Exploring the Six Worlds of Gröbner Basis Cryptanalysis: Application to Anemoi

Katharina Koschatko, Reinhard Lüftenegger, and Christian Rechberger

Graz University of Technology (Austria)
firstname.lastname@iaik.tugraz.at

Abstract. Gröbner basis cryptanalysis of hash functions and ciphers, and their underlying permutations, has seen renewed interest recently. Anemoi (Crypto'23) is a permutation-based hash function that is arithmetization-friendly, i.e., efficient for a variety of arithmetizations used in zero-knowledge proofs. In this paper, exploring both theoretical bounds as well as experimental validation, we present new complexity estimates for Gröbner basis attacks on the Anemoi permutation over prime fields.

We cast our findings in what we call the six worlds of Gröbner basis cryptanalysis. As an example, keeping the same security arguments of the design, we conclude that at least 23/45 instead of 17/33 rounds would need to be used for 128/256-bit security before adding a security margin.

Keywords: Algebraic Cryptanalysis · Arithmetization-Friendly Hash Functions · Gröbner Basis Attack · Anemoi · Multihomogeneous Bézout.

1 Introduction

The idea of solving systems of polynomial equations that stem from problems in block cipher or hash function cryptanalysis by means of symbolic computation has a decades-long tradition. Such means include, among others, Gröbner basis techniques or polynomial factorization.

Symbolic computation approaches for cryptanalysis of block ciphers and hash functions saw a major wave of attention around the time Rijndael was standardized as AES and the years afterwards [CP02; CMR05; AC09; CL05; SKP+07], albeit with an unclear impact on designs at that time. More recently, however, such approaches have been having more impact on new designs, especially in the area of MPC/FHE/ZK-friendly ciphers and hashing. Examples include Gröbner basis attacks on Friday and Jarvis [ACG+19a; FP22], attacks on MiMC combining higher-order differential distinguishers with polynomial factorization [EGL+20; BCP23; LP19; RAS20], and an attack on Grendel [GKR+22b] leveraging polynomial factorization.

A recurring theme in recent works that propose designs in symmetric cryptography for encryption or hashing is the *choice of a secure number of rounds.* Usually, all known attack vectors are considered, and the most performant one determines a secure number of rounds, including a certain security margin. Recent arithmetization-friendly designs often assume Gröbner basis cryptanalysis to be the most crucial attack vector. This assertion seems sound since often better understood statistical and other algebraic attacks cover fewer rounds. However, estimating the complexity of Gröbner basis attacks is, in general, difficult. We briefly review the state-of-the-art approach for Gröbner basis cryptanalysis in Section 1.1. Immediately afterwards, we outline our contributions and discuss a concrete application to Anemoi in Section 1.2. Anemoi [BBC+23] is a permutation-based hash function that is arithmetization-friendly, i.e., efficient for a variety of arithmetizations used in zero-knowledge proofs.

1.1 The Common Approach of Gröbner Basis Attacks

Conceptually, using Gröbner bases in cryptanalysis comprises two steps.

(I) Modeling a cryptographic primitive as a system of polynomial equations with unknown parameters as variables. A parameter of interest might be the secret key of a block cipher, a solution to the CICO problem of a permutation, or the preimage of a given hash value. Often, it is possible to describe the same primitive using different models.

(II) Solving the system of polynomial equations using Gröbner basis techniques.

We note that equation systems stemming from problems in symmetric cryptography often have a finite number of solutions. Hence, we usually deal with equation systems that generate a zero-dimensional ideal, see Definition 3. In step (II), “solving” commonly means finding exactly one solution. Step (II) encompasses a triad of computations, namely,

(1) computing a *degree reverse lexicographic* (`DRL`) Gröbner basis using an off-the-shelf Gröbner basis algorithm such as, e.g., F4 [Fau99],

(2) converting the `DRL` Gröbner basis (of a zero-dimensional ideal) to the (reduced) *lexicographic* (`LEX`) Gröbner basis using a conversion algorithm such as the FGLM algorithm [FGL+93],

(3) factorizing the (unique) univariate polynomial in the (reduced) `LEX` Gröbner basis using a polynomial factoring algorithm such as a fast version of Cantor-Zassenhaus [KS98]. The roots of the univariate polynomial determine partial solutions of the equation system. If needed, back-substitute any partial solution into the other equations from the `LEX` Gröbner basis to obtain (a candidate for) a full solution.

A Gröbner basis attack reduces the problem of multivariate root finding to the problem of univariate root finding. This can be seen as follows: a (reduced) `LEX` Gröbner basis is in triangular form [Bar04], much like the reduced row echelon form after Gaussian elimination yields a matrix in triangular form. This means that a (reduced) `LEX` basis always contains a univariate polynomial, which we can factor (step *(3)*). In practice, instead of directly computing a `LEX` Gröbner basis, it is faster to compute a Gröbner basis with respect to a fast[1] monomial order, usually the `DRL` order (step *(1)*), and then convert the `DRL` Gröbner basis to a `LEX` basis using a conversion algorithm (step *(2)*).

