n, r \geq 1$ be integers, and let $\mathbf{K} \in \mathbb{F}_q^{n\times(r+1)}$ be a matrix. We index the columns of $\mathbf{K}$ by $0, \ldots, r$, the i^{th} column $\mathbf{k}_i$ denotes the i^{th} round key. Let $\mathcal{K} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the key addition function, and let $\mathcal{R}^{(1)}, \ldots, \mathcal{R}^{(r)} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the round functions. Then a block cipher is defined as the following composition*

$$\mathcal{C}_r : \mathbb{F}_q^n \times \mathbb{F}_q^{n\times(r+1)} \to \mathbb{F}_q^n, \qquad (\mathbf{x}, \mathbf{K}) \mapsto \mathcal{R}^{(r)}_{\mathbf{k}_r} \circ \cdots \circ \mathcal{R}^{(1)}_{\mathbf{k}_1} \circ \mathcal{K}_{\mathbf{k}_0}(\mathbf{x}).$$

We abbreviate $\mathcal{C}_{r,\mathbf{K}} = \mathcal{C}_r(\_, \mathbf{K})$, and if the round functions are clear from context or identical, then we also abbreviate $\mathcal{R}^r_{\mathbf{k}} = \mathcal{R}^{(r)}_{\mathbf{k}_r} \circ \cdots \circ \mathcal{R}^{(1)}_{\mathbf{k}_1}$.

For the remaining parts of the paper a keyed permutation or a block cipher should be understood as a function described as in Definition 10, unless specified otherwise. We stress that a generic definition of an iterative block cipher may only use the notion of round key(s) (as defined with $\mathbf{K}$ in Definition 10) and does not require explicit definition of a key scheduling function. The specific definition of a key scheduling function can depend on the input key size and specific instantiations of the iterative block cipher. Also, in most of the cryptography literature the generic definition, (security) analysis and security proofs of iterative block ciphers (e.g. SPN, Even-Mansour etc.) only use the notion of round keys [39,22,18], without an explicit scheduling function.

4 Instantiating Block Ciphers

In this section we will show that the GTDS-based algebraic definition of iterative permutations is able to describe different design strategies.

We note with respect to GTDS that well-known design strategies such as SPN, partial SPN, Feistel, generalized Feistel and Lai–Massey are constructed with trivial polynomials g_i in the GTDS, namely $g_i = 1$.

4.1 Feistel Networks

For simplicity, we only show how the GTDS based algebraic definition can describe the unbalanced Feistel with expanding round function. The classical two branch Feistel is then a special case of the unbalanced expanding one. Moreover, it is straight-forward to show that GTDS-based algebraic definition can describe other types of Feistel networks such as unbalanced Feistel with expanding round functions, Nyberg's GFN, etc.

Unbalanced Feistel. Let $n > 1$, and let $f \in \mathbb{F}_q[x]$ be any function represented by a polynomial. The unbalanced Feistel network with expanding round function is defined as

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_n \\ x_1 + f(x_n) \\ \vdots \\ x_{n-1} + f(x_n) \end{pmatrix}. \tag{5}$$

The GTDS

$$\begin{aligned} f_i(x_1, \ldots, x_n) &= x_i + f(x_n), \quad 1 \leq i \leq n-1, \\ f_n(x_1, \ldots, x_n) &= x_n, \end{aligned} \tag{6}$$

together with the shift permutation $(x_1, \ldots, x_{n-1}, x_n) \mapsto (x_n, x_1, \ldots, x_{n-1})$ describe the unbalanced Feistel network with expanding round function.

4.2 Substitution-Permutation Networks

In [36, §7.2.1] a handy description of Substitution-Permutation networks (SPN) was given. Let $S \in \mathbb{F}_q[x]$ be a permutation polynomial, the so called S-box. Then the round function of a SPN consists of three parts:

(1) Addition of the round keys and round constants.
(2) Application of the S-box, i.e., $(x_1, \ldots, x_n) \mapsto \big(S(x_1), \ldots, S(x_n)\big)$.
(3) Permutation and mixing of the blocks.

The mixing in the last step is usually done via linear/affine transformations. In this case the GTDS of a SPN reduces to

$$f_i(x_1, \ldots, x_n) = S(x_i), \tag{7}$$

where $1 \leq i \leq n$.

AES-128. At the time of writing the most famous SPN is the AES family [1,19]. If we use the description of AES-128 given in [16], then it is easy to see that AES-128 is also covered by our definition of block ciphers. AES-128 is defined over the field $\mathbb{F} = \mathbb{F}_{2^8} = \mathbb{F}_2[X]/\left(X^8 + X^4 + X^3 + X + 1\right)$ and has 16 blocks, i.e., it is a keyed permutation over $\mathbb{F}^{16}$. The GTDS of AES-128 is given by Equation (7) and the polynomial $S(x)$ over $\mathbb{F}$ is given in Appendix B.

Let us now describe the permuting and mixing of the blocks via linear transformations. The `ShiftRows` operations can be described with the block matrix

$$D_{\mathrm{SR}} = \mathsf{diag}(D_{\mathrm{SR}_0}, D_{\mathrm{SR}_0}, D_{\mathrm{SR}_0}, D_{\mathrm{SR}_0}) \in \mathbb{F}^{16\times 16} \tag{8}$$

where D_{SR} is a block diagonal matrix with $D_{\mathrm{SR}_t} = \left(\Delta_{i,(j-t) \mod 4}\right) \in \mathbb{F}^{4\times 4}$ and $\Delta_{i,j}$ is the Kronecker delta. The `MixColumns` operation can be described as the following tensor product

$$D_{\mathrm{MC}} = \begin{pmatrix} \mathtt{02} & \mathtt{03} & \mathtt{01} & \mathtt{01} \\ \mathtt{01} & \mathtt{02} & \mathtt{03} & \mathtt{01} \\ \mathtt{01} & \mathtt{01} & \mathtt{02} & \mathtt{03} \\ \mathtt{03} & \mathtt{01} & \mathtt{01} & \mathtt{02} \end{pmatrix} \otimes I_4 \in \mathbb{F}^{16\times 16}, \tag{9}$$

where the entries in the left matrix are hexadecimal representations of field elements. The linear mixing layer $\mathcal{L}$ of AES-128 can now be represented by the following matrix D

$$D = P \cdot D_{\mathrm{MC}} \cdot D_{\mathrm{SR}} \cdot P, \tag{10}$$

where $P \in \mathbb{F}^{16\times 16}$ denotes the transposition matrix. In the last round the `MixColumns` operation is dropped, hence $\tilde{\mathcal{L}}$ is represented by $\tilde{D}$

$$\tilde{D} = P \cdot D_{\mathrm{SR}} \cdot P. \tag{11}$$

Similarly, we can also describe the key schedule of AES-128.

Partial SPN. In a partial SPN the S-box is only applied to some input variables and not all of them. This construction was proposed for ciphers like `LowMC` [5], the Hades design strategy [33] and the Poseidon family [32] that are efficient in the MPC setting. Clearly, any partial SPN is also covered by the GTDS.

4.3 Lai–Massey Ciphers and GTDS

Another well-known design strategy for block ciphers is the Lai–Massey design which was first introduced in [37]. For two branches let $g \in \mathbb{F}_q[x]$ be a polynomial, then the round function of the Lai–Massey cipher is defined as

$$\mathcal{F}_{\mathrm{LM}} : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x + g(x-y) \\ y + g(x-y) \end{pmatrix}. \tag{12}$$

Since the difference between the branches is invariant under application of $\mathcal{F}_{\mathrm{LM}}$ it is possible to invert the construction. At the first look it may appear that the Lai–Massey can not be described with GTDS. However, a careful analysis shows one round of Lai–Massey is in fact a composition of a Feistel Network and two linear permutations. We consider the following triangular dynamical systems

$$\mathcal{F}_1(x,y) = \begin{pmatrix} x-y \\ y \end{pmatrix}, \quad \mathcal{F}_2(x,y) = \begin{pmatrix} x \\ y+g(x) \end{pmatrix}, \quad \mathcal{F}_3(x,y) = \begin{pmatrix} x+y \\ y \end{pmatrix}. \tag{13}$$

Then, it is easily checked that $\mathcal{F}_{\mathrm{LM}} = \mathcal{F}_3 \circ \mathcal{F}_2 \circ \mathcal{F}_1$. Due to simpler structure of polynomials (p_i), the Lai–Massey permutation can be described using the triangular system in [44].

