IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2024, No. 1, pp. 357–411. DOI:10.46586/tosc.v2024.i1.357-411

Solving Degree Bounds for Iterated Polynomial Systems

Matthias Johann Steiner

Alpen-Adria-Universität Klagenfurt, Klagenfurt am Wörthersee, Austria
matthias.steiner@aau.at

Abstract. For Arithmetization-Oriented ciphers and hash functions Gröbner basis attacks are generally considered as the most competitive attack vector. Unfortunately, the complexity of Gröbner basis algorithms is only understood for special cases, and it is needless to say that these cases do not apply to most cryptographic polynomial systems. Therefore, cryptographers have to resort to experiments, extrapolations and hypotheses to assess the security of their designs. One established measure to quantify the complexity of linear algebra-based Gröbner basis algorithms is the so-called solving degree. Caminata & Gorla revealed that under a certain genericity condition on a polynomial system the solving degree is always upper bounded by the Castelnuovo-Mumford regularity and henceforth by the Macaulay bound, which only takes the degrees and number of variables of the input polynomials into account. In this paper we extend their framework to iterated polynomial systems, the standard polynomial model for symmetric ciphers and hash functions. In particular, we prove solving degree bounds for various attacks on `MiMC`, Feistel-`MiMC`, Feistel-`MiMC`-Hash, Hades and `GMiMC`. Our bounds fall in line with the hypothesized complexity of Gröbner basis attacks on these designs, and to the best of our knowledge this is the first time that a mathematical proof for these complexities is provided.
Moreover, by studying polynomials with degree falls we can prove lower bounds on the Castelnuovo-Mumford regularity for attacks on `MiMC`, Feistel-`MiMC` and Feistel-`MiMC`-Hash provided that only a few solutions of the corresponding iterated polynomial system originate from the base field. Hence, regularity-based solving degree estimations can never surpass a certain threshold, a desirable property for cryptographic polynomial systems.

Keywords: Gröbner basis · Solving degree · MiMC · GMiMC · Hades

1 Introduction

With the increasing adaption of Multi-Party Computation (MPC) and Zero-Knowledge (ZK) proof systems new ciphers and hash functions are needed to implement these constructions efficiently without compromising security. These new cryptographic primitives are commonly referred to as *Arithmetization-Oriented* (AO) designs. The main objective of AO is to minimize multiplicative complexity, the minimum number of multiplications needed to evaluate a function. However, this comes at a cost: a very simple algebraic representation. Examples of recently proposed AO ciphers and hash functions are `LowMC` [ARS+15], `MiMC` [AGR+16], `GMiMC` [AGP+19a], `Jarvis` [AD18], Hades [GLR+20], Poseidon [GKR+21] and Poseidon2 [GKS23], `Vision` and `Rescue` [AAB+20], `Ciminion` [DGGK21], `Reinforced Concrete` [GKL+22], `Anemoi` [BBC+23], Griffin [GHR+23], Hydra [GØSW23] and Arion [RST23]. Unfortunately, with AO an often-neglected threat reemerged in cryptography: *Gröbner bases*. While being a minor concern for well-established ciphers like the Advanced Encryption Standard (AES) [BPW06, DR20], certain

Received: 2023-06-01 Revised: 2023-11-23 Accepted: 2024-01-23 Published: 2024-03-01

proposed AO designs have already been broken with off-the-shelf computing hardware and standard implementations of Gröbner bases, see for example [ACG+19, GKRS22]. Therefore, to ensure computational security against Gröbner basis attacks cryptographers ask for tight complexity bounds of Gröbner basis computations [AAB+20, SS21].

Unfortunately, the Gröbner basis cryptanalysis of the aforementioned AO designs is lacking mathematical rigor. Broadly speaking, the Gröbner basis analysis of AO designs usually falls into two categories:

(I) It is assumed that the polynomial system satisfies some genericity condition for which Gröbner basis complexity estimates are known. E.g., being regular or semi-regular.

(II) Empirical complexities from small scale experiments are extrapolated.

In this paper on the other hand, we present a rigor mathematical formalism to derive provable complexity estimates for cryptographic polynomial systems. In particular, we rigorously obtain Gröbner basis complexity estimates for various attacks on `MiMC`, Feistel-`MiMC`, Feistel-`MiMC`-Hash, HADES and `GMiMC`. We note that our bounds fall in line with the hypothesized cost of Gröbner basis attacks on these designs (see [GLR+20, §4.3] and [AGP+19a, §4.1.1]). To the best of our knowledge these are the first rigor mathematical proofs for the Gröbner basis cryptanalysis of these designs. Moreover, for `MiMC`, Feistel-`MiMC` and Feistel-`MiMC`-Hash we prove limitations of our complexity estimations, i.e., we derive lower bounds which can never be surpassed by our estimation method.

The cryptographic constructions of our interest all follow the same design principle. Let $\mathbb{F}_q$ be a finite field with q elements and let $n \geq 1$ be an integer, one chooses a round function $\mathcal{R} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$, which depends on the input variable $\mathbf{x}$ and the key variable $\mathbf{y}$, and then iterates it r times with respect to the input variable. Such a design admits a very simple model of keyed iterated polynomials

$$F_{\mathcal{R}}(\mathbf{x}_{i-1}, \mathbf{y}) - \mathbf{x}_i = \mathbf{0}, \tag{1}$$

where $F_{\mathcal{R}}$ denotes the polynomial vector representing the round function $\mathcal{R}$, the $\mathbf{x}_i$'s intermediate state variables, $\mathbf{y}$ the key variable and $\mathbf{x}_0, \mathbf{x}_r \in \mathbb{F}_q^n$ a plain/ciphertext pair given by the encryption function. This leads us to standard Gröbner basis attacks on ciphers which proceed in four steps:

(1) Model the cipher function with an iterated system of polynomials.

(2) Compute a Gröbner basis with respect to an efficient term order, e.g., the degree reverse lexicographic order.

(3) Perform a term order conversion to an elimination order, e.g., the lexicographic order.

(4) Solve the univariate equation.

Let us for the moment assume that a Gröbner basis has already been found and focus on the complexity of the remaining steps. Let $I \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a zero-dimensional ideal modeling a cipher, and denote with $d = \dim_{\mathbb{F}_q}(\mathbb{F}_q[x_1, \ldots, x_n]/I)$ the $\mathbb{F}_q$-vector space dimension of the quotient space. With the original FGLM algorithm [FGLM93] the complexity of term order conversion is $\mathcal{O}\left(n \cdot d^3\right)$, but improved versions with probabilistic methods achieve $\mathcal{O}\left(n \cdot d^\omega\right)$ [FGHR14], where $2 \leq \omega < 2.37286$ [AW21], and sparse linear algebra algorithms [FM17] achieve $\mathcal{O}\left(\sqrt{n} \cdot d^{2+\frac{n-1}{n}}\right)$. To extract the $\mathbb{F}_q$-valued roots of the univariate polynomial most efficiently we compute its greatest common divisor with the field equation $x^q - x$ via the algorithm of Bariant et al. [BBLP22, §3.1]. The complexity of this step is then

$$\mathcal{O}\Big(d \cdot \log(q) \cdot \log(d) \cdot \log\big(\log(d)\big) + d \cdot \log(d)^2 \cdot \log\big(\log(d)\big)\Big), \tag{2}$$

provided that $d \leq q$ otherwise one has to replace the roles of d and q in the complexity estimate.

Furthermore, in [FP19] it was proven that one can also use d to upper bound the complexity of linear algebra-based Gröbner basis algorithms. Since d is in general not known one has to estimate d via the Bézout bound.

To the best of our knowledge, the aforementioned AO designs all admit a very high quotient space dimension. Hence, to improve the capabilities of Gröbner basis attacks one must reduce this dimension. For this problem we have two generic approaches:

(i) Alter the standard representation, e.g., choose polynomials in the model which approximate the round function with high probability. This approach was successfully deployed in [ACG+19, GKRS22].

(ii) Add polynomials to the system to remove parasitic solutions that lie in algebraic closure. E.g., the polynomial system for an additional plain/ciphertext pair or the field equations. This approach is the concern of this paper.

If one successfully filters all solutions from the algebraic closure, then one expects that steps (3) and (4) are not a major concern anymore. Therefore, we need tight estimates for the complexity of Gröbner basis computations.

1.1 Contributions & Related Work

Our main tool to bound the complexity of Gröbner basis computations will be the *solving degree* of *linear algebra-based Gröbner basis algorithms* which was first formalized in [DS13]. Linear algebra-based Gröbner basis algorithms perform Gaussian elimination on matrices associated to a polynomial system. Given the number of equations, the number of variables and the solving degree one can then estimate the maximal size of these matrices and henceforth also the cost of Gaussian elimination. In [CG21] the solving degree was upper bounded via the *Castelnuovo-Mumford regularity* if the polynomial system is in *generic coordinates*. This genericity notion can be traced back to the influential work of Bayer & Stillman [BS87]. In essence, a polynomial system $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$ is in generic coordinates if its homogenization $\mathcal{F}^{\text{hom}} = \{f_1^{\text{hom}}, \ldots, f_m^{\text{hom}}\} \subset P[x_0]$ does not admit a solution with $x_0 = 0$ in the projective space $\mathbb{P}^n_K$, where x_0 denotes the homogenization variable. Moreover, the Castelnuovo-Mumford regularity is always upper bounded by the *Macaulay bound* [Cha07, Theorem 1.12.4]. Hence, if a polynomial system is in generic coordinates, then we can estimate the complexity of a Gröbner basis computation via the degrees of the input polynomials.

Our paper is divided into two parts. In the first part (Sections 2 to 5), we develop a rigor framework for complexity estimates of Gröbner attacks on `MiMC`, Feistel-`MiMC`, Feistel-`MiMC`-Hash, Hades and `GMiMC`. To streamline the application of the technique developed by Caminata & Gorla, we prove in Theorem 3.2 that a polynomial system is in generic coordinates if and only if it admits a finite *degree of regularity* [BFS04]. This in turn permits efficient proofs that the keyed iterated polynomial systems of `MiMC`, Feistel-`MiMC`, Feistel-`MiMC`-Hash, Hades and `GMiMC` are in generic coordinates.

In the second part (Sections 7 and 8), we study *polynomials with degree falls*. For an inhomogeneous polynomial system $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_m]$, we say that a polynomial $f \in (\mathcal{F})$ has a degree fall in $d > \deg(f)$, if it cannot be constructed below degree d via $\mathcal{F}$, i.e. there does not exist a sum $f = \sum_{i=1}^{m} g_i \cdot f_i$ such that $\deg(g_i \cdot f_i) < d$ for all i. We define the *last fall degree* as the largest integer d for which there exists a polynomial $f \in (\mathcal{F})$ with a degree fall in d. For polynomial systems in generic coordinates we prove that the last fall degree is equal to the *satiety* of $\mathcal{F}^{\text{hom}}$ (Theorem 7.5). Moreover, it is well-known that the satiety of $\mathcal{F}^{\text{hom}}$ is always upper bounded by the Castelnuovo-Mumford regularity of $\mathcal{F}^{\text{hom}}$. Therefore, if we find a polynomial with a degree fall in

$(\mathcal{F})$ then we immediately have a lower bound for the Castelnuovo-Mumford regularity of $\mathcal{F}^{\text{hom}}$. As consequence one then has a limit on the capabilities of Castelnuovo-Mumford regularity-based complexity estimates.

We note that a different notion of last fall degree was already introduced by Huang et al. [HKY15, HKYY18]. Therefore, in Remark 7.7 we discuss the difference between Huang et al.'s and our notion of last fall degree.

Let MiMC with r rounds be defined over $\mathbb{F}_q$ and assume that the MiMC polynomial systems have fewer than three solutions in $\mathbb{F}_q$, applying our bounds we obtain the following ranges on the Castelnuovo-Mumford regularity. For MiMC and the field equation for the key variable we have, see Examples 5.1 and 8.3,

$$q + 2 \cdot r - 2 \leq \operatorname{reg}\left(\mathcal{F}^{\text{hom}}_{\texttt{MiMC}} + \left(y^q - y \cdot x_0^{q-1}\right)\right) \leq q + 2 \cdot r. \tag{3}$$

For the two plain/ciphertext attack on MiMC we have, see Examples 5.3 and 8.6,

$$4 \cdot r - 3 \leq \operatorname{reg}\left(\mathcal{F}^{\text{hom}}_{\texttt{MiMC},1} + \mathcal{F}^{\text{hom}}_{\texttt{MiMC},2}\right) \leq 4 \cdot r + 1. \tag{4}$$

For a Feistel-$2n/n$ network based on the MiMC round function we have, see Examples 5.4 and 8.8,

$$2 \cdot r - 1 \leq \operatorname{reg}\left(\mathcal{F}^{\text{hom}}_{\texttt{MiMC-}2n/n}\right) \leq 2 \cdot r + 1. \tag{5}$$

For a Feistel-$2n/n$ network operated in sponge mode [BDPV08] based on the MiMC round function we have for the preimage attack, see Examples 5.5 and 8.10,

$$q + 2 \cdot r - 6 \leq \operatorname{reg}\left(\mathcal{F}^{\text{hom}}_{\text{preimage}} + \left(x_2^q - x_2 \cdot x_0^{q-1}\right)\right) \leq q + 2 \cdot r - 2. \tag{6}$$

Arguably, the bounds that include the size of the finite field q do not have direct cryptographic significance. We note that these bounds can be significantly improved by an auxiliary division by remainder computation, see the discussions after Examples 5.1, 5.5, 8.3 and 8.10. We restricted our analysis to the field equation due to generic treatment as well as simple algebraic representations. Moreover, we point out that our analysis of MiMC polynomial system serves as role model to showcase that tight complexity estimates for cryptographic polynomial systems are achievable without the evasion to unproven hypotheses.

1.1.1 Comparison With Existing Cryptanalysis

In this paper we derive various proven Gröbner basis complexity estimates for the MiMC family, GMiMC and Hades. Let us now shortly discuss how these estimates relate to established cryptanalysis of these designs. In Table 1 we collect our complexity estimates, see Tables 2 to 5 and 7, next to the estimates of established attacks that are closely related to our Gröbner basis attacks.

The attack on MiMC with a field equation (first three rows in the MiMC row in Table 1) can be considered as sparse low degree representation of the greatest common divisor (GCD) attack on MiMC [AGR+16, §4.2]. In the GCD attack with a known plain/ciphertext attack one represents the MiMC encryption function as univariate polynomial in the key variable y and then computes the GCD with the field equation $y^q - y$. The number of MiMC rounds is chosen so that $r \geq \log_3(q)$, where q is the size of the underlying finite field, to avoid an interpolation attack [LP19]. So the complexity of the GCD computation can be estimated as $\mathcal{O}\Big(d \cdot \log(d)^2 \cdot \log\big(\log(d)\big)\Big)$ with $d = 3^r$ (or $d = q$ if one considers the first division by remainder computation in the GCD algorithm to be for free). If we do not consider the construction of the univariate polynomial to be for free, we can refine this

estimate. The keyed iterated MiMC polynomial system is already a Gröbner basis, so the univariate polynomial can be constructed via the probabilistic FGLM algorithm [FGHR14] which has complexity $\mathcal{O}(n \cdot d^{\omega})$, and for key extraction we can use the efficient factoring algorithm of Bariant et al. whose complexity is given in Equation (2). In the Gröbner basis attack on the other hand, the univariate MiMC encryption function is decomposed into its r round functions of degree 3 and together with the field equation the Gröbner basis is computed. As Table 1 shows, MiMC achieves a security level of at least 128 bits for various field sizes when the sparse low degree representation is used to mount a key recovery attack with the field equation.

Alternatively to the GCD with the field equation, one can consider two plain/ciphertexts to set up two univariate encryption polynomials and compute their GCD. As before, we can represent the encryption functions with r sparse polynomials of degree 3 respectively which share the key variable. A similar two plain/ciphertext attack was investigated by Albrecht et al. [ACG+19, §6.1]. Since an iterated MiMC polynomial system is already Gröbner basis, they proposed to run the FGLM algorithm twice to construct two univariate polynomials in the key variable and then compute their GCD. This approach is obviously equivalent to the standard two plain/ciphertext GCD attack on MiMC, only difference is that Albrecht et al. did not consider the univariate polynomial construction to be for free. Note that Albrecht et al.'s estimate can be refined by again utilizing the probabilistic FGLM algorithm as well as Bariant et al.'s factoring technique.[1] On the other hand, we will discuss in Example 5.3 that the joint polynomial system removes almost all superfluous solutions coming from the algebraic closure of $\mathbb{F}_q$. Hence, the complexity of running FGLM on the joint system can be neglected after a Gröbner basis has been found. As Table 1 shows, MiMC achieves a security level of at least 128 bits for the two plain/ciphertexts Gröbner basis computation already for 50 rounds.

For MiMC-$2n/n$ one utilizes a two branch Feistel network to encrypt two field elements with one field element. As consequence, one can represent the left and the right branch as univariate polynomials in the key variable of degrees 3^r and 3^{r-1} respectively. So we can again utilize the GCD to recover the key. In Proposition 4.7 we find a DRL Gröbner basis for MiMC-$2n/n$ when the output of the right branch is ignored. Moreover, the univariate polynomials that represent the left and the right branch are again present in the LEX Gröbner basis. So once again, we can refine the complexity of this attack via the probabilistic FGLM algorithm and Bariant et al.'s factoring algorithm.[1] On the other hand, similar to the two plain/ciphertext attack on MiMC the Gröbner basis computation on MiMC-$2n/n$ removes almost all superfluous solutions coming from the algebraic closure of $\mathbb{F}_q$, see Example 5.4. So the complexity of term order conversion via FGLM can again be ignored. As Table 1 shows, MiMC-$2n/n$ achieves a security level of at least 128 bits against Gröbner basis computations already for 50 rounds.

For Feistel-MiMC-Hash one utilizes the MiMC-$2n/n$ permutation in sponge mode, though for the hash function we have only one generic choice for the second polynomial to mount a GCD attack: the field equation. Again, the complexity estimate of the GCD attack can be refined via the probabilistic FGLM algorithm and Bariant et al.'s factoring method. As Table 1 shows, Feistel-MiMC-Hash also achieves a security level of at least 128 bits for various field sizes with respect to the Gröbner basis computations with the field equation.

Hades is a family of Substitution-Permutation Network (SPN) ciphers targeted for MPC applications. In the Hades proposal the designers analyze the keyed iterated polynomial system for the resistance against Gröbner basis attacks [GLR+19, §E.3].[2] We revisit this modeling, in particular we prove in Theorem 6.2 that for a single plain/ciphertext pair one can produce a Hades DRL Gröbner basis via affine transformations. Moreover,

[1] In Table 1 we still use the standard GCD complexity estimate, since the MiMC two plain/ciphertext and the MiMC-$2n/n$ Gröbner basis attacks do not depend on the underlying field while Bariant et al.'s method does.

[2] The keyed iterated polynomial model is called *second strategy* in the Hades proposal.

any DRL Gröbner basis immediately implies being in generic coordinates (Corollary 3.3), so after the affine transformations we have proven complexity estimates for *any* Gröbner basis computation on HADES. The HADES designers on the other hand had to assume that the polynomial systems are generic in the sense of Fröberg's conjecture [Frö85, Par10] to derive complexity estimates. Moreover, with the property of being in generic coordinates we can reproduce the complexity estimate of the designers as minimal baseline for all DRL Gröbner basis computations on the iterated polynomial model of HADES. Therefore, our Gröbner basis complexity estimates coincide with the cryptanalysis of the HADES designers. In [GLR+20, Table 1] round numbers for HADES proposed, the HADES parameters in Table 1 are chosen so that every instance in [GLR+20, Table 1] exceeds at least one instance in Table 1. As Table 1 shows, all proposed HADES instances achieve at least 128 bits of security with respect to Gröbner basis computations.

Finally, to the best of our knowledge the keyed iterated polynomial system has not been considered for `GMiMC` in the literature before. The `GMiMC` designers only considered models where the encryption function is represented in n key variables for known plain/ciphertext pairs. Moreover, they assumed that `GMiMC` polynomial systems behave like generic polynomial systems in the sense of Fröberg's conjecture [Frö85, Par10] to derive complexity estimates. For `GMiMC` with contracting round function (crf) they derived the estimate $\binom{n+3^{r-2\cdot n+2}}{3^{r-2\cdot n+2}}^{\omega}$ [AGP+19a, §4.1.2], and for `GMiMC` with expanding round function (erf) they derived the estimate $\binom{n+3^{r-n}}{3^{r-n}}^{\omega}$ [AGP+19b, §C.3] for Gröbner basis computations. On the other hand, in Example 6.6 we will see that $\texttt{GMiMC}_{\text{crf}}$ and $\texttt{GMiMC}_{\text{erf}}$ share the same complexity estimate for the keyed iterated polynomial system, provided that they are in generic coordinates. In particular, the complexity estimate does not depend on the number of branches n. Moreover, being in generic coordinates for `GMiMC` can be verified by computing the rank of a linear equation system, see Theorem 6.5. As Table 1 shows, 50 rounds are sufficient to achieve at least 128 bits of security for `GMiMC`.

Table 1: Comparison of Gröbner basis complexity estimates for `MiMC`, `MiMC`-$2n/n$, Feistel-`MiMC`-Hash, HADES and `GMiMC` with established cryptanalysis. With r we denote the number of rounds of a primitive, with n the number of blocks, with d the degree of a power permutation and with m the number of samples for an attack. The total number of HADES rounds is given by $r = 2 \cdot r_f + r_p$. For all complexities the linear algebra constant $\omega = 2$ has been used.

			Established Cryptanalysis	
Primitive	Parameters	Gröbner Basis Complexity (bits)	Complexity (bits)	Attack Strategy
`MiMC`	$\log_2(q) = 64$, $r = 50$	337.5	164.1	Probabilistic FGLM + Efficient factoring
	$\log_2(q) = 128$, $r = 81$	527.4	263.1	Probabilistic FGLM + Efficient factoring
	$\log_2(q) = 256$, $r = 162$	1156.2	520.9	Probabilistic FGLM + Efficient factoring
	$r = 10$, $m = 2$	99.4	36.0	Probabilistic FGLM + GCD
	$r = 50$, $m = 2$	538.1	165.1	Probabilistic FGLM + GCD
`MiMC`-$2n/n$	$r = 10$	48.6	35.0	Probabilistic FGLM + GCD
	$r = 50$	266.7	164.1	Probabilistic FGLM + GCD
Feistel-`MiMC`-Hash	$\log_2(q) = 64$, $r = 51$	337.5	167.3	Probabilistic FGLM + Efficient factoring
	$\log_2(q) = 128$, $r = 82$	527.4	266.2	Probabilistic FGLM + Efficient factoring
	$\log_2(q) = 256$, $r = 163$	1156.2	524.0	Probabilistic FGLM + Efficient factoring
HADES	$r_f = 3$, $r_p = 13$, $n = 2$, $d = 3$	130.0	130.0	Gröbner basis computation
	$r_f = 4$, $r_p = 10$, $n = 2$, $d = 3$	135.4	135.4	Gröbner basis computation
	$r_f = 5$, $r_p = 5$, $n = 2$, $d = 3$	130.0	130.0	Gröbner basis computation
	$r_f = 3$, $r_p = 10$, $n = 2$, $d = 5$	149.0	149.0	Gröbner basis computation
	$r_f = 4$, $r_p = 10$, $n = 2$, $d = 5$	177.5	177.5	Gröbner basis computation
	$r_f = 5$, $r_p = 4$, $n = 2$, $d = 5$	163.3	163.3	Gröbner basis computation
`GMiMC`	$r = 10$, $n = 3$, $d = 3$	48.6	crf: 51.9, erf: 61.4	Gröbner basis computation
	$r = 25$, $n = 3$, $d = 3$	130.0	crf: 194.5, erf: 204.0	Gröbner basis computation
	$r = 50$, $n = 3$, $d = 3$	266.7	crf: 432.3, erf: 441.8	Gröbner basis computation
	$r = 10$, $n = 3$, $d = 5$	63.5	crf: 78.4, erf: 92.4	Gröbner basis computation
	$r = 25$, $n = 3$, $d = 5$	170.5	crf: 287.4, erf: 301.3	Gröbner basis computation
	$r = 50$, $n = 3$, $d = 5$	350.0	crf: 635.7, erf: 649.6	Gröbner basis computation

1.1.2 Organization of the Paper

In Section 2 we will formally introduce univariate keyed iterated polynomial systems (Section 2.1), the MiMC cipher, Feistel-$2n/n$ networks, and recall required definitions and results for the solving degree (Section 2.2) and generic coordinates (Section 2.3). In Section 3 we prove that being in generic coordinates is equivalent for the ideal of the highest degree components to be zero-dimensional (Theorem 3.2). Moreover, we prove that a large class of univariate keyed iterated polynomial systems, including MiMC polynomial systems, is already in generic coordinates (Theorem 3.7). As preparation for our bounds on the solving degree we study in Section 4 properties of the lexicographic Gröbner basis of the univariate keyed iterated polynomial system and Feistel-$2n/n$. In Section 5 we finally provide upper bounds for the solving degree of various attacks on MiMC and MiMC-$2n/n$. In Section 6 we extend our framework to multivariate ciphers, in particular we investigate when the keyed iterated polynomial systems for Substitution-Permutation and generalized Feistel Networks are in generic coordinates. With our formalism we can then demonstrate that the security analysis of HADES and GMiMC against Gröbner basis attacks is indeed mathematically sound. In Figure 1 we provide a directed graph to illustrate the derivation of the main results of the first part of the paper.

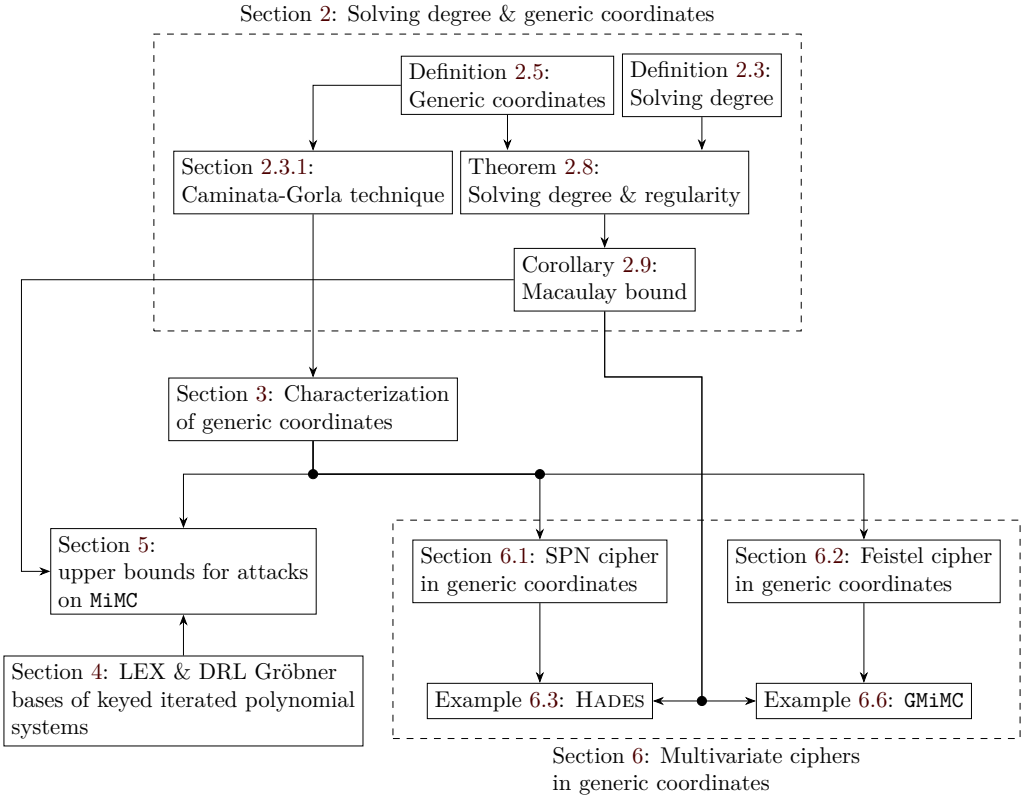

Figure 1: Graphical overview for the development of solving degree upper bounds.