1.2 Our Contribution Cast into the Six Worlds of Gröbner Basis Cryptanalysis

As discussed above, we have three distinct steps: *(1)* computing the Gröbner basis, *(2)* converting it, and *(3)* the final solving step. Depending on the choice of the algebraic model, usually either *(1)* or *(2)* has a higher complexity and, hence, informs the choice of the number of rounds. An exceptional case happens when very aggressive (i.e., optimistic from an attacker's point of view) assumptions about complexity estimates of *(1)* and *(2)* are made, or, when the algebraic model directly yields a Gröbner basis, without any computation. In this case, *(3)* can remain the most expensive step.

For each of these steps, there are (E) experimental and (T) theoretical approaches to determine their complexity in terms of computational effort. In total, these six approaches give rise to what we call the *six worlds of Gröbner basis cryptanalysis*. Establishing complexity estimates for each of these six worlds contributes to a more comprehensive understanding of Gröbner basis cryptanalysis and, thus, offers better guidance for choosing a secure number of rounds or evaluating an attack's performance. Our contributions extend existing and offer new methods to assess the hardness of steps *(1)*, and *(2)*. In that capacity, we discuss a new search approach for variable orderings, effectively minimizing the cost of step *(1)* among all tested variable orderings. Furthermore, we extend results in [Wam92; BGL20a] and leverage multihomogeneous Bézout theory to estimate the complexity of converting between Gröbner bases in *(2)*. Similarly to step *(1)*, we employ a search approach for variable set partitions that minimizes the multihomogeneous Bézout bound, hence minimizing the estimated cost of step *(2)* among all tested variable set partitions, see Section 3.3. Our discussion of these six worlds is reflected in a refined methodology for Gröbner basis cryptanalysis, which we present in Section 3.1.

As a concrete application of our refined methodology, we analyze the Anemoi permutation [BBC+23] instantiated over prime fields in Section 4. Our findings indicate that to uphold the asserted security level, it is necessary to increase the number of rounds in various full-round instances of Anemoi. Table 1 summarizes our findings in the six worlds for the popular choice of using $\alpha = 3$ as the degree of the power map in the S-box function and gives a comparison with previous analysis results in [BBC+23].
Under the assumption that none of the steps in the Gröbner basis attack are trivial, Table 1 and the six worlds are interpreted as follows:

(E) In the experimental world, results are to be understood as a lower bound on the number of rounds to reach the targeted security level against a particular step in the Gröbner basis attack.

[1] 'Fast' is to be understood heuristically here.

Table 1. The Six Worlds of Gröbner Basis Cryptanalysis to derive round numbers. Application to Anemoi : $\mathbb{F}_p^2 \to \mathbb{F}_p^2$ for the case $\alpha = 3$, with $\omega = 2$. The numbers in brackets $(\cdot)$ denote results derived from previous work.

		(E) **Experimental approach**			(T) **Theoretical approach**		
s	[BBC+23]	*(1)* GB	*(2) FGLM*	*(3) FAC*	*(1) GB*	*(2) FGLM*	*(3) FAC*
128	21	23 (17)	27 (27)	31 (?)	? (?)	23 (20)	26 (?)
256	37	45 (33)	54 (54)	61 (?)	? (?)	45 (40)	51 (?)

(T) In the theoretical world, round numbers below the given values are proven to be insecure since they evidentially do not reach the asserted security level against a particular step in the Gröbner basis attack. Implicitly, this also yields a lower bound on the number of rounds.

The previous analysis of Anemoi assumed to live in world (E1) and arrived at 17/33 rounds for a security level of 128/256 bits. After adding security margins for each security level, 21/37 rounds were proposed. Due to our new variable ordering, we have arrived at a necessary round number of 23/45 already for world (E1). If instead of experimental extrapolation, more theoretical, rigorous results are preferred, our improved upper bounds for the *FGLM* step (i.e., world (T2)) also imply that round numbers below 23/45 are insufficient to reach the targeted security level. See Section 4 for more details. Previous analysis has not covered worlds (E3) and (T3). Our analysis, however, also considers these worlds and presents a more complete picture. Especially the fact that our security analysis discovered a shape position structure (cf. Definition 4) provides strong evidence for arguing the complexity of step *(3)*. Neither previous analysis nor our work discusses dedicated theoretical results for (T1) (that go beyond genericity assumptions such as regular sequences). We deem this to be an important open problem.

1.3 Open Problems

A natural question to ask is the following: Given that the new methods lead to new results on Anemoi, could other designs that exhibit similar properties, such as Griffin [GHR+23] or Arion [RST23], and perhaps to a lesser extent also Poseidon [GKR+21] or Rescue [AAB+20] be affected? Also beyond the area of arithmetization-friendly hashing, there are potential targets, e.g., big-field FHE-friendly permutation-based symmetric encryption [DGH+23; HKC+20; HKL+22], and MPC-friendly big field designs [GLR+20b; AGR+16; DGG+21; GØS+23].