Generalized Lai–Massey. Recently, a generalization of the Lai–Massey was proposed in [35, §3.3] by Grassi et al. It is based on the following observation: If one is given field elements $\omega_1, \ldots, \omega_n \in \mathbb{F}_q$ such that $\sum_{i=1}^n \omega_i = 0$, then the mapping

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 + g(\sum_{i=1}^n \omega_i x_i) \\ \vdots \\ x_n + g(\sum_{i=1}^n \omega_i x_i) \end{pmatrix} \tag{14}$$

is invertible for any polynomial $g \in \mathbb{F}_q[x]$.

We will use this observation to propose an even more general version of the Lai–Massey from the GTDS and linear permutations.

Definition 11 (Generalized Lai–Massey). *Let $\mathbb{F}_q$ be a finite field, and let $n \geq 2$ be an integer. Let $\omega_1, \ldots, \omega_n \in \mathbb{F}_q$ be such that $\sum_{i=1}^{n} \omega_i = 0$, and denote with m the largest index $1 \leq i \leq n$ such that ω_i is non-zero. For $1 \leq i \leq n$ let $p_i \in \mathbb{F}_q[x]$ be permutation polynomials, and let $g \in \mathbb{F}_q[x, x_{m+1}, \ldots, x_n]$ be a polynomial. Then we define the generalized Lai–Massey $\mathcal{F}_{LM} = \{f_1, \ldots, f_n\}$ as follows*

$$\begin{aligned}
f_1(x_1, \ldots, x_n) &= p_1(x_1) + g\left(\sum_{i=1}^{m} \omega_i \cdot p_i(x_i), x_{m+1}, \ldots, x_n\right), \\
&\ldots \\
f_m(x_1, \ldots, x_n) &= p_m(x_m) + g\left(\sum_{i=1}^{m} \omega_i \cdot p_i(x_i), x_{m+1}, \ldots, x_n\right), \\
f_{m+1}(x_1, \ldots, x_n) &= p_{m+1}(x_{m+1}), \\
&\ldots \\
f_n(x_1, \ldots, x_n) &= p_n(x_n).
\end{aligned}$$

Remark 12. If $n \equiv 0 \mod 2$, then it is evident from the first equation in the proof of [34, Proposition 5] that Grassi et al.'s generalized Lai–Massey permutation is also covered by Definition 11 and a linear transformation.

For completeness, we establish that the generalized Lai–Massey is indeed invertible.

Lemma 13. *Let $\mathbb{F}_q$ be a finite field. The generalized Lai–Massey is an orthogonal system.*

The proof of this lemma is given in Appendix A.3.
Before we prove the reduction of the generalized Lai–Massey to the GTDS we explain the rationale behind Definition 11. Usually, in the Lai–Massey the polynomial g is added to all the branches, but our definition allows the concatenation of two independent Lai–Massey permutations

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + g_1(x_1 - x_2) \\ x_2 + g_1(x_1 - x_2) \\ x_3 + g_2(x_3 - x_4) \\ x_4 + g_2(x_3 - x_4) \end{pmatrix}, \tag{15}$$

or the construction of intertwined Lai–Massey permutations

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + g_1(x_1 - x_2, x_3 - x_4) \\ x_2 + g_1(x_1 - x_2, x_3 - x_4) \\ x_3 + g_2(x_3 - x_4) \\ x_4 + g_2(x_3 - x_4) \end{pmatrix} \tag{16}$$

Analog to the classical two branch Lai–Massey we can describe the generalized Lai–Massey as composition of several GTDS and linear permutations.

Theorem 14. *Let $\mathbb{F}_q$ be a finite field. The generalized Lai–Massey can be constructed via compositions of generalized triangular dynamical systems and affine permutations.*

Proof. The first dynamical system is the application of the univariate permutation polynomials to the first m branches

$$\mathcal{F}_1 : (x_1, \ldots, x_n)^\intercal \mapsto \begin{pmatrix} \{p_i(x_i)\}_{1 \le i \le m} \\ \{x_i\}_{m+1 \le i \le n} \end{pmatrix}.$$

In the second one we construct the sum with the ω_i's

$$\mathcal{F}_2 : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \left\{ \begin{array}{ll} \omega_i \cdot x_i, & \omega_i \neq 0, \\ x_i, & \omega_i = 0 \end{array} \right\}_{1 \le i \le m-1} \\ \sum_{i=1}^{m} \omega_i \cdot x_i \\ \{x_i\}_{m+1 \le i \le n} \end{pmatrix}.$$

In the third one we add the polynomial g to the first $m-1$ branches, though we have to do a case distinction whether $\omega_i \neq 0$ or not,

$$\mathcal{F}_3 : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \left\{ \begin{array}{ll} x_i + \omega_i \cdot g(x_m, x_{m+1}, \ldots, x_n), & \omega_i \neq 0, \\ x_i + g(x_m, x_{m+1}, \ldots, x_n), & \omega_i = 0 \end{array} \right\}_{1 \le i \le m-1} \\ \{x_i\}_{m \le i \le n} \end{pmatrix}$$

Then we add the polynomial g to the m^{th} branch and cancel the factors ω_i whenever necessary

$$\mathcal{F}_4 : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \left\{ \begin{array}{ll} \omega_i^{-1} \cdot x_i, & \omega_i \neq 0, \\ x_i, & \omega_i = 0 \end{array} \right\}_{1 \le i \le m-1} \\ \omega_m^{-1} \cdot \left(x_m - \sum_{\substack{1 \le i \le m-1 \\ \omega_i \neq 0}} x_i \right) \\ \{x_i\}_{m+1 \le i \le n} \end{pmatrix}.$$

Lastly, we apply the univariate permutation polynomials to the remaining branches

$$\mathcal{F}_5 : (x_1, \ldots, x_n)^\intercal \mapsto \begin{pmatrix} \{x_i\}_{1 \le i \le m} \\ \{p_i(x_i)\}_{m+1 \le i \le n} \end{pmatrix}.$$

Now it follows from a simple calculation that indeed $\mathcal{F}_5 \circ \cdots \circ \mathcal{F}_1$ implements the generalized Lai–Massey construction. □

4.4 Constructions with Non-Trivial g_i's

Recall that for $1 \le i \le n-1$ the i^{th} branch in a GTDS is given by

$$f_i(x_1, \ldots, x_n) = p_i(x_i) \cdot g_i(x_{i+1}, \ldots, x_n) + h_i(x_{i+1}, \ldots, x_n), \tag{17}$$

where g_i is a polynomial that does not have any zeros. All constructions we have investigated so far have one thing in common, they all use trivial g_i's, that is $g_i = 1$. Therefore, it is now time to cover constructions that have non-trivial g_i's.

Horst & Griffin. The `Horst` scheme [30] was introduced as generalization of the Feistel scheme. It is defined as

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 \cdot g_1(x_2, \ldots, x_n) + h_1(x_2, \ldots, x_n) \\ \vdots \\ x_{n-1} \cdot g_{n-1}(x_n) + h_{n-1}(x_n) \\ x_n \end{pmatrix}, \tag{18}$$

where $g_i, h_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$. If the polynomials g_i's do not have any zeros over $\mathbb{F}_q$, then `Horst` induces a permutation. Clearly, this is a special instance of a GTDS. The permutation Griffin-π [30] is a concatenation of a SPN and a `Horst` permutation, so it is also covered by the GTDS framework. Note that the simpler structure of polynomials p_i allows describing Griffin-π with the triangular dynamical system of [44].

`Reinforced Concrete`. The `Reinforced Concrete` [31] hash function is the first Arithmetization-Oriented hash function that utilizes lookup tables. At round level the `Reinforced Concrete` permutation over $\mathbb{F}_p^3$, where $p \gtrsim 2^{64}$ is a prime, consists of three small permutations. The first permutation is the mapping `Bricks`

$$\begin{aligned} &\texttt{Bricks} : \mathbb{F}_p^3 \to \mathbb{F}_p^3, \\ &\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1^d \\ x_2 \cdot \left(x_1^2 + \alpha_1 \cdot x_1 + \beta_1\right) \\ x_3 \cdot \left(x_2^2 + \alpha_2 \cdot x_2 + \beta_2\right) \end{pmatrix}, \end{aligned} \tag{19}$$

where $d = 5$, note that the prime must be suitable chosen such that $\gcd(d, p-1) = 1$ else the first component does not induce a permutation, and $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_p$ such that $\alpha_i^2 - 4\beta_i$ is not quadratic residue module p, then the quadratic polynomials do not have any zeros over $\mathbb{F}_p$. The second permutation is called `Concrete` and is given by matrix multiplication and constant addition. The third permutation `Bars` is an S-box that is implemented via a lookup table. Clearly, these mappings are covered by the GTDS framework.