In Section 7 we investigate polynomials with degree falls and the last fall degree. In particular, we establish that for a polynomial system in generic coordinates the last fall degree is equal to the satiety (Theorem 7.5). In Section 8 we construct polynomials with degree falls for the keyed iterated polynomial systems for univariate ciphers and Feistel-$2n/n$. Finally, this yields regularity lower bounds for various attacks on MiMC, Feistel-MiMC and Feistel-MiMC-Hash. In Figure 2 we provide a directed graph to illustrate

the derivation of the main results of the second part of the paper.

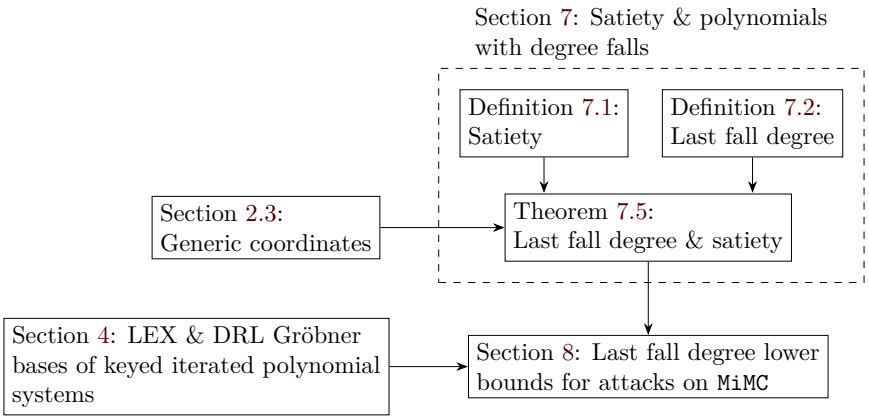

Figure 2: Graphical overview for the development of satiety lower bounds.

Finally, we finish with a short discussion in Section 9.

2 Preliminaries

By K we will always denote a field, by $\bar{K}$ its algebraic closure, and we abbreviate the polynomial ring $P = K[x_1, \ldots, x_n]$ if the base field and the number of variables are clear from context. If $I \subset K[x_1, \ldots, x_n]$ is an ideal, then we denote the zero locus of I over $\bar{K}$ as

$$\mathcal{Z}(I) = \left\{\mathbf{p} \in \bar{K}^n \mid f(\mathbf{p}) = 0,\ \forall f \in I\right\} \subset \mathbb{A}^n_{\bar{K}}. \tag{7}$$

If moreover I is homogeneous, then we denote the projective zero locus over $\bar{K}$ by $\mathcal{Z}_+(I) \subset \mathbb{P}^{n-1}_{\bar{K}}$.

Let $f \in K[x_1, \ldots, x_n]$ be a polynomial, and let x_0 be an additional variable, we call

$$f^{\text{hom}}(x_0, \ldots, x_n) = x_0^{\deg(f)} \cdot f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in K[x_0, \ldots, x_n] \tag{8}$$

the homogenization of f with respect to x_0, and analog for the homogenization of ideals $I^{\text{hom}} = \left\{f^{\text{hom}} \mid f \in I\right\}$ and finite systems of polynomials $\mathcal{F}^{\text{hom}} = \left\{f_1^{\text{hom}}, \ldots, f_m^{\text{hom}}\right\}$. Let $F \in K[x_0, \ldots, x_n]$ be a homogeneous polynomial, we call

$$F^{\text{deh}}(x_1, \ldots, x_n) = F(1, x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \tag{9}$$

the dehomogenization of F with respect to x_0, and analog for the dehomogenization of homogeneous ideals $I^{\text{deh}} = \left\{f^{\text{deh}} \mid f \in I\right\}$. Further, we will always assume that we can extend a term order on $K[x_1, \ldots, x_n]$ to a term order on $K[x_0, \ldots, x_n]$ according to [CG21, Definition 8].

For a homogeneous ideal $I \subset P$ and an integer $d \geq 0$ we denote

$$I_d = \{f \in I \mid \deg(f) = d,\ f \text{ homogeneous}\}, \tag{10}$$

and for inhomogeneous ideals $I \subset P$ we denote

$$I_{\leq d} = \{f \in I \mid \deg(f) \leq d\}. \tag{11}$$

For a term order $>$ and an ideal $I \subset P$ we denote with

$$\text{in}_>(I) = \{\text{LT}_>(f) \mid f \in I\} \tag{12}$$

the initial ideal of I, i.e. the ideal of leading terms of I, with respect to $>$.

Every polynomial $f \in [x_1, \ldots, x_n]$ can be written as $f = f_d + f_{d-1} + \ldots + f_0$, where f_i is homogeneous of degree i. We denote the highest degree component f_d of f with f^{top}, and analog we denote $\mathcal{F}^{\text{top}} = \left\{ f_1^{\text{top}}, \ldots, f_m^{\text{top}} \right\}$.

Let $I, J \subset K[x_1, \ldots, x_n]$ be ideals, then we denote with

$$I : J = \{ f \in K[x_1, \ldots, x_n] \mid \forall g \in J \colon f \cdot g \in I \} \tag{13}$$

the usual ideal quotient, and with

$$I : J^{\infty} = \bigcup_{i \geq 1} I : J^i \tag{14}$$

the saturation of I with respect to J.

Let $I, \mathfrak{m} \in K[x_0, \ldots, x_n]$ be homogeneous ideals where $\mathfrak{m} = (x_0, \ldots, x_n)$, then we call $I^{\text{sat}} = I : \mathfrak{m}^{\infty}$ the saturation of I.

Let $>$ be a term order on P, we recall the definition of Buchberger's S-polynomial of $f, g \in P$ with respect to $>$ (cf. [CLO15, Chapter 2 §6 Definition 4]). Denote with $x^{\gamma} = \operatorname{lcm}\big(\operatorname{LT}_{>}(f), \operatorname{LT}_{>}(g)\big)$, then the S-polynomial is defined as

$$S_{>}(f, g) = \frac{x^{\gamma}}{\operatorname{LT}_{>}(f)} \cdot f - \frac{x^{\gamma}}{\operatorname{LT}_{>}(g)} \cdot g. \tag{15}$$

We will often encounter the lexicographic and the degree reverse lexicographic term order which we will abbreviate as LEX and DRL respectively.

2.1 Keyed Iterated Polynomial Systems

A natural description of a univariate keyed function over a finite field is to write the function as composition of low degree polynomials. This idea leads us to the general notion of keyed iterated polynomial systems.

Definition 2.1 (Univariate keyed iterated polynomial system)**.** *Let K be a field, let $g_1, \ldots, g_n \in K[x, y]$ be non-constant polynomials, and let $p, c \in K$ be field elements which will commonly be called plain/ciphertext pair. We say that $f_1, \ldots, f_n \in K[x_1, \ldots, x_{n-1}, y]$ is a univariate keyed iterated polynomial system, if the polynomials are of the form*

$$\begin{aligned} f_1 &= g_1(p, y) - x_1, \\ f_2 &= g_2(x_1, y) - x_2, \\ &\ldots \\ f_n &= g_n(x_{n-1}, y) - c. \end{aligned}$$

Moreover, we require that

$$\mathcal{Z}(f_1, \ldots, f_n) \cap K^n \neq \emptyset.$$

Before we continue we discuss why the zero locus must contain K-valued points. Let us for the moment replace p with the symbolic variable x and ignore c. Iteratively we can now substitute $f_1, \ldots, f_{n-1}$ into $g_n(x_{n-1}, y)$, then we obtain a polynomial f in the variables x and y. We can view $f : K \times K \to K$ as a keyed function, where y is the key variable. The intersection condition states that if $f(p, y) = c$, then there must exist $y \in K$ that satisfies the equation. I.e., all computations involving a Gröbner basis for $f_1, \ldots, f_n$ are non-trivial, that is $1 \notin (f_1, \ldots, f_n)$.

2.1.1 MiMC

Our main example of a univariate keyed iterated polynomial system is MiMC, an AO cipher proposed in [AGR+16, §2.1]. It is based on the cubing map $x \mapsto x^3$ over finite fields. If $\mathbb{F}_q$ is a field with q elements, then cubing induces a permutation if $\gcd(3, q-1) = 1$, see [LN97, 7.8. Theorem]. Let $k \in \mathbb{F}_q$ denote the key, let $r \in \mathbb{N}$ be the number of rounds, and let $c_1, \ldots, c_r \in \mathbb{F}_q$ be round constants. Then the round function of MiMC is defined as

$$F_{i,k}(x) = \begin{cases} (x + k + c_i)^3, & 1 \leq i \leq r-1, \\ (x + k + c_r)^3 + k, & i = r. \end{cases} \tag{16}$$

The MiMC cipher function is now defined as

$$F(x, k) = F_{r,k} \circ \cdots \circ F_{1,k}(x), \tag{17}$$

which is a permutation for every fixed key k. Given a plain/ciphertext pair $(p, c) \in \mathbb{F}_q^2$ it is straight-forward to describe the univariate keyed iterated polynomial system $I_{\texttt{MiMC}} \subset \mathbb{F}_q[x_1, \ldots, x_{r-1}, y]$ for MiMC

$$\begin{aligned} (p + y + c_1)^3 - x_1 &= 0, \\ (x_{i-1} + y + c_i)^3 - x_i &= 0, \quad 1 \leq i \leq r-1, \\ (x_{r-1} + y + c_r)^3 + y - c &= 0. \end{aligned} \tag{18}$$

It was first observed in [ACG+19] that for the DRL term order this system is already a Gröbner basis. It is now straight-forward to compute that

$$\dim_{\mathbb{F}_q}\left(\mathbb{F}_q[x_1, \ldots, x_{r-1}, y]/I_{\texttt{MiMC}}\right) = 3^r. \tag{19}$$

For all proposals of MiMC one has that at least $r \geq 60$. Hence, using this Gröbner basis we do not expect a successful key recovery with today's computational capabilities.

2.1.2 Feistel-MiMC

With the Feistel network we can construct block ciphers with cubing as round function. Note that a Feistel network induces a permutation irrespective of the size or characteristic of the finite field $\mathbb{F}_q$. A very special case is the Feistel-$2n/n$ network which encrypts two message blocks of size n with a key of size n. As previously, let $\mathbb{F}_q$ be a finite field, let r be the number of rounds, let $k \in \mathbb{F}_q$ denote the key, and let $c_1, \ldots, c_r \in \mathbb{F}_q$ be round constants. Then the MiMC-$2n/n$ [AGR+16, §2.1] round function is defined as

$$F_{i,k}\begin{pmatrix} x_L \\ x_R \end{pmatrix} = \begin{cases} \begin{pmatrix} x_R + (x_L + k + c_i)^3 \\ x_L \end{pmatrix}, & 1 \leq i \leq r-1, \\ \begin{pmatrix} x_R + (x_L + k + c_r)^3 + k \\ x_L \end{pmatrix}, & i = r. \end{cases} \tag{20}$$

Again the cipher is defined as iteration of the round functions with respect to the plaintext variables

$$F_k(x_L, x_R) = F_{r,k} \circ \cdots \circ F_{0,k}(x_L, x_R). \tag{21}$$

Analog to MiMC we can model Feistel-MiMC with a "multivariate" system of keyed iterated polynomials.

Definition 2.2 (Keyed iterated polynomial system for Feistel-$2n/n$)**.** *Let K be a field, let $g_1, \ldots, g_n \in K[x, y]$ be non-constant polynomials, and let $(p_L, p_R), (c_L, c_R) \in K^2$ be field elements which will commonly be called plain/ciphertext pair. We say that*

$f_{L,1}, f_{R,1}, \ldots, f_{L,n}, f_{R,n} \in K[x_{L,1}, x_{R,1}, \ldots, x_{L,n-1}, x_{R,n-1}, y]$ is keyed iterated polynomial system for Feistel-$2n/n$, if the polynomials are of the form

$$\begin{pmatrix} f_{L,i} \\ f_{R,i} \end{pmatrix} = \begin{cases} \begin{pmatrix} p_R + g_1(p_L, y) - x_{L,1} \\ p_L - x_{R,1} \end{pmatrix}, & i = 1, \\ \begin{pmatrix} x_{R,i-1} + g_i(x_{L,i-1}, y) - x_{L,i} \\ x_{L,i-1} - x_{R,i} \end{pmatrix}, & 2 \leq i \leq n-1 \\ \begin{pmatrix} x_{R,n-1} + g_n(x_{L,n-1}, y) - c_L \\ x_{L,n-1} - c_R \end{pmatrix}, & i = n. \end{cases}$$

Moreover, we require that

$$\mathcal{Z}\left(f_{L,1}, f_{R,1}, \ldots, f_{L,n}, f_{R,n}\right) \cap K^{2n-1} \neq \emptyset.$$

2.2 Linear Algebra-Based Gröbner Basis Algorithms & the Solving Degree

Let $I \subset P = K[x_1, \ldots, x_n]$ be an ideal, and let $>$ be a term order on P. A finite basis $\mathcal{G} = \{g_1, \ldots, g_m\}$ of I is said to be a *$>$-Gröbner basis* [Buc65] if $\mathrm{in}_>(I) = \left(\mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_m)\right)$. For any term order $>$ on P and any non-trivial ideal I a finite $>$-Gröbner basis exists. For a general introduction to Gröbner bases we refer to [CLO15].

Today two classes of Gröbner basis algorithms are known: *Buchberger's algorithm* and *linear algebra-based algorithms*. In this paper we are only concerned with the latter. These algorithms perform Gaussian elimination on the *Macaulay matrices* which under certain conditions produces a Gröbner basis. This idea can be traced back to [Laz83], examples for modern linear algebra-based algorithms are F4 [Fau99] and Matrix-F5 [Fau02].

The Macaulay matrices are defined as follows, let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P$ be a system of homogeneous polynomials and fix a term order $>$. The *homogeneous Macaulay matrix* M_d has columns indexed by monomials in P_d sorted from left to right with respect to $>$, and the rows of M_d are indexed by polynomials $s \cdot f_i$, where $s \in P$ is a monomial such that $\deg(s \cdot f_i) = d$. The entry of the row $s \cdot f_i$ at the column t is then simply the coefficient of the polynomial $s \cdot f_i$ at the monomial t. For an inhomogeneous system we replace M_d with $M_{\leq d}$ and similar the degree equality with an inequality. By performing Gaussian elimination on $M_0, \ldots, M_d$ respectively $M_{\leq d}$ for a large enough value of d one produces a $>$-Gröbner basis for $\mathcal{F}$.

Obviously, the sizes of the Macaulay matrices M_d and $M_{\leq d}$ depend on d, therefore following the idea of [DS13] we define the solving degree as follows.

Definition 2.3 (Solving degree, [CG21, Definition 6])**.** *Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ and let $>$ be a term order. The solving degree of $\mathcal{F}$ is the least degree d such that Gaussian elimination on the Macaulay matrix $M_{\leq d}$ produces a Gröbner basis of $\mathcal{F}$ with respect to $>$. We denote it by $\mathrm{sd}_>(\mathcal{F})$.*

If $\mathcal{F}$ is homogeneous, we consider the homogeneous Macaulay matrix M_d and let the solving degree of $\mathcal{F}$ be the least degree d such that Gaussian elimination on $M_0, \ldots, M_d$ produces a Gröbner basis of $\mathcal{F}$ with respect to $>$.

Algorithms like F4/5 perform Gaussian elimination on the Macaulay matrix for increasing values of d, such an algorithm needs a stopping criterion to decide whether a Gröbner basis has already been found. Algorithms like the method we described perform Gaussian elimination on a single matrix $M_{\leq d}$ for a large enough value of d. For this class of algorithms one would like to find sharp bounds on d via the solving degree to keep the Macaulay matrix as small as possible. Nevertheless, for both classes of algorithms one may choose to artificially stop a computation in the degree corresponding to the solving degree.

Due to this reason we consider the solving degree as a complexity measure of Gröbner basis computations and do not discuss termination criteria further.

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P$ be a system of polynomials, and let $\mathcal{F}^{\text{hom}}$ be its homogenization in $P[x_0]$. One has that $\left(\mathcal{F}^{\text{hom}}\right) \subseteq (\mathcal{F})^{\text{hom}}$, and it is easy to construct examples for which the inclusion is strict. Nevertheless, it was demonstrated in [CG21, Theorem 7] that for the DRL term order one still has that

$$\text{sd}_{DRL}(\mathcal{F}) \leq \text{sd}_{DRL}\left(\mathcal{F}^{\text{hom}}\right). \tag{22}$$

2.2.1 Complexity Estimates via the Solving Degree

Storjohann [Sto00, §2.2] has shown that a reduced row echelon form of a matrix $\mathbf{A} \in K^{M \times N}$, where K is a field and $r = \text{rank}(\mathbf{A})$, can be computed in $\mathcal{O}\left(M \cdot N \cdot r^{\omega-2}\right)$ field operations, where $2 \leq \omega < 2.37286$ is a linear algebra constant [AW21].

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$ be a system of homogeneous polynomials. It is well-known that the number of monomials in P of degree d is given by the binomial coefficient

$$N(n,d) = \binom{n+d-1}{d}. \tag{23}$$

So the Macaulay matrix M_d has $N(n,d)$ many columns and $N\big(n, d-\deg(f_1)\big) + \ldots + N\big(n, d-\deg(f_m)\big)$ many rows, hence we can upper bound the size of M_d by $m \cdot N(n,d) \times N(n,d)$. Overall we can estimate the complexity of Gaussian elimination on the Macaulay matrices $M_0, \ldots, M_d$ by

$$\mathcal{O}\left(m \cdot d \cdot \binom{n+d-1}{d}^{\omega}\right). \tag{24}$$

Now let $\mathcal{F} \subset P$ be an inhomogeneous polynomial system and let $\mathcal{F}^{\text{hom}} \subset P[x_0]$ be its homogenization. If $\mathcal{G}$ is a DRL Gröbner basis of $\mathcal{F}^{\text{hom}}$, then $\mathcal{G}^{\text{deh}}$ is a DRL Gröbner basis of $\mathcal{F}$, see [KR05, Proposition 4.3.18]. Therefore, we can also consider Equation (24) as complexity estimate for inhomogeneous Gröbner basis computations.

For ease of numerical computation we approximate the binomial coefficient with

$$\binom{n}{k} \approx \sqrt{\frac{n}{\pi \cdot k \cdot (n-k)}} \cdot 2^{n \cdot H_2(k/n)}, \tag{25}$$

where $H_2(p) = -p \cdot \log_2(p) - (1-p) \cdot \log_2(1-p)$ denotes the binary entropy (cf. [CJ06, Lemma 17.5.1]). Moreover, since in general $N(n,d) \gg m \cdot d$ we absorb the factor $m \cdot d$ into the implied constant. Therefore, for solving degree d and number of variables n, we estimate the bit complexity κ of a Gröbner basis attack via

$$\kappa \approx \omega \cdot \left(\frac{1}{2} \cdot \log_2\left(\frac{n+d-1}{\pi \cdot d \cdot (n-1)}\right) + (n+d-1) \cdot H_2\left(\frac{d}{n+d-1}\right)\right). \tag{26}$$

2.3 Solving Degree & Castelnuovo-Mumford Regularity

The mathematical foundation to estimate the solving degree via the Macaulay bound draws heavily from commutative and homological algebra. For readers unfamiliar with the latter subject we point out that Definition 2.5, the notion of generic coordinates, is the key mathematical technique in this paper. Although this notion dates at least back to the influential work of Bayer & Stillman [BS87], it was just recently revealed by Caminata & Gorla [CG21] that for the DRL term order the solving degree of a polynomial system in generic coordinates can always be upper bounded by the Macaulay bound. Although the theory requires heavy mathematical machinery, we will discuss in Section 2.3.1 that being in generic coordinates can be verified with rather simple arithmetic operations. For

a concise treatment and as reference point for interested readers we now introduce the mathematical details that serve as foundation of our theory.

The Castelnuovo-Mumford regularity is a well-established invariant from commutative algebra and algebraic geometry. We recap the definition from [Eis05, Chapter 4]. Let $P = K[x_0, \ldots, x_n]$ be the polynomial ring and let

$$\mathbf{F} : \cdots \to F_i \to F_{i-1} \to \cdots \tag{27}$$

be a graded complex of free P-modules, where $F_i = \sum_j P(-a_{i,j})$.

Definition 2.4. *The Castelnuovo-Mumford regularity of* $\mathbf{F}$ *is defined as*

$$\operatorname{reg}(\mathbf{F}) = \sup_i a_{i,j} - i.$$

By Hilbert's Syzygy theorem [Eis05, Theorem 1.1] any finitely graded P-module has a finite free graded resolution. I.e., for every homogeneous ideal $I \subset P$ the regularity of I is computable.

Before we can introduce the connection between Castelnuovo-Mumford regularity and solving degree we must introduce the notion of generic coordinates from [BS87]. Let $I \subset P$ be an ideal, and let $f \in P$. We use the shorthand notation "$f \nmid 0 \mod I$" for expressing that f is not a zero-divisor on P/I.

Definition 2.5 ([CG21, CG22, Definition 5])**.** *Let K be an infinite field. Let $I \subset K[x_0, \ldots, x_n]$ be a homogeneous ideal with $|\mathcal{Z}_+(I)| < \infty$. We say that I is in generic coordinates if either $|\mathcal{Z}_+(I)| = 0$ or $x_0 \nmid 0 \mod I^{\mathrm{sat}}$.*

Let K be any field, and let $K \subset L$ be an infinite field extension. I is in generic coordinates over K if $I \otimes_K L[x_0, \ldots, x_n] \subset L[x_0, \ldots, x_n]$ is in generic coordinates.

In general, computing the saturation of an ideal is a difficult problem on its own, but if a homogeneous ideal is in generic coordinates, then the saturation is exactly the homogenization of its dehomogenization.

Lemma 2.6. *Let K be an infinite field, and let $P = K[x_1, \ldots, x_n]$. Let $I \subset P[x_0]$ be a homogeneous ideal with $|\mathcal{Z}_+(I)| \neq 0$. Then I is in generic coordinates if and only if*

$$I^{\mathrm{sat}} = \left(I^{\mathrm{deh}}\right)^{\mathrm{hom}}.$$

Proof. "$\Rightarrow$": Let $F \in I^{\mathrm{sat}} = I : \mathfrak{m}^\infty$, then there exists an $N \geq 0$ such that $x_0^N \cdot F \in I$. On the other hand by [KR05, Proposition 4.3.5] we have that $\left(I^{\mathrm{deh}}\right)^{\mathrm{hom}} = I : x_0^\infty$, so also $F \in \left(I^{\mathrm{deh}}\right)^{\mathrm{hom}}$.

By our assumption $|\mathcal{Z}_+(I)| \neq 0$ and contraposition of the projective weak Nullstellensatz [CLO15, Chapter 8 §3 Theorem 8], we have that $I^{\mathrm{deh}} \neq (1)$. Now let $F \in \left(I^{\mathrm{deh}}\right)^{\mathrm{hom}}$, since $F^{\mathrm{deh}} \notin K$ then also by [KR05, Proposition 4.3.5] there must exist an $N \geq 0$ such that $x_0^N \cdot F \in I$. By definition $I \subset I^{\mathrm{sat}}$ so also $x_0^N \cdot F \in I^{\mathrm{sat}}$. By assumption $x_0 \nmid 0 \mod I^{\mathrm{sat}}$, hence we must already have that $x_0^{N-1} \cdot F \in J^{\mathrm{sat}}$. Iterating this argument we conclude that $F \in J^{\mathrm{sat}}$.

"$\Leftarrow$": We have the ideal equality $I^{\mathrm{sat}} = \left(I^{\mathrm{deh}}\right)^{\mathrm{hom}} = I : x_0^\infty$, so

$$I^{\mathrm{sat}} : x_0 = (I : x_0^\infty) : x_0 = I : x_0^\infty = I^{\mathrm{sat}}.$$

So if $x_0 \cdot f \in I^{\mathrm{sat}}$, then already $f \in I^{\mathrm{sat}}$ which implies $x_0 \nmid 0 \mod I^{\mathrm{sat}}$. □

We provide a simple counterexample to the ideal equality when the ideal is not in generic coordinates.

Example 2.7. Let K be a field and let $I = \left(x^2, y \cdot z\right) \subset K[x, y, z]$ be an ideal where we consider z as the homogenization variable. Then $I^{\text{sat}} = I$ but $I : z^\infty = (x^2, y)$.

Let us now present the connection between the solving degree and the Castelnuovo-Mumford regularity.

Theorem 2.8 ([CG21, Theorem 9, 10])**.** *Let K be an algebraically closed field, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ be an inhomogeneous polynomial system such that $\left(\mathcal{F}^{\text{hom}}\right)$ is in generic coordinates. Then*

$$\text{sd}_{DRL}\left(\mathcal{F}\right) \leq \text{reg}\left(\mathcal{F}^{\text{hom}}\right).$$

By a classical result one can always bound the regularity of an ideal via the Macaulay bound (see [Cha07, Theorem 1.12.4]).

Corollary 2.9 (Macaulay bound, [Laz83, Theorem 2], [CG21, Corollary 2])**.** *Consider a system of equations $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ with $d_i = \deg\left(f_i\right)$ and $d_1 \geq \ldots \geq d_m$. Set $l = \min\{n+1, m\}$. Assume that $\left|\mathcal{Z}_+\left(\mathcal{F}^{\text{hom}}\right)\right| < \infty$ and that $\left(F^{\text{hom}}\right)$ is in generic coordinates over $\bar{K}$. Then*

$$\text{sd}_{DRL}\left(\mathcal{F}\right) \leq \text{reg}\left(\mathcal{F}^{\text{hom}}\right) \leq d_1 + \ldots + d_l - l + 1.$$

In particular, if $m > n$ and $d = d_1$, then

$$\text{sd}_{DRL}\left(\mathcal{F}\right) \leq (n+1) \cdot (d-1) + 1.$$

A sufficient condition for a polynomial system to be in generic coordinates is that the system contains the field equations or their fake Weil descent [CG21, Theorem 11].