Furthermore, studying more dedicated Gröbner basis algorithms exploiting structures in the algebraic systems might be fruitful. In particular, this could allow to (1) derive even tighter upper bounds and, potentially, also meaningful lower bounds and (2) get a more concrete idea of the actual solving complexity.

2 Preliminaries

We present an outline of essential results in the context of solving equation systems with Gröbner basis techniques. Equation systems stemming from problems in symmetric cryptography most often have a finite number of solutions (over the algebraic closure). Expressed in commutative algebra lingo, this means the equation system generates a zero-dimensional ideal.[2] While some of the more general results in this section are valid for any ideal, we are primarily interested in the zero-dimensional case. One major focus point of our outline deals with bounds on the number of solutions of (zero-dimensional) equation systems[3] and, in that capacity, discusses the classical Bézout bound. This discussion prepares the ground for our motivation of the multihomogeneous Bézout bound in Section 3.3. A tight bound on the number of solutions, in turn, is an important determinant for the complexity of step *(2)* and *(3)* in Gröbner basis cryptanalysis.

In the following, $\mathbb{F}$ denotes a field. All results in this section hold for any field. We note, however, that the most relevant case for equation systems stemming from problems in symmetric cryptography is the case of finite fields. In general, we use $\mathbb{F}[x_1, \dots, x_n]$ to denote the polynomial ring over $\mathbb{F}$ in the n indeterminates $x_1, \dots, x_n$. Sometimes, it is convenient to emphasize the connection between the number of variables n_v in an equation system and the polynomial ring over which this system lives. In this case, we presume to write $\mathbb{F}[x_1, \dots, x_{n_v}]$. For a more comprehensive introduction to background results, we recommend the excellent textbooks [CLO15; KR00; KR05].

From a geometric perspective, the set of solutions to an equation system defined by m polynomials over a field in n variables

$$f_1(x_1, \dots, x_n) = \dots = f_m(x_1, \dots, x_n) = 0,$$

is given by the *variety* of the ideal generated by $f_1, \dots, f_m$.

Definition 1 (Affine variety). *Let $m, n \in \mathbb{N}$, and let $\mathcal{I} = \langle f_1, \dots, f_m \rangle$ be an ideal in $\mathbb{F}[x_1, \dots, x_n]$. The set*

$$V(\mathcal{I}) = V(f_1, \dots, f_m) \coloneqq \{z \in A^n(\mathbb{F}) \, : \, f_i(z) = 0 \;\; \forall \, 1 \leq i \leq m\}$$

is called the affine variety *of the ideal $\mathcal{I}$, where $A^n(\mathbb{F}) = \mathbb{F}^n$ denotes the n-dimensional affine space over $\mathbb{F}$. For any field $\mathbb{F}'$ with $\mathbb{F} \subset \mathbb{F}'$ we denote by $V_{\mathbb{F}'}(\mathcal{I})$ the set of solutions over $A^n(\mathbb{F}')$. In particular, $V_{\bar{\mathbb{F}}}(\mathcal{I})$ denotes the variety of $\mathcal{I}$ over the algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}$.*

The variety of an ideal is independent of the actual choice of the generating set, i.e., if $\mathcal{I} = \langle f_1, \dots, f_m \rangle = \langle g_1, \dots, g_k \rangle$, then $V(f_1, \dots, f_m) = V(g_1, \dots, g_k)$. To reason about $V(\mathcal{I})$, switching to a different generating set of the ideal is often advantageous. One important subclass of generating sets is the class of *Gröbner bases.*

[2] In particular, this is also the case for our algebraic model of Anemoi.

[3] If an equation system generates a zero-dimensional ideal, we also informally say the equation system itself is zero-dimensional.

Definition 2 (Gröbner basis). *Let $\mathcal{I} = \langle f_1, \dots, f_m \rangle \subset \mathbb{F}[x_1, \dots, x_n]$ be an ideal. A* Gröbner basis *for $\mathcal{I}$ with respect to a fixed monomial ordering $\succ$ is a subset $G = \{g_1, \dots, g_t\} \subseteq \mathcal{I}$ with the property*

$$\langle \mathrm{LM}(g_1), \dots, \mathrm{LM}(g_t) \rangle = \langle \mathrm{LM}(\mathcal{I}) \rangle,$$

where $\mathrm{LM}(\cdot)$ *denotes the largest monomial (also called leading monomial) of a polynomial with respect to $\succ$.*