Arion. The Arion block cipher and ArionHash [46] are the first designs that utilize the full GTDS structure at round level. It is defined over prime fields with $p \geq 2^{60}$, and its GTDS is

$$\begin{aligned} f_i(x_1, \ldots, x_n) &= x_i^{d_1} \cdot g_i(\sigma_{i+1,n}) + h_i(\sigma_{i+1,n}), \qquad 1 \leq i \leq n-1, \\ f_n(x_1, \ldots, x_n) &= x_n^e, \end{aligned} \tag{20}$$

where $d_1 \in \mathbb{Z}_{>1}$ is the smallest integer such that $\gcd(d_1, p-1) = 1$, for one $d_2 \in \{121, 123, 125, 129, 161, 257\}$ $e \in \mathbb{Z}_{>1}$ is such that $e \cdot d_2 \equiv 1 \mod p-1$, $g_i, h_i \in \mathbb{F}_p[x]$ are quadratic polynomials such that the g_i's are irreducible, and

$$\sigma_{i+1,n} = \sum_{j=i+1}^{n} x_i + f_i. \tag{21}$$

5 Analysis of GTDS-based Permutations

5.1 Bounding the Differential Uniformity of the GTDS

Differential cryptanalysis [14] and its variants are one of the most widely used attack vectors in modern cryptography. It is based on the observation that certain input differences can propagate through the rounds of a block cipher with high probability. The key measure to quantify whether a function is weak to differential cryptanalysis is the so-called differential uniformity. In this section we prove an upper bound for the differential uniformity of the GTDS under minimal assumptions on the polynomials p_i, g_i and h_i. We recall the definition of differential uniformity.

Definition 15 ([43]). *Let $\mathbb{F}_q$ be a finite field, and let $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function. The differential distribution table of f at $\mathbf{a} \in \mathbb{F}_q^n$ and $\mathbf{b} \in \mathbb{F}_q^m$ is defined as*

$$\delta_f(\mathbf{a}, \mathbf{b}) = \left|\{\mathbf{x} \in \mathbb{F}_q^n \mid f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}) = \mathbf{b}\}\right|.$$

The differential uniformity of f is defined as $\delta(f) = \max_{\mathbf{a}\in\mathbb{F}_q^n\setminus\{\mathbf{0}\},\mathbf{b}\in\mathbb{F}_q^m} \delta_f(\mathbf{a}, \mathbf{b})$.

The following lemma will play an essential role in the proof of the main result of this section.

Lemma 16. *Let $\mathbb{F}_q$ be a finite field, and let $f \in \mathbb{F}_q[x]/(x^q - x)$. Then $\delta(f) < q$ if and only if $\deg\big(f(x+a) - f(x)\big) > 0$ for all $a \in \mathbb{F}_q^\times$. In particular, if $\delta(f) < q$ then $\delta(f) < \deg(f)$.*

The proof of this lemma is given in Appendix A.4. Next we compute an upper bound for the differential uniformity of a GTDS.

Theorem 17. *Let $\mathbb{F}_q$ be a finite field, let $n \geq 1$ be an integer, and let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a GTDS. Let $p_1, \ldots, p_n \in \mathbb{F}_q[x]/(x^q - x)$ be the univariate permutation polynomials of the GTDS $\mathcal{F}$ such that for every i either*

(i) $\deg(p_i) = 1$, *or*
(ii) $\deg(p_i) \geq 2$ *and* $\delta(p_i) < q$.

Let $\boldsymbol{\Delta x}, \boldsymbol{\Delta y} \in \mathbb{F}_q^n$ be such that $\boldsymbol{\Delta x} \neq \mathbf{0}$. Then the differential distribution table of $\mathcal{F}$ at $\boldsymbol{\Delta x}$ and $\boldsymbol{\Delta y}$ is bounded by

$$\delta_{\mathcal{F}}(\boldsymbol{\Delta x}, \boldsymbol{\Delta y}) \leq \left\{\begin{array}{ll} \delta(p_n), & \boldsymbol{\Delta x}_n \neq 0, \\ q, & \boldsymbol{\Delta x}_n, \boldsymbol{\Delta y}_n = 0, \\ 0, & \boldsymbol{\Delta x}_n = 0,\ \boldsymbol{\Delta y}_n \neq 0 \end{array}\right\} \cdot \prod_{i=1}^{n-1} \left\{\begin{array}{ll} \deg(p_i), & \boldsymbol{\Delta x}_i \neq 0,\ \deg(p_i) > 1, \\ q, & \boldsymbol{\Delta x}_i \neq 0,\ \deg(p_i) = 1, \\ q, & \boldsymbol{\Delta x}_i = 0 \end{array}\right\}.$$

The proof of the theorem is detailed in Appendix A.6.
Let the function $\mathrm{wt} : \mathbb{F}_q^n \to \mathbb{Z}$ denote the Hamming weight, i.e. it counts the number of non-zero entries of a vector in $\mathbb{F}_q^n$.

Corollary 18. *Let $\mathbb{F}_q$ be a finite field, let $n \geq 1$ be an integer, and let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a GTDS. Let $p_1, \ldots, p_n \in \mathbb{F}_q[x]/(x^q - x)$ be the univariate permutation polynomials of the GTDS $\mathcal{F}$, and let $\boldsymbol{\Delta x}, \boldsymbol{\Delta y} \in \mathbb{F}_q^n$ be such that $\boldsymbol{\Delta x} \neq \mathbf{0}$. If for all $1 \leq i \leq n$ one has that $1 < \deg(p_i) \leq d$ and $\delta(p_i) < q$, then*

$$\delta_{\mathcal{F}}(\boldsymbol{\Delta x}, \boldsymbol{\Delta y}) \leq q^{n - \mathrm{wt}(\boldsymbol{\Delta x})} \cdot d^{\mathrm{wt}(\boldsymbol{\Delta x})}.$$

In particular,

$$\mathbb{P}\left[\mathcal{F} \colon \boldsymbol{\Delta x} \to \boldsymbol{\Delta y}\right] \leq \left(\frac{d}{q}\right)^{\mathrm{wt}(\boldsymbol{\Delta x})}.$$

Proof. By our assumptions we can apply Theorem 17 for the first inequality. The second inequality follows from the first and division by q^n. □

Let $p_1, \ldots, p_n \in \mathbb{F}_q[x]$ be univariate permutation polynomials that satisfy the assumption from Theorem 17 and assume that $1 < \delta(p_i) \leq d$ for all i. Let us consider the SPN

$$S : (x_1, \ldots, x_n) \mapsto \big(p_1(x_1), \ldots, p_n(x_n)\big). \tag{22}$$

It is well-known that

$$\mathbb{P}\left[S \colon \boldsymbol{\Delta x} \to \boldsymbol{\Delta y}\right] \leq \left(\frac{d}{q}\right)^{\mathrm{wt}(\boldsymbol{\Delta x})}. \tag{23}$$

Now let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a GTDS with the univariate permutation polynomials $p_1, \ldots, p_n$. Provided that $\delta(p_i) \approx \deg(p_i)$ when compared to q, then we expect that the bound from Corollary 18 almost coincides with Equation (23). I.e., the GTDS $\mathcal{F}$ and the SPN S are in almost the same security class with respect to differential cryptanalysis. What is the contribution of the polynomials g_i and h_i in the GTDS $\mathcal{F}$ then? Conceptually, they can only lower the probability compared to the "SPN bounds" from Equation (23) but never increase it.

Of course, this now raises the question of how this contribution can be incorporated into an improved bound. If we recall the proof of the theorem, then we can translate this question into the following problem: Let $f \in \mathbb{F}_q[x]$ be a polynomial, let $\alpha, \beta, \Delta x \in \mathbb{F}_q^\times$ and $\delta, \Delta y \in \mathbb{F}_q$. How many solutions does the equation

$$\alpha \cdot f(x + \Delta x) - \beta \cdot f(x) + \gamma = \Delta y \tag{24}$$

have? Moreover, one could try to estimate the codomains of the g_i's and h_i's to exclude values for α, β, γ that can never arise in the differential equation of the GTDS.

For the application of Theorem 17 it is crucial that one knows that the univariate permutation polynomials have non-trivial differential uniformity. Therefore, we derive two efficient criteria that bypass the computation of the full differential distribution table.

Lemma 19. *Let $\mathbb{F}_q$ be a finite field of characteristic p, let $a \in \mathbb{F}_q^\times$, and let $f = \sum_{i=0}^{d} b_i \cdot x^i \in \mathbb{F}_q[x]/(x^q - x)$ be such that $d = \deg(f) > 1$.*

(1) If q is prime, then $f(x+a)-f(x)$ is a non-constant polynomial.
(2) If q is a prime power, let $d' = \max\left\{\deg\left(f - b_d \cdot x^d\right), 1\right\}$. If there exists $d' \leq k \leq d-1$ such that $\gcd\left(p, \binom{d}{k}\right) = 1$, then $f(x+a)-f(x)$ is a non-constant polynomial.