Via inclusion of the field equations we obtain the following solving degree bound for `MiMC`.

Example 2.10 (`MiMC` and all field equations I)**.** Let `MiMC` be defined over $\mathbb{F}_q$, and let r be the number of rounds. Denote the ideal of all field equations by F, and the `MiMC` ideal with $I_{\texttt{MiMC}}$. Then by [CG21, Theorem 11] the solving degree is bounded by

$$\text{sd}_{DRL}\left(I_{\texttt{MiMC}} + F\right) \leq r \cdot (q-1) + 3.$$

However, this bound is very unsatisfying, because it only takes the field equations into account except for one summand. On the other hand, it suffices to add only the field equation for the key variable to $I_{\texttt{MiMC}}$ to restrict all solutions to $\mathbb{F}_q^r$. However, this modification is not covered by [CG21, Theorem 11].

2.3.1 The Caminata-Gorla Technique

Since we are going to emulate the proof of [CG21, Theorem 11] several times in this paper, we recapitulate its main argument. By [BS87, Theorem 2.4] a homogeneous ideal $I \subset P = \bar{K}[x_0, \ldots, x_n]$ with $\dim\left(P/I\right) = 1$ and $\left|\mathcal{Z}_+(I)\right| < \infty$ is in generic coordinates if and only if $\text{in}_{DRL}(I)$ is in generic coordinates. Assume that

$$\mathcal{Z}_+\big(\text{in}_{DRL}(I)\big) \cap \mathcal{Z}_+\left(x_0\right) = \mathcal{Z}_+\Big(\big(\text{in}_{DRL}(I), x_0\big)\Big) = \emptyset, \tag{28}$$

then by the projective weak Nullstellensatz [CLO15, Chapter 8 §3 Theorem 8] there exists some $r \geq 1$ such that $\mathfrak{m}^r = (x_0, \ldots, x_n)^r \subset \big(\text{in}_{DRL}(I), x_0\big)$. This also implies that for every $1 \leq i \leq n$ there exists some $r_i \geq 1$ such that $x_i^{r_i} \in \text{in}_{DRL}(I)$.[3] Now suppose that $x_0 \cdot f \in \text{in}_{DRL}(I)^{\text{sat}}$, then for every $g \in \mathfrak{m}$ there exists $N \geq 1$ such that $g^N \cdot (x_0 \cdot f) \in \text{in}_{DRL}(I)$. Let g be a monomial, we do a case distinction.

[3] Let B be a basis of $\text{in}_{DRL}(I)$ and B' be basis of $\big(\text{in}_{DRL}(I), x_0\big)$. If $\mathfrak{m}^r \subset \big(\text{in}_{DRL}(I), x_0\big)$ for some $r \geq 1$, then for all $0 \leq i \leq n$ there exists a smallest integer $r_i \in \mathbb{Z}$ such that $x_i^{r_i} \in B'$. Observe that a monomial $m \in B$ is also an element of B' if $x_0 \nmid m$. Conversely, any basis element from B' different to x_0 must come from B.

- For $\gcd(g, x_0) = 1$, we increase the power of g until $x_i^{r_i} \mid g^M \cdot f$, for some $1 \leq i \leq n$ and $M \geq 1$, hence $g^M \cdot f \in \mathrm{in}_{DRL}(I)$.
- For $\gcd(g, x_0) \neq 1$, we use the factorization $g^{N+1} = \frac{g}{x_0} \cdot g^N \cdot x_0$, hence $g^{N+1} \cdot f \in \mathrm{in}_{DRL}(I)$.

Now let $g \in \mathfrak{m}$ be a polynomial, then we can find $N \geq 0$ big enough so that for every monomial present in g one of the two previous cases applies. So if $x_0 \cdot f \in \mathrm{in}_{DRL}(I)^{\mathrm{sat}}$ we also have that $f \in \mathrm{in}_{DRL}(I)^{\mathrm{sat}}$. Hence, $x_0 \nmid 0 \mod \mathrm{in}_{DRL}(I)^{\mathrm{sat}}$ and by [BS87, Theorem 2.4] also $x_0 \nmid 0 \mod I^{\mathrm{sat}}$.

Finally, in practice Equation (28) can efficiently be checked with the following ideal equality [BS87, Lemma 2.2]

$$\mathrm{in}_{DRL}(I, x_0) = \big(\mathrm{in}_{DRL}(I), x_0\big). \tag{29}$$

3 Characterization of Polynomial Systems in Generic Coordinates

Let $\mathcal{F}$ be a polynomial system which contains equations $x_i^{d_i} - p_i(x_1, \ldots, x_n)$, where $\deg(p_i) < d_i$, for all i, then the Caminata-Gorla technique implies that $\big(\mathcal{F}^{\mathrm{hom}}\big)$ is in generic coordinates, see [CG21, Remark 13]. Though, the polynomial systems of our interest are not of this form in general, e.g. the keyed iterated polynomial system for `MiMC`. However, it is already implicit in the Caminata-Gorla technique that for a homogenized polynomial system to be in generic coordinates the associated ideal of the highest degree components has to be zero-dimensional. If this is the case, then we can indeed find equations $x_i^{d_i} - p_i(x_1, \ldots, x_n)$ in $(\mathcal{F})$ that lift to $x_i^{d_i} - x_0^{d_i - \deg(p_i)} \cdot p_i(x_1, \ldots, x_n)$ in $\big(\mathcal{F}^{\mathrm{hom}}\big)$ which implies genericity.

To formally prove this observation we need a lemma.

Lemma 3.1. *Let K be a field, and let $I \subset K[x_0, \ldots, x_n]$ be a radical monomial ideal such that $(x_1, \ldots, x_n) \subset I \subset (x_0, \ldots, x_n)$. Then either $I = (x_1, \ldots, x_n)$ or $I = (x_0, \ldots, x_n)$.*

Proof. Let $P = K[x_1, \ldots, x_n]$, by the isomorphism theorems for rings we have that

$$P[x_0]/I \cong \big(P[x_0]/(x_1, \ldots, x_n)\big)/\big(I/(x_1, \ldots, x_n)\big) \cong K[x_0]/\big(I/(x_1, \ldots, x_n)\big).$$

Moreover, if $I/(x_1, \ldots, x_n) \neq (0)$, then $I/(x_1, \ldots, x_n) = (f)$, where $f \in K[x_0]$. I is radical, so f has to be reduced. Since I is also a monomial ideal this implies that $f = x_0$. □

Now we can prove the following characterization of generic coordinates.

Theorem 3.2. *Let K be an algebraically closed field, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ be a polynomial system such that*

(i) $(\mathcal{F}) \neq (1)$, *and*

(ii) $\dim(\mathcal{F}) = 0$.

Then the following are equivalent.

(1) $\big(\mathcal{F}^{\mathrm{hom}}\big)$ *is in generic coordinates.*

(2) $\sqrt{\mathcal{F}^{\mathrm{top}}} = (x_1, \ldots, x_n)$.

(3) $(\mathcal{F}^{\mathrm{top}})$ *is zero-dimensional in* $K[x_1, \ldots, x_n]$.

(4) For every $1 \leq i \leq n$ *there exists* $d_i \in \mathbb{Z}_{\geq 1}$ *such that* $x_i^{d_i} \in \mathrm{in}_{DRL}\big(\mathcal{F}^{\mathrm{hom}}\big)$.

Proof. "(1) ⇒ (4)": Let $\left(\mathcal{F}^{\mathrm{hom}}\right)$ be in generic coordinates and suppose that $\mathcal{Z}_+\left(\mathcal{F}^{\mathrm{hom}}\right) = \emptyset$. Then by the projective weak Nullstellensatz [CLO15, Chapter 8 §3 Theorem 8] $x_0^k \in \left(\mathcal{F}^{\mathrm{hom}}\right)$, where $k \geq 1$. In particular, this implies that $1 \in \left(\mathcal{F}^{\mathrm{hom}}\right)^{\mathrm{deh}} = (\mathcal{F})$, a contradiction to $(\mathcal{F}) \neq (1)$. So $\left|\mathcal{Z}_+\left(\mathcal{F}^{\mathrm{hom}}\right)\right| \neq 0$, then by Lemma 2.6 we have that

$$\left(\mathcal{F}^{\mathrm{hom}}\right)^{\mathrm{sat}} = \left(\left(\mathcal{F}^{\mathrm{hom}}\right)^{\mathrm{deh}}\right)^{\mathrm{hom}} = (\mathcal{F})^{\mathrm{hom}}.$$

By assumption $(\mathcal{F})$ is zero-dimensional, so for every $1 \leq i \leq n$ there exists $f \in (\mathcal{F})$ such that $\mathrm{LM}_{DRL}(f) = x_i^d$, where $d > 0$, see [Kem11, Theorem 5.11] and [CLO15, Chapter 5 §3 Theorem 6]. Therefore, $f^{\mathrm{hom}} \in \left(\mathcal{F}^{\mathrm{hom}}\right)^{\mathrm{sat}}$. By definition of the saturation, for every $s \in \mathfrak{m}$ there exists an integer $N \geq 0$ such that $s^N \cdot f^{\mathrm{hom}} \in \left(\mathcal{F}^{\mathrm{hom}}\right)$, thus for $s = x_i$ also $x_i^N \cdot f^{\mathrm{hom}} \in \left(\mathcal{F}^{\mathrm{hom}}\right)$. Obviously, we have that $\mathrm{LM}_{DRL}\left(x_i^N \cdot f^{\mathrm{hom}}\right) = x_i^{N+d}$.

"(4) ⇒ (3)": By assumption, for every $1 \leq i \leq n$ there exists $f \in \left(\mathcal{F}^{\mathrm{hom}}\right)$ such that $\mathrm{LM}_{DRL}(f) = x_i^{d_i}$, where $d_i > 0$. Without loss of generality we can assume that f is homogeneous, so we can represent it as

$$f = \sum_{j=1}^{m} g_i \cdot f_i^{\mathrm{hom}},$$

where $g_i \in K[x_0, \ldots, x_n]$ is homogeneous for all i. Now we split the g_i's and f_i's as

$$\begin{aligned} f_i^{\mathrm{hom}} &= f_i^{\mathrm{top}} + x_0 \cdot \tilde{f}_i, \\ g_i &= g_i^{\mathrm{top}} + x_0 \cdot \tilde{g}_i, \end{aligned}$$

where $\tilde{f}_i, \tilde{g}_i \in K[x_0, \ldots, x_n]$ are homogeneous and if $\tilde{f}_i, g_i, \tilde{g}_i \neq 0$, then

$$\begin{aligned} \deg\left(f_i^{\mathrm{hom}}\right) = \deg\left(f_i^{\mathrm{top}}\right) &= \deg\left(x_0 \cdot \tilde{f}_i\right), \\ \deg\left(g_i\right) = \deg\left(g_i^{\mathrm{top}}\right) &= \deg\left(x_0 \cdot \tilde{g}_i\right), \\ \deg\left(g_i\right) &= \deg\left(f\right) - \deg\left(f_i\right). \end{aligned}$$

We can now further decompose

$$f = \sum_{j=1}^{m} \left(g_i^{\mathrm{top}} + x_0 \cdot \tilde{g}_i\right) \cdot \left(f_i^{\mathrm{top}} + x_0 \cdot \tilde{f}_i\right) = \sum_{j=1}^{m} g_i^{\mathrm{top}} \cdot f_i^{\mathrm{top}} + x_0 \cdot \tilde{f}, \tag{30}$$

where $\deg\left(\tilde{f}\right) = \deg\left(f\right) - 1$. Since $\sum_{j=1}^{m} g_i^{\mathrm{top}} \cdot f_i^{\mathrm{top}} >_{DRL} x_0 \cdot \tilde{f}$ we must have that $\mathrm{LM}_{DRL}\left(f\right) = \mathrm{LM}_{DRL}\left(\sum_{j=1}^{m} g_i^{\mathrm{top}} \cdot f_i^{\mathrm{top}}\right)$. We can also decompose the left-hand side of the last equation $f = f^{\mathrm{top}} + x_0 \cdot \hat{f}$, and by rearranging we yield that

$$\underbrace{\left(f^{\mathrm{top}} - \sum_{j=1}^{m} g_i^{\mathrm{top}} \cdot f_i^{\mathrm{top}}\right)}_{\in K[x_1, \ldots, x_n]} = x_0 \cdot \left(\tilde{f} - \hat{f}\right).$$

The only element in $K[x_1, \ldots, x_n]$ divisible by x_0 is 0, so we have constructed an element in $(\mathcal{F}^{\mathrm{top}})$ with leading monomial $x_i^{d_i}$. Again by [Kem11, Theorem 5.11] and [CLO15, Chapter 5 §3 Theorem 6] this implies zero-dimensionality of $(\mathcal{F}^{\mathrm{top}})$.

"(3) ⇒ (4)": Suppose $(\mathcal{F}^{\mathrm{top}})$ is zero-dimensional. For the claim we can work through the arguments of the previous claim in a backwards manner. Since $(\mathcal{F}^{\mathrm{top}})$ is homogeneous

and zero-dimensional we can find $f^{\text{top}} = \sum_{j=1}^{m} g_i^{\text{top}} \cdot f_i^{\text{top}}$, where g_i^{top} homogeneous, such that $\text{LM}_{DRL}\left(f^{\text{top}}\right) = x_i^{d_i}$, where $d_i > 0$. With Equation (30) we can lift this decomposition (with $\tilde{g}_i = 0$) to $\left(\mathcal{F}^{\text{hom}}\right)$. Now let $s, t \in K[x_0, \ldots, x_n]$ be monomials such that $\deg(s) = \deg(t)$ and $x_0 \nmid s$ and $x_0 \mid t$. For compatibility with homogenization we have set x_0 as least variable with respect to DRL, this immediately implies that $s >_{DRL} t$ and the claim follows.

"(2) $\Leftrightarrow$ (3)": This is just a reformulation of the projective weak Nullstellensatz [CLO15, Chapter 8 §3 Theorem 8], [CLO15, Chapter 5 §3 Theorem 6] and [Kem11, Theorem 5.11].

"(2) $\Rightarrow$ (1)": Assume that $\sqrt{\mathcal{F}^{\text{top}}} = (x_1, \ldots, x_n)$ in $K[x_1, \ldots, x_n]$. To apply [BS87, Theorem 2.4] in the Caminata-Gorla technique (Section 2.3.1) we have to show that $\dim\left(\mathcal{F}^{\text{hom}}\right) = 1$. By the equivalence of (2) and (4) we know that

$$(x_1, \ldots, x_n) \subset \sqrt{\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right)}.$$

So by Lemma 3.1 either $\sqrt{\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right)} = (x_1, \ldots, x_n)$ or $\sqrt{\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right)} = (x_0, \ldots, x_n)$. Assume the latter, then there exists a homogeneous $f \in \left(\mathcal{F}^{\text{hom}}\right)$ such that $\text{LM}_{DRL}(f) = x_0^d$, where $d > 0$. Since x_0 is the least variable with respect to DRL this already implies that $f = x_0^d$. Thus, $1 \in \left(\mathcal{F}^{\text{hom}}\right)^{\text{deh}} = (\mathcal{F})$, a contradiction to the non-triviality of $\mathcal{F}$. So $\sqrt{\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right)} = (x_1, \ldots, x_n)$. Note that this also implies that $\mathcal{Z}_+\left(\mathcal{F}^{\text{hom}}\right) \neq \emptyset$ by a contraposition of the equivalence in the projective weak Nullstellensatz [CLO15, Chapter 8 §3 Theorem 3]. It is well-known that $\left(\mathcal{F}^{\text{hom}}\right)$ and $\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right)$ have the same affine Hilbert function, see [CLO15, Chapter 9 §3 Proposition 4]. Moreover, for any ideal $I \subset K[x_0, \ldots, x_n]$ the affine Hilbert polynomials of I and $\sqrt{I}$ have the same degree, see [CLO15, Chapter 9 §3 Proposition 6]. Since dimension of an affine ideal is equal to the degree of the affine Hilbert polynomial, see [Kem11, Theorem 11.13], the two previous observations imply that

$$\dim\left(\mathcal{F}^{\text{hom}}\right) = \dim\left(\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right)\right) = \dim\left(\sqrt{\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right)}\right) = \dim\left(x_1, \ldots, x_n\right) = 1$$

in $K[x_0, \ldots, x_n]$. Also, the dimension of an affine variety $\mathcal{Z}(I)$, where $I \subset K[x_0, \ldots, x_n]$, is defined as the degree of the affine Hilbert polynomial of I, see [CLO15, Chapter 9 §3]. If I is in addition homogeneous and $\mathcal{Z}_+(I) \neq \emptyset$, then by [CLO15, Chapter 9 §3 Theorem 12] we have for the dimension of the projective variety $\mathcal{Z}_+(I)$ that

$$\dim\left(\mathcal{Z}_+(I)\right) = \dim\left(\mathcal{Z}(I)\right) - 1 = \dim(I) - 1.$$

Combining, all our previous observations we yield that $\dim\left(\mathcal{Z}_+\left(\mathcal{F}^{\text{hom}}\right)\right) = 0$, and it is well-known that zero-dimensional projective varieties have only finitely many points, i.e. $\left|\mathcal{Z}_+\left(\mathcal{F}^{\text{hom}}\right)\right| < \infty$, see [CLO15, Chapter 9 §4 Proposition 6]. To apply the Caminata-Gorla technique (Section 2.3.1) it is left to show that $\mathcal{Z}_+\Big(\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right), x_0\Big) = \emptyset$. Note that

$$\left(\mathcal{F}^{\text{hom}}, x_0\right) = \left(\mathcal{F}^{\text{hom}}, x_0\right) = \left(\mathcal{F}^{\text{top}}, x_0\right),$$

so by [BS87, Lemma 2.2]

$$\Big(\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right), x_0\Big) = \text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}, x_0\right) = \text{in}_{DRL}\left(\mathcal{F}^{\text{top}}, x_0\right) = \Big(\text{in}_{DRL}\left(\mathcal{F}^{\text{top}}\right), x_0\Big).$$

Finally, by our initial assumption and the projective weak Nullstellensatz [CLO15, Chapter 8 §3 Theorem 3] we have

$$\mathcal{Z}_+\Big(\text{in}_{DRL}\left(\mathcal{F}^{\text{hom}}\right), x_0\Big) = \mathcal{Z}_+\Big(\text{in}_{DRL}\left(\mathcal{F}^{\text{top}}\right), x_0\Big) = \emptyset.$$

So we can apply the Caminata-Gorla technique (Section 2.3.1) to deduce that $x_0 \nmid 0 \mod \left(\mathcal{F}^{\text{hom}}\right)^{\text{sat}}$. □

As consequence, we can conclude that every zero-dimensional affine polynomial system has a set of generators that is in generic coordinates.

Corollary 3.3. *Let K be an algebraically closed field, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ be a polynomial system such that*

(i) $(\mathcal{F}) \neq (1)$, *and*

(ii) $\dim(\mathcal{F}) = 0$.

For every DRL Gröbner basis $\mathcal{G} \subset (\mathcal{F})$ the ideal $(\mathcal{G}^{\text{hom}})$ is in generic coordinates.

Another quantity that is often studied in the Gröbner basis complexity literature is the so-called degree of regularity of a polynomial system.

Definition 3.4 (Degree of regularity, [BFS04, Definition 4])**.** *Let K be a field, and let $\mathcal{F} \subset P = K[x_1, \ldots, x_n]$. Assume that $(\mathcal{F}^{\text{top}})_d = P_d$ for some integer $d \geq 0$. The degree of regularity is defined as*

$$d_{\text{reg}}(\mathcal{F}) = \min\left\{d \geq 0 \;\middle|\; \left(\mathcal{F}^{\text{top}}\right)_d = P_d\right\}.$$

It follows from the projective weak Nullstellensatz [CLO15, Chapter 8 §3 Theorem 8] and [Kem11, Theorem 5.11] that $d_{\text{reg}}(\mathcal{F}) < \infty$ is equivalent to $\dim(\mathcal{F}^{\text{top}}) = 0$.

Corollary 3.5. *Let K be an algebraically closed field, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ be a polynomial system such that*

(i) $(\mathcal{F}) \neq (1)$, *and*

(ii) $\dim(\mathcal{F}) = 0$.

Then $\left(\mathcal{F}^{\text{hom}}\right)$ is in generic coordinates if and only if $d_{\text{reg}}(\mathcal{F}) < \infty$.

Theorem 3.2 also significantly simplifies application of the Caminata-Gorla technique. For an inhomogeneous polynomial system $\mathcal{F} \subset K[x_1, \ldots, x_n]$ we can verify Theorem 3.2 (2) as follows.

(1) Homogenize $\mathcal{F}$.

(2) Extract the highest degree components via $\mathcal{F}^{\text{top}} = \mathcal{F}^{\text{hom}} \mod (x_0)$.

(3) For $x_1, \ldots, x_n$, construct a polynomial $f \in \sqrt{\mathcal{F}^{\text{top}}}$ such that $f = x_i^d$, where $d > 0$. Then replace $\mathcal{F}^{\text{top}}$ by $\mathcal{F}^{\text{top}} \mod (x_i)$.

Remark 3.6. The notion of generic coordinates is not the only genericity notion for polynomial respectively monomial ideals. Other worthwhile mentioning notions are being in quasi-stable position [HSS18, Definition 3.1] and Noether position [HSS18, Definition 4.1]. Let $\mathcal{F} \subset K[x_1, \ldots, x_n]$ be such that $\mathcal{F}^{\text{hom}}$ is in generic coordinates. Then, by the proof of Theorem 3.2 we have that $\dim\left(\mathcal{F}^{\text{hom}}\right) = 1$. It follows from Lemma 2.6 that being in generic coordinates coincides with being in quasi-stable position [HSS18, Proposition 3.2] and Noether position [BG01, Lemma 4.1] in dimension 1. For a survey of different genericity notions and their relations we refer to [HSS18].

Utilizing Theorem 3.2 we can finally provide an elementary proof that a keyed iterated polynomial system is in generic coordinates.

Theorem 3.7. *Let K be an algebraically closed field, and let $P = K[x_1, \ldots, x_{n-1}, y]$. Let $\mathcal{F} = \{f_1, \ldots, f_n\} \subset P$ be a univariate keyed iterated system of polynomials such that*

(i) $d_i = \deg(f_i) \geq 2$ *for all* $1 \leq i \leq n$, *and*

(ii) f_i *has the monomial* $x_{i-1}^{d_i}$ *for all* $2 \leq i \leq n$.

Then every non-trivial homogeneous ideal $I \subset P[x_0]$ *with* $\mathcal{Z}_+(I) \neq \emptyset$ *and* $\mathcal{F}^{\text{hom}} \subset I$ *is in generic coordinates.*

Proof. Let us substitute $x_0 = 0$ into the equations $f_i^{\text{hom}} = 0$. For f_1 we then have $y^{d_1} = 0$ and hence also $y = 0$. Substituting $x_0 = y = 0$ into f_2 then yields $x_1 = 0$, hence by iteration we obtain that $x_0 = y = x_1 = \ldots = x_{n-1} = 0$. Therefore, $\sqrt{I^{\text{top}}} = (y, x_1, \ldots, x_n)$ and the claim follows from Theorem 3.2. □

4 DRL & LEX Gröbner Bases of Keyed Iterated Polynomial Systems

In this section we investigate the DRL & LEX Gröbner basis of univariate keyed iterated polynomial systems and Feistel-$2n/n$ polynomial systems. Consequently, we will see that the solving degree of `MiMC` and all field equations can be upper bounded by `MiMC` and the field equation for the key variable, and that under a mild assumption also Feistel-$2n/n$ polynomial systems are in generic coordinates. Moreover, understanding the degrees of polynomials in the lexicographic Gröbner basis will be a key ingredient in the proofs of the Castelnuovo-Mumford regularity lower bounds.

The following lemma certainly has been proven by many students of computer algebra.

Lemma 4.1 ([CLO15, Chapter 4 §5 Exercise 13])**.** *Let* K *be a field, let* $f_1, \ldots, f_n \in K[x_1]$ *be polynomials in one variable such that* $\deg(f_1) > 0$*, and let*

$$I = \big(f_1(x_1), x_2 - f_2(x_1), \ldots, x_n - f_n(x_1)\big) \subset K[x_1, \ldots, x_n]$$

be an ideal.

(1) Every $f \in K[x_1, \ldots, x_n]$ *can be written uniquely as* $f = q + r$ *where* $q \in I$ *and* $r \in K[x_1]$ *with either* $r = 0$ *or* $\deg(r) < \deg(f_1)$.

(2) Let $f \in K[x_1]$*, then* $f \in I$ *if and only if* f *is divisible by* $f_1 \in K[x_1]$.

(3) I *is a prime ideal if and only if* $f_1 \in K[x_1]$ *is irreducible.*

(4) I *is a radical ideal if and only if* $f_1 \in K[x_1]$ *is square-free.*

(5) Let $f_{1,red} \in K[x_1]$ *be the generator of the radical ideal* $(f_{1,red}) = \sqrt{(f_1)}$*, then* $\sqrt{I} = (f_{1,red}) + I$.

If we use the LEX term order $x_2 > \ldots > x_n > x_1$, then it's easy to see that the generators of I are already a LEX Gröbner basis. Now we establish that the LEX Gröbner basis of a univariate keyed iterated polynomial system has exactly the shape of Lemma 4.1.

Lemma 4.2 (Keyed Iterated Shape Lemma I)**.** *Let* K *be a field, let* $f_1, \ldots, f_n \in K[x_1, \ldots, x_{n-1}, y]$ *be a univariate keyed iterated polynomial system together with the LEX term order* $x_1 > \ldots > x_{n-1} > y$*. Let* $\hat{f}_1, \ldots, \hat{f}_n \in K[x_1, \ldots, x_{n-1}, y]$ *be constructed via the following iteration:*

(i) For $i = 1$*, set* $\hat{f}_1 = -f_1$.

(ii) For $2 \leq i \leq n$*, let* $\hat{f}_i = \left(-f_i \mod \hat{f}_{i-1}\right)$ *where the modulo operation is computed with respect to the LEX term order.*

Then

(1) For $1 \leq i < n$, we have that $\hat{f}_i = x_i - \hat{g}_i(y)$ for some $\hat{g}_i \in K[y]$ and $\hat{f}_n \in K[y]$.

(2) $I = (f_1, \ldots, f_n) = \left(\hat{f}_1, \ldots, \hat{f}_n\right)$, in particular $\hat{f}_1, \ldots, \hat{f}_n$ is a LEX Gröbner basis of I.