Two of the most prominent monomial orderings in practice are the *lexicographic* (LEX) and the *degree reverse lexicographic* (DRL) ordering, see [CLO15]. For every nonzero ideal $\mathcal{I} \subset \mathbb{F}[x_1, \dots, x_n]$ and every fixed monomial ordering $\succ$ there exists a unique *reduced* Gröbner basis G. Here, reduced means that every $g \in \mathrm{G}$ is monic and no monomial of g is divisible by any of $\mathrm{LM}(G \setminus \{g\})$. An important property of Gröbner bases is that polynomial division modulo a Gröbner basis yields unique division remainders, see [CLO15, §6, Prop. 1]. This, in turn, allows us to uniquely represent residue classes in the quotient ring $\mathbb{F}[x_1, \dots, x_n] / \mathcal{I}$ by division remainders modulo G, where G is a Gröbner basis of $\mathcal{I}$. Moreover, a Gröbner basis G allows us to compute residue classes in the quotient ring by computing division remainders modulo G.[4] In a more technical speech, a Gröbner basis G of the ideal $\mathcal{I}$ defines an isomorphism of rings

$$\mathbb{F}[x_1, \dots, x_n] / \mathcal{I} \;\cong\; \mathbb{F}[x_1, \dots, x_n] \bmod G,$$

where $\mathbb{F}[x_1, \dots, x_n] \bmod G$ denotes the ring of all division remainders modulo G of elements in $\mathbb{F}[x_1, \dots, x_n]$. The quotient ring $\mathbb{F}[x_1, \dots, x_n] / \mathcal{I}$ is an $\mathbb{F}$-vector space, called the *quotient space.* A basis for this (potentially infinite-dimensional) vector space is given by the set of monomials[5]

$$\mathrm{B}_{\mathcal{I}} \coloneqq \{X^\alpha : X^\alpha \notin \langle \mathrm{LM}(\mathcal{I}) \rangle\} = \{X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : X^\alpha \notin \langle \mathrm{LM}(\mathrm{G}) \rangle\}.$$

The elements of $\mathrm{B}_{\mathcal{I}}$ are called *basis monomials*, and $\mathrm{B}_{\mathcal{I}}$ is called the *standard basis* of the quotient space.

Definition 3 (Zero-dimensional ideal). *Let $\mathcal{I}$ be a nonzero ideal in $R = \mathbb{F}[x_1, \dots, x_n]$, let $\succ$ be a monomial ordering, and let G be a Gröbner basis of $\mathcal{I}$ with respect to $\succ$. If the quotient space $R/\mathcal{I}$ is finite-dimensional, that is,*

$$d_{\mathcal{I}} = \dim_{\mathbb{F}}(R/\mathcal{I}) = |B_{\mathcal{I}}| < \infty,$$

then the ideal $\mathcal{I}$ is called zero-dimensional*.*

There is an essential connection between zero-dimensional ideals, its Gröbner bases, and the variety of the ideal.

[4] This does, e.g., not hold for an arbitrary ideal basis that is not a Gröbner basis.

[5] Technically speaking, the corresponding set of residue classes $\{X^\alpha + I : X^\alpha \notin \langle \mathrm{LM}(\mathcal{I}) \rangle\}$ generates the quotient space.

Theorem 1 (Finiteness Theorem, [KR00, Prop. 3.7.1]). *Let $\mathcal{I}$ be a nonzero ideal in $R = \mathbb{F}[x_1, \dots, x_n]$ and let $\succ$ be a fixed monomial ordering. The following statements are equivalent.*

1. *The $\mathbb{F}$-vector space $R/\mathcal{I}$ is finite-dimensional.*
2. *The variety $V_{\overline{\mathbb{F}}}(\mathcal{I})$ is a finite set.*
3. *For each $1 \leq i \leq n$ there is some $m_i \geq 0$ such that $x_i^{m_i} \in \langle \mathrm{LM}(\mathcal{I}) \rangle$.*
4. *Let G be a Gröbner basis for $\mathcal{I}$. Then for each $1 \leq i \leq n$ there exists some $m_i \in \mathbb{N}$ such that $x_i^{m_i} = \mathrm{LM}(g)$ for some $g \in G$.*

For zero-dimensional ideals, the number of solutions to a polynomial equation system equals the dimension of the quotient space, if counted appropriately.

Theorem 2. *Let $\mathcal{I} \subset \mathbb{F}[x_1, \dots, x_n]$ be a zero-dimensional ideal. Then there exist well-defined multiplicities*[6] *m_P at each point $P \in V_{\overline{\mathbb{F}}}(\mathcal{I})$ such that*

$$d_{\mathcal{I}} = \sum_{P \in V_{\overline{\mathbb{F}}}(\mathcal{I})} m_P.$$

That is, the number of solutions over the algebraic closure counted with multiplicities equals the dimension of the quotient space.

Ideals in *shape position* are an important subclass of zero-dimensional ideals as they have a particularly well-structured `LEX` Gröbner basis [BMM+94; FM11; BND22].

Definition 4 (Shape position). *Let $\mathcal{I} \subseteq \mathbb{F}[x_1, \dots, x_n]$ be an ideal. We say $\mathcal{I}$ is in* shape position *if the reduced `LEX` Gröbner basis of $\mathcal{I}$ has the form*

$$\{x_1 - g_1(x_n), x_2 - g_2(x_n), \dots, g_n(x_n)\},$$

where $\deg(g_i) < \deg(g_n)$ *for* $1 \leq i < n$.