Proof of this lemma is given in Appendix A.5.
By (1), over prime fields we can apply Theorem 17 for every univariate permutation polynomial of degree greater than 1. With (2) we can settle some polynomials $f \in \mathbb{F}_q[x]/(x^q - x)$ such that $\gcd\left(q, \deg(f)\right) \neq 1$. E.g., let $q = 2^n$, and let $f = x^{2^n-2}$, then

$$\binom{2^n - 2}{2^n - 4} = (2^n - 3) \cdot \left(2^{n-1} - 1\right) \equiv 1 \mod 2. \tag{25}$$

Finally, Theorem 17 performs best for designs where either $\deg(p_i) \ll q$ or $\deg\left(p_i^{-1}\right) \ll q$ for all i. Arithmetization-Oriented primitives for Multi-Party Computation and Zero-Knowledge protocols often satisfy this condition. Main performance measure in these applications is the number of multiplications necessary for evaluation. So low degree polynomials at round level are an attractive choice to instantiate these primitives. Typically, these protocols are instantiated over prime fields $p \geq 2^{64}$ and one utilizes a univariate permutation polynomial $f \in \mathbb{F}_p[x]/(x^p - x)$ such that $\deg(f) < 2^9$ or $\deg\left(f^{-1}\right) < 2^9$. So we obtain a bound which is less than $\frac{2^9}{2^{64}}$ for the respective component. For an iterated design this bound is small enough to provide resistance against differential cryptanalysis and its variants. It is worthwhile mentioning that some AO primitives rely on high degree permutations, e.g. Vision [6] which is based on the inverse permutation x^{q-2}. For such designs one will need different techniques to estimate resistance against differential cryptanalysis and its variants. We also highlight that Theorem 17 has been applied in the differential cryptanalysis of Arion [46, §3.1].

5.2 A Bound on the Correlation of the GTDS

Linear cryptanalysis was introduced in [42] and extended to non-binary ciphers in [8]. In this cryptanalysis one tries to find linear approximations of the rounds of a block cipher for a sample of known plaintexts. The key measure to quantify whether a function is weak under linear cryptanalysis is the so-called correlation. In this section we will prove an upper bound for the maximum absolute correlation of the GTDS under minimal assumptions on the polynomials p_i, g_i and h_i. We recall a modern definition of the correlation over finite fields, see [13, Definition 3.3] and the equation thereafter.

Definition 20. *Let $\mathbb{F}_q$ be a finite field, let $n \geq 1$, let $\chi, \psi : \mathbb{F}_q^n \to \mathbb{C}$ be non-trivial additive characters, and let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a function. The correlation for the characters (χ, ψ) of F is defined as*

$$\mathrm{CORR}_F(\chi, \psi) = \frac{1}{q^n} \cdot \sum_{\mathbf{x} \in \mathbb{F}_q^n} \overline{\chi\big(F(\mathbf{x})\big)} \cdot \psi(\mathbf{x}).$$

Let $\mathbb{F}_q$ be a finite field of characteristic p, and let $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the absolute trace function, see [40, 2.22. Definition]. For all $x \in \mathbb{F}_q$ we define the function χ_1 as

$$\chi_1(x) = \exp\left(\frac{2\pi i}{p} \cdot \mathrm{Tr}(x)\right). \tag{26}$$

Then, every additive character $\chi : \mathbb{F}_q \to \mathbb{C}$ is of the form $\chi(x) = \chi_1(a \cdot x)$ for some $a \in \mathbb{F}_q$, see [40, 5.7. Theorem]. Moreover, any additive character $\chi : \mathbb{F}_q^n \to \mathbb{C}$ is of the form $\chi(\mathbf{x}) = \chi_1\big(\langle \mathbf{a}, \mathbf{x}\rangle\big)$ for some $\mathbf{a} \in \mathbb{F}_q^n$. (The proof of this statement is a simple generalization of [40, 5.7. Theorem].) So without loss of generality we can express the correlation of a function F as

$$\mathrm{CORR}_F(\chi, \psi) = \mathrm{CORR}_F(\mathbf{a}, \mathbf{b}) = \frac{1}{q^n} \cdot \sum_{\mathbf{x} \in \mathbb{F}_q^n} \chi_1\Big(\langle \mathbf{b}, \mathbf{x}\rangle - \big\langle \mathbf{a}, F(\mathbf{x})\big\rangle\Big), \tag{27}$$

for some $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$.

As preparation, we prove a bound on univariate character sums which follows as corollary to [40, 5.38. Theorem].

Lemma 21. *Let $\mathbb{F}_q$ be a finite field, let $\chi : \mathbb{F}_q \to \mathbb{C}$ be a non-trivial additive character, let $f \in \mathbb{F}_q[x]$ be a permutation polynomial such that $\gcd\left(\deg\left(f\right), q\right) = \gcd\left(\deg\left(f^{-1}\right), q\right) = 1$, and let $a, b \in \mathbb{F}_q^{\times}$. Then*

$$\left|\sum_{x \in \mathbb{F}_q} \chi\left(a \cdot f(x) + b \cdot x\right)\right| \leq \left(\min\left\{\deg\left(f\right), \deg\left(f^{-1}\right)\right\} - 1\right) \cdot q^{1/2}.$$

The proof of this lemma is given in Appendix A.7. Now we can compute an upper bound on the correlation of the GTDS.

Theorem 22. *Let $\mathbb{F}_q$ be a finite field, let $n \geq 1$, let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, let $\mathcal{F} = \{f_1, \ldots, f_n\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a GTDS, and let $p_1, \ldots, p_n \in \mathbb{F}_q[x]/(x^q - x)$ be the univariate permutation polynomials in the GTDS $\mathcal{F}$ such that $\gcd\left(\deg\left(p_i\right), q\right) = \gcd\left(\deg\left(p_i^{-1}\right), q\right) = 1$ for all $1 \leq i \leq n$. If $\mathbf{a} \neq \mathbf{0}$ denote with $1 \leq j \leq n$ the first index such that $a_j \neq 0$. Then*

$$|\mathrm{CORR}_{\mathcal{F}}(\mathbf{a}, \mathbf{b})| \leq \begin{cases} 1, & \mathbf{a}, \mathbf{b} = \mathbf{0}, \\ 0, & \begin{cases} \mathbf{a} = \mathbf{0}, \ \mathbf{b} \neq \mathbf{0}, \\ \mathbf{a} \neq \mathbf{0}, \ \mathbf{b} = \mathbf{0}, \end{cases} \\ 0, & b_j = 0, \\ 1, & b_j \neq 0, \ \deg\left(p_j\right) = 1, \\ \dfrac{\min\left\{\deg\left(p_j\right), \deg\left(p_j^{-1}\right)\right\} - 1}{\sqrt{q}}, & b_j \neq 0, \ \deg\left(p_j\right) > 1. \end{cases}$$

The proof of this theorem is detailed in Appendix A.8. Note if q is a prime number and $f \in \mathbb{F}_q[x]/(x^q - x)$, then the coprimality condition is always satisfied.

Analog to the differential uniformity, let us compare Theorem 22 to a SPN of the form $S : (x_1, \ldots, x_n) \mapsto \big(p_1(x_1), \ldots, p_n(x_n)\big)$, where the p_i's are univariate permutation polynomials with $1 < \deg(p_i) \leq d \ll q$ and $\gcd(\deg(p_i), q) = 1$ for all i. It is well-known that

$$\mathrm{CORR}_S(\mathbf{a}, \mathbf{b}) \leq \begin{cases} 1, & \mathbf{a}, \mathbf{b} = \mathbf{0}, \\ 0, & \exists i \colon a_i \neq 0,\ b_i = 0, \\ & \exists i \colon a_i = 0,\ b_i \neq 0, \\ \left(\dfrac{d-1}{\sqrt{q}}\right)^{\mathrm{wt}(\mathbf{a})}, & \textit{else}. \end{cases} \tag{28}$$

(This inequality essentially follows from rearranging the character sum and Weil's bound [40, 5.38. Theorem].) This bound decreases with $\mathcal{O}\left(q^{-\frac{\mathrm{wt}(\mathbf{a})}{2}}\right)$ while our bound from Theorem 22 (if non-trivial) is always in $\mathcal{O}\left(q^{-1}\right)$. Therefore, we leave improving Theorem 22 as open problem for future work.