(3) If $|K| = q$, then $I + (y^q - y) = \left(\hat{f}_1, \ldots, \hat{f}_{n-1}, \gcd\left(\hat{f}_n, y^q - y\right)\right)$, and this ideal is radical. In particular,

$$I + (y^q - y) = I + (x_1^q - x_1, \ldots, y^q - y)\,,$$

and

$$\mathrm{sd}_{DRL}\,(f_1, \ldots, f_n, x_1^q - x_1, \ldots, y^q - y) \leq \mathrm{sd}_{DRL}\,(f_1, \ldots, f_n, y^q - y)\,.$$

Proof. For (1), follows from the construction of the $\hat{f}_i$'s.

For (2), if we record the "quotients" which we drop in the modulo operation in the construction of the $\hat{f}_i$'s, then we can reconstruct the f_i's with the $\hat{f}_i$'s. So the $\hat{f}_i$'s are indeed an ideal basis. Moreover, they have coprime leading monomials under LEX, so by [CLO15, Chapter 2 §9 Theorem 3, Proposition 4] they are a LEX Gröbner basis of I.

For (3), let $d = \gcd\left(\hat{f}_n, y^q - y\right)$. Clearly, $\left(\hat{f}_1, \ldots, \hat{f}_{n-1}, d\right)$ is an ideal basis of $I + (y^q - y)$, and again the leading monomials are pairwise coprime under LEX, so they are a Gröbner basis of $I + (y^q - y)$. Since $y^q - y$ is square-free also d must be square-free, so by Lemma 4.1 $I + (y^q - y)$ is a radical ideal. It is obvious from the shape of the $\hat{f}_i$'s that already $\mathcal{Z}\big(I + (y^q - y)\big) \subset \mathbb{F}_q^n$. Now we can conclude from Hilbert's Nullstellensatz and [Gao09, Theorem 3.1.2] that $I + (y^q - y) = I + (x_1^q - x_1, \ldots, y^q - y)$. For the inequality observe that the Macaulay matrix of the polynomial system with one field equation is a submatrix of the Macaulay matrix of the polynomial system with all field equations. So the claim follows. □

With an additional assumption on the leading monomials of a univariate keyed iterated polynomial system we can compute the degrees in the LEX Gröbner basis.

Corollary 4.3. *Let K field, and let $f_1, \ldots, f_n \in K[x_1, \ldots, x_{n-1}, y]$ be a univariate keyed iterated polynomial system such that*

(i) $d_i = \deg(f_i) \geq 2$ for all $1 \leq i \leq n$, and

(ii) f_i has the monomial $x_{i-1}^{d_i}$ for all $2 \leq i \leq n$.

Let $\hat{f}_1, \ldots, \hat{f}_n$ be the LEX Gröbner basis of $f_1, \ldots, f_n$. Then

$$\deg\left(\hat{f}_i\right) = \prod_{k=1}^{i} d_k.$$

Proof. The assertion follows straight-forward from the monomial assumption and the LEX Gröbner basis construction procedure. □

Conversely, we can transform any lexicographic Gröbner basis with the shape of Lemma 4.1 into a univariate keyed iterated polynomial system.

Lemma 4.4 (Keyed Iterated Shape Lemma II)**.** *Let K be a field, and assume that the ideal $I \subset K[x_1, \ldots, y]$ has a LEX Gröbner basis of the form*

$$x_1 - g_1(y), \ldots, x_{n-1} - g_{n-1}(y), g_n(y)$$

such that $1 \leq \deg(g_1) \leq \ldots \leq \deg(g_n)$. Then I has an ideal basis of the form

$$\hat{g}_1(y) - x_1, \hat{g}_2(x_1, y) - x_2, \ldots, \hat{g}_{n-1}(x_{n-2}, y) - x_{n-1}, \hat{g}_n(x_{n-1}, y).$$

I.e., the ideal is generated by a univariate keyed iterated polynomial system.

Proof. For the proof we work with the DRL term order $x_1 > \ldots > x_{n-1} > y$. Let $f_1, \ldots, f_n$ denote the polynomials in the LEX Gröbner basis, and let $\hat{f}_1, \ldots, \hat{f}_n$ denote the polynomials that we claim are the univariate keyed iterated basis. We set $\hat{f}_1 = -\big(x_1 - f_1(y)\big)$. For $2 \leq i \leq n$ we now compute $\hat{f}_i = -f_i \mod \hat{f}_{i-1}$ with respect to DRL. Since we assumed that $1 \leq \deg(f_1) \leq \ldots \leq \deg(f_n)$ the modulo operation indeed constructs non-trivial polynomials $\hat{g}_i(x_{i-1}, y)$. □

Note that the keyed iterated system from Lemma 4.4 is in general not a DRL Gröbner basis. We present a simple counterexample.

Example 4.5. Let K be a field, and let

$$I = (x_1 - y^3, x_2 - y^5, y^7) \in K[x_1, x_2, y].$$

The respective keyed iterated polynomial system of I is then given by

$$y^3 - x_1,\ x_1 \cdot y^2 - x_2,\ x_2 \cdot y^2,$$

but the DRL Gröbner basis of I is given by

$$x_1 \cdot y^2 - x_2,\ x_2 \cdot y^2,\ y^3 - x_1,\ x_1^2 - x_2 \cdot y,\ x_1 \cdot x_2,\ x_2^2.$$

With Lemma 4.1 (1) and Lemma 4.2 we can transform every polynomial $f \in K[x_1, \ldots, x_n, y]$ into a univariate polynomial $\hat{f} \in K[y]$ using only ideal operations, i.e. by performing division by remainder with respect to the LEX Gröbner basis. Understanding the degree of these univariate polynomials will be our main ingredient in proving lower bounds on the regularity.

Proposition 4.6. *Let K be a field, and let $I = (f_1, \ldots, f_n) \subset P = K[x_1, \ldots, x_{n-1}, y]$ be an ideal generated by a univariate keyed iterated polynomial system such that*

(i) $d_i = \deg(f_i) \geq 2$ for all $1 \leq i \leq n$, and

(ii) f_i has the monomial $x_{i-1}^{d_i}$ for all $2 \leq i \leq n$.

Let $f \in P$ be a polynomial, then we denote with $\hat{f} \in K[y]$ the unique univariate polynomial obtained via division by remainder of f by I with respect to LEX. Then

(1) Let $a \in P \setminus \mathrm{in}_{DRL}(I)$ be a monomial, in the computation of $\hat{a}$ via division by remainder there is never a reduction modulo the univariate LEX polynomial.

(2) Let $a, b \in P \setminus \mathrm{in}_{DRL}(I)$ be monomials such that $a|b$, then $\hat{a}|\hat{b}$ and $\deg(\hat{a}) \leq \deg\left(\hat{b}\right)$.

(3) Let $a, b, c \in P \setminus \mathrm{in}_{DRL}(I)$ be monomials such that $a \cdot c, b \cdot c \in P \setminus \mathrm{in}_{DRL}(I)$. If $\deg(\hat{a}) \leq \deg\left(\hat{b}\right)$, then $\deg(\hat{a} \cdot \hat{c}) \leq \deg\left(\hat{b} \cdot \hat{c}\right)$.

Let $s_i = \prod_{j=i}^{n-1} x_i^{d_{i+1}-1}$. Then

(4) The degree of $\hat{s}_i$ is given by

$$\deg(\hat{s}_i) = \prod_{k=1}^{n} d_k - \prod_{k=1}^{i} d_k.$$

(5) Let $t \in P \setminus \mathrm{in}_{DRL}(I)$ be a monomial such that $\deg(t) \leq \deg(s_i)$. Then we also have that $\deg\left(\hat{t}\right) \leq \deg(\hat{s}_i)$, and the inequality is strict if $t \neq s$.

Proof. Let $I = \left(x_1 - \tilde{f}_1(y), \ldots, x_{n-1} - \tilde{f}_{n-1}(y), \tilde{f}_n(y)\right)$ be the LEX Gröbner basis of I, see Lemma 4.2 (1).

For (1), let $m = y^{d_1-1} \cdot \prod_{i=1}^{n-1} x_i^{d_{i+1}-1}$, then any monomial $a \in P \setminus \mathrm{in}_{DRL}(I)$ divides m. So if there is a reduction modulo $\tilde{f}_n$ in the construction of $\hat{a}$, then there also must be a reduction in the construction of $\hat{m}$. Via Corollary 4.3 let us compute

$$\begin{aligned}\deg\left(m(\tilde{f}_1, \ldots, \tilde{f}_{n-1}, y)\right) &= d_1 - 1 + \sum_{i=1}^{n-1}(d_{i+1}-1) \cdot \prod_{k=1}^{i} d_k \\ &= d_1 - 1 + \sum_{i=1}^{n-1}\left(\prod_{k=1}^{i+1} d_k - \prod_{k=1}^{i} d_k\right) \\ &= d_1 - 1 + \prod_{k=1}^{n} d_k - d_1 = \prod_{k=1}^{n} d_k - 1.\end{aligned}$$

Since $\deg\left(\tilde{f}_n\right) = \prod_{k=1}^{n} d_k$, there cannot be a reduction modulo $\tilde{f}_n$ in the construction of $\hat{m}$ anymore. So we have already computed $\deg(\hat{m})$. By contraposition the claim follows.

For (2) and (3), by (1) there is no reduction modulo $\tilde{f}_n$ in the construction of $\hat{a}$, $\hat{b}$ and $\hat{c}$, so the claims follow from standard polynomial arithmetic.

For (4), the computation is analog to the degree computation in (1)

$$\deg(\hat{s}_i) = \sum_{j=i}^{n-1}(d_{j+1}-1) \cdot \prod_{k=1}^{j} d_k = \sum_{j=i}^{n-1}\left(\prod_{k=1}^{j+1} d_k - \prod_{k=1}^{j} d_k\right) = \prod_{k=1}^{n} d_k - \prod_{k=1}^{i} d_k.$$

For (5), we do a downwards induction. Assume that there is a monomial $t \in P \setminus \mathrm{in}_{DRL}(I)$ such that $t \neq s_i$, $\deg(t) \leq \deg(s_i)$ and $\deg\left(\hat{t}\right) > \deg(\hat{s}_i)$. The monomial t must differ from s_i in at least one variable. Assume that the difference is in the variable x_{n-1}, then t must divide the monomial

$$u_{n-1} = y^{d_1-1} \cdot x_{n-1}^{d_n-2} \cdot \prod_{i=1}^{n-2} x_i^{d_{i+1}-1}.$$

Let us compute the degree of the LEX remainder degree analog to (1) and (4)

$$\begin{aligned}\deg(\hat{u}_{n-1}) &= d_1 - 1 + (d_n - 2) \cdot \prod_{k=1}^{n-1} d_k + \sum_{j=1}^{n-2}(d_{j+1}-1) \cdot \prod_{k=1}^{j} d_k \\ &= d_1 - 1 - \prod_{k=1}^{n-1} d_k + \sum_{j=1}^{n-1}(d_{j+1}-1) \cdot \prod_{k=1}^{j} d_k \\ &= \prod_{k=1}^{n} d_k - \prod_{k=1}^{n-1} d_k - 1 < \deg(\hat{s}_i).\end{aligned}$$

On the other hand, by (2) we have that $\deg\left(\hat{t}\right) \leq \deg(\hat{u}_{n-1})$. Therefore, t has to coincide with s_i on x_{n-1}, else we already have $\deg\left(\hat{t}\right) < \deg(\hat{s}_i)$. Now we replace s_i and t by $s_i/x_{n-1}^{d_n-1}$ and $t/x_{n-1}^{d_n-1}$ respectively, then we perform the same argument for x_{n-2}. Inductively we now conclude that either $t = s_i$ or $\deg\left(\hat{t}\right) < \deg(\hat{s}_i)$. □

4.1 DRL & LEX Gröbner Bases for Feistel-2n/n

Having studied the LEX Gröbner basis of univariate keyed iterated polynomial systems we now describe LEX and DRL Gröbner bases of Feistel-$2n/n$ polynomial systems, see Definition 2.2.

Proposition 4.7. *Let K be a field, and let $\mathcal{F} = \{f_{L,1}, f_{R,1}, \ldots, f_{L,n}, f_{R,n}\} \subset K[x_{L,1}, x_{R,1}, \ldots, x_{L,n-1}, x_{R,n-1}, y]$ be a keyed iterated polynomial system for Feistel-$2n/n$ such that*

(i) $d_i = \deg(f_{L,i}) \geq 2$ *for all* $1 \leq i \leq n$, *and*

(ii) f_i *has the monomial* $x_{L,i-1}^{d_i}$ *for all* $2 \leq i \leq n$.

Then

(1) For the DRL term order $x_{L,1} > x_{R,1} > \ldots > x_{L,n-1} > x_{R,n-1} > y$, a DRL Gröbner basis $\mathcal{G}$ of $\mathcal{F} \setminus \{f_{R,n}\}$ is given by

$$\begin{pmatrix} \tilde{f}_{L,i} \\ \tilde{f}_{R,i} \end{pmatrix} = \begin{cases} \begin{pmatrix} p_R + g_1(p_L, y) - x_{R,2} \\ p_L - x_{R,1} \end{pmatrix}, & i = 1, \\ \begin{pmatrix} p_L + g_2(x_{R,2}, y) - x_{R,3} \\ x_{L,1} - x_{R,2} \end{pmatrix}, & i = 2, \\ \begin{pmatrix} x_{R,i-1} + g_i(x_{R,i}, y) - x_{R,i+1} \\ x_{L,i-1} - x_{R,i} \end{pmatrix}, & 3 \leq i \leq n-2, \\ \begin{pmatrix} x_{R,n-2} + g_{n-1}(x_{R,n-1}, y) - x_{L,n-1} \\ x_{L,n-2} - x_{R,n-1} \end{pmatrix}, & i = n-1, \\ \begin{pmatrix} x_{R,n-1} + g_n(x_{L,n-1}, y) - c_R \\ 0 \end{pmatrix}, & i = n. \end{cases}$$

(2) If we remove the linear polynomials from the DRL Gröbner basis $\mathcal{G}$, then this downsized polynomial system $\mathcal{H} \subset P = K[x_{R,2}, \ldots, x_{R,n-1}, x_{L,n-1}, y]$ is already a zero-dimensional Gröbner basis. Moreover, $(\mathcal{H}^{\text{hom}}, f_{R,n}^{\text{hom}})$ is in generic coordinates over $\bar{K}$.

(3) For the LEX term order $x_{R,2} > \ldots > x_{R,n-1} > x_{L,n-1} > y$ the Gröbner basis of $(\mathcal{H})$ is of the form

$$x_{L,1} - \hat{f}_1, x_{R,2} - \hat{f}_2, \ldots, x_{R,n-1} - \hat{f}_{n-1}, \hat{f}_n$$

where the $\hat{f}_i \in K[y]$ are constructed analog to the LEX Gröbner basis in Lemma 4.2.

(4) The degree of $\hat{f}_i$ is given by

$$\deg\left(\hat{f}_i\right) = \prod_{k=1}^{i} d_k.$$

Let $f \in P$ be a polynomial, then we denote with $\hat{f} \in K[y]$ the unique univariate polynomial obtained via division by remainder of f by $(\mathcal{H})$ with respect to LEX, and for $2 \leq i \leq n-1$ let $s_i = x_{L,n-1}^{d_n - 1} \cdot \prod_{j=i}^{n-2} x_{R,i}^{d_i - 1}$ where $s_{n-1} = x_{L,n-1}^{d_n - 1}$. Then

(5) The degree of $\hat{s}_i$ is given by

$$\deg(\hat{s}_i) = \prod_{k=1}^{n} d_k - \prod_{k=1}^{i} d_k.$$

(6) Let $t \in P \setminus \text{in}_{DRL}(I)$ be a monomial such that $\deg(t) \leq \deg(s_i)$. Then we also have that $\deg(\hat{t}) \leq \deg(\hat{s}_i)$, and the inequality is strict if $t \neq s$.

Proof. For (1), the polynomials $\tilde{f}_{L,i}$ are constructed by substituting the linear polynomials of $\mathcal{F} \setminus \{f_{R,n}\}$ into the non-linear ones. After the substitution all leading monomials are coprime so by [CLO15, Chapter 2 §9 Theorem 3, Proposition 4] we have constructed a Gröbner basis.

For (2), it is easy to see that $\mathcal{H} = \{\tilde{f}_{L,1}, \ldots, \tilde{f}_{L,n}\} \subset P = K[x_{R,2}, \ldots, x_{R,n-1}, x_{L,n-1}, y]$ and that $\mathrm{in}_{DRL}(\mathcal{H}) = \left(y^{d_1}, x_{R,2}^{d_2}, \ldots, x_{R,n-1}^{d_{n-1}}, x_{L,n-1}^{d_n}\right)$. Observe that only a finite number of monomials of P is not contained in $\mathrm{in}_{DRL}(\mathcal{H})$. I.e., $\dim_K \left(P/\,\mathrm{in}_{DRL}(\mathcal{H})\right) < \infty$ as K-vector space and by a well-known equivalence from commutative algebra (see [Kem11, Theorem 5.11]) this implies zero-dimensionality. Lastly, being in generic coordinates is proven analog to Theorem 3.7.

For (3), given the DRL Gröbner basis from (1) and (2) the LEX Gröbner basis can be constructed via iterated substitutions.

For (4), this follows analog to Corollary 4.3.

For (5) and (6), the proofs are identical to Proposition 4.6 (4) and (5). □

We provide a counterexample that in general the generators of the DRL Gröbner basis of Feistel-$2n/n$ cannot be transformed into a univariate keyed iterated polynomial system.

Example 4.8. Consider MiMC-$2n/n$ over $\mathbb{F}_{13}$ with the round constants and plain/ciphertext pair

$$c_1 = 0, \quad c_2 = 0, \quad c_3 = 0, \quad c_4 = 0, \quad \begin{pmatrix} p_L \\ p_R \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} c_L \\ c_R \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

The downsized DRL Gröbner basis is

$$\begin{aligned}
&y^3 - x_{R,2},\\
&x_{R,2}^3 - 2 \cdot x_{R,2}^2 \cdot y - 2 \cdot x_{R,2} \cdot y^2 + y^3 - x_{R,3},\\
&x_{R,3}^3 - 2 \cdot x_{R,3}^2 \cdot y - 2 \cdot x_{R,3} \cdot y^2 + 2 \cdot y^3 - x_{L,3},\\
&x_{L,3}^3 - 2 \cdot x_{L,3}^2 \cdot y - 2 \cdot x_{L,3} \cdot y^2 + y^3 + y + x_{R,3}.
\end{aligned}$$

But the univariate keyed iterated generators of this system are

$$\begin{aligned}
&y^3 - x_{R,2},\\
&x_{R,2}^3 - 2 \cdot x_{R,2}^2 \cdot y - 2 \cdot x_{R,2} \cdot y^2 + x_{R,2} - x_{R,3},\\
&x_{R,3}^3 - 2 \cdot x_{R,3}^2 \cdot y - 2 \cdot x_{R,3} \cdot y^2 + 2 \cdot y^3 - x_{L,3},\\
&y^9 - 2 \cdot y^7 - 2 \cdot y^5 + x_{L,3}^3 - 2 \cdot x_{L,3}^2 \cdot y - 2 \cdot x_{L,3} \cdot y^2 + 2 \cdot y^3 + y.
\end{aligned}$$

4.2 DRL & LEX Gröbner Bases for Univariate Keyed Iterated Polynomial Systems With Two Plain/ciphertexts

If one has multiple plain/ciphertext samples for a cipher, then one can combine the respective iterated polynomial systems into a joint system and compute its Gröbner basis. Analog to Lemma 4.2 and Proposition 4.6 we now describe DRL Gröbner bases for a two plain/ciphertext attack on a univariate cipher. With the same assumptions as in Theorem 3.7 we can also prove that the polynomial system of a two plain/ciphertext attack is in generic coordinates.

Proposition 4.9. *Let K be a field, and let*

$$\begin{aligned}
f_1, \ldots, f_n &\in K[u_1, \ldots, u_{n-1}, y], \text{ and}\\
h_1, \ldots, h_n &\in K[v_1, \ldots, v_{n-1}, y]
\end{aligned}$$

be two univariate keyed iterated polynomial systems which are constructed with the same $g_1, \ldots, g_n \in K[x, y]$ but with different plain/ciphertext pairs $(p_1, c_1), (p_2, c_2) \in K^2$. Let $\mathcal{F} = \{f_1, \ldots, f_n, h_1, \ldots, h_n\}$, and assume that

(i) $d_i = \deg(g_i) \geq 2$ for all $1 \leq i \leq n$, and

(ii) g_i *has the monomial* x^{d_i} *for all* $2 \leq i \leq n$.

Then

(1) The sets

$$\{f_1, \ldots, f_n\}, \quad \{h_1, \ldots, h_n\}, \quad \mathcal{F} \setminus \{h_1\}, \quad \mathcal{F} \setminus \{f_1\},$$

are DRL Gröbner bases.

(2) If in addition K *is algebraically closed, then* $\left(\mathcal{F}^{\text{hom}}\right)$ *is in generic coordinates.*

Proof. (1) follows from [CLO15, Chapter 2 §9 Theorem 3, Proposition 4], and the proof of (2) is analog to Theorem 3.7. □

Note that it is also straight-forward to generalize (2) for any number of plain/ciphertext pairs.

5 Solving Degree Upper Bounds For Attacks On MiMC

Combining our results from Sections 3 and 4 we can now derive upper bounds for the solving degree of various attacks on MiMC, Feistel-MiMC and Feistel-MiMC-Hash. To illustrate our bounds in practice we also compute the bit complexity of Equation (24) for sample values.

5.1 Adding a Minimal Number of Field Equations

In the original bound for MiMC, see Example 2.10, we had to include all field equations into the system, but as we saw in Lemma 4.2 it suffices to include a single field equation to limit all solutions to the base field.

Example 5.1 (MiMC and one field equation I)**.** Let MiMC be defined over $\mathbb{F}_q$, and let r be the number of rounds. We denote with $I_{\texttt{MiMC}}$ the MiMC ideal. It follows from Lemma 4.2 (3) that one only needs to include the field equation for the key variable y to limit all solutions to $\mathbb{F}_q$. Hence, by applying Corollary 2.9 and Theorem 3.7 to this system we yield

$$\text{sd}_{DRL}\left(I_{\texttt{MiMC}} + (y^q - y)\right) \leq q + 2 \cdot r.$$

As an immediate consequence we can also improve the bound of the attack with all field equations.

Example 5.2 (MiMC and all field equations II)**.** Let MiMC be defined over $\mathbb{F}_q$, and let r be the number of rounds. Denote the ideal of all field equations by F and the MiMC ideal with $I_{\texttt{MiMC}}$. Then by Lemma 4.2 (3) and Example 5.1 the solving degree is bounded by

$$\text{sd}_{DRL}(I_{\texttt{MiMC}} + F) \leq q + 2 \cdot r.$$

Moreover, small scale experiments indicate that the solving degree of this attack is always less than or equal to $q + r - 1$.

Since the MiMC polynomials are already a DRL Gröbner basis, we can also replace the field equation $y^q - y$ by its remainder r_y modulo $I_{\texttt{MiMC}}$ with respect to DRL. Then the solving degree bound becomes

$$\text{sd}_{DRL}\left(I_{\texttt{MiMC}} + (y^q - y)\right) \leq \deg\left(r_y\right) + 2 \cdot r. \tag{31}$$

Let $r \geq \lceil \log_3(q) \rceil$, then experimentally we observed that

$$\deg\left(r_y\right) \leq 2 \cdot \lceil \log_3(q) \rceil. \tag{32}$$

In Table 2 we provide complexity estimates in bits for a Gröbner basis computation of MiMC and the field equation for the key for an optimal adversary with $\omega = 2$. For ease of computation we estimated the logarithm of the binomial coefficient with Equation (26). For the chosen field sizes and the least round number such that $r \geq \lceil \log_3(q) \rceil$ MiMC achieves a security level of at least 128 bits against the field equation attack.

Table 2: Complexity estimation of Gröbner basis computation for MiMC and the field equation for the key variable with $\omega = 2$. κ_{rem} denotes the complexity estimate for the remainder of the field equation with the empirically observed degree bound (Equation (32)). The number of rounds r is the least integer such that $r \geq \lceil \log_3(q) \rceil$.

$\log_2(q)$	64	128	256
r	50	81	162
κ_{rem} (bits)	337.5	572.4	1156.2

5.2 The Two Plain/Ciphertext Attack

Intuitively, with a single plain/ciphertext pair one can construct a fully determined polynomial system a cipher. By adding more plain/ciphertext pairs one constructs an overdetermined system, and it is expected that the additional information reduces the difficulty of solving the system. Let $I, J \subset P$ be ideals representing a cipher for different plain/ciphertext pairs. Combining these two systems into a single system geometrically corresponds to the intersection of two varieties, i.e.,

$$\mathcal{Z}(I + J) = \mathcal{Z}(I) \cap \mathcal{Z}(J). \tag{33}$$

Let us now apply these considerations to MiMC.

Example 5.3 (MiMC and two plain/ciphertext pairs I)**.** Let MiMC be defined over $\mathbb{F}_q$, let r be the number of rounds, and let $(p_1, c_1), (p_2, c_2) \in \mathbb{F}_q^2$ be two distinct plain/ciphertext pairs generated with the same key by a MiMC encryption function. For these pairs we can construct the univariate polynomials $f_1, f_2 \in \mathbb{F}_q[y]$ in the respective LEX Gröbner basis of degree 3^r. These two polynomials must have at least one common root, namely the key $k \in \mathbb{F}_q$. If one divides f_1 and f_2 by $y - k$ and considers them as random polynomials, then with high probability they are coprime. Now let $I_{\texttt{MiMC},1} \subset \mathbb{F}_q[u_1, \ldots, u_{r-1}, y]$ and $I_{\texttt{MiMC},2} \subset \mathbb{F}_q[v_1, \ldots, v_{r-1}, y]$ denote the ideals corresponding to the plain/ciphertext pairs. Then, with high probability $\mathcal{Z}(I_{\texttt{MiMC},1} + I_{\texttt{MiMC},2})$ contains only a single point. By Corollary 2.9 and Proposition 4.9 (2) we now obtain the following bound for the solving degree of $I_{\texttt{MiMC},1} + I_{\texttt{MiMC},2}$

$$\text{sd}_{DRL}\left(I_{\texttt{MiMC},1} + I_{\texttt{MiMC},2}\right) \leq 4 \cdot r + 1.$$

In Table 3 we provide complexity estimates in bits for a Gröbner basis computation of MiMC and two plain/ciphertexts for an optimal adversary with $\omega = 2$. For ease of computation we estimated the logarithm of the binomial coefficient with Equation (26). Recall from Table 2 that for $q \geq 2^{64}$ we have that $r \geq 50$, hence 50 rounds are sufficient to achieve 128 bits security against the two plain/ciphertext attack.