An immediate consequence of an ideal $\mathcal{I}$ in $R = \mathbb{F}[x_1, \dots, x_n]$ being in shape position is the fact that [BND22]

$$d_{\mathcal{I}} = \dim_{\mathbb{F}}(R/\mathcal{I}) = \deg(g_n). \tag{1}$$

As we will discuss further in Section 3.2, $d_{\mathcal{I}}$ is an important determinant for the complexities of step *(2)* and *(3)* in a Gröbner basis attack. Therefore, by Theorem 2, (tightly) bounding the number of solutions of an equation system allows to establish (tight) bounds on the complexities of these steps. In this context, it is beneficial to resort to projective space (and, thus, to homogeneous polynomials) since this opens up a fruitful theory of counting the solutions of zero-dimensional equation systems.

[6] We do not elaborate on the intrinsics here. For a definition and discussion of (intersection) multiplicities, see [Sha13, Chapter 2 & 3].

Definition 5 (Projective space). *The n-dimensional* projective space *over a field $\mathbb{F}$, denoted by $\mathbb{P}^n(\mathbb{F})$, is the set of equivalence classes of $\mathbb{F}^{n+1} \setminus \{0\}$ under the equivalence relation*

$$\begin{aligned}(x'_0, \dots, x'_n) &\sim (x_0, \dots, x_n) \\ &\iff \exists\, \lambda \in \mathbb{F} \setminus \{0\} \,:\, (x'_0, \dots, x'_n) = \lambda \cdot (x_0, \dots, x_n)\,.\end{aligned}$$

Given an $(n+1)$-tuple $(x_0, \dots, x_n) \in \mathbb{F}^{n+1} \setminus \{0\}$, we call its equivalence class

$$p = [(x_0, \dots, x_n)]_\sim = \{\lambda \cdot (x_0, \dots, x_n) \,:\, \lambda \in \mathbb{F} \setminus \{0\}\} \in \mathbb{P}^n(\mathbb{F})$$

a projective point *and denote it by $[x_0 : \dots : x_n]$. The coordinates of such a projective point p are also called* homogeneous coordinates.

Definition 6 (Homogeneous polynomial). *$f \in \mathbb{F}[x_0, x_1, \dots, x_n]$ is called* homogeneous of degree d *if every term in f has total degree d. We denote the set of all homogeneous polynomials in $x_0, x_1, \dots, x_n$ with coefficients in $\mathbb{F}$ by $\mathbb{F}^{\mathrm{H}}[x_0, x_1, \dots, x_n]$.*

Theorem 3 (Bézout's Theorem). *Let $\mathbb{F}$ be algebraically closed and let $f_1, \dots, f_n \in \mathbb{F}^{\mathrm{H}}[x_0, x_1, \dots, x_n]$ be homogeneous polynomials of respective total degrees $d_1, \dots, d_n$. If the number of solutions in $\mathbb{P}^n(\mathbb{F})$ is finite, then the number of solutions (counted with multiplicities) of $f_1 = \dots = f_m = 0$ is given by*

$$\mathrm{B} \coloneqq \prod_{i=1}^{n} d_i.$$

Bézout's Theorem can be used to bound the quotient space dimension $d_{\mathcal{I}}$ of a zero-dimensional ideal $\mathcal{I} = \langle f_1, \dots, f_n \rangle \subset \mathbb{F}[x_1, \dots, x_n]$.

Theorem 4 (Bézout bound). *Let $\mathcal{I} = \langle f_1, \dots, f_n \rangle \subset \mathbb{F}[x_1, \dots, x_n]$ be a zero-dimensional ideal and let $d_i = \deg(f_i)$ denote the total degree of f_i, for $1 \leq i \leq n$. Then*

$$d_{\mathcal{I}} \overset{(Thm.2)}{=} \sum_{P \in V_{\overline{\mathbb{F}}}(\mathcal{I})} m_P \leq \mathrm{B}.$$

We present an outline of the proof of Theorem 4 since we deem it insightful for our later motivation of the multihomogeneous Bézout bound in Theorem 5.

Proof Sketch. Denote by f_i^{H} the *homogenization* of f_i for every $1 \leq i \leq n$, i.e.,

$$f_i^{\mathrm{H}}(x_0, \dots, x_n) \coloneqq x_0^{d_i} \cdot f_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{F}^{\mathrm{H}}[x_0, \dots, x_n]\,.$$

Given f_i^{H}, the original polynomial f_i can be recovered by setting $x_0 = 1$:

$$f_i^{\mathrm{H}}(1, x_1, \dots, x_n) = f_i(x_1, \dots, x_n).$$

Thus, every affine solution $a = (a_1, \dots, a_n) \in V_{\bar{\mathbb{F}}}(\mathcal{I})$ corresponds to a projective solution $[1 : a_1 : \cdots : a_n] \in \mathbb{P}^n\left(\bar{\mathbb{F}}\right)$ to the system defined by the homogeneous polynomials $f_1^{\text{H}}, \dots, f_n^{\text{H}} \in \mathbb{F}^{\text{H}}[x_0, x_1, \dots, x_n]$. Conversely, every projective solution in $\mathbb{P}^n\left(\bar{\mathbb{F}}\right)$ to the homogeneous polynomial equation system $f_1^{\text{H}} = \cdots = f_n^{\text{H}} = 0$ with $x_0 = 1$ recovers an affine solution of the original system. Naturally, projective solutions with $x_0 \neq 0$ are called *affine* or *finite*, while those with $x_0 = 0$ are called *solutions at infinity.*