As for the differential uniformity bound, Theorem 22 performs best for GTDS instances where either $\deg(p_i) \ll q$ or $\deg\left(p_i^{-1}\right) \ll q$ for all i. Moreover, over prime fields the coprimality condition is always satisfied. On the other hand, over binary fields Theorem 22 restricts us to univariate permutation polynomials of odd degree. In particular, Theorem 22 cannot be applied to x^{2^m-2} over $\mathbb{F}_{2^m}$.

We highlight that Theorem 22 has been applied in the linear cryptanalysis of Arion [46, §3.1].

5.3 Degree Growth Of Block Ciphers

For algebraic security analysis of block ciphers it is important to understand the polynomial degree growth over $\mathbb{F}_q[x_1, \ldots, x_n]$ of the polynomials that represent the branches. For certain classes of GTDS the degree growth can be described via triangular matrices.

Definition 23 (Well-behaved GTDS). *Let $\mathbb{F}_q$ be a finite field, and let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a GTDS.*

Case 1 If $\deg(h_i) \leq \deg(g_i) + \deg(p_i)$ for all $1 \leq i \leq n$, and g_i has a unique leading monomial, i.e., $g_i(x_{i+1}, \ldots, x_n) = x_{i+1}^{s_{i,i+1}} \cdots x_n^{s_{i,n}} + \tilde{g}_i(x_{i+1}, \ldots, x_n)$, for some $\tilde{g}_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ with $\deg(\tilde{g}_i) < s_{i,i+1} + \ldots + s_{i,n}$, then we define

$$\mathbf{S} = \begin{pmatrix} d_1 & s_{1,2} & s_{1,3} & \ldots & s_{1,n} \\ 0 & d_2 & s_{2,3} & \ldots & s_{2,n} \\ & & \ddots & & \\ 0 & 0 & 0 & 0 & d_n \end{pmatrix} \in \mathbb{Z}^{n \times n},$$

where $d_i = \deg(p_i)$ for all $1 \leq i \leq n$.

Case 2 If $\deg(h_i) > \deg(g_i) + \deg(p_i)$ *for all* $1 \leq i \leq n$ *and* h_i *has a unique leading monomial, i.e.,* $h_i(x_{i+1}, \ldots, x_n) = x_{i+1}^{t_{i,i+1}} \cdots x_n^{t_{i,n}} + \tilde{h}_i(x_{i+1}, \ldots, x_n)$*, for some* $\tilde{h}_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ *with* $\deg(\tilde{h}_i) < t_{i,i+1} + \ldots + t_{i,n}$*, then we define*

$$\mathbf{T} = \begin{pmatrix} 0 & t_{1,2} & t_{1,3} & \ldots & t_{1,n} \\ 0 & 0 & t_{2,3} & \ldots & t_{2,n} \\ & & \ddots & & \\ 0 & 0 & 0 & 0 & d_n \end{pmatrix} \in \mathbb{Z}^{n \times n}.$$

Let $\mathbf{d}_0 = (1, \ldots, 1)^\intercal$, then $\mathbf{S}\mathbf{d}_0$ and $\mathbf{T}\mathbf{d}_0$ respectively describe the polynomial degrees of the components of $\mathcal{F}(\mathbf{x})$.

If the polynomial degrees of the round functions of a block cipher $\mathcal{C}$ are bounded by d, then after r iterations one has the trivial upper bound d^r among all components. While this bound is straight forward, obtaining a better bound *without any assumption of the polynomial forms* in GTDS appears to be difficult. We leave this question open for future research.

6 Discussion

Hash Functions and PRFs. Our generic description of (keyed) permutations when viewed as a vector of functions over $\mathbb{F}_q^n$, can be used to define a hash function $H : \mathbb{F}_q^* \to \mathbb{F}_q^t$ where the domain of H is of arbitrary length over $\mathbb{F}_q$ and the hash value is of length $t > 0$ over $\mathbb{F}_q$. For example, an instantiation of GTDS-based permutations can be used in a sponge mode [10,11] to define such a hash function. Thus, all our analysis can be easily extrapolated to hash functions. The invertibility conditions in GTDS can be dropped if the goal is not to construct a permutation but possibly a pseudo-random function. Potentially, such a GTDS (without the necessary constraints for invertibility) can be used to construct PRFs over $\mathbb{F}_q$ and is an interesting direction for future work.

Beyond the GTDS. The quasi-Feistel cipher idea [49] provides a unified framework for Feistel and Lai–Massey ciphers. While our approach utilizes the polynomial structure over finite fields, [49] uses a contrarian approach by requiring as little algebraic structure as possible. In particular, they demonstrate that invertible Feistel and Lai–Massey ciphers can be instantiated over quasigroups (cf. [48]). Furthermore, this little algebraic structure is already sufficient to prove theoretical security bounds in the Luby-Rackoff model for quasi-Feistel ciphers.

Acknowledgments. The authors thank all reviewers for their helpful comments on improving the paper and Tim Beyne for shepherding the paper.

Matthias Steiner has been supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 725042) and the enCRYPTON project (grant agreement No. 101079319).

References

1. Advanced Encryption Standard (AES). National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce (Nov 2001)
2. Albrecht, M.R., Cid, C., Grassi, L., Khovratovich, D., Lüftenegger, R., Rechberger, C., Schofnegger, M.: Algebraic cryptanalysis of STARK-friendly designs: Application to MARVELlous and MiMC. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019, Part III. Lecture Notes in Computer Science, vol. 11923, pp. 371–397. Springer, Heidelberg, Germany, Kobe, Japan (Dec 8–12, 2019). https://doi.org/10.1007/978-3-030-34618-8_13
3. Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schofnegger, M.: Feistel structures for MPC, and more. In: Sako, K., Schneider, S., Ryan, P.Y.A. (eds.) ESORICS 2019: 24th European Symposium on Research in Computer Security, Part II. Lecture Notes in Computer Science, vol. 11736, pp. 151–171. Springer, Heidelberg, Germany, Luxembourg (Sep 23–27, 2019). https://doi.org/10.1007/978-3-030-29962-0_8
4. Albrecht, M.R., Grassi, L., Rechberger, C., Roy, A., Tiessen, T.: MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology – ASIACRYPT 2016, Part I. Lecture Notes in Computer Science, vol. 10031, pp. 191–219. Springer, Heidelberg, Germany, Hanoi, Vietnam (Dec 4–8, 2016). https://doi.org/10.1007/978-3-662-53887-6_7
5. Albrecht, M.R., Rechberger, C., Schneider, T., Tiessen, T., Zohner, M.: Ciphers for MPC and FHE. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015, Part I. Lecture Notes in Computer Science, vol. 9056, pp. 430–454. Springer, Heidelberg, Germany, Sofia, Bulgaria (Apr 26–30, 2015). https://doi.org/10.1007/978-3-662-46800-5_17
6. 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). https://doi.org/10.13154/tosc.v2020.i3.1-45
7. Andreeva, E., Daemen, J., Mennink, B., Assche, G.V.: Security of keyed sponge constructions using a modular proof approach. In: Leander, G. (ed.) Fast Software Encryption – FSE 2015. Lecture Notes in Computer Science, vol. 9054, pp. 364–384. Springer, Heidelberg, Germany, Istanbul, Turkey (Mar 8–11, 2015). https://doi.org/10.1007/978-3-662-48116-5_18
8. Baignères, T., Stern, J., Vaudenay, S.: Linear cryptanalysis of non binary ciphers. In: Adams, C.M., Miri, A., Wiener, M.J. (eds.) SAC 2007: 14th Annual International Workshop on Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 4876, pp. 184–211. Springer, Heidelberg, Germany, Ottawa, Canada (Aug 16–17, 2007). https://doi.org/10.1007/978-3-540-77360-3_13
9. Bard, G.V.: Algebraic Cryptanalysis. Springer US, Boston, MA, 1 edn. (2009). https://doi.org/10.1007/978-0-387-88757-9
10. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Sponge functions. ECRYPT Hash Workshop (2007), https://keccak.team/files/SpongeFunctions.pdf
11. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: On the indifferentiability of the sponge construction. In: Smart, N.P. (ed.) Advances in Cryptology – EUROCRYPT 2008. Lecture Notes in Computer Science, vol. 4965, pp. 181–197. Springer, Heidelberg, Germany, Istanbul, Turkey (Apr 13–17, 2008). https://doi.org/10.1007/978-3-540-78967-3_11

12. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Duplexing the sponge: Single-pass authenticated encryption and other applications. In: Miri, A., Vaudenay, S. (eds.) SAC 2011: 18th Annual International Workshop on Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 7118, pp. 320–337. Springer, Heidelberg, Germany, Toronto, Ontario, Canada (Aug 11–12, 2012). https://doi.org/10.1007/978-3-642-28496-0_19
13. Beyne, T.: A geometric approach to linear cryptanalysis. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2021, Part I. Lecture Notes in Computer Science, vol. 13090, pp. 36–66. Springer, Heidelberg, Germany, Singapore (Dec 6–10, 2021). https://doi.org/10.1007/978-3-030-92062-3_2
14. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) Advances in Cryptology – CRYPTO'90. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 11–15, 1991). https://doi.org/10.1007/3-540-38424-3_1
15. Boura, C., Canteaut, A., De Cannière, C.: Higher-order differential properties of Keccak and Luffa. In: Joux, A. (ed.) Fast Software Encryption – FSE 2011. Lecture Notes in Computer Science, vol. 6733, pp. 252–269. Springer, Heidelberg, Germany, Lyngby, Denmark (Feb 13–16, 2011). https://doi.org/10.1007/978-3-642-21702-9_15
16. Buchmann, J., Pyshkin, A., Weinmann, R.P.: A zero-dimensional Gröbner basis for AES-128. In: Robshaw, M.J.B. (ed.) Fast Software Encryption – FSE 2006. Lecture Notes in Computer Science, vol. 4047, pp. 78–88. Springer, Heidelberg, Germany, Graz, Austria (Mar 15–17, 2006). https://doi.org/10.1007/11799313_6
17. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.P.: Minimizing the two-round Even-Mansour cipher. In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology – CRYPTO 2014, Part I. Lecture Notes in Computer Science, vol. 8616, pp. 39–56. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2014). https://doi.org/10.1007/978-3-662-44371-2_3
18. Cogliati, B., Seurin, Y.: On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015, Part I. Lecture Notes in Computer Science, vol. 9056, pp. 584–613. Springer, Heidelberg, Germany, Sofia, Bulgaria (Apr 26–30, 2015). https://doi.org/10.1007/978-3-662-46800-5_23
19. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography, Springer Berlin, Heidelberg, 2 edn. (2020). https://doi.org/10.1007/978-3-662-60769-5
20. Deligne, P.: La conjecture de Weil: I. Publications Mathématiques de l'IHÉS **43**, 273–307 (1974), http://www.numdam.org/item/PMIHES_1974__43__273_0/
21. Data encryption standard. National Bureau of Standards, NBS FIPS PUB 46, U.S. Department of Commerce (Jan 1977)
22. Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: Cryptanalysis of iterated Even-Mansour schemes with two keys. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology – ASIACRYPT 2014, Part I. Lecture Notes in Computer Science, vol. 8873, pp. 439–457. Springer, Heidelberg, Germany, Kaoshiung, Taiwan, R.O.C. (Dec 7–11, 2014). https://doi.org/10.1007/978-3-662-45611-8_23
23. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in cryptography: The Even-Mansour scheme revisited. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012. Lecture Notes in Computer Science, vol. 7237, pp. 336–354. Springer, Heidelberg, Germany, Cambridge, UK (Apr 15–19, 2012). https://doi.org/10.1007/978-3-642-29011-4_21

24. Dutta, A.: Minimizing the two-round tweakable Even-Mansour cipher. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12491, pp. 601–629. Springer, Heidelberg, Germany, Daejeon, South Korea (Dec 7–11, 2020). https://doi.org/10.1007/978-3-030-64837-4_20
25. Dworkin, M., Barker, E., Nechvatal, J., Foti, J., Bassham, L., Roback, E., Dray, J.: Advanced encryption standard (AES) (11 2001). https://doi.org/10.6028/NIST.FIPS.197
26. Eichlseder, M., Grassi, L., Lüftenegger, R., Øygarden, M., Rechberger, C., Schofnegger, M., Wang, Q.: An algebraic attack on ciphers with low-degree round functions: Application to full MiMC. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12491, pp. 477–506. Springer, Heidelberg, Germany, Daejeon, South Korea (Dec 7–11, 2020). https://doi.org/10.1007/978-3-030-64837-4_16
27. Farshim, P., Procter, G.: The related-key security of iterated Even-Mansour ciphers. In: Leander, G. (ed.) Fast Software Encryption – FSE 2015. Lecture Notes in Computer Science, vol. 9054, pp. 342–363. Springer, Heidelberg, Germany, Istanbul, Turkey (Mar 8–11, 2015). https://doi.org/10.1007/978-3-662-48116-5_17
28. Freitag, C., Ghoshal, A., Komargodski, I.: Time-space tradeoffs for sponge hashing: Attacks and limitations for short collisions. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology – CRYPTO 2022, Part III. Lecture Notes in Computer Science, vol. 13509, pp. 131–160. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 15–18, 2022). https://doi.org/10.1007/978-3-031-15982-4_5
29. Gazi, P., Tessaro, S.: Provably robust sponge-based PRNGs and KDFs. In: Fischlin, M., Coron, J.S. (eds.) Advances in Cryptology – EUROCRYPT 2016, Part I. Lecture Notes in Computer Science, vol. 9665, pp. 87–116. Springer, Heidelberg, Germany, Vienna, Austria (May 8–12, 2016). https://doi.org/10.1007/978-3-662-49890-3_4
30. Grassi, L., Hao, Y., Rechberger, C., Schofnegger, M., Walch, R., Wang, Q.: Horst meets fluid-SPN: Griffin for zero-knowledge applications. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023, Part III. Lecture Notes in Computer Science, vol. 14083, pp. 573–606. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 2023). https://doi.org/10.1007/978-3-031-38548-3_19
31. Grassi, L., Khovratovich, D., Lüftenegger, R., Rechberger, C., Schofnegger, M., Walch, R.: Reinforced concrete: A fast hash function for verifiable computation. In: Yin, H., Stavrou, A., Cremers, C., Shi, E. (eds.) ACM CCS 2022: 29th Conference on Computer and Communications Security. pp. 1323–1335. ACM Press, Los Angeles, CA, USA (Nov 7–11, 2022). https://doi.org/10.1145/3548606.3560686
32. Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., Schofnegger, M.: Poseidon: A new hash function for zero-knowledge proof systems. In: Bailey, M., Greenstadt, R. (eds.) USENIX Security 2021: 30th USENIX Security Symposium. pp. 519–535. USENIX Association (Aug 11–13, 2021)
33. Grassi, L., Lüftenegger, R., Rechberger, C., Rotaru, D., Schofnegger, M.: On a generalization of substitution-permutation networks: The HADES design strategy. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, Part II. Lecture Notes in Computer Science, vol. 12106, pp. 674–704. Springer, Heidelberg, Germany, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45724-2_23

34. Grassi, L., Onofri, S., Pedicini, M., Sozzi, L.: Invertible quadratic non-linear layers for MPC-/FHE-/ZK-friendly schemes over $\mathbb{F}_p^n$. Cryptology ePrint Archive, Report 2021/1695 (2021), https://eprint.iacr.org/2021/1695
35. 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 Transactions on Symmetric Cryptology **2022**(3), 20–72 (2022). https://doi.org/10.46586/tosc.v2022.i3.20-72
36. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. Chapman & Hall / CRC, Boca Raton, 3 edn. (2020). https://doi.org/10.1201/9781351133036
37. Lai, X.: On the design and security of block ciphers. Ph.D. thesis, ETH Zurich, Konstanz (1992). https://doi.org/10.3929/ethz-a-000646711, diss. Techn. Wiss ETH Zürich, Nr. 9752, 1992. Ref.: J. L. Massey ; Korref.: H. Bühlmann.
38. Lai, X., Massey, J.L.: A proposal for a new block encryption standard. In: Damgård, I. (ed.) Advances in Cryptology – EUROCRYPT'90. Lecture Notes in Computer Science, vol. 473, pp. 389–404. Springer, Heidelberg, Germany, Aarhus, Denmark (May 21–24, 1991). https://doi.org/10.1007/3-540-46877-3_35
39. Lampe, R., Patarin, J., Seurin, Y.: An asymptotically tight security analysis of the iterated Even-Mansour cipher. In: Wang, X., Sako, K. (eds.) Advances in Cryptology – ASIACRYPT 2012. Lecture Notes in Computer Science, vol. 7658, pp. 278–295. Springer, Heidelberg, Germany, Beijing, China (Dec 2–6, 2012). https://doi.org/10.1007/978-3-642-34961-4_18
40. Lidl, R., Niederreiter, H.: Finite fields. Encyclopedia of mathematics and its applications, Cambridge Univ. Press, Cambridge, 2 edn. (1997)
41. Liu, T., Tessaro, S., Vaikuntanathan, V.: The t-wise independence of substitution-permutation networks. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology – CRYPTO 2021, Part IV. Lecture Notes in Computer Science, vol. 12828, pp. 454–483. Springer, Heidelberg, Germany, Virtual Event (Aug 16–20, 2021). https://doi.org/10.1007/978-3-030-84259-8_16
42. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) Advances in Cryptology – EUROCRYPT'93. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer, Heidelberg, Germany, Lofthus, Norway (May 23–27, 1994). https://doi.org/10.1007/3-540-48285-7_33
43. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) Advances in Cryptology – EUROCRYPT'93. Lecture Notes in Computer Science, vol. 765, pp. 55–64. Springer, Heidelberg, Germany, Lofthus, Norway (May 23–27, 1994). https://doi.org/10.1007/3-540-48285-7_6
44. Ostafe, A., Shparlinski, I.E.: On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators. Math. Comput. **79**(269), 501–511 (2010). https://doi.org/10.1090/S0025-5718-09-02271-6
45. Roy, A., Andreeva, E., Sauer, J.F.: Interpolation cryptanalysis of unbalanced Feistel networks with low degree round functions. In: Dunkelman, O., Jr., M.J.J., O'Flynn, C. (eds.) SAC 2020: 27th Annual International Workshop on Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 12804, pp. 273–300. Springer, Heidelberg, Germany, Halifax, NS, Canada (Virtual Event) (Oct 21-23, 2020). https://doi.org/10.1007/978-3-030-81652-0_11
46. Roy, A., Steiner, M.J., Trevisani, S.: Arion: Arithmetization-oriented permutation and hashing from generalized triangular dynamical systems. arXiv: 2303.04639 (2023). https://doi.org/10.48550/ARXIV.2303.04639, Version: 3
47. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Biryukov, A. (ed.) Fast Software Encryption –