Table 3: Complexity estimation of Gröbner basis computation for MiMC and two plain/ciphertext pairs with $\omega = 2$ over a finite field $\mathbb{F}_q$ with $\gcd(3, q - 1) = 1$.

r	κ (bits)
10	99.4
50	538.1

5.3 Feistel-MiMC

Interestingly, MiMC-$2n/n$ behaves very similar to the two plaintext attack on MiMC, in the sense that with high probability the standard polynomial model of MiMC-$2n/n$ does not have any solutions in the algebraic closure and its Gröbner basis is expected to be linear.

Example 5.4 (MiMC-$2n/n$ I)**.** Let $\mathbb{F}_q$ be a finite field, let r be the number of rounds, and let $k \in \mathbb{F}_q$ denote the key. Suppose we are given a plain/ciphertext pair $(p_L, p_R), (c_L, c_R) \in \mathbb{F}_q^2$ for MiMC-$2n/n$ generated by the key k. By substituting this pair into the cipher function we obtain two univariate polynomials $F_y(p_L, p_R) - (c_L, c_R) = (0, 0)$ in the key variable y. These polynomials have at least one common root, namely $y - k$. If we divide these polynomials by $y - k$ and consider them as random polynomials, then with high probability they are coprime. Now, to launch an efficient Gröbner basis attack we first compute the downsized DRL Gröbner basis of the Feistel-$2n/n$ polynomial system from Proposition 4.7 (1). Then we add the missing polynomial and compute the Gröbner basis. By Proposition 4.7 (2) the polynomial system is in generic coordinates, therefore we can also apply Corollary 2.9 to obtain the following bound for the solving degree

$$\mathrm{sd}_{DRL}\left(I_{\texttt{MiMC-}2n/n}\right) \leq 2 \cdot r + 1.$$

In the following table we provide complexity estimates in bits for a Gröbner basis computation of Feistel-MiMC for an optimal adversary with $\omega = 2$. For ease of computation we estimated the logarithm of the binomial coefficient with Equation (26). As in Tables 2 and 3, 50 rounds are sufficient for Feistel-MiMC to achieve 128 bits security.

Table 4: Complexity estimation of Gröbner basis computation for Feistel-MiMC with $\omega = 2$ over a finite field $\mathbb{F}_q$.

r	κ (bits)
10	48.6
50	266.7

5.4 Feistel-MiMC-Hash

For Feistel-MiMC-Hash the Feistel-MiMC permutation is instantiated in the sponge framework [BDPV08]. For a preimage attack on Feistel-MiMC-Hash we have to, as the name suggest, compute a preimage to a given hash value $\alpha \in \mathbb{F}_q$. We have two generic choices to do so. First, we can guess the second permutation output value and then simply invert the permutation. If the preimage is of the form $(\beta, 0)$, for some $\beta \in \mathbb{F}_q$, then the attack was successful. Though, the success probability of this approach is $1/q$, and q is at least a 64-bit prime number, which is too small for a practical attack. Second, we can use an indeterminate x_2 for the second permutation output, then we have to find a solution for the equation

$$\text{Feistel-MiMC}\begin{pmatrix} x_1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ x_2 \end{pmatrix}. \tag{34}$$

Further, for the preimage problem we have only one generic choice of polynomials to restrict all solutions to the base field: field equations.

Example 5.5 (Feistel-MiMC-Hash preimage attack I)**.** Let $\mathbb{F}_q$ be a finite field, and let r be the number of rounds. We can construct the polynomial system for Feistel-MiMC-Hash from the one for the keyed permutation, see Definition 2.2, by setting $y = 0$, $p_L = x_1$, $p_R = 0$, $c_L = \alpha$ and $c_R = x_2$, where x_1 and x_2 are indeterminates and $\alpha \in \mathbb{F}_q$ is the hash value. Moreover, we choose the DRL term order such that the intermediate state

variables are naturally ordered, $x_1 > x_2$ and all intermediate state variables are bigger than x_1. Analog to Proposition 4.7 we can compute the DRL Gröbner basis of the system by substituting the linear polynomials into the non-linear ones, but this time we do not have to remove any linear polynomial. Since $p_R = 0$ there are only $r-1$ polynomials of degree 3 in $r-1$ variables. To find a solution (if it exists) we now either have to compute the LEX Gröbner basis and factor a polynomial of degree 3^{r-1} or add the field equation for x_2 to the polynomial system. For the latter case we obtain the following bound on the solving degree

$$\mathrm{sd}_{DRL}\left(I_{\mathrm{hash}} + (x_2^q - x_2)\right) \leq q + 2 \cdot r - 2.$$

Analog to the field equation attack on `MiMC` we can also compute the remainder of the field equation modulo the DRL Gröbner basis to further reduce the solving degree. Note that the solving degrees of Examples 5.1 and 5.5 differ only by 2, therefore we refer to Table 2 for the complexity of Gröbner basis computations of Feistel-`MiMC`-Hash.

6 Multivariate Ciphers in Generic Coordinates

So far all our complexity estimates are only applicable to univariate ciphers and two branch Feistel networks. Naturally, one would like to extend the theory to more advanced multivariate constructions. Therefore, in Section 6.1 we derive that Substitution-Permutation Network (SPN) based ciphers are in generic coordinates, hence we can apply the Macaulay bound to estimate the solving degree. In Section 6.2 we study three classes of generalized Feistel Networks for which we derive efficient criteria to check whether the corresponding polynomial systems are in generic coordinates.

For starters, let us fix some notation. Let $n, r \geq 1$ be integers, n always denotes the number of blocks and r the number of rounds of a cipher. Throughout this section we will denote plaintext variables with $\mathbf{x} = (x_1, \ldots, x_n)^\intercal$ and key variables with $\mathbf{y} = (y_1, \ldots, y_n)^\intercal$. With

$$\begin{aligned} \mathcal{K}_{\mathbf{y}} : \mathbb{F}_q^n \times \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (\mathbf{x}, \mathbf{y}) &\mapsto \mathbf{x} + \mathbf{y} \end{aligned} \tag{35}$$

we denote the key addition function, and with

$$\begin{aligned} \mathcal{A} : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ \mathbf{x} &\mapsto \mathbf{A}\mathbf{x} + \mathbf{c} \end{aligned} \tag{36}$$

we denote affine permutations where $\mathbf{A} \in \mathrm{GL}_n(\mathbb{F}_q)$ and $\mathbf{c} \in \mathbb{F}_q$. For $1 \leq i \leq r$ let $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(r)} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be affine permutations and let $\mathcal{P}^{(1)}, \ldots, \mathcal{P}^{(r)} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ some arbitrary permutations. Then a block cipher without key schedule is defined to be the following composition

$$\begin{aligned} \mathcal{C}_{n,r} : \mathbb{F}_q^n \times \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (\mathbf{x}, \mathbf{y}) &\mapsto \left(\mathcal{K}_{\mathbf{y}} \circ \mathcal{A}^{(r)} \circ \mathcal{P}^{(r)}\right) \circ \cdots \circ \left(\mathcal{K}_{\mathbf{y}} \circ \mathcal{A}^{(1)} \circ \mathcal{P}^{(1)}\right)(\mathbf{x} + \mathbf{y}), \end{aligned} \tag{37}$$

where the composition is taken with respect to the plaintext variable.

For $1 \leq i \leq r-1$, let $\mathbf{x}^{(i)} = \left(x_1^{(i)}, \ldots, x_n^{(i)}\right)^\intercal$ denote intermediate state variables, and let $\mathbf{y} = (y_1, \ldots, y_n)^\intercal$ denote the key variables. Let $\mathbf{p}, \mathbf{c} \in \mathbb{F}_q^n$ be a plain/ciphertext pair given by the block cipher $\mathcal{C}_{n,r}$ Since every function $\mathbb{F}_q^n \to \mathbb{F}_q$ can be represented with polynomials, we define the multivariate keyed iterated polynomial system $\mathcal{F} =$

$\left\{\mathbf{f}^{(1)},\ldots,\mathbf{f}^{(r)}\right\} \subset \mathbb{F}_q\left[\mathbf{x}^{(1)},\ldots,\mathbf{x}^{(r-1)},\mathbf{y}\right]$ for the cipher $\mathcal{C}_{n,r}$ as

$$\mathbf{f}^{(i)} = \begin{cases} \mathbf{A}_1\mathcal{P}^{(1)}\left(\mathbf{p}+\mathbf{y}\right)+\mathbf{c}_1+\mathbf{y}-\mathbf{x}^{(1)}, & i=1, \\ \mathbf{A}_i\mathcal{P}^{(i)}\left(\mathbf{x}^{(i-1)}\right)+\mathbf{c}_i+\mathbf{y}-\mathbf{x}^{(i)}, & 2\leq i\leq r-1, \\ \mathbf{A}_r\mathcal{P}^{(r)}\left(\mathbf{x}^{(r-1)}\right)+\mathbf{c}_r+\mathbf{y}-\mathbf{c}, & i=r. \end{cases} \tag{38}$$

If a key schedule is applied we have two options for the polynomial model. Either we substitute the key schedule directly into Equation (38) or we add additional iterated key schedule equations to $\mathcal{F}$.

6.1 Substitution-Permutation Networks

In symmetric key cryptography the Substitution Permutation Network (SPN) is the most widely adopted strategy to construct block ciphers. For example, the Advanced Encryption Standard (AES) [AES01, DR20] is an SPN. Moreover, so-called partial SPNs have been adopted for AO designs [ARS+15, GLR+20, GKR+21, GKS23]. We start with the formal definition of SPN-based ciphers.

Definition 6.1 (SPN cipher)**.** *Let $\mathbb{F}_q$ be a finite field, and let $n,r\geq 1$ be integers.*

(1) Let $f_1,\ldots,f_n\in\mathbb{F}_q[x]$ be permutation polynomials. Then the full Substitution Layer is defined as

$$\begin{aligned}\mathcal{S}_{f_1,\ldots,f_n}&:\mathbb{F}_q^n\to\mathbb{F}_q^n,\\ &(x_1,\ldots,x_n)\mapsto\left(f_1(x_1),\ldots,f_n(x_n)\right).\end{aligned}$$

(2) Let $f\in\mathbb{F}_q[x]$ be permutation polynomial. Then the partial Substitution Layer is defined as

$$\begin{aligned}\mathcal{S}_f&:\mathbb{F}_q^n\to\mathbb{F}_q^n,\\ &(x_1,\ldots,x_n)\mapsto\left(f(x_1),x_2,\ldots,x_n\right).\end{aligned}$$

(3) For $1\leq n\leq r$, let $\mathcal{S}^{(i)}:\mathbb{F}_q^n\to\mathbb{F}_q^n$ be either a full or a partial Substitution Layer and let $\mathcal{A}_i:\mathbb{F}_q^n\to\mathbb{F}_q^n$ be an affine permutation. Then the SPN cipher is defined as

$$\begin{aligned}\mathcal{C}_{n,r}&:\mathbb{F}_q^n\times\mathbb{F}_q^n\to\mathbb{F}_q^n,\\ &(\mathbf{x},\mathbf{y})\mapsto\left(\mathcal{K}_{\mathbf{y}}\circ\mathcal{A}^{(r)}\circ\mathcal{S}^{(r)}\right)\circ\cdots\circ\left(\mathcal{K}_{\mathbf{y}}\circ\mathcal{A}^{(1)}\circ\mathcal{S}^{(1)}\right)(\mathbf{x}+\mathbf{y}),\end{aligned}$$

where the composition is taken with respect to the plaintext variable.

Accordingly, a round where a full/partial Substitution Layer is applied is called a full/partial round.

Under a mild assumption on the first round of an SPN cipher $\mathcal{C}_{n,r}$ we can compute a DRL Gröbner basis of the multivariate keyed iterated polynomial system.

Theorem 6.2. *Let $\mathbb{F}_q$ be a finite field, let $\overline{\mathbb{F}_q}$ be its algebraic closure, let $n,r\geq 1$ be integers, and let $\mathcal{C}_{n,r}:\mathbb{F}_q^n\times\mathbb{F}_q^n\to\mathbb{F}_q^n$ be an SPN cipher such that $\mathcal{S}^{(1)}$ is a full SPN and every univariate permutation polynomial in $\mathcal{S}^{(1)}$ has degree greater than 1. Let $\mathcal{F}=\left\{\mathbf{f}^{(1)},\ldots,\mathbf{f}^{(r)}\right\}\subset P=\overline{\mathbb{F}_q}\left[\mathbf{x}^{(1)},\ldots,\mathbf{x}^{(r-1)},\mathbf{y}\right]$ be the multivariate keyed iterated polynomial system for $\mathcal{C}_{n,r}$, and let*

$$\mathcal{G}=\left\{\mathbf{A}_1^{-1}\mathbf{f}^{(1)},\ldots,\mathbf{A}_r^{-1}\mathbf{f}^{(r)}\right\}.$$

Then

(1) $\mathcal{G}$ *is a DRL Gröbner basis.*

(2) Every homogeneous ideal $I \subset P[x_0]$ *such that* $\mathcal{Z}_+(I) \neq \emptyset$ *and* $\mathcal{G}^{\text{hom}} \subset I$ *is in generic coordinates.*

Proof. For (1), we consider the DRL term order $x_1^{(1)} > \ldots > x_n^{(1)} > x_1^{(2)} > \ldots > x_n^{(n-1)} > y_1 > \ldots > y_n$. Let $f_1^{(j)}, \ldots, f_n^{(j)}$ denote the functions of the SPN in the j^{th} round, then

$$\begin{aligned} \text{LM}_{DRL}\left(\mathbf{A}_1^{-1}\mathbf{f}^{(1)}\right) &= \left(y_i^{\deg\left(f_i^{(1)}\right)}\right)_{1\leq i\leq n}, \\ \text{LM}_{DRL}\left(\mathbf{A}_1^{-1}\mathbf{f}^{(j)}\right) &= \left(x_i^{(j)\deg\left(f_i^{(j)}\right)}\right)_{1\leq i\leq n}, \quad 2 \leq j \leq r, \end{aligned}$$

since $\deg\left(f_i^{(1)}\right) > 1$ for all i and $\mathbf{x}^{(1)} > \ldots > \mathbf{x}^{(r-1)} > \mathbf{y}$. So the polynomials in $\mathcal{G}$ have pairwise coprime leading monomials and the claim follows from [CLO15, Chapter 2 §9 Theorem 3, Proposition 4].

For (2), this follows from (1) and Corollary 3.3. □

Let us now apply Theorem 6.2 to a cipher that utilizes partial as well as full Substitution Layers: the HADES strategy [GLR+20], a cipher family for MPC applications. The keyed HADES permutation starts with r_f full rounds, then it applies r_p partial rounds, and it finishes with another application of r_f full rounds. So, in total HADES has $r = 2 \cdot r_f + r_p$ many rounds. All SPNs apply the same univariate permutation x^d for some appropriate d. HADES has an affine key schedule [GLR+20, §3.1], and it is straight-forward to incorporate an affine key schedule into the multivariate keyed iterated polynomial system from Equation (38). Moreover, an affine key schedule does not affect the proof of Theorem 6.2 as long as the master key was added before application of the first Substitution Layer.

Example 6.3 (Solving degree bounds for HADES)**.** Let $\mathbb{F}_q$ be a finite field, let $n \geq 1$ denote the number of branches, and let $d \in \mathbb{Z}_{>1}$ be an integer such that $\gcd(d, q-1) = 1$. Let $r_f, r_p \geq 1$ denote the number full and partial rounds, and let I_{HADES} denote the HADES ideal. Then by Corollary 2.9 and Theorem 6.2

$$\text{sd}_{DRL}\left(I_{\text{HADES}}\right) \leq (d-1) \cdot (2 \cdot n \cdot r_f + r_p) + 1.$$

Now let $I_{\text{HADES},1}$ and $I_{\text{HADES},2}$ denote HADES ideals for two different plain/ciphertext pairs. It is straight-forward to extend Theorem 6.2 to $I_{\text{HADES},1} + I_{\text{HADES},2}$, cf. Proposition 4.9 (2), therefore by Corollary 2.9

$$\text{sd}_{DRL}\left(I_{\text{HADES},1} + I_{\text{HADES},2}\right) \leq 2 \cdot (d-1) \cdot (2 \cdot n \cdot r_f + r_p) + 1.$$

The HADES designers use Equation (24) and the Macaulay bound (Corollary 2.9) to estimate the resistance of HADES against Gröbner basis attacks, see [GLR+20, §4.3] and [GLR+19, §E.3]. In particular, their *second strategy* is the multivariate keyed iterated polynomial system from Equation (38). To justify this approach the authors hypothesized that the HADES polynomial system is a *generic* polynomial system in the sense of Fröberg's conjecture [Frö85, Par10]. With Theorem 6.2 and Example 6.3 this hypothesis can be bypassed, and we have proven that the complexity estimation of the HADES designers is indeed mathematically sound.

In Table 2 we provide complexity estimates in bits for a Gröbner basis computation of HADES where we use the Macaulay bound of the keyed iterated HADES polynomial system as minimal baseline of the solving degree for an optimal adversary with $\omega = 2$. We assume that the key schedule equations have been substituted into Equation (38). Recall from Theorem 6.2 that a partial HADES round only contributes one non-linear equation

but $n-1$ affine equations. Therefore, we can eliminate $r_p \cdot (n-1)$ many variables in the HADES polynomial system in advance, i.e. after the elimination the number of variables and equations in the HADES polynomial system is $2 \cdot n \cdot r_f + r_p$. Note that this elimination does not affect the Macaulay bound from Example 6.3. We stress that after the substitution we exactly reproduce the complexity estimation of the second strategy [GLR+19, p. 48-51], though with a proof and not under a hypothesis. For ease of computation we estimated the logarithm of the binomial coefficient with Equation (26).

Table 5: Complexity estimation of Gröbner basis computations for HADES via the Macaulay bound for I_{HADES} with $n = 2$, and $\omega = 2$ over a finite field $\mathbb{F}_q$ such that $\gcd(d, q-1) = 1$.

	$d = 3$			$d = 5$		
r_f	3	4	5	3	4	5
r_p	13	10	5	10	10	4
κ (bits)	130.0	135.4	130.0	149.0	177.6	163.3

In [GLR+20, Table 1] round numbers for HADES instantiations are proposed, as can be derived from our table all instantiations achieve a security level of 128 bits already for $n = 2$ and $d = 3$.

We also mention that it is straight-forward to compute HADES' quotient space dimension

$$\dim_{\mathbb{F}_q}(I_{\text{HADES}}) = d^{2 \cdot n \cdot r_f + r_p}. \tag{39}$$

6.2 Generalized Feistel Networks

The second permutation that has been dominant in block cipher design in the past is the so-called Feistel Network, named after its inventor Horst Feistel. For example, the predecessor of AES the Data Encryption Standard (DES) [DES77] is based on the Feistel Network. Moreover, so-called unbalanced generalized Feistel Networks have been proposed for AO designs [AGP+19a]. We start with the formal definition of Feistel-based ciphers.

Definition 6.4 (Generalized Feistel cipher)**.** *Let $\mathbb{F}_q$ be a finite field, and let $n, r \geq 1$ be integers.*

(1) For $1 \leq i \leq n-1$, let $f_i \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ be a polynomial. Then the generalized Feistel Layer is defined as

$$\begin{aligned} &\mathcal{F}_{f_1,\ldots,f_{n-1}} : \mathbb{F}_q^n \to \mathbb{F}_q^n, \\ &\quad (x_1, \ldots, x_n) \mapsto \big(x_1 + f_1(x_2, \ldots, x_n), \ldots, x_{n-1} + f_{n-1}(x_n), x_n\big). \end{aligned}$$

(2) For $1 \leq n \leq r$, let $\mathcal{F}^{(i)} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a generalized Feistel Layer and let $\mathcal{A}_i : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an affine permutation. Then the Feistel cipher is defined as

$$\begin{aligned} &\mathcal{C}_{n,r} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n, \\ &\qquad (\mathbf{x}, \mathbf{y}) \mapsto \big(\mathcal{K}_{\mathbf{y}} \circ \mathcal{A}^{(r)} \circ \mathcal{F}^{(r)}\big) \circ \cdots \circ \big(\mathcal{K}_{\mathbf{y}} \circ \mathcal{A}^{(1)} \circ \mathcal{F}^{(1)}\big)(\mathbf{x} + \mathbf{y}), \end{aligned}$$

where the composition is taken with respect to the plaintext variable.

For special types of Feistel ciphers we can derive efficient criteria to verify whether the corresponding multivariate keyed iterated polynomial system is in generic coordinates.

Theorem 6.5. *Let $\mathbb{F}_q$ be a finite field, let $\overline{\mathbb{F}_q}$ be its algebraic closure, let $n, r \geq 1$ be integers, and let $\mathcal{C}_{n,r} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a Feistel cipher. Let $\mathcal{F} = \{\mathbf{f}^{(1)}, \ldots, \mathbf{f}^{(r)}\} \subset P = \overline{\mathbb{F}_q}\left[\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(r-1)}, \mathbf{y}\right]$ be a multivariate keyed iterated polynomial system for $\mathcal{C}_{n,r}$.*

(1) For $1 \leq i \leq r$, *let* $f^{(i)} \in \mathbb{F}_q[x_n]$ *be polynomials such that* $\deg\left(f^{(i)}\right) > 1$, *and assume that the* i^{th} *Feistel Layer of* $\mathcal{C}_{n,r}$ *is* $\mathcal{F}_{f^{(i)},\ldots,f^{(i)}}$. *Let the polynomial system* $\mathcal{G} = \left\{\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(r)}\right\}$ *be defined as follows*

$$\left(\mathbf{g}^{(i)}\right)_j = \begin{cases} \left(\mathbf{A}_i^{-1}\mathbf{f}^{(i)}\right)_j, & j = 1, n, \\ \left(\mathbf{A}_i^{-1}\mathbf{f}^{(i)}\right)_j - \left(\mathbf{A}_i^{-1}\mathbf{f}^{(i)}\right)_1, & 2 \leq j \leq n-1. \end{cases}$$

Then every homogeneous ideal $I \subset P[x_0]$ *such that* $\mathcal{Z}_+(I) \neq \emptyset$ *and* $\mathcal{G}^{\text{hom}} \subset I$ *is in generic coordinates if the following linear system has rank* $r \cdot (n-1)$

$$\begin{aligned} y_j - y_1 + \left(\mathbf{A}_1^{-1}\left(\hat{\boldsymbol{x}}^{(1)} - \hat{\boldsymbol{y}}\right)\right)_1 + \left(\mathbf{A}_1^{-1}\left(\hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}^{(1)}\right)\right)_j &= 0, \\ \left(\mathbf{A}_1^{-1}\left(\hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}^{(1)}\right)\right)_n &= 0, \\ x_j^{(i-1)} - x_1^{(i-1)} + \left(\mathbf{A}_i^{-1}\left(\hat{\boldsymbol{x}}^{(i)} - \hat{\boldsymbol{y}}\right)\right)_1 + \left(\mathbf{A}_i^{-1}\left(\hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}^{(i)}\right)\right)_j &= 0, \\ \left(\mathbf{A}_i^{-1}\left(\hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}^{(i)}\right)\right)_n &= 0, \\ x_j^{(r-1)} - x_1^{(r-1)} + \left(\mathbf{A}_r^{-1}\left(\hat{\boldsymbol{x}}^{(r-1)} - \hat{\boldsymbol{y}}\right)\right)_1 + \left(\mathbf{A}_r^{-1}\left(\hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}^{(r-1)}\right)\right)_j &= 0, \\ \left(\mathbf{A}_r^{-1}\hat{\boldsymbol{y}}\right)_n &= 0, \end{aligned}$$

where $2 \leq i \leq r-1$, $2 \leq j \leq n-1$, $\hat{\boldsymbol{x}}^{(i)} = \left(x_1^{(i)}, \ldots, x_{n-1}^{(i)}, 0\right)$ *and* $\hat{\boldsymbol{y}} = (y_1, \ldots, y_{n-1}, 0)$.

(2) For $1 \leq i \leq r$ *and* $1 \leq j \leq n-1$, *let* $f_j^{(i)} \in \mathbb{F}_q[x_{i+1}, \ldots, x_n]$ *be polynomials such that* $\deg\left(f^{(i)}\right) > 1$ *and the monomial* $x_{i+1}^{\deg\left(f_j^{(i)}\right)}$ *is present in* $f_j^{(i)}$, *and assume that the* i^{th} *Feistel Layer of* $\mathcal{C}_{n,r}$ *is* $\mathcal{F}_{f_1^{(i)},\ldots,f_{n-1}^{(i)}}$. *Let*

$$\mathcal{G} = \left\{\mathbf{A}_1^{-1}\mathbf{f}^{(1)}, \ldots, \mathbf{A}_r^{-1}\mathbf{f}^{(r)}\right\}.$$

Then every homogeneous ideal $I \subset P[x_0]$ *such that* $\mathcal{Z}_+(I) \neq \emptyset$ *and* $\mathcal{G}^{\text{hom}} \subset I$ *is in generic coordinates if the following linear system has rank* r

$$\begin{aligned} \left(\mathbf{A}_1^{-1}\left(\hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}^{(1)}\right)\right)_n &= 0, \\ \left(\mathbf{A}_i^{-1}\left(\hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}^{(i)}\right)\right)_n &= 0, \\ \left(\mathbf{A}_r^{-1}\hat{\boldsymbol{y}}\right)_n &= 0, \end{aligned}$$

where $2 \leq i \leq r-1$, $\hat{\boldsymbol{x}}^{(i)} = \left(x_1^{(i)}, 0 \ldots, 0\right)$ *and* $\hat{\boldsymbol{y}} = (y_1, 0, \ldots, 0)$.

(3) For $1 \leq i \leq r$, *let* $f^{(i)} \in \mathbb{F}_q[x_2, \ldots, x_n]$ *be such that*

$$f^{(i)}(x_2, \ldots, x_n) = \hat{f}^{(i)}\left(\sum_{j=2}^{n} a_{i,j} \cdot x_j\right)$$

with $\hat{f}^{(i)} \in \mathbb{F}_q[x]$ *such that* $\deg\left(\hat{f}^{(i)}\right) > 1$ *and* $a_{i,2}, \ldots, a_{i,n} \in \mathbb{F}_q$*, and assume that the* i^{th} *Feistel Layer of* $\mathcal{C}_{n,r}$ *is* $\mathcal{F}_{f^{(i)},0,\ldots,0}$*. Let*

$$\mathcal{G} = \left\{\mathbf{A}_1^{-1}\mathbf{f}^{(1)}, \ldots, \mathbf{A}_r^{-1}\mathbf{f}^{(r)}\right\}.$$

Then every homogeneous ideal $I \subset P[x_0]$ *such that* $\mathcal{Z}_+(I) \neq \emptyset$ *and* $\mathcal{G}^{\text{hom}} \subset I$ *is in generic coordinates if the following linear system has rank* $r \cdot n$

$$\begin{aligned}
\sum_{k=2}^{n} a_{1,k} \cdot y_k &= 0,\\
\left(\mathbf{A}_1^{-1}\left(\mathbf{y} - \mathbf{x}^{(1)}\right)\right)_j &= 0,\\
\sum_{k=2}^{n} a_{i,k} \cdot x_k^{(i-1)} &= 0,\\
x_j^{(i-1)} + \left(\mathbf{A}_1^{-1}\left(\mathbf{y} - \mathbf{x}^{(i)}\right)\right)_j &= 0,\\
\sum_{k=2}^{n} a_{r,k} \cdot x_k^{(r-1)} &= 0,\\
x_j^{(r-1)} + \left(\mathbf{A}^{-1}\mathbf{y}\right)_j &= 0,
\end{aligned}$$

where $2 \leq i \leq r-1$ *and* $2 \leq j \leq n$*.*

Proof. For all cases we show that $\sqrt{\mathcal{G}^{\text{top}}} = (x_1, \ldots, x_n)$.