It can be shown that if the number of solutions in $\bar{\mathbb{F}}$ is finite, that is, if $\mathcal{I}$ is zero-dimensional, then the homogenization only adds a finite number of additional solutions at infinity over $\mathbb{P}^n\left(\bar{\mathbb{F}}\right)$ [MW83]. Thus Theorem 3 can be applied. The bound is sharp if and only if the number of solutions at infinity is zero. □

Example 1 (Bézout bound). Consider $f_1, f_2, f_3 \in \mathbb{Q}[x_1, x_2, x_3]$, where

$$f_1 = x_1x_2^2 + x_1x_3^2 - x_2, \qquad f_2 = x_2 + 1, \qquad f_3 = x_1x_2^2 + 2x_2x_3^2 - 2x_3 + 1.$$

$\mathcal{I} = \langle f_1, f_2, f_3 \rangle$ is a zero-dimensional ideal in $\mathbb{Q}[x_1, x_2, x_3]$, where the quotient space dimension is given by

$$d_{\mathcal{I}} = \dim_{\bar{\mathbb{Q}}}(\mathbb{Q}[x_1, x_2, x_3]/\mathcal{I}) = \dim_{\mathbb{C}}(\mathbb{Q}[x_1, x_2, x_3]/\mathcal{I}) = 4.$$

By Theorem 2, the number of solutions to the polynomial equation system $f_1 = f_2 = f_3 = 0$, over the algebraic closure of $\mathbb{Q}$ and counted with multiplicities, is thus four. Indeed, there is one solution in $\mathbb{Q}^3$, one additional in $\mathbb{R}^3$ and two additional in $\mathbb{C}^3$. The Bézout bound (cf. Theorem 4) is given by

$$\text{B} = \deg(f_1) \cdot \deg(f_2) \cdot \deg(f_3) = 3 \cdot 1 \cdot 3 = 9.$$

Thus, there exist $9 - 4 = 5$ solutions at infinity.

3 The Six Worlds of Gröbner Basis Cryptanalysis

3.1 Refined Methodology for Gröbner Basis Attacks

Highly algebraic, round-based primitives such as Anemoi are prone to Gröbner basis attacks. The main goal of a Gröbner basis attack is to compute the reduced `LEX` Gröbner basis for a zero-dimensional ideal generated by a polynomial equation system modeling a given cryptographic primitive and, subsequently, factor the unique univariate polynomial in the reduced `LEX` Gröbner basis. We have outlined the individual steps of a Gröbner basis attack in Section 1.1.

We present a refined version of this methodology. In particular, we discuss and elaborate on the details of *(1)* and *(2)*. Our methodology suggests two perspectives for each of the steps *(1)*, *(2)*, and *(3)*: a theoretical and an experimental perspective. In total, this leads to six perspectives (or 'worlds') that a designer, as well as an attacker, may consider.

Modeling the Primitive. Represent the round-based primitive as a system of n_e polynomial equations over the underlying finite field in n_v variables. For permutations, typically the so-called *constrained-input constrained-output problem* (CICO) problem is considered [BDP+11]. To allow certain analysis strategies later on, it is advantageous to have an algebraic model where the number of equations n_e equals the number of variables n_v for every fixed round number N.

Gröbner Basis Attack on Small-Scale Variants of the Primitive. To gain insight into the hardness of the Gröbner basis attack, experiments are performed on weakened variants of the primitives. See also [CMR05] for a further discussion. This includes the *reduction of the round number* N and the *reduction of the state size* by considering smaller finite fields. However, in some cases, it might be nontrivial to properly scale down a full-scale primitive to some small-scale variant that is tractable by practical experiments.

When conducting experiments, several factors influence the performance of solving algorithms for steps *(1)*, *(2)*, and *(3)*, besides the global choice of a particular algebraic model. In the case of step *(1)*, the monomial order and the variable order within this monomial order highly affect the runtime of a Gröbner basis computation. It is known that in extreme cases, a well-chosen monomial order directly yields a Gröbner basis (without any computation) [BPW06; AAB+20]. In essence, this means that step *(1)* can be skipped, leaving only steps *(2)* and *(3)* to deal with. For step *(2)*, a similar perspective arises: although the quotient space dimension $d_{\mathcal{I}}$ is an invariant of the ideal, concrete experiments may help to understand the structure in the multiplication matrices, which also depends on the monomial order from which we convert to the `LEX` order. Therefore, as a step towards a more thorough analysis, we suggest exploring the influence of the monomial/variable order on the runtime of step *(1)* and *(2)*. For example, in our analysis on Anemoi in Section 4, we tested different variable orders and chose the most performant one for our security analysis.