FSE 2007. Lecture Notes in Computer Science, vol. 4593, pp. 181–195. Springer, Heidelberg, Germany, Luxembourg, Luxembourg (Mar 26–28, 2007). https://doi.org/10.1007/978-3-540-74619-5_12
48. Smith, J.D.: An Introduction to Quasigroups and Their Representations. Studies in Advanced Mathematics, Chapman & Hall / CRC Press, New York (2006). https://doi.org/10.1201/9781420010633
49. Yun, A., Park, J.H., Lee, J.: On Lai–Massey and quasi-Feistel ciphers. Des. Codes Cryptogr. **58**(1), 45–72 (1 2011). https://doi.org/10.1007/s10623-010-9386-8

A Proofs

A.1 Proof of Theorem 4

Proof. "⇐": If we choose $g_i = x_i$, then by assumption the equations

$$g_i(f_1, \ldots, f_m, y_1, \ldots, y_{n_2}) = f_i(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}) = \beta_i,$$

where $1 \leq i \leq m$, have q^{n_1-m} many solutions for every fixed $(y_1, \ldots, y_{n_2}) \in \mathbb{F}_q^{n_2}$. I.e., $f_1, \ldots, f_m$ is a keyed orthogonal system.
"⇒": Suppose we are given a system of equations

$$\begin{aligned} g_1(f_1, \ldots, f_m, y_1, \ldots, y_{n_2}) &= \beta_1, \\ &\ldots \\ g_m(f_1, \ldots, f_m, y_1, \ldots, y_{n_2}) &= \beta_m, \end{aligned}$$

where $\beta_1, \ldots, \beta_m \in \mathbb{F}_q$ and $\{f_i\}_{1 \leq i \leq n_1}$ and $\{g_i\}_{1 \leq i \leq m}$ are keyed orthogonal systems. Fix $\mathbf{y} = (y_1, \ldots, y_{n_2}) \in \mathbb{F}_q^{n_2}$ and substitute $\hat{x}_i = f_i$, then the equations $g_i(\hat{x}_1, \ldots, \hat{x}_m, \mathbf{y}) = \beta_i$ have a unique solution for the $\hat{x}_i$'s. Since $\mathbf{y}$ is fixed also the equations $\hat{x}_i = f_i$ admit q^{n_2-m} many solutions. Therefore, the composition of keyed orthogonal systems is again keyed orthogonal. □

A.2 Proof of Proposition 7

Proof. Suppose for $1 \leq i \leq n$ we are given equations

$$f_i(x_i, \ldots, x_n) = \alpha_i,$$

where $\alpha_i \in \mathbb{F}_q$. To solve the system we work upwards. The last polynomial f_n is a univariate permutation polynomial, so we can find a unique solution β_n for x_n. We plug this solution into the next equation, i.e.,

$$f_{n-1}(x_{n-1}, \beta_n) = p_{n-1}(x_{n-1}) \cdot g_{n-1}(\beta_n) + h_{n-1}(\beta_n).$$

To solve for x_{n-1} we subtract $h_{n-1}(\beta_n)$, divide by $g_{n-1}(\beta_n)$, this division is possible since $g_i(x_{i+1}, \ldots, x_n) \neq 0$ for all $(x_{i+1}, \ldots, x_n) \in \mathbb{F}_q^{n-i}$, and invert p_{n-1}. Iterating this procedure we can find a unique solution for all x_i. □

A.3 Proof of Lemma 13

Proof. Suppose we are given equations $f_i(x_1, \ldots, x_n) = \alpha_i$, where $\alpha_i \in \mathbb{F}_q$. For $i = m+1, \ldots, n$ we simply invert p_i to solve for x_i. For $i = 1, \ldots, m$ we compute $\sum_{i=1}^{m} \omega_i f_i = \sum_{i=1}^{m} \omega_i p_i(x_i) = \sum_{i=1}^{m} \omega_i \alpha_i = \alpha$. Now we plug α and the solutions for $x_{m+1}, \ldots, x_n$ into the polynomial g in the first m equations, rearrange them, and invert the univariate permutation polynomials to obtain a unique solution. □

A.4 Proof of Lemma 16

Proof. "⇐": By assumption, for all $a \in \mathbb{F}_q^\times$ and all $b \in \mathbb{F}_q$ we have that $f(x+a) - f(x) - b$ is a non-constant polynomial whose degree is less than $\deg(f)$, so we have that $\delta(f) < \deg(f) < q$.

"⇒": Suppose there exists an $a \in \mathbb{F}_q^\times$ such that $\deg\big(f(x-a) - f(x)\big) \leq 0$.[4] Then we can find $b \in \mathbb{F}_q$ such that $f(x+a) - f(x) - b = 0$, so $\delta(f) = q$. Now the claim follows by contraposition. □

A.5 Proof of Lemma 19

Proof. For (1), we expand f via the binomial formula

$$\begin{aligned} f(x+a) - f(x) &= \sum_{i=0}^{\deg(f)} b_i \cdot \big((x+a)^i - x^i\big) \\ &= \sum_{i=0}^{\deg(f)} b_i \cdot \left(\sum_{k=0}^{i-1} \binom{i}{k} \cdot a^{i-k} \cdot x^k\right) \\ &= b_d \cdot \binom{d}{d-1} \cdot a \cdot x^{d-1} + g(x), \end{aligned}$$

where $\deg(g) < d-1$. Since $d < q$ and q is prime we always have that $\binom{d}{d-1} \not\equiv 0 \mod q$.

For (2), the assumption on the binomial coefficient guarantees that at least one binomial coefficient $\binom{d}{k}$, where $d' \leq k \leq d-1$, is non-zero in $\mathbb{F}_q$. □

A.6 Proof of Theorem 17

Proof. Suppose we are given the differential equation

$$\mathcal{F}(\mathbf{x} + \boldsymbol{\Delta x}) - \mathcal{F}(\mathbf{x}) = \boldsymbol{\Delta y}, \tag{29}$$

Then, the last component of the differential equation only depends on the variable x_n, i.e.,

$$p_n(x_n + \boldsymbol{\Delta x}_n) - p_n(x_n) = \boldsymbol{\Delta y}_n.$$

[4] Some textbooks define $\deg(0) = -1$ or $\deg(0) = -\infty$, hence the inequality.

If $\boldsymbol{\Delta x}_n \neq 0$, then this equation has at most $\delta(p_n)$ many solutions. If $\boldsymbol{\Delta x}_n = \boldsymbol{\Delta y}_n = 0$, then this equation has q many solutions for x_n. Lastly, if $\boldsymbol{\Delta x}_n = 0$ and $\boldsymbol{\Delta y}_n \neq 0$, then there cannot be any solution for x_n.