For (1), note that for all $1 \leq i \leq r$ we have that the degree of the first component of $\mathbf{g}^{(i)}$ is $\deg\left(f^{(i)}\right)$ and 1 for the other components. Substituting $x_0 = 0$ into $\mathcal{G}^{\text{hom}}$ we yield from the first components of the $\left(\mathbf{g}^{(i)}\right)^{\text{hom}}$'s that $y_n^{\deg\left(f^{(1)}\right)} = {x_n^{(1)}}^{\deg\left(f^{(2)}\right)} = \ldots = {x_n^{(r-1)}}^{\deg\left(f^{(r)}\right)} = 0$ so also $y = x_n^{(1)} = \ldots = x_n^{(r-1)} = 0$. Now we substitute these coordinates into the remaining equations. This yields the linear system from the assertion. If the linear system is of rank $r \cdot (n-1)$, then $\sqrt{\mathcal{G}^{\text{hom}}} = (x_1, \ldots, x_n)$.

For (2), note that for $1 \leq i \leq r$ and $1 \leq j \leq n-1$ we have that $\deg\left(\left(A_i^{-1}\mathbf{f}^{(i)}\right)_j\right) = \deg\left(f_j^{(i)}\right)$. Now we substitute $x_0 = 0$ into $\mathcal{G}^{\text{hom}}$, in the i^{th} round in the $(n-1)^{\text{th}}$ component this yields ${x_n^{(i)}}^{\deg\left(f_{n-1}^{(i)}\right)} = 0$. Inductively we now work through all higher branches in the i^{th} round and then through all rounds to obtain that $y_2 = \ldots = y_n = x_2^{(1)} = \ldots = x_n^{(1)} = \ldots = x_2^{(r-1)} = \ldots = x_n^{(r-1)} = 0$. Substituting these variables into the remaining equations that come from the last branch of the $\mathbf{f}^{(i)}$'s yields the linear system from the assertion which proves the claim.

For (3), after substituting $x_0 = 0$ into $\mathcal{G}^{\text{hom}}$ we obtain for the first branch of each round

$$\begin{aligned}
\left(\sum_{k=2}^{n} a_{1,k} \cdot y_k\right)^{\deg\left(\hat{f}^{(1)}\right)} &= \left(\sum_{k=2}^{n} a_{i,k} \cdot x_k^{(i-1)}\right)^{\deg\left(\hat{f}^{(i)}\right)} = 0\\
&\Longrightarrow\\
\sum_{k=2}^{n} a_{1,k} \cdot y_k &= \sum_{k=2}^{n} a_{i,k} \cdot x_k^{(i-1)} = 0,
\end{aligned}$$

where $2 \leq i \leq r$. Combining these linear equations with the remaining equations from $\mathcal{G}^{\text{hom}}$ we obtain the linear system from the assertion. □

The Feistel Networks from Theorem 6.5 (1) and (3) are also known as *expanding round function* (erf) and *contracting round function* (crf) respectively. An example for block ciphers with these round functions is the GMiMC family [AGP+19a, §2.1], which is targeted for MPC applications. Moreover, the designers of GMiMC use Equation (24) and the Macaulay bound (Corollary 2.9) to estimate the resistance of GMiMC against Gröbner basis attacks, see [AGP+19a, §4.1.1].[4] To justify this approach the authors hypothesized that the GMiMC polynomial systems are *generic* polynomial systems in the sense of Fröberg's conjecture [Frö85, Par10]. With Theorem 6.5 this hypothesis can be bypassed for GMiMC without a key schedule. For GMiMC an affine key schedule was proposed, hence one can extend Theorem 6.5 to this scenario by replacing the key variables with intermediate key variables after the first round and by adding the linear part of the affine key schedule to the linear systems. Thus, we have derived efficient criteria to verify that the complexity estimations of the GMiMC designers can indeed be mathematically sound.

Example 6.6 (Solving degree bounds for GMiMC)**.** Let $\mathbb{F}_q$ be a finite field, let $n, r \geq 1$ denote the number of branches and rounds, and let $d \geq 1$ be the degree of the degree increasing function. In the proof of Theorem 6.5 we saw that the $\texttt{GMiMC}_{\text{erf}}$ polynomial system can be transformed so that there is only one non-linear polynomial in every round. Therefore, $\texttt{GMiMC}_{\text{crf}}$ and $\texttt{GMiMC}_{\text{erf}}$ have the same Macaulay bound. Let $I_{\texttt{GMiMC}}$ be a GMiMC ideal and assume that n and r are such that the corresponding matrix from Theorem 6.5 has full rank, i.e. GMiMC is in generic coordinates. Therefore, by Corollary 2.9

$$\mathrm{sd}_{DRL}\left(I_{\texttt{GMiMC}}\right) \leq (d-1) \cdot r + 1.$$

Now let $I_{\texttt{GMiMC},1}$ and $I_{\texttt{GMiMC},2}$ denote GMiMC ideals for two different plain/ciphertext pairs. It is straight-forward to extend Theorem 6.5 to $I_{\texttt{GMiMC},1} + I_{\texttt{GMiMC},2}$, cf. Proposition 4.9 (2). Provided that n and r are such that $I_{\texttt{GMiMC},1} + I_{\texttt{GMiMC},2}$ is in generic coordinates we have by Corollary 2.9

$$\mathrm{sd}_{DRL}\left(I_{\texttt{GMiMC},1} + I_{\texttt{GMiMC},2}\right) \leq 2 \cdot (d-1) \cdot r + 1.$$

For small primes we applied Theorem 6.5 to $\texttt{GMiMC}_{\text{crf}}$ and $\texttt{GMiMC}_{\text{erf}}$ without key schedules. Depending on the parameters n and r we noticed a highly regular pattern when the matrices from the theorem have full rank. In Table 6 we record this pattern for small sample parameters.

Table 6: Matrix criteria from Theorem 6.5 for sample parameters for $\texttt{GMiMC}_{\text{crf}}$ and $\texttt{GMiMC}_{\text{erf}}$ with the shift permutation $(x_1, \ldots, x_n) \mapsto (x_n, x_1, \ldots, x_{n-1})$ in the affine layer and without key schedules.

$n = 3$		$n = 4$		$n = 5$	
r	Full rank	r	Full rank	r	Full rank
10	True	12	True	10	True
11	False	13	True	11	False
12	True	14	False	12	True
13	False	15	True	13	False
		16	True		
		17	False		

We observed that for the shift permutation $(x_1, \ldots, x_n) \mapsto (x_n, x_1, \ldots, x_{n-1})$ in the affine layer the matrix criteria for $\texttt{GMiMC}_{\text{crf}}$ and $\texttt{GMiMC}_{\text{erf}}$ behave identical. On the other

[4] For completeness, we mention that the GMiMC designers did not analyze the keyed iterated polynomial system (Equation (38)). They only studied systems where all rounds are substituted into each other, i.e. one has n equations in n variables.

hand, if we instantiate GMiMC with the circulant matrix $\mathrm{circ}(1,\ldots,n)$[5], then we observed that $\texttt{GMiMC}_{\mathrm{erf}}$ is always in generic coordinates and for $\texttt{GMiMC}_{\mathrm{crf}}$ the criterion is identical to Table 6.

In Table 7 we provide complexity estimates in bits for a Gröbner basis computation of GMiMC where we use the Macaulay bound of the keyed iterated GMiMC polynomial system as minimal baseline of the solving degree for an optimal adversary with $\omega = 2$. We assume that the key schedule equations have been substituted into Equation (38). Also, recall from Theorem 6.5 that we can transform a GMiMC polynomial system so that every round contains only one non-linear polynomial. Thus, we can use the affine equations to eliminate $r \cdot (n-1)$ many variables in the GMiMC polynomial system in advance, i.e. after the elimination the number of variables and equations in the GMiMC polynomial system is r. Note that the elimination does not affect the Macaulay bound in Example 6.6. For ease of computation we estimated the logarithm of the binomial coefficient with Equation (26).

Table 7: Complexity estimation of Gröbner basis computations for GMiMC via the Macaulay bound with $\omega = 2$ over any finite field $\mathbb{F}_q$.

	$d=3$			$d=5$		
r	10	25	50	10	25	50
κ (bits)	48.6	130.0	266.7	63.5	170.5	350.0

In [AGP+19b, Table 7] round number for $\texttt{GMiMC}_{\mathrm{erf}}$ instantiations are proposed, as can be derived from our table all instantiations achieve a security level of 128.

6.3 The Problem With Sponge Constructions & Generic Coordinates

Let us return to the sponge construction [BDPV07, BDPV08]. Let $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an arbitrary permutation which we instantiate in sponge mode with capacity $1 < c < n$ and rate $r = n - c$. Let $\texttt{IV} \in \mathbb{F}_q^c$ be a fixed initial value, and let $\alpha \in \mathbb{F}_q$ be a hash output. To find a preimage $\mathbf{x} \in \mathbb{F}_q^r$ we have to solve the equation

$$\mathcal{P}\begin{pmatrix}\mathbf{x}\\ \texttt{IV}\end{pmatrix} = \begin{pmatrix}\alpha\\ \mathbf{y}\end{pmatrix}, \tag{40}$$

where $\mathbf{y} \in \mathbb{F}_q^{n-1}$ is an indeterminate variable. First, we observe that this polynomial system is only fully determined if $c = n-1$, else one always has $r + n - 1 > n$ many variables for $\mathbf{x}$ and $\mathbf{y}$. Otherwise, we have to guess some entries of $\mathbf{x}$ and $\mathbf{y}$ which we expect to be successful with probability $1/q$. Second, if we model the sponge $\mathcal{P}$ with iterated polynomials, then the Caminata-Gorla technique (Section 2.3.1) will fail whenever the last round of $\mathcal{P}$ is non-linear in all its components. In this case, after homogenizing the keyed iterated polynomial system and setting $x_0 = 0$ we will always remove the variables $\mathbf{y}$ from the equations. So Theorem 3.2 (2) cannot be satisfied, and the naive homogenization of a sponge polynomial system cannot be in generic coordinates.

We illustrate this property with a simple example.

Example 6.7. We work over the field $\mathbb{F}_5$. We consider an SPN sponge function based on the cubing map with $n = 2$ and $r = 3$ where the first and the last round are full SPNs and

[5]We understand circulant matrices as right shift circulant matrices, i.e.

$$\mathrm{circ}(a_1,\ldots,a_n) = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n-1} & a_n \\ a_n & a_1 & \ldots & a_{n-2} & a_{n-1} \\ & & \vdots & & \\ a_2 & a_3 & \ldots & a_n & a_1 \end{pmatrix}.$$

the middle round is a partial SPN. In every round the mixing matrix is $\mathrm{circ}(1,2)$ and all round constants are $\mathbf{0}$. The matrix is also applied before application of the first SPN. We illustrate this sponge function in Figure 3.

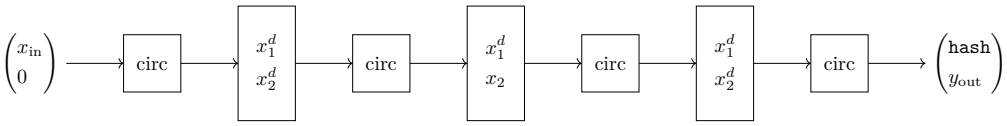

Figure 3: Illustration of a simple SPN sponge function.

For hash value 0 the iterated polynomial system $\mathcal{F} \subset \mathbb{F}_5\left[x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)} x_{\text{in}}, y_{\text{out}}\right]$ is

$$\begin{aligned}
x_{\text{in}}^3 + 2 \cdot x_1^{(1)} + x_2^{(1)} &= 0, \\
-2 \cdot x_{\text{in}}^3 + x_1^{(1)} + 2 \cdot x_2^{(1)} &= 0, \\
{x_1^{(1)}}^3 + 2 \cdot x_1^{(2)} + x_2^{(2)} &= 0, \\
x_2^{(1)} + x_1^{(2)} + 2 \cdot x_2^{(2)} &= 0, \\
{x_1^{(2)}}^3 + y_{\text{out}} &= 0, \\
{x_2^{(2)}}^3 + 2 \cdot y_{\text{out}} &= 0.
\end{aligned}$$

Note that $(\mathcal{F})$ is zero-dimensional. Let x_0 denote the homogenization variable. Then $I^{\text{sat}} = \left(\mathcal{F}^{\text{hom}}\right)^{\text{sat}}$ is generated by

$$\begin{aligned}
x_{\text{in}}^3 + 2 \cdot x_1^{(1)} \cdot x_0 &= 0, \\
x_2^{(1)} + x_1^{(2)+2 \cdot x_2(2)} &= 0, \\
\left(x_1^{(2)} + x_2^{(2)}\right) \cdot x_0^2 &= 0, \\
{x_2^{(2)}}^3 + 2 \cdot y_{\text{out}} \cdot x_0^2 &= 0, \\
{x_1^{(1)}}^3 + y_{\text{out}} \cdot x_0^2 &= 0, \\
{x_1^{(1)}}^3 + 2 \cdot x_2^{(2)} \cdot x_0^2 &= 0, \\
y_{\text{out}} \cdot x_0^4 &= 0.
\end{aligned}$$

Hence, after reducing modulo (x_0) we remove the variable y_{out}.

To resolve this problem we have to add additional polynomials to the system. Over finite fields we can always add the field equations for $\mathbf{y}$ though for AO designs this introduces high degree equations to a low degree polynomial system. On the other hand, we could add the inverse of the last round of an iterated construction to the polynomial system to introduce polynomials with leading monomials in $\mathbf{y}$. Though, in general we also expect that this trick introduces high degree equations.

6.4 The Problem With Non-Affine Key Schedules & Generic Coordinates

We face a similar obstacle for the Caminata-Gorla technique if we deploy a non-affine key schedule. For sake of example let us return to `MiMC` with the key schedule

$$y_i = y_{i-1}^3, \tag{41}$$

for $2 \leq i \leq r$ and $y_1 \in \mathbb{F}_q$ the master key. We then add the i^{th} key in the i^{th} round. Obviously, we then have to add the equations $y_{i-1}^3 - y_i = 0$ to the MiMC keyed iterated polynomial system. Now we homogenize this new system and set $x_0 = 0$, like in Theorem 3.7 we can iterate through the rounds to deduce that $y_1 = \ldots = y_{r-1} = x_1 = \ldots = x_{r-2} = 0$. But for the last round we obtain that $y_r + x_{r-1} = 0$, and we do not have any more equations left to cancel one of the variables. Again, we would have to add polynomials to the system to fix our method like the field equations, or if possible the inverse of the last key schedule equation.

7 Polynomials With Degree Falls & The Satiety

We now return to studying MiMC, Feistel-MiMC and Feistel-MiMC-Hash. In Section 5 we derived solving degree estimates for various attacks on these primitives. A natural question for the cryptanalyst is tightness of these bounds. To partially answer this question we derive Castelnuovo-Mumford regularity lower bounds for the attacks on these primitives. Essentially, if we find a non-trivial lower bound for the Castelnuovo-Mumford regularity, then regularity-based complexity estimates can never improve upon the lower bound.

In this section we develop the theoretical foundation for our regularity lower bounds. First we introduce the notion of last fall degree of $\mathcal{F} \subset P$, that is the largest $d \in \mathbb{Z} \cup \{\infty\}$ such that the row space of the inhomogeneous Macaulay matrix $M_{\leq d}$ is unequal to $(\mathcal{F})_{\leq d}$ (as K-vector space). Then we prove that in generic coordinates the last fall degree of $\mathcal{F}$ is equal to the satiety of $\mathcal{F}^{\text{hom}}$, another invariant closely related to the regularity.

Let $I \subset P = K[x_0, \ldots, x_n]$ be a homogeneous ideal, it is well-known that the saturation $I^{\text{sat}} = I : \mathfrak{m}^{\infty}$ is the unique largest ideal $J \subset P$ such that there exists $m \geq 0$ and for all $l \geq m$ one has $I_l = J_l$. This motivates the following definition.

Definition 7.1. *Let $I \subset K[x_0, \ldots, x_n]$ be a homogeneous ideal. The satiety of I, denoted by $\operatorname{sat}(I)$ is the smallest positive integer m such that $I_l = I_l^{\text{sat}}$ for all $l \geq m$.*

We recall some properties of the satiety. If $x_0 \nmid 0 \mod I^{\text{sat}}$, then by [BS87, Lemma 1.8] one has that

$$\operatorname{sat}(I) \leq \operatorname{reg}(I), \tag{42}$$

and by [Has12, Proposition 2.2] one has that

$$\operatorname{sat}(I) = \operatorname{sat}\left(\operatorname{in}_{DRL}(I)\right). \tag{43}$$

Moreover, if I is in generic coordinates and $\mathcal{Z}_+(I) \neq \emptyset$, then by [Gre98, Theorem 2.30] one has that

$$\operatorname{reg}(I) = \max\left\{\operatorname{sat}(I), \operatorname{reg}\left(I^{\text{sat}}\right)\right\}. \tag{44}$$

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$ be a polynomial system, and let $M_{\leq d}$ be the inhomogeneous Macaulay matrix in degree d. We denote with

$$W_{\mathcal{F},d} = \left\{ f \in P \;\middle|\; f = \sum_{i=1}^{m} g_i \cdot f_i,\ \deg(g_i \cdot f_i) \leq d \right\} \tag{45}$$

the row space of $M_{\leq d}$. Next we define the last fall degree.

Definition 7.2. *Let K be a field, and let $\mathcal{F} \subset K[x_1, \ldots, x_n]$ be a polynomial system.*

(1) For any $f \in (\mathcal{F})$ let

$$d_f = \min\{d \in \mathbb{Z}_{\geq 0} \mid f \in W_{\mathcal{F},d}\}.$$

(2) If $d_f > \deg(f)$, then we say that f has a degree fall in degree d_f. We say that $\mathcal{F}$ has a degree fall if there is an $f \in (\mathcal{F})$ such that f has a degree fall. Else we say that $\mathcal{F}$ has no degree falls.

(3) Let $W_{\mathcal{F},\infty} = (\mathcal{F})$ and $V_{\mathcal{F},-1} = \emptyset$. The last fall degree of $\mathcal{F}$ is

$$d_{\mathcal{F}} = \min\left\{d \in \mathbb{Z}_{\geq 0} \cup \{\infty\} \mid f \in W_{\mathcal{F},\max\{d,\deg(f)\}} \text{ for all } f \in (\mathcal{F})\right\}.$$

Note that the definition implies that for all $d \geq d_{\mathcal{F}}$ we have that $W_{\mathcal{F},d} = (\mathcal{F}) \cap P_{\leq d} = (\mathcal{F})_{\leq d}$.

Next we collect some alternative characterizations of the last fall degree.

Proposition 7.3. *Let K be a field, and let $\mathcal{F} \subset P = K[x_1, \ldots, x_n]$ be a polynomial system.*

(1) If there exists a largest $d \in \mathbb{Z}_{\geq 0}$ such that $W_{\mathcal{F},d} \cap P_{\leq d-1} \neq W_{\mathcal{F},d-1}$, then $d_{\mathcal{F}} = d$. Else $d_{\mathcal{F}} = \infty$.

(2) $d_{\mathcal{F}} \geq \sup\{d_f \mid f \in (\mathcal{F}),\ d_f > \deg(f)\}$.

(3) If $d_{\mathcal{F}} < \infty$, then $d_{\mathcal{F}} = \max\{d_f \mid f \in (\mathcal{F}),\ d_f > \deg(f)\}$.

Proof. For (1), let $d < \infty$ be as asserted. By definition of the last fall degree $d_{\mathcal{F}} \geq d$. If $f \in (\mathcal{F})$ is such that $\deg(f) \leq d_{\mathcal{F}}$, then by definition of the last fall degree $f \in W_{\mathcal{F},d_{\mathcal{F}}}$. Therefore, we have that

$$W_{\mathcal{F},d_{\mathcal{F}}} \cap P_{\leq d_{\mathcal{F}}-1} = (\mathcal{F}) \cap P_{\leq d_{\mathcal{F}}-1} \neq W_{\mathcal{F},d_{\mathcal{F}}-1},$$

which implies that $d_{\mathcal{F}} \leq d$. If such a $d \in \mathbb{Z}_{\geq 0}$ does not exist, then obviously $d_{\mathcal{F}} = \infty$.

For (2), let $f \in (\mathcal{F})$ be such that $d_f > \deg(f)$. Then for all $d < d_f$ we have $f \notin W_{\mathcal{F},d}$. Therefore, by definition of the last fall degree $d_{\mathcal{F}} > d_f - 1$. Hence, $d_{\mathcal{F}} \geq \sup\{d_f \mid f \in (\mathcal{F}),\ d_f > \deg(f)\}$.

For (3), since the last fall degree is finite by assumption the supremum from (2) is indeed a maximum. Now let $d = \max\{d_f \mid f \in (\mathcal{F}),\ d_f > \deg(f)\}$ and fix $f \in (\mathcal{F})$. If $d_f > \deg(f)$, then $f \in W_{\mathcal{F},d_f} \subset W_{\mathcal{F},d}$ and $d = \max\{d, \deg(f)\}$ since $d \geq d_f > \deg(f)$. If $d_f = \deg(f)$, then we always have that $W_{\mathcal{F},\deg(f)} \subset W_{\mathcal{F},\max\{d,\deg(f)\}}$. Thus, for all $f \in (\mathcal{F})$ we have $f \in W_{\mathcal{F},\max\{d,\deg(f)\}}$. So $d \in \{e \in \mathbb{Z}_{\geq 0} \cup \{\infty\} \mid f \in W_{\mathcal{F},\max\{e,\deg(f)\}} \text{ for all } f \in (\mathcal{F})\}$ which implies that $d_{\mathcal{F}} \leq d$. □

Unsurprisingly, the last fall degree can also be considered as a measure of the complexity of solving polynomial systems. Let $\max.\,\mathrm{GB}.\deg_{>}(\mathcal{F})$ denote the maximal degree of the polynomials appearing in the reduced $>$-Gröbner basis of $\mathcal{F}$.

Lemma 7.4. *Let K be a field, and let $\mathcal{F} \subset P = K[x_1, \ldots, x_n]$ be a polynomial system with $d_{\mathcal{F}} < \infty$. Then*

$$\mathrm{sd}_{DRL}(\mathcal{F}) \leq \max\left\{d_{\mathcal{F}}, \max.\,\mathrm{GB}.\deg_{DRL}(\mathcal{F})\right\}.$$

Proof. Let $g \in \mathcal{G}$ be an element of the reduced DRL Gröbner basis of $\mathcal{F}$. If g has a degree fall, then by Proposition 7.3 $g \in W_{\mathcal{F},d_g} \subset W_{\mathcal{F},d_{\mathcal{F}}}$. If g does not have a degree fall, then $g \in W_{\mathcal{F},\deg(g)}$. Thus, the upper bound follows by taking the maximum over the last fall degree and the maximal degree in the reduced DRL Gröbner basis. □

If a polynomial system is in generic coordinates, then one can guarantee that the last fall degree is finite.

Theorem 7.5. *Let K be an algebraically closed field, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ be an inhomogeneous polynomial system such that $\left(\mathcal{F}^{\mathrm{hom}}\right)$ is in generic coordinates and $\left|\mathcal{Z}_+\left(\mathcal{F}^{\mathrm{hom}}\right)\right| \neq 0$. If $d \geq \mathrm{sat}\left(\mathcal{F}^{\mathrm{hom}}\right)$ is an integer, then*

$$(\mathcal{F})_{\leq d} = W_{\mathcal{F},d}.$$

In particular,

$$d_{\mathcal{F}} = \mathrm{sat}\left(\mathcal{F}^{\mathrm{hom}}\right).$$

Proof. As always we abbreviate $P = K[x_1, \dots, x_n]$. $W_{\mathcal{F},d} \subset (\mathcal{F})_{\leq d}$ is trivial, so let $f \in (\mathcal{F})_{\leq d}$. Recall that by Lemma 2.6 $(\mathcal{F})^{\text{hom}} = \left(\mathcal{F}^{\text{hom}}\right)^{\text{sat}}$. Therefore, by definition of the satiety $x_0^{d-\deg(f)} \cdot f^{\text{hom}} \in (\mathcal{F})_d^{\text{hom}} = \left(\mathcal{F}^{\text{hom}}\right)_d$. So we can construct $x_0^{d-\deg(f)} \cdot f^{\text{hom}} = \sum_{i=1}^m g_i \cdot f_i^{\text{hom}}$, where g_i homogeneous and $\deg\left(g_i \cdot f_i^{\text{hom}}\right) = d$. Then by [KR05, Proposition 4.3.2]

$$f = \left(x_0^{d-\deg(f)} \cdot f^{\text{hom}}\right)^{\text{deh}} = \sum_{i=1}^m g_i^{\text{deh}} \cdot f_i,$$

where $\deg\left(g_i^{\text{deh}} \cdot f_i\right) \leq d$. So $f \in W_{\mathcal{F},d}$. Therefore, $W_{\mathcal{F},d} \cap P_{\leq d-1} = (\mathcal{F})_{\leq d} \cap P_{\leq d-1} = (\mathcal{F})_{\leq d-1} = W_{\mathcal{F},d-1}$ for all $d > \text{sat}\left(\mathcal{F}^{\text{hom}}\right)$. So by Proposition 7.3 we can conclude that $d_{\mathcal{F}} \leq \text{sat}\left(\mathcal{F}^{\text{hom}}\right)$.