Following our discussion of complexity estimates in Section 3.2, important metrics of interest during the experiments are the solving degree d_{solv}, the quotient space dimension $d_{\mathcal{I}}$, and the degree of the univariate polynomial in the reduced `LEX` Gröbner basis. We record the values of these metrics for different round numbers and establish a growth trend depending on the number of rounds. This approach provides empirical evidence for subsequent security arguments based on extrapolation. A comparison of concrete runtime results, moreover, allows for a first assessment of which step is the hardest one. We also suggest performing experiments over different field sizes to ensure that the derived results are robust and not only an artifact of a particular field choice. If the original (full-scale) field has a particular structure, the small-scale fields should (as closely as possible) resemble this structure.

Security analysis. For a targeted security level of s bits, the number of rounds N has to be chosen such that $N \geq N^*$, where

$$N^* = \min \left\{ N \in \mathbb{N} \, : \, \mathcal{C}_{\text{alg}}(N) \geq 2^s \right\}. \tag{2}$$

Here, $\mathcal{C}_{\mathrm{alg}} \in \{\mathcal{C}_{\mathrm{GB}}, \mathcal{C}_{\mathrm{FGLM}}, \mathcal{C}_{\mathrm{FAC}}\}$ denotes the algebraic complexity (cf. Section 3.2) of the corresponding step in the Gröbner basis attack. The (E) *experimental estimation* and (T) *theoretical approximation* of these determinants give rise to what we call the *six worlds of Gröbner basis cryptanalysis.* Our security analysis discusses different suggestions for N^* when based on the hardness of solving *(1)*, *(2)*, and *(3)*, respectively.

Exploring the Six Worlds of Gröbner Basis Cryptanalysis. For the concrete instantiation of the complexities, different approaches can be taken:

(E) *Experimental approach*: Computing d_{solv} and $d_{\mathcal{I}}$ is, in general, as difficult as computing the Gröbner basis. By performing Gröbner basis attacks on small-scale variants, d_{solv}, and $d_{\mathcal{I}}$ are retrieved for round-reduced systems. Estimates can be made from these values for d_{solv} and $d_{\mathcal{I}}$. While in some cases, a clear structure evolves (see, for example, Conjecture 2 for $d_{\mathcal{I}}$ in Anemoi), often only bounds or approximations based on very few data points can be given. From a designer's perspective, it is common practice to use lower bounds, thus potentially underestimating the respective complexities and, in turn, overestimating N^* as stated in Equation (2). On the other hand, an attacker might instead work with upper bounds or tight estimates using regression. Note that the experimental approach is highly limited by the number of available data points, and there is no certainty in whether the retrieved formulas hold for larger round numbers as well.

(T) *Theoretical approach*: To overcome the limitations of the experimental approach, theoretical bounds for d_{solv} and $d_{\mathcal{I}}$ can be used. Using theoretical upper bounds increases confidence in the results, at the cost of potentially overestimating the true complexity, and thus underestimating N^*. In particular, any round number N below N^* is *proven to be insufficient* to reach the targeted security level in the corresponding step of the Gröbner basis attack, under the assumption that asymptotic constants can be ignored.

  (1) *GB* step: For regular sequences, the solving degree d_{solv} is bounded by the so-called Macaulay bound [BFS15b], which can be easily computed. In practice, however, the assumption of regular sequences often does not hold, and the Macaulay bound might only serve as a rough indicator for d_{solv}. However, since it is one of the few available explicit bounds, recent design and attack papers tend to use the Macaulay bound in their security arguments [ACG+19b; GKR+22b; AAB+20; GKR+21].

  (2) *FGLM* step: For a zero-dimensional ideal $\mathcal{I}$, the quotient space dimension $d_{\mathcal{I}}$ is tightly connected to the variety $V_{\overline{\mathbb{F}}}(\mathcal{I})$ and thus to the number of solutions to the polynomial equation system (cf. Theorem 2). By inserting into the formula for $\mathcal{C}_{\mathrm{FGLM}}$ (cf. Equation (9)), N^* with respect to an a priori fixed security level of s bits can be derived using

$$N^* = \min\{N \in \mathbb{N} : n_v(N) \cdot D(N)^{\omega} \geq 2^s\}, \tag{3}$$

  where $n_v(N)$ denotes the number of variables and $D(N)$ denotes the number of solutions to the system (over the algebraic closure, counted with multiplicities). If the considered system is square, $D(N)$ can be approximated using the theoretical *Bézout bound*. However, this bound is often loose because of many solutions at infinity, which leads to heavily underestimating the necessary number of rounds. Alternatively, the *minimal multihomogeneous Bézout bound* can be used instead, as it "takes advantage of the structure and leads to tighter complexity results"[FP22]. Notably, the *minimal* multihomogeneous Bézout bound is at least as good as the classical one. See Section 3.3.