Now suppose we have a solution for the last component, say $\hat{x}_n \in \mathbb{F}_q$. Then, we can substitute it in Equation (29) into the $(n-1)^{\text{th}}$ component

$$f_{n-1}(x_{n-1} + \boldsymbol{\Delta x}_{n-1}, \hat{x}_n + \boldsymbol{\Delta x}_n) - f_{n-1}(x_{n-1}, \hat{x}_n) = \boldsymbol{\Delta y}_{n-1}.$$

Since $\hat{x}_n$ is a field element we can reduce this equation to

$$\alpha \cdot p_{n-1}(x_{n-1} + \boldsymbol{\Delta x}_{n-1}) - \beta \cdot p_{n-1}(x_{n-1}) + \gamma = \boldsymbol{\Delta y}_{n-1}, \tag{30}$$

where $\alpha, \beta, \gamma \in \mathbb{F}_q$ and $\alpha, \beta \neq 0$. Now we have to do a case distinction on the various case for α, β, $\boldsymbol{\Delta x}_{n-1}$ and $\deg(p_{n-1})$.

- For $\boldsymbol{\Delta x}_{n-1} \neq 0$ and $\alpha \neq \beta$, then Equation (30) has at most $\deg(p_{n-1})$ many solutions.
- For $\boldsymbol{\Delta x}_{n-1} \neq 0$, $\alpha = \beta$ and $\deg(p_{n-1}) > 1$, Equation (30) is the differential equation for p_{n-1} scaled by α and by assumption this equation has at most $\delta(p_{n-1}) < q$ many solutions. So we can apply Lemma 16 to immediately conclude that $\delta(p_{n-1}) < \deg(p_{n-1})$.
- For $\alpha = \beta$ and $\deg(p_{n-1}) = 1$, then only constant terms remain in Equation (30). In principle, it can happen that $\alpha \cdot a_{n-1,1} \cdot \boldsymbol{\Delta x}_{n-1} + \gamma = \boldsymbol{\Delta y}_{n-1}$, where $a_{n-1,1} \in \mathbb{F}_q^\times$ is the coefficient of the linear term of p_{n-1}. So this case can have at most q many solutions.
- For $\boldsymbol{\Delta x}_{n-1} = 0$, then in principle it can happen that $\alpha = \beta$ and $\boldsymbol{\Delta y}_{n-1} = \gamma$. So this case can have at most q many solutions.

Summarizing these cases we conclude that

- If $\boldsymbol{\Delta x}_{n-1} \neq 0$ and $\deg(p_{n-1}) > 1$, then Equation (30) has at most $\deg(p_{n-1})$ many solutions.
- If $\boldsymbol{\Delta x}_{n-1} \neq 0$ and $\deg(p_{n-1}) = 1$, then Equation (30) has at most q many solutions.
- If $\boldsymbol{\Delta x}_{n-1} = 0$, then Equation (30) has at most q many solutions.

Inductively, we now work upwards through the branches to derive the claim. □

A.7 Proof of Lemma 21

Proof. Since f is a permutation polynomial we can rewrite the character sum

$$\begin{aligned}\sum_{x \in \mathbb{F}_q} \chi(a \cdot f(x) + b \cdot x) &= \sum_{y \in \mathbb{F}_q} \chi\Big(a \cdot f\left(f^{-1}(y)\right) + b \cdot f^{-1}(y)\Big) \\ &= \sum_{y \in \mathbb{F}_q} \chi\Big(a \cdot y + b \cdot f^{-1}(y)\Big),\end{aligned}$$

where the second equality follows from $f\big(f^{-1}(x)\big) \equiv x \mod (x^q - x)$. By our assumptions we can then apply the Weil bound [40, 5.38. Theorem] to obtain the inequality. □

A.8 Proof of Theorem 22

Proof. The first case is trivial, for the second and the third we recall that any non-trivial linear combination of an orthogonal system is a multivariate permutation polynomial, cf. [40, 7.39. Corollary]. Recall that for any multivariate permutation polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ the equation $f(x_1, \ldots, x_n) = \alpha$ has q^{n-1} many solutions for every $\alpha \in \mathbb{F}_q$. So the exponential sum of the correlation collapses to

$$q^{n-1} \cdot \sum_{x \in \mathbb{F}_q} \chi_1(x) = 0,$$

which is zero by [40, 5.4. Theorem].

Now let us assume that $a_j \neq 0$. Then we apply the triangular inequality to the variables $x_{j+1}, \ldots, x_n$ as follows

$$\begin{aligned}
&\left| \sum_{\mathbf{x} \in \mathbb{F}_q^n} \chi_1\Big(\langle \mathbf{b}, \mathbf{x} \rangle - \big\langle \mathbf{a}, F(\mathbf{x}) \big\rangle \Big) \right| \\
&= \left| \sum_{\mathbf{x} \in \mathbb{F}_q^n} \chi_1 \left(\sum_{i=j+1}^{n} b_i \cdot x_i - a_i \cdot f_i(\mathbf{x}) \right) \cdot \chi_1\Big(b_j \cdot x_j - a_j \cdot f_j(\mathbf{x}) \Big) \right| \\
&\leq \sum_{x_{j+1}, \ldots, x_n \in \mathbb{F}_q} \left| \chi_1 \left(\sum_{i=j+1}^{n} b_i \cdot x_i - a_i \cdot f_i(\mathbf{x}) \right) \cdot \sum_{x_1, \ldots, x_j \in \mathbb{F}_q} \chi_1\Big(b_j \cdot x_j - a_j \cdot f_j(\mathbf{x}) \Big) \right| \\
&= \sum_{x_{j+1}, \ldots, x_n \in \mathbb{F}_q} \left| \chi_1 \left(\sum_{i=j+1}^{n} b_i \cdot x_i - a_i \cdot f_i(\mathbf{x}) \right) \right| \cdot \left| \sum_{x_1, \ldots, x_j \in \mathbb{F}_q} \chi_1\Big(b_j \cdot x_j - a_j \cdot f_j(\mathbf{x}) \Big) \right| \\
&= \sum_{x_{j+1}, \ldots, x_n \in \mathbb{F}_q} \left| q^{j-1} \cdot \sum_{x_j \in \mathbb{F}_q} \chi_1\Big(b_j \cdot x_j - a_j \cdot f_j(x_j, \ldots, x_n) \Big) \right| = (*).
\end{aligned}$$

For any fixed $(x_{j+1}, \ldots, x_n) \in \mathbb{F}_q^{n-j}$ we have that

$$\hat{f}_j(x_j) = -a_j \cdot f_j(x_j, \ldots, x_n) + b_j \cdot x_j = -a_j \cdot \big(p_j(x_j) \cdot \alpha + \beta \big) + b_j \cdot x_j,$$

where $\alpha = g_j(x_{j+1}, \ldots, x_n) \in \mathbb{F}_q^\times$, and $\beta = h_j(x_{j+1}, \ldots, x_n) \in \mathbb{F}_q$. If $b_j = 0$, then $\hat{f}_j$ is a univariate permutation polynomial in x_j. So the exponential sum inside the absolute value of $(*)$ must vanish for every $(x_{j+1}, \ldots, x_n) \in \mathbb{F}_q^{n-j}$.

For $b_j \neq 0$, if $\deg(p_j) = 1$, then in principle $\hat{f}_j$ can be a constant polynomial. Since we do not know for how many $(x_{j+1}, \ldots, x_n) \in \mathbb{F}_q^{n-j}$ this happens we have to use the trivial bound.

For the final case $\deg(p_j) > 1$, recall that we assumed

$$\gcd\left(\deg\left(p_i\right), q\right) = \gcd\left(\deg\left(p_i^{-1}\right), q\right) = 1$$

for all $1 \leq i \leq n$. So for every fixed $(x_{j+1}, \ldots, x_n) \in \mathbb{F}_q^{n-j}$ we can now apply Lemma 21 to bound the absolute value in $(*)$. This yields

$$\begin{aligned}(*) &\leq p^{j-1} \cdot \sum_{k=j+1}^{n} \sum_{x_k \in \mathbb{F}_q} \Big(\min\left\{ \deg\left(p_j\right), \deg\left(p_j^{-1}\right) \right\} - 1 \Big) \cdot p^{1/2} \\ &= p^{n-1/2} \cdot \Big(\min\left\{ \deg\left(p_j\right), \deg\left(p_j^{-1}\right) \right\} - 1 \Big),\end{aligned}$$

which concludes the proof. □

B AES S-Box Polynomial

$$\begin{aligned}S : x \mapsto \mathtt{05}x^{254} + \mathtt{09}x^{253} + \mathtt{F9}x^{251} + \mathtt{25}x^{247} + \mathtt{F4}x^{239} \\ + x^{223} + \mathtt{B5}x^{191} + \mathtt{8F}x^{127} + \mathtt{63},\end{aligned} \tag{31}$$