For the second claim let $f \in (\mathcal{F})_{\leq d_{\mathcal{F}}}$, then it can be constructed as

$$f = \sum_{i=1}^m g_i \cdot f_i,$$

where $\deg(g_i \cdot f_i) \leq d_{\mathcal{F}}$. Let $\hat{d} = \max_{1 \leq i \leq m} \deg(g_i \cdot f_i) \leq d_{\mathcal{F}}$. Then by [KR05, Proposition 4.3.2]

$$x_0^{\hat{d}-\deg(f)} \cdot f^{\text{hom}} = \sum_{i=1}^m x_0^{\hat{d}-\deg(f_i \cdot g_i)} \cdot g_i^{\text{hom}} \cdot f_i^{\text{hom}}.$$

Multiplying this equation by $x_0^{d_{\mathcal{F}}-\hat{d}}$ lifts it to $(\mathcal{F})_{d_{\mathcal{F}}}^{\text{hom}}$. Since $f \in (\mathcal{F})_{\leq d_{\mathcal{F}}}$ was arbitrary we can then conclude that

$$\left(\mathcal{F}^{\text{hom}}\right)_{d_{\mathcal{F}}} = \left\{ x_0^{d_{\mathcal{F}}-\deg(f)} \cdot f^{\text{hom}} \;\middle|\; f \in (\mathcal{F})_{\leq d_{\mathcal{F}}} \right\} = (\mathcal{F})_{d_{\mathcal{F}}}^{\text{hom}}.$$

Obviously, the latter equality extends to all $d \geq d_{\mathcal{F}}$, so by minimality of the saturation we also have that $\text{sat}\left(\mathcal{F}^{\text{hom}}\right) \leq d_{\mathcal{F}}$. □

Corollary 7.6. *In the situation of Theorem 7.5, if $f \in (\mathcal{F})$ has a degree fall in d_f, then*

$$d_f \leq \text{sat}\left(\mathcal{F}^{\text{hom}}\right).$$

Proof. This is a consequence of Proposition 7.3 and Theorem 7.5. □

So by Equation (42) the construction of a polynomial with a degree fall yields a lower bound on the regularity of $\mathcal{F}^{\text{hom}}$.

Remark 7.7. We note that the first notion of "last fall degree" already appeared in Huang et al. [HKY15, HKYY18]. They define their last fall degree as follows: Let $\mathcal{F} \subset P = K[x_1, \dots, x_n]$ be a polynomial system the vector space of constructible polynomials $V_{\mathcal{F},d}$ in degree $d \geq 0$ is defined via

(i) $\{f \in \mathcal{F} \mid \deg(f) \leq d\} \subset V_{\mathcal{F},d}$,

(ii) if $g \in V_{\mathcal{F},d}$ and $h \in P$ with $\deg(g \cdot h) \leq d$, then $h \cdot g \in V_{\mathcal{F},d}$.

Analog to Definition 7.2 Huang et al. define the last fall degree as

$$\overline{d}_{\mathcal{F}} = \min\left\{ d \in \mathbb{Z}_{\geq 0} \cup \{\infty\} \mid f \in V_{\mathcal{F},\max\{d,\deg(f)\}} \text{ for all } f \in (\mathcal{F}) \right\}.$$

For Huang et al.'s last fall degree one can also prove analog characterizations to Proposition 7.3, see [HKYY18, Propostion 2.6] and [CG23, Theorem 2.8]. Moreover, Huang et al.'s last fall degree is always finite [HKYY18, Propostion 2.6].

Huang et al.'s last fall degree can also be interpreted in terms of Macaulay matrices. Let $>$ be a degree compatible term order on P, and let $M_{\leq d}$ be the inhomogeneous Macaulay matrix for $\mathcal{F}$ in degree d. First we compute the basis $\mathcal{B}$ of the row space of $M_{\leq d}$ via Gaussian elimination. Now we generate the Macaulay matrix $M_{\leq d}$ for $\mathcal{B}$ and again compute the row space basis $\mathcal{B}'$ via Gaussian elimination. We repeat this procedure until $\mathcal{B} = \mathcal{B}'$. We then denote with $\overline{W}_d$ the row space of the final stationary Macaulay matrix in that procedure. It is clear that for d large enough $\mathcal{B}$ contains a Gröbner basis, in analogy to Definition 2.3 one can define another notion of solving degree $\overline{\mathrm{sd}}_{>}(\mathcal{F})$ to be the minimal d such that the iterated Macaulay matrix construction produces a $>$-Gröbner basis for $\mathcal{F}$. Gorla et al. proved that $\overline{W}_d = V_{\mathcal{F},d}$ [GMP22, Theorem 1], and Caminata & Gorla proved that [CG23, Theorem 3.1]

$$\overline{\mathrm{sd}}_{>}(\mathcal{F}) = \max\left\{\overline{d}_{\mathcal{F}}, \max.\,\mathrm{GB}.\deg_{>}(\mathcal{F})\right\}.$$

With the Macaulay matrix interpretation the difference between Huang et al.'s and our last fall degree notion becomes clear. Our last fall degree is defined via a single Macaulay matrix in degree d, i.e. it is a *last fall degree of the first order*. Huang et al.'s last fall degree is defined via an iteration of Macaulay matrices in degree d, i.e. it is a *last fall degree of higher order*.

Finally, it follows easily from the definitions that

$$\begin{aligned}\overline{d}_{\mathcal{F}} &\leq d_{\mathcal{F}},\\ \overline{\mathrm{sd}}_{>}(\mathcal{F}) &\leq \mathrm{sd}_{>}(\mathcal{F}).\end{aligned}$$

8 Lower Bounds for the Last Fall Degree of Iterated Polynomial Systems

In this section we prove lower bounds for the Castelnuovo-Mumford regularity of attacks on `MiMC`, Feistel-`MiMC` and Feistel-`MiMC`-Hash. Essentially, we will achieve this by constructing S-polynomials with degree falls.

8.1 Lower Bound for Univariate Keyed Iterated Polynomial Systems With a Field Equation

Before we present the theorem we first outline our proof strategy for all results in this section. First we pick a polynomial $f \in (I, g)$, where I is an ideal with known DRL and LEX Gröbner bases and g is an additional polynomial, and assume that f does not have a degree fall in some degree d_f. Now we express as sum $f = f_I + f_g \cdot g$, where $f_I \in I$, that is compatible with d_f and rearrange this equation so that the right-hand side only consists of elements of I, i.e. $f - f_g \cdot g = f_I$. Additionally, we reduce f_g modulo I with respect to DRL, so without loss of generality we can assume that no monomial of f_g is an element of $\mathrm{in}_{DRL}(I)$. Then we use the LEX Gröbner basis of I to transform the left-hand side into a univariate polynomial. Finally, we compare the degrees of the univariate left-hand side polynomial and the univariate LEX polynomial of I. If f has a degree fall, then we expect that the degree of the left-hand side polynomial is less than the degree of the univariate LEX polynomial, i.e. we have constructed a contradiction.

Theorem 8.1. *Let $\mathbb{F}_q$ be a finite field, let $n \geq 2$ be an integer, and let $f_1, \ldots, f_n \in \mathbb{F}_q[x_1, \ldots, x_{n-1}, y]$ be a univariate keyed iterated polynomial system such that*

(i) $d_i = \deg(f_i) \geq 2$ for all $1 \leq i \leq n$ and $d_1 \leq q$, and

(ii) f_i has the monomial $x_{i-1}^{d_i}$ for all $2 \leq i \leq n$.

Let $f_{n+1} = y^q - y$ be the field equation for y, let $\mathcal{F} = \{f_1, \ldots, f_{n+1}\}$, and let $\tilde{f}_n \in \mathbb{F}_q[y]$ be the univariate polynomial in the LEX Gröbner basis of $(f_1, \ldots, f_n)$. Further, assume that

(iii) $f_{n+1} \notin (f_1, \ldots, f_n)$, *and*

(iv) $\tilde{f}_n$ *has less than* d_1 *many roots in* $\mathbb{F}_q$.

Then

$$d_{\mathcal{F}} \geq q + \sum_{i=2}^{n} (d_i - 1).$$

Moreover, if $d_i \geq d$ *for all* $1 \leq i \leq n$, *then*

$$d_{\mathcal{F}} \geq q + (n-1) \cdot (d-1).$$

Proof. Without loss of generality we can assume that $\mathrm{LC}_{DRL}(f_1) = 1$. Let $I = (f_1, \ldots, f_n)$, and let $x^\gamma = \prod_{i=1}^{n-1} x_i^{d_{i+1}-1}$. We consider the S-polynomial

$$s = x^\gamma \cdot S_{DRL}(f_1, f_{n+1}),$$

and the degree $d_s = q + \sum_{i=2}^{n}(d_i - 1)$. By Assumption (iii) $S_{DRL}(f_1, f_{n+1}) = y^{q-d_1} \cdot f_1 - f_{n+1}$ has a degree fall in q, so we also have that $\deg(s) < d_s$. For a contradiction let us assume that s does not have a degree fall in d_s, i.e.,

$$s = \sum_{i=1}^{n} s_i \cdot f_i + s_{n+1} \cdot f_{n+1},$$

where $\deg(s_i \cdot f_i) < d_s$ for all $1 \leq i \leq n+1$. Expanding the definition for s and by rearranging we yield that

$$(x^\gamma + s_{n+1}) \cdot f_{n+1} = \sum_{i=1}^{n} \tilde{s}_i \cdot f_i \in I.$$

Via division by remainder we can split $s_{n+1} = s_I + s_r$, where $s_I \in I$ and no term of s_r lies in $\mathrm{in}_{DRL}(I)$. Note that for a degree compatible term order the degree of polynomials involved in the division by remainder algorithm can never reach d_s. Now we move $s_I \cdot f_{n+1}$ to the right-hand side of the equation, so without loss of generality we can assume that no term of s_{n+1} lies in $\mathrm{in}_{DRL}(I)$. Via the LEX Gröbner basis of I, see Lemma 4.2, we can transform any polynomial in $g \in \mathbb{F}_q[x_1, \ldots, x_{n-1}, y]$ into a univariate polynomial $\hat{g} \in K[y]$ such that

$$g \equiv \hat{g} \mod (f_1, \ldots, f_n)$$

by simply substituting $x_i \mapsto \tilde{f}_i$. Via the substitution we now obtain univariate polynomials $\hat{f}_\gamma, \hat{f}_{s_{n+1}} \in \mathbb{F}_q[y]$ such that

$$(x^\gamma + s_{n+1}) \cdot f_{n+1} \equiv \left(\hat{f}_\gamma + \hat{f}_{s_{n+1}}\right) \cdot f_{n+1} \equiv 0 \mod I. \tag{46}$$

By our assumption that s does not have a degree fall, we have that $\deg(s_{n+1}) < \deg(x^\gamma)$. So by Proposition 4.6 (5) we also have that $\deg\left(\hat{f}_{s_{n+1}}\right) < \deg\left(\hat{f}_\gamma\right)$. Recall that the degree of $\hat{f}_\gamma$ is given by Proposition 4.6 (4),

$$\deg\left(\hat{f}_\gamma\right) = \prod_{i=1}^{n} d_i - d_1. \tag{47}$$

Combining Lemma 4.1 (2) and Equation (46) we now conclude that

$$(x^\gamma + s_{n+1}) \cdot f_{n+1} \in (f_1, \ldots, f_n) \Leftrightarrow \left(\hat{f}_\gamma + \hat{f}_{s_{n+1}}\right) \cdot f_{n+1} \in \left(\tilde{f}_n\right), \tag{48}$$

where $\tilde{f}_n$ is the univariate polynomial in the LEX Gröbner basis of I. I.e., $\left(\hat{f}_\gamma + \hat{f}_{s_{n+1}}\right) \cdot f_{n+1}$ must be a multiple of $\tilde{f}_n$. By Assumption (iv) $\tilde{f}_n$ has less than d_1 many roots in $\mathbb{F}_q$ and $f_{n+1} = \prod_{a \in \mathbb{F}_q}(y - a)$ is a square-free polynomial, so

$$\deg\left(\gcd\left(\hat{f}_n, f_{n+1}\right)\right) < d_1. \tag{49}$$

Before our final step we recall the following property of univariate polynomial greatest common divisors: If $p, q, r \in K[x]$, K a field, and $\gcd(p, r) = 1$, then $\gcd(p, q \cdot r) = \gcd(p, q)$. Combining this property with Equation (48) we conclude that the following equation must be true

$$\begin{aligned}\tilde{f}_n &= \gcd\left(\tilde{f}_n, \left(\hat{f}_\gamma + \hat{f}_{s_{n+1}}\right) \cdot f_{n+1}\right) \\ &= \gcd\left(\tilde{f}_n, \left(\hat{f}_\gamma + \hat{f}_{s_{n+1}}\right) \cdot \gcd\left(\tilde{f}_n, f_{n+1}\right)\right).\end{aligned}$$

On the other hand, by Equations (47) and (49) we have that

$$\begin{aligned}\deg\left(\tilde{f}_n\right) = \prod_{i=1}^{n} d_i &\leq \deg\left(\left(\hat{f}_\gamma + \hat{f}_{s_{n+1}}\right) \cdot \gcd\left(\tilde{f}_n, f_{n+1}\right)\right) \\ &= \deg\left(\hat{f}_\gamma + \hat{f}_{s_{n+1}}\right) + \deg\left(\gcd\left(\tilde{f}_n, f_{n+1}\right)\right) \\ &< \prod_{i=1}^{n} d_i - d_1 + d_1 = \prod_{i=1}^{n} d_i.\end{aligned}$$

A contradiction. □

Remark 8.2. (1) If the number of roots of $\hat{f}_n$ in $\mathbb{F}_q$ is greater than or equal to d_1, then one can still apply the strategy in the proof to obtain a weaker upper bound. It suffices to choose $x^\gamma = \prod_{i=j}^{n-1} x_i^{d_{i+1}}$ for a suitable $j > 1$ such that the degrees of the polynomials in the final gcd equation yield a contradiction.

(2) We note that small non-trivial bounds can also be proven without Assumption (iv). In particular, one can prove that

(i) If $d_1 + q < d_n$, then $d_{\mathcal{F}} \geq q + 1$.

(ii) If $q + \prod_{i=1}^{n-1} d_i < d_n$, then $d_{\mathcal{F}} \geq q + 2$.

One considers the polynomials $x_1 \cdot S_{DRL}(f_1, f_{n+1})$ and $x_1^2 \cdot S_{DRL}(f_1, f_{n+1})$ respectively, and then applies the same strategy as in the proof of Theorem 8.1 to deduce that these polynomials have degree falls.

Let us now apply the lower bound to `MiMC`.

Example 8.3 (`MiMC` and one field equation II)**.** Let `MiMC` be defined over $\mathbb{F}_q$, and let r be the number of rounds. The first two conditions of Theorem 8.1 are trivially satisfied by `MiMC`. For the third assumption, if we consider $\hat{f}_n$, the univariate polynomial in the LEX Gröbner basis, as random polynomial, then for q large enough it has on average only one root in $\mathbb{F}_q$ (cf. [Leo06]). Thus, with high probability we can assume that `MiMC` has only one root in $\mathbb{F}_q$. Now we pick a random $k \in \mathbb{F}_q$ and evaluate whether $\texttt{MiMC}(p, k) = c$ or

not. If the equality is true we can return K as proper key guess, otherwise it implies that $f_{n+1} \notin I_{\texttt{MiMC}}$. So we can combine Example 5.1 and Theorem 8.1 to obtain the following range for the solving degree of `MiMC` and one field equation

$$q + 2 \cdot r - 2 \leq \operatorname{reg}\left(\mathcal{F}^{\text{hom}}_{\texttt{MiMC}} + \left(y^q - y \cdot x_0^{q-1}\right)\right) \leq q + 2 \cdot r.$$

Small scale experiments indicate that the solving degree of this attack is always equal to $q + 2r - 1$.

For any polynomial system $\mathcal{F} \subset P$ such that $\mathcal{F}^{\text{hom}}$ is in generic coordinates we have by Corollary 3.5 and [CG23, Theorem 5.3] that

$$d_{\text{reg}}\left(\mathcal{F}\right) \leq \operatorname{reg}\left(\mathcal{F}^{\text{hom}}\right). \tag{50}$$

Obviously, this bound also applies to the scenario of Theorem 8.1, though under the assumptions of the theorem $\mathcal{F}^{\text{top}} \subset P$ is a DRL Gröbner basis since $f_1^{\text{top}} = y^{d_1} \mid y^q$. Therefore, $\text{in}_{DRL}\left(\mathcal{F}^{\text{top}}\right) = \left(y^{d_1}, x_1^{d_2}, \ldots, x_{n-1}^{d_n}\right)$. Note that a homogeneous ideal and its DRL initial ideal have to have the same degree of regularity, and it is easy to see that

$$d_{\text{reg}}\left(\mathcal{F}^{\text{top}}\right) = \sum_{i=1}^{n} d_i - n + 1, \tag{51}$$

i.e. the degree of regularity is equal to the Macaulay bound of the keyed iterated polynomial system.

Recall from Section 5.1 that we can always replace $y^q - y$ by its remainder r_y modulo I_{MiMC} with respect to DRL. For `MiMC` experimentally we observed that the highest degree component of r_y is always a monomial and $y^{d_1-1} \mid r_y$. To compute the degree of regularity one then computes the DRL Gröbner basis of $(\mathcal{F}^{\text{top}})$ and utilizes it to compute the Hilbert series h of $\text{in}_{DRL}\left(\mathcal{F}^{\text{top}}\right)$. The degree of regularity is then given by $\deg\left(h\right) + 1$.

Under some additional assumptions on r_y we can adapt the proof of Theorem 8.1. Suppose that the highest degree component of r_y is of the form $y^{d_1-1} \cdot \prod_{i=1}^{k} x_i^{d_{i+1}-1}$ for some $k \leq n-2$. We set $x^\gamma = \prod_{i=j}^{n-1} x_i^{d_{i+1}-1}$, where $j \geq k+1$, and consider the S-polynomial

$$s = x^\gamma \cdot S_{DRL}(f_1, r_y) = x^\gamma \cdot \left(f_1 \cdot \prod_{i=1}^{k} x_i^{d_{i+1}-1} - y \cdot r_y\right). \tag{52}$$

Again we assume that s does not have a degree fall in $d_s = \deg\left(r_y\right) + \sum_{i=j+1}^{n}(d_i - 1) + 1$. By rearranging we then yield that

$$(y \cdot x^\gamma + s_y) \cdot r_y \in I = (f_1, \ldots, f_n), \tag{53}$$

where $\deg\left(s_y\right) \leq \deg\left(x^\gamma\right)$. Now we transform again to univariate polynomials in y via the LEX Gröbner basis. Obviously, $r_y \equiv y^q - y \mod I$, and the univariate degree of $y \cdot x^\gamma + s_y$ can again be computed by Proposition 4.6 $\deg\left(\hat{f}_\gamma\right) = \prod_{i=1}^{n} d_i - \prod_{i=1}^{j} d_i + 1$. Provided that

$$\begin{aligned} \prod_{i=1}^{n} d_i - \prod_{i=1}^{j} d_i + 1 + \deg\left(\gcd\left(y^q - y, \tilde{f}_{n+1}\right)\right) &< \prod_{i=1}^{n} d_i \\ \Leftrightarrow \deg\left(\gcd\left(y^q - y, \tilde{f}_{n+1}\right)\right) &< \prod_{i=1}^{j} d_i - 1 \end{aligned} \tag{54}$$

we can then again construct a contradiction via the greatest common divisor. Under these additional assumptions one then has the lower bound

$$d_{\mathcal{F}} \geq \deg(r_y) + \sum_{i=j+1}^{n} (d_i - 1) + 1. \tag{55}$$

In case of `MiMC`, if there is a unique solution for the key variable, then we obtain the lower bound

$$d_{\mathcal{F}} \geq \deg(r_y) + 2 \cdot r - 1, \tag{56}$$

and if there is less than 8 solutions for the key variable, then we obtain the lower bound

$$d_{\mathcal{F}} \geq \deg(r_y) + 2 \cdot r - 3. \tag{57}$$

8.2 Lower Bound for the Two Plain/Ciphertext Attack of Univariate Keyed Iterated Polynomial Systems

Next we turn to the attack with two plain/ciphertexts. For this lower bound we work with the degree of regularity and [CG23, Theorem 5.3].

Theorem 8.4. *Let $\mathbb{F}_q$ be a finite field, let $n \geq 1$ be an integer, and let*

$$f_1, \ldots, f_n \in \mathbb{F}_q[u_1, \ldots, u_n, y], \text{ and}$$
$$h_1, \ldots, h_n \in \mathbb{F}_q[v_1, \ldots, v_n, y]$$

be two univariate keyed iterated polynomial systems which are constructed with the same $g_1, \ldots, g_n \in \mathbb{F}_q[x, y]$ but have different plain/ciphertext pairs $(p_1, c_1), (p_2, c_2) \in \mathbb{F}_q^2$. Assume that

(i) $d_i = \deg(g_i) \geq 2$ for all $1 \leq i \leq n$,

(ii) g_i has the monomial $x_{i-1}^{d_i}$ for all $2 \leq i \leq n$, and

Then for the polynomial system $\mathcal{F} = \{f_1, \ldots, f_n, h_1, \ldots, h_n\} \subset \mathbb{F}_q[u_1, \ldots, u_n, v_1, \ldots, v_n, y]$ we have that

$$\operatorname{reg}\left(\mathcal{F}^{\text{hom}}\right) \geq 2 \cdot \left(\sum_{i=1}^{n} (d_i - 1)\right) - d_1.$$

Moreover, if $\deg(g_i) \geq d$ for all $1 \leq i \leq n$, then

$$\operatorname{reg}\left(\mathcal{F}^{\text{hom}}\right) \geq 2 \cdot n \cdot (d - 1) - d.$$

Proof. We have that $(\mathcal{F}^{\text{top}})$ is a DRL Gröbner basis since $f_1^{\text{top}} = h_1^{\text{top}}$ and that $\text{in}_{DRL}(\mathcal{F}^{\text{top}}) = \left(y^{d_1}, u_1^{d_2}, \ldots, u_{n-1}^{d_n}, v_1^{d_2}, \ldots, v_{n-1}^{d_n}\right)$, therefore

$$d_{\text{reg}}\left(\mathcal{F}^{\text{top}}\right) = d_1 - 1 + 2 \cdot \sum_{i=2}^{n} (d_i - 1) + 1 = 2 \cdot \sum_{i=1}^{n} (d_i - 1) - d_1, \tag{58}$$

and the claim follows from [CG23, Theorem 5.3]. □

Remark 8.5. Under the additional assumption that $\deg\left(S_{DRL}(f_1, h_1)\right) \geq 2$ it can also be proven that

$$d_{\mathcal{F}} \geq 2 \cdot \left(\sum_{i=1}^{n} (d_i - 1)\right) - d_1.$$

Though, it requires slightly more effort

Let us apply this theorem to MiMC.

Example 8.6 (MiMC and two plain/ciphertext pairs II)**.** Let $\mathbb{F}_q$ be a finite field of odd characteristic, let MiMC be defined over $\mathbb{F}_q$, and let r be the number of rounds. Let $(p_1, c_1), (p_2, c_2) \in \mathbb{F}_q^2$ be two different plain/ciphertext pairs given by MiMC. By Example 5.3 and Theorem 8.4 we have the following range for the Castelnuovo-Mumford regularity of this attack

$$4 \cdot r - 3 \leq \operatorname{reg}\left(\mathcal{F}^{\text{hom}}_{\texttt{MiMC},1} + \mathcal{F}^{\text{hom}}_{\texttt{MiMC},2}\right) \leq 4 \cdot r + 1.$$

Moreover, small scale experiments indicate that the solving degree of this attack is always equal to $4 \cdot r$.

8.3 Lower Bound for Feistel-$2n/n$

Recall that the DRL Gröbner basis of Feistel-MiMC, see Proposition 4.7 (1), is almost a univariate keyed iterated polynomial system. Therefore, we can utilize the same strategy as for MiMC and a field equation to prove the lower bound for Feistel-$2n/n$.

Theorem 8.7. *Let $\mathbb{F}_q$ be a finite field, let $n \geq 2$ be an integer, and let $\mathcal{F} = \{f_{L,1}, f_{R,1}, \ldots, f_{L,n}, f_{R,n}\} \subset \mathbb{F}_q[x_{L,1}, x_{R,1}, \ldots, x_{L,n-1}, x_{R,n-1}, y]$ be a keyed iterated polynomial system for Feistel-$2n/n$ such that*

(i) $d_i = \deg(f_{L,i}) \geq 2$ *for all* $1 \leq i \leq n$,

(ii) $f_{i,L}$ *has the monomial* $x_{L,i-1}^{d_i}$ *for all* $2 \leq i \leq n$,

(iii) $d_1 \leq d_n$ *and* $f_{L,n}$ *has the monomial* y^{d_n}, *and*

(iv) the greatest common divisor of the univariate polynomials in y that represent the left and the right branch have degree less than d_1.

Then

$$d_{\mathcal{F}} \geq d_n + \sum_{i=2}^{n-1} (d_i - 1).$$

Moreover, if $\deg(f_{L,i}) \geq d$ *for all* $2 \leq i \leq n$, *then*

$$d_{\mathcal{F}} \geq d + (n-2) \cdot (d-1).$$

Proof. By Assumption (i) and (ii) we can efficiently compute the DRL Gröbner basis of $\mathcal{F} \setminus \{f_{R,n}\}$ with Proposition 4.7 (1). Next we remove the linear polynomials from the Gröbner basis, we denote this downsized base with $\mathcal{G} = \{\tilde{f}_{L,1}, \ldots, \tilde{f}_{L,n}\} \subset P = \mathbb{F}_q[x_{R,2}, \ldots, x_{R,n-1}, x_{L,n-1}, y]$. Let $x^\gamma = \prod_{i=2}^{n-1} x_{R,i}^{d_i - 1}$, and let $t \in P$ be the polynomial which is obtained by substituting $x_{L,n-1} \mapsto c_R$ into $\tilde{f}_{L,n} = f_{L,n}$. Note that this substitution can be constructed via

$$t = \tilde{f}_{L,n} + \tilde{t} \cdot f_{R,n},$$

where $\tilde{t} \in \mathbb{F}_q[x_{L,n-1}, y]$ and $\operatorname{LM}_{DRL}(\tilde{t}) = x_{L,n-1}^{d_n - 1}$, and by Assumption (iii) $\deg(t) = d_n$. Now we consider the polynomial

$$s = x^\gamma \cdot S_{DRL}\left(t, \tilde{f}_{L,1}\right).$$

By Assumption (iii) $S_{DRL}(f_{L,1}, t)$ has a degree fall in d_n. For a contradiction we now assume that s does not have a degree fall in $d_s = d_n + \sum_{i=2}^{n-1} (d_i - 1)$, i.e.

$$s = \sum_{i=1}^{n} s_i \cdot \tilde{f}_{L,i} + s_{n+1} \cdot f_{R,n} \quad \Longleftrightarrow \quad (x^\gamma \cdot t - s_{n+1}) \cdot f_{R,n} = \sum_{i=1}^{n} \tilde{s}_i \cdot \tilde{f}_{L,i} \in (\mathcal{G}),$$

where $\deg\left(s_i \cdot \tilde{f}_{L,i}\right) < d_s$ for all $1 \leq i \leq n$ and $\deg\left(s_{n+1}\right) < d_s - 1$. By expanding t we can further rewrite the last equation as

$$\left(x^\gamma \cdot \tilde{t} - s_{n+1}\right) \cdot f_{R,n} \in (\mathcal{G}).$$

Without loss of generality we can assume that no monomial present in $x^\gamma \cdot \tilde{t}$ and s_{n+1} is an element of $\mathrm{in}_{DRL}(\mathcal{G})$. Note that by construction

$$\begin{aligned} \mathrm{LM}_{DRL}\left(x^\gamma \cdot \tilde{t}\right) &= x_{L,n-1}^{d_n-1} \cdot \prod_{i=2}^{n-1} x_{R,i}^{d_i-1}, \\ \deg\left(s_{n+1}\right) < d_s - 1 &= \deg\left(x^\gamma \cdot \tilde{t}\right). \end{aligned}$$

With the LEX Gröbner basis of $(\mathcal{G})$, see Proposition 4.7 (3), we now construct univariate polynomials $\hat{f}_\gamma, \hat{f}_{s_{n-1}}, \hat{f}_R, \hat{t} \in \mathbb{F}_q[y]$ such that

$$x^\gamma \equiv \hat{f}_\gamma,\ s_{n+1} \equiv \hat{f}_{s_{n+1}},\ f_{R,n} \equiv \hat{f}_R,\ \tilde{t} \equiv \hat{t} \mod (\mathcal{G}).$$

By Proposition 4.7 (6) the leading monomial of $x^\gamma \cdot \tilde{t}$ has the largest univariate degree among all monomials in $m \in P \setminus \mathrm{in}_{DRL}(\mathcal{G})$ with $\deg(m) \leq \deg\left(x^\gamma \cdot \tilde{t}\right)$, therefore by Proposition 4.7 (5)

$$\deg\left(\hat{f}_\gamma \cdot \hat{t} - \hat{f}_{s_{n+1}}\right) = \prod_{i=1}^{n} d_i - d_1.$$

Denote with $\hat{f}_L$ the univariate polynomial in the LEX Gröbner basis of $(\mathcal{G})$, this is exactly the polynomial that describes encoding in the left branch of Feistel-$2n/n$. Similar the univariate polynomial $\hat{f}_R \in \mathbb{F}_q[y]$ equivalent to $f_{R,n}$ represents encoding in the right branch of Feistel-$2n/n$. By Lemma 4.1 and elementary properties of the polynomial greatest common divisor the following equality must be true

$$\begin{aligned} f_L &= \gcd\left(\hat{f}_L, \left(\hat{f}_\gamma \cdot \hat{t} - \hat{f}_{s_{n+1}}\right) \cdot \hat{f}_R\right) \\ &= \gcd\left(\hat{f}_L, \left(\hat{f}_\gamma \cdot \hat{t} - \hat{f}_{s_{n+1}}\right) \cdot \gcd\left(\hat{f}_L, \hat{f}_R\right)\right). \end{aligned}$$

On the other hand, by Assumption (iv) $\gcd\left(\hat{f}_L, \hat{f}_R\right)$ has degree less than d_1. So with Proposition 4.7 (4) we have the following inequality

$$\begin{aligned} \deg\left(\hat{f}_L\right) = \prod_{i=1}^{n} d_i &\leq \deg\left(\left(\hat{f}_\gamma \cdot \hat{t} - \hat{f}_{s_{n+1}}\right) \cdot \gcd\left(\hat{f}_L, \hat{f}_R\right)\right) \\ &= \deg\left(\hat{f}_\gamma \cdot \hat{t} - \hat{f}_{s_{n+1}}\right) + \deg\left(\gcd\left(\hat{f}_L, \hat{f}_R\right)\right) \\ &< \prod_{i=1}^{n} d_i - d_1 + d_1 = \prod_{i=1}^{n} d_i. \end{aligned}$$

A contradiction. □

Applying the theorem to MiMC-$2n/n$ we obtain the following range on the regularity.

Example 8.8 (MiMC-2n/n II)**.** Let MiMC-$2n/n$ be defined over $\mathbb{F}_q$, and let r be the number of rounds. We construct the downsized DRL polynomial system from Proposition 4.7 $\tilde{\mathcal{F}} \cup \{f_{L,r}\}$ and embed it into the polynomial ring which has only the variables present in the system. Let $f_L, f_R \in \mathbb{F}_q[y]$ be the univariate polynomials that represent encryption

in the left and the right branch. If we consider them as random polynomials and divide them with $y - k$, where $k \in \mathbb{F}_q$ is the key, then with high probability they are coprime. Combining Example 5.4 and Theorem 8.7 we now obtain the following range for the Castelnuovo-Mumford regularity of MiMC-2n/n

$$2 \cdot r - 1 \leq \operatorname{reg}\left(\mathcal{F}^{\text{hom}}_{\texttt{MiMC-}2n/n}\right) \leq 2 \cdot r + 1.$$

Small scale experiments indicate that the solving degree of this attack is always equal to $2 \cdot r$.

Let us again compare Theorem 8.7 to Equation (50), since $\text{in}_{DRL}\left(\mathcal{F}^{\text{top}}\right) = \left(y_1^{d_1}, x_{R,2}^{d_2}, \ldots, x_{R,n-1}^{d_{n-1}}, y^{d_n}, x_{L,n-1}\right)$ we have

$$d_{\text{reg}}\left(\mathcal{F}^{\text{top}}\right) = \sum_{i=1}^{n-1}(d_i - 1) + 1. \tag{59}$$

So if $d_n > d_1$, then the bound from the theorem is an improvement.

8.4 Lower Bound for Feistel-Hash

We have seen in Proposition 4.7 and Section 5.4 that the LEX Gröbner basis of the preimage attack of Feistel-MiMC-Hash has the shape of Lemma 4.1. Further, we had to include the field equation for the variable x_2 to remove the parasitic solutions from the algebraic closure of $\mathbb{F}_q$. Consequently, to prove a lower bound on the last fall degree we have a mix of the situations in Theorems 8.1 and 8.7. At this point we expect the reader to be familiar with our techniques, therefore we just mention the polynomials for which it can be proven that they have a degree fall.

Theorem 8.9. *Let $\mathbb{F}_q$ be a finite field, let $n \geq 3$ be an integer, and let $\{f_{L,1}, f_{R,1}, \ldots, f_{L,n}, f_{R,n}\} \subset K[x_{L,1}, x_{R,1}, \ldots, x_{L,n-1}, x_{R,n-1}, x_1, x_2]$ denote the keyed iterated polynomial system for the Feistel-2n/n-Hash preimage attack*

$$\textit{Feistel-}2n/n\begin{pmatrix} x_1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ x_2 \end{pmatrix},$$

where $\alpha \in \mathbb{F}_q$. Assume that the keyed iterated polynomial system of Feistel-2n/n-Hash is such that

(i) $d_i = \deg\left(f_{L,i}\right) \geq 2$ for all $2 \leq i \leq n$,

(ii) f_i has the monomial $x_{L,i-1}^{d_i}$ for all $2 \leq i \leq n$, and

(iii) the univariate polynomial $\tilde{f} \in \mathbb{F}_q[x_2]$ of the LEX Gröbner basis of Feistel-2n/n has less than d_2 many roots in $\mathbb{F}_q$.

Then for the polynomial system $\mathcal{F} = \{f_{L,1}, f_{R,1}, \ldots, f_{L,n}, f_{R,n}, x_2^q - x_2\}$ we have that

$$d_{\mathcal{F}} \geq q + \sum_{i=3}^{n}\left(d_i - 1\right).$$

Moreover, if $\deg\left(f_{L,i}\right) \geq d$ for all $3 \leq i \leq n$, then

$$d_{\mathcal{F}} \geq q + (n-3) \cdot (d-1).$$

Sketch of proof. As a preparation one has to extend Proposition 4.7 to Feistel-Hash. To do so one sets $y = 0$ and introduces two variables x_1, x_2 and sets $p_L = x_1$, $p_R = 0$, $c_L = \alpha$, where α is the hash value, and $c_R = x_2$. Now one orders the variables as $x_{R,n-1} > x_{L,n-1} > \ldots > x_{R,1} > x_{L,1} > x_1 > x_2$ for the DRL and LEX term order. Now one can extend Proposition 4.7 (1)-(6) to Feistel-Hash.

We denote with $g \in \mathcal{G}$ the polynomial in the DRL Gröbner basis with leading monomial $y_1^{d_2}$. Let

$$x^\gamma = x_1^{d_n-1} \cdot \prod_{i=3}^{n-1} x_{R,i}^{d_i-1},$$

then the polynomial

$$s = x^\gamma \cdot S_{DRL}\left(g, y_1^q - y_1\right)$$

has a degree fall in $q + (d_n - 1) + \sum_{i=3}^{n-1}(d_i - 1)$. □

For the attacks on Feistel-MiMC-Hash we now obtain the following regularity ranges.

Example 8.10 (Feistel-MiMC-Hash preimage attack II)**.** Let Feistel-MiMC-Hash be defined over $\mathbb{F}_q$, and let r be the number of round. Under the assumptions of Theorem 8.9 we obtain with Example 5.5 the following range for the Castelnuovo-Mumford regularity of the Feistel-MiMC-Hash preimage attack together with a field equation

$$q + 2 \cdot r - 6 \leq \operatorname{reg}\left(\mathcal{F}_{\text{preimage}}^{\text{hom}} + \left(x_2^q - x_2 \cdot x_0^{q-1}\right)\right) \leq q + 2 \cdot r - 2.$$

Small scale experiments indicate that the solving degree of the preimage attack is always equal to $q + 2r - 3$.

Like for MiMC and the field equation we can replace $x_2^q - x_2$ by its remainder and obtain a lower bound on $d_{\mathcal{F}}$ via Equation (50).

9 Discussion

In this paper we utilized a rigorous mathematical framework to prove Gröbner basis complexity estimates for various AO designs. For Hades and the GMiMC family we proved that the Gröbner basis cryptanalysis of these designs is indeed mathematically sound. Our analysis of the MiMC family revealed that for mildly overdetermined systems we can compute small ranges for the Castelnuovo-Mumford regularity, hence putting a limit on the capabilities of regularity-based solving degree estimates. Arguably, since our regularity/solving degree estimates for MiMC polynomial systems that involve field equations exceed the size of the underlying field, these bounds do not have direct cryptographic implications. Instead, they should be viewed as showcase that for well-behaved cryptographic polynomial systems provable upper as well as lower bounds for the regularity are achievable. Moreover, as we discussed below Examples 5.1 and 8.3 these bounds can be significantly improved via an auxiliary division by remainder computation. The reason why we did not work with the remainder directly is quite simple: For every possible MiMC instantiation and plain/ciphertext sample the remainder polynomial is different. So unless one can reveal structural properties of the remainder polynomial one has to do an individual analysis for every possible instantiation. On the other hand, by working with the field equation itself we could keep our analysis generic.

To the best of our knowledge this paper is the first time that AO Gröbner basis analysis has been performed without evasion to assumptions and hypotheses that could fail in practice. Of course, from an AO designer's point of view this raises whether more advanced AO primitives are also provable in generic coordinates. We point out that recent designs

like `Reinforced Concrete` [GKL+22], `Anemoi` [BBC+23], Griffin [GHR+23] and Arion [RST23] have deviated heavily from classical design strategies, and these deviations seem to be in conflict with elementary applications of the Caminata-Gorla technique. For example one of the `Reinforced Concrete` permutations over $\mathbb{F}_p$ is of the form

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1^d \\ x_2 \cdot \left(x_1^2 + \alpha_1 \cdot x_1 + \beta_1\right) \\ x_3 \cdot \left(x_2^2 + \alpha_2 \cdot x_2 + \beta_2\right) \end{pmatrix}, \tag{60}$$

where $d \in \mathbb{Z}_{>1}$ such that $\gcd(d, p-1) = 1$ and $\alpha_i, \beta_i \in \mathbb{F}_p$ are such that $\alpha_i^2 - 4 \cdot \beta_i$ are non-squares in $\mathbb{F}_p$. Let us naively apply the Caminata-Gorla technique for this permutation. After homogenizing it and substituting $x_0 = 0$ we yield that $x_1^d = x_2 \cdot x_1^2 = x_3 \cdot x_2^2 = 0$, but it is not true that $x_1 = x_2 = x_3 = 0$ is the only solution over $\overline{\mathbb{F}_p}$ to these equations. Hence, our proving technique for generic coordinates fails. We also want to point out that we face a similar situation for Griffin and Arion.

For all our regularity lower bounds we were given a DRL Gröbner basis together with an additional polynomial. Via careful analysis of the arithmetic of the polynomial systems we could then discover polynomials with degree falls. Of course, we would like to provide lower bounds in the presence of two or more additional equations. Our readers might also recall that the attack on `MiMC` with all field equations was missing in Section 8. From small scale experiments we raise the following conjecture for this attack.

Conjecture 9.1. *Let $\mathbb{F}_q$ a finite field. Let $\mathcal{F} = \{f_1, \ldots, f_n\} \subset P = \mathbb{F}_q[x_1, \ldots, x_{n-1}, y]$ be a keyed iterated system of polynomials such that*

(i) $d_i = \deg(f_i) \geq 2$ for all $1 \leq i \leq n$, and

(ii) f_i has the monomial $x_{i-1}^{d_i}$ for all $2 \leq i \leq n$.

Let $F \subset P$ be the ideal of all field equations. Further, assume that

(iii) $(F) \not\subset (f_1, \ldots, f_n)$, and

(iv) the univariate LEX polynomial has less than d_1 many roots in $\mathbb{F}_q$.

Then the polynomial

$$\left(\prod_{i=1}^{n-1} x_i\right) \cdot S_{DRL}(f_1, y^q - y)$$

has a degree fall for the polynomial system $\mathcal{F} + F$.

We expect that a resolution to this `MiMC` problem will also reveal insight into the more general cryptographic polynomial systems.

Acknowledgments

The author would like to thank the anonymous reviewers at ToSC for their valuable comments and helpful suggestions which improved both the quality and presentation of this paper. The author would like to thank Arnab Roy for his suggestion to study Gröbner basis attacks on Arithmetization-Oriented designs. Matthias Steiner has been supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 725042).

References

[AAB+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. Design of symmetric-key primitives for advanced cryptographic protocols. *IACR Trans. Symm. Cryptol.*, 2020(3):1–45, 2020. doi:10.13154/tosc.v2020.i3.1-45.

[ACG+19] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Algebraic cryptanalysis of STARK-friendly designs: Application to MARVELlous and MiMC. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 371–397. Springer, Heidelberg, December 2019. doi:10.1007/978-3-030-34618-8_13.

[AD18] Tomer Ashur and Siemen Dhooghe. MARVELlous: a STARK-friendly family of cryptographic primitives. Cryptology ePrint Archive, Report 2018/1098, 2018. https://eprint.iacr.org/2018/1098.

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce, November 2001.

[AGP+19a] Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. Feistel structures for MPC, and more. In Kazue Sako, Steve Schneider, and Peter Y. A. Ryan, editors, *ESORICS 2019, Part II*, volume 11736 of *LNCS*, pages 151–171. Springer, Heidelberg, September 2019. doi:10.1007/978-3-030-29962-0_8.

[AGP+19b] Martin R. Albrecht, Lorenzo Grassi, Leo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. Feistel structures for MPC, and more. Cryptology ePrint Archive, Report 2019/397, 2019. https://eprint.iacr.org/2019/397.

[AGR+16] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 191–219. Springer, Heidelberg, December 2016. doi:10.1007/978-3-662-53887-6_7.

[ARS+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. Ciphers for MPC and FHE. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 430–454. Springer, Heidelberg, April 2015. doi:10.1007/978-3-662-46800-5_17.

[AW21] Josh Alman and Virginia Vassilevska Williams. A refined laser method and faster matrix multiplication. In Dániel Marx, editor, *32nd SODA*, pages 522–539. ACM-SIAM, January 2021. doi:10.1137/1.9781611976465.32.

[BBC+23] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems. New design techniques for efficient arithmetization-oriented hash functions: Anemoi permutations and Jive compression mode. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part III*, volume 14083 of *LNCS*, pages 507–539. Springer, Heidelberg, August 2023. doi:10.1007/978-3-031-38548-3_17.

[BBLP22] Augustin Bariant, Clémence Bouvier, Gaëtan Leurent, and Léo Perrin. Algebraic attacks against some arithmetization-oriented primitives. *IACR Trans. Symm. Cryptol.*, 2022(3):73–101, 2022. doi:10.46586/tosc.v2022.i3.73-101.

[BDPV07] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Sponge functions. Ecrypt Hash Workshop, 2007. URL: https://keccak.team/files/SpongeFunctions.pdf.

[BDPV08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 181–197. Springer, Heidelberg, April 2008. doi:10.1007/978-3-540-78967-3_11.

[BFS04] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

[BG01] Isabel Bermejo and Philippe Gimenez. Computing the Castelnuovo–Mumford regularity of some subschemes of $\mathbb{P}_k^n$ using quotients of monomial ideals. *J. Pure Appl. Algebra*, 164(1):23–33, 2001. doi:10.1016/S0022-4049(00)00143-2.

[BPW06] Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann. A zero-dimensional Gröbner basis for AES-128. In Matthew J. B. Robshaw, editor, *FSE 2006*, volume 4047 of *LNCS*, pages 78–88. Springer, Heidelberg, March 2006. doi:10.1007/11799313_6.

[BS87] David Bayer and Michael Stillman. A criterion for detecting m-regularity. *Invent. Math.*, 87(1):1–11, 2 1987. doi:10.1007/BF01389151.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Universität Innsbruck, 1965.

[CG21] Alessio Caminata and Elisa Gorla. Solving multivariate polynomial systems and an invariant from commutative algebra. In Jean-Claude Bajard and Alev Topuzoğlu, editors, *Arithmetic of Finite Fields - 8th International Workshop, WAIFI 2020, Rennes, France, July 6-8, 2020, Revised Selected and Invited Papers*, volume 12542 of *Lecture Notes in Computer Science*, pages 3–36, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-68869-1_1.

[CG22] Alessio Caminata and Elisa Gorla. Solving multivariate polynomial systems and an invariant from commutative algebra, 2022. Version: 7. arXiv:1706.06319.

[CG23] Alessio Caminata and Elisa Gorla. Solving degree, last fall degree, and related invariants. *J. Symb. Comput.*, 114:322–335, 2023. doi:10.1016/j.jsc.2022.05.001.

[Cha07] Marc Chardin. Some results and questions on Castelnuovo-Mumford regularity. In Irena Peeva, editor, *Syzygies and Hilbert Functions*, volume 254 of *Lecture Notes in Pure and Applied Mathematics*, pages 1–40. Chapman and Hall/CRC, 2007.

[CJ06] Thomas M. Cover and Thomas A. Joy. *Elements of Information Theory.* John Wiley & Sons, Ltd, Hoboken, New Jersey, 2 edition, 2006. doi:10.1002/0471200611.

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 4 edition, 2015. doi:10.1007/978-3-319-16721-3.

[DES77] Data encryption standard. National Bureau of Standards, NBS FIPS PUB 46, U.S. Department of Commerce, January 1977.

[DGGK21] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters. Ciminion: Symmetric encryption based on Toffoli-gates over large finite fields. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 3–34. Springer, Heidelberg, October 2021. doi:10.1007/978-3-030-77886-6_1.

[DR20] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer Berlin, Heidelberg, 2 edition, 2020. doi:10.1007/978-3-662-60769-5.

[DS13] Jintai Ding and Dieter Schmidt. Solving degree and degree of regularity for polynomial systems over a finite fields. In Marc Fischlin and Stefan Katzenbeisser, editors, *Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday*, pages 34–49, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. doi:10.1007/978-3-642-42001-6_4.

[Eis05] David Eisenbud. *The Geometry of Syzygies: A Second Course Commutative Algebra and Algebraic Geometry*. Springer New York, 1 edition, 2005. doi:10.1007/b137572.

[Fau99] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *J. Pure Appl. Algebra*, 139(1):61–88, 1999. doi:10.1016/S0022-4049(99)00005-5.

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, page 75–83. Association for Computing Machinery, 2002. doi:10.1145/780506.780516.

[FGHR14] Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, and Guénaël Renault. Sub-cubic change of ordering for Gröbner basis: A probabilistic approach. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, page 170–177, New York, NY, USA, 2014. Association for Computing Machinery. doi:10.1145/2608628.2608669.

[FGLM93] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comput.*, 16(4):329–344, 1993. doi:10.1006/jsco.1993.1051.

[FM17] Jean-Charles Faugère and Chenqi Mou. Sparse FGLM algorithms. *J. Symb. Comput.*, 80:538–569, 2017. doi:10.1016/j.jsc.2016.07.025.

[FP19] Jean-Charles Faugère and Ludovic Perret. Algebraic attacks against `stark`-friendly ciphers. Appearing as Appendix A in https://eprint.iacr.org/2020/948, 2019. Version 1.2.

[Frö85] Ralf Fröberg. An inequality for Hilbert series of graded algebras. *Math. Scand.*, 56:117–144, 12 1985. doi:10.7146/math.scand.a-12092.

[Gao09] Sicun Gao. Counting zeros over finite fields using Gröbner bases. Master's thesis, Carnegie Mellon University, 2009. URL: https://www.cs.cmu.edu/~sicung/papers/MS_thesis.pdf.

[GHR+23] Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang. Horst meets fluid-SPN: Griffin for zero-knowledge applications. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part III*, volume 14083 of *LNCS*, pages 573–606. Springer, Heidelberg, August 2023. doi:10.1007/978-3-031-38548-3_19.

[GKL+22] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. Reinforced concrete: A fast hash function for verifiable computation. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *ACM CCS 2022*, pages 1323–1335. ACM Press, November 2022. doi:10.1145/3548606.3560686.

[GKR+21] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. In Michael Bailey and Rachel Greenstadt, editors, *USENIX Security 2021*, pages 519–535. USENIX Association, August 2021.

[GKRS22] Lorenzo Grassi, Dmitry Khovratovich, Sondre Rønjom, and Markus Schofnegger. The Legendre symbol and the modulo-2 operator in symmetric schemes over $\mathbb{F}_p^n$: Preimage attack on full Grendel. *IACR Trans. Symm. Cryptol.*, 2022(1):5–37, 2022. doi:10.46586/tosc.v2022.i1.5-37.

[GKS23] Lorenzo Grassi, Dmitry Khovratovich, and Markus Schofnegger. Poseidon2: A faster version of the poseidon hash function. In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, *AFRICACRYPT 23*, volume 14064 of *LNCS*, pages 177–203. Springer Nature, July 2023. doi:10.1007/978-3-031-37679-5_8.

[GLR+19] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. On a generalization of substitution-permutation networks: The HADES design strategy. Cryptology ePrint Archive, Report 2019/1107, 2019. https://eprint.iacr.org/2019/1107.

[GLR+20] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. On a generalization of substitution-permutation networks: The HADES design strategy. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 674–704. Springer, Heidelberg, May 2020. doi:10.1007/978-3-030-45724-2_23.

[GMP22] Elisa Gorla, Daniela Mueller, and Christophe Petit. Stronger bounds on the cost of computing gröbner bases for HFE systems. *J. Symb. Comput.*, 109:386–398, 2022. doi:10.1016/j.jsc.2020.07.011.

[GØSW23] Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, and Roman Walch. From farfalle to megafono via ciminion: The PRF hydra for MPC applications. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part IV*, volume 14007 of *LNCS*, pages 255–286. Springer, Heidelberg, April 2023. doi:10.1007/978-3-031-30634-1_9.

[Gre98] Mark L. Green. Generic initial ideals. In J. Elias, J. M. Giral, R. M. Miró-Roig, and S. Zarzuela, editors, *Six Lectures on Commutative Algebra*, pages 119–186, Basel, 1998. Birkhäuser Basel. doi:10.1007/978-3-0346-0329-4_2.

[Has12] Amir Hashemi. Efficient computation of Castelnuovo-Mumford regularity. *Math. Comput.*, 81(278):1163–1177, 2012. doi:10.1090/S0025-5718-2011-02515-9.

[HKY15] Ming-Deh A. Huang, Michiel Kosters, and Sze Ling Yeo. Last fall degree, HFE, and Weil descent attacks on ECDLP. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 581–600. Springer, Heidelberg, August 2015. doi:10.1007/978-3-662-47989-6_28.

[HKYY18] Ming-Deh A. Huang, Michiel Kosters, Yun Yang, and Sze Ling Yeo. On the last fall degree of zero-dimensional Weil descent systems. *J. Symb. Computat.*, 87:207–226, 2018. doi:10.1016/j.jsc.2017.08.002.

[HSS18] Amir Hashemi, Michael Schweinfurter, and Werner M. Seiler. Deterministic genericity for polynomial ideals. *J. Symb. Computat.*, 86:20–50, 2018. doi:10.1016/j.jsc.2017.03.008.

[Kem11] Gregor Kemper. *A Course in Commutative Algebra*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 1 edition, 2011. doi:10.1007/978-3-642-03545-6.

[KR05] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1 edition, 2005. doi:10.1007/3-540-28296-3.

[Laz83] Daniel Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In J. A. van Hulzen, editor, *Computer Algebra, EUROCAL '83, European Computer Algebra Conference, London, England, March 28-30, 1983, Proceedings*, volume 162 of *Lecture Notes in Computer Science*, pages 146–156. Springer Berlin Heidelberg, 1983. doi:10.1007/3-540-12868-9_99.

[Leo06] V. K. Leont'ev. Roots of random polynomials over a finite field. *Math. Notes*, 80(1):300–304, 07 2006. doi:10.1007/s11006-006-0139-y.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Encyclopedia of mathematics and its applications. Cambridge Univ. Press, Cambridge, 2 edition, 1997.

[LP19] Chaoyun Li and Bart Preneel. Improved interpolation attacks on cryptographic primitives of low algebraic degree. In Kenneth G. Paterson and Douglas Stebila, editors, *SAC 2019*, volume 11959 of *LNCS*, pages 171–193. Springer, Heidelberg, August 2019. doi:10.1007/978-3-030-38471-5_8.

[Par10] Keith Pardue. Generic sequences of polynomials. *J. Algebra*, 324(4):579–590, 2010. doi:10.1016/j.jalgebra.2010.04.018.

[RST23] Arnab Roy, Matthias Johann Steiner, and Stefano Trevisani. Arion: Arithmetization-oriented permutation and hashing from generalized triangular dynamical systems, 2023. Version: 3. arXiv:2303.04639.

[SS21] Jan Ferdinand Sauer and Alan Szepieniec. SoK: Gröbner basis algorithms for arithmetization oriented ciphers. Cryptology ePrint Archive, Report 2021/870, 2021. https://eprint.iacr.org/2021/870.

[Sto00] Arne Storjohann. *Algorithms for matrix canonical forms*. Doctoral thesis, ETH Zurich, Zürich, 2000. Diss., Technische Wissenschaften ETH Zürich, Nr. 13922, 2001. doi:10.3929/ethz-a-004141007.