(3) *FAC* step: The degree of the univariate polynomial in the reduced LEX Gröbner basis is bounded from above by the quotient space dimension $d_{\mathcal{I}}$. Notably, this bound is tight if the ideal is in shape position. Thus, theoretical bounds for $d_{\mathcal{I}}$, such as the Bézout bounds, can be used in the security analysis.

3.2 Complexity Estimates for Gröbner Basis Algorithms

As discussed in Section 1.1, Gröbner basis assisted polynomial system solving involves the steps *(1)*, *(2)*, and *(3)*. We denote the corresponding complexities by $\mathcal{C}_{\text{GB}}$, $\mathcal{C}_{\text{FGLM}}$, and $\mathcal{C}_{\text{FAC}}$, respectively.

In the following, ω denotes the *linear algebra constant*, with $2 \leq \omega \leq 3$. The ideal $\mathcal{I} \subseteq \mathbb{F}[x_1, \ldots, x_{n_v}]$ is generated by the polynomials $\{f_1, \ldots, f_{n_e}\}$. We assume $\mathcal{I}$ to be zero-dimensional.

Complexity of Computing a Gröbner Basis. Runtime complexities for Gröbner basis algorithms are based on the analysis of matrix-based algorithms such as Lazard [Laz79; Laz83], F4 [Fau99], or Matrix-F5 [BFS15a]. The runtime complexity is generally bounded by [BFS15a]

$$\mathcal{O}\left(n_e \cdot \binom{n_v + d_{\text{solv}}}{n_v}^{\omega}\right) \tag{4}$$

operations in $\mathbb{F}$. We use a slightly tighter upper bound given by

$$\mathcal{O}\left(\sum_{i=0}^{d_{\text{solv}}} \binom{n_v + i - 1}{i}^{\omega-1} \cdot \sum_{j=1}^{n_e} \binom{n_v + i - \deg(f_j) - 1}{i - \deg(f_j)}\right) \tag{5}$$

operations in $\mathbb{F}$ [Spa12, Th. 1.72]. Here, d_{solv} denotes the solving degree. Intuitively, d_{solv} corresponds to the maximum degree reached during a Gröbner basis computation. Thus, the overall complexity of computing a Gröbner basis can be understood as being bounded by row-reducing (full-rank) matrices of size $\sum_{j=1}^{n_e} \binom{n_v+i-1}{i} \times \binom{n_v+i-1}{i}$, for $i = 0, 1, \ldots, d_{\text{solv}}$, eventually leading to the bound in (5). In practice, the Macaulay matrices built during a Gröbner basis computation might be sparse and have a substantial rank defect. Note that the bound in (5) does not account for this particular structure in the Macaulay matrices. Knowledge about this structure potentially allows further improvement of this bound. In practice, it is customary to drop any factors from the asymptotic $\mathcal{O}(\cdot)$ notation, which is why we directly use

$$\mathcal{C}_{\mathrm{GB}}(n_e, n_v, d_{\mathrm{solv}}) = \sum_{i=0}^{d_{\mathrm{solv}}} \binom{n_v + i - 1}{i}^{\omega - 1} \cdot \sum_{j=1}^{n_e} \binom{n_v + i - \deg(f_j) - 1}{i - \deg(f_j)} \tag{6}$$

for estimating the runtime complexity of computing a Gröbner basis.

Complexity of Changing the Monomial Order. A general upper bound on the runtime complexity of the FGLM algorithm [FGL+93] is

$$\mathcal{O}\left(n_v \cdot {d_{\mathcal{I}}}^3\right) \tag{7}$$

operations in $\mathbb{F}$, where n_v is the number of variables in $R = \mathbb{F}[x_1, \ldots, x_{n_v}]$ and $d_{\mathcal{I}} = \dim_{\mathbb{F}}(R/\mathcal{I})$ is the dimension of the quotient ring $R/\mathcal{I}$ as $\mathbb{F}$-vector space. The bound in (7) can be improved using fast linear algebra techniques, leading to a runtime complexity of

$$\mathcal{O}\left(n_v \cdot {d_{\mathcal{I}}}^{\omega}\right) \tag{8}$$

operations in $\mathbb{F}$ [BGL20a]. Again, we drop any factors from the $\mathcal{O}(\cdot)$ notation and directly use

$$\mathcal{C}_{\mathrm{FGLM}}(n_v, d_{\mathcal{I}}) = n_v \cdot {d_{\mathcal{I}}}^{\omega}. \tag{9}$$

Complexity of Factoring Polynomials. Polynomial factorization is a classic problem, and for this purpose, we may choose one of many factoring algorithms [Ber71; CZ81; KS98; Gen07; KU11]. See also [Vas07, Section 6.7] for a summary of classical factorization algorithms. For example, a fast version of the (probabilistic) Cantor-Zassenhaus algorithm [CZ81] for factoring a univariate polynomial of degree D over a finite field with constant cardinality uses an expected number of

$$\mathcal{O}\left(D^{1.815}\right) \tag{10}$$

field operations [KS98]. In step *(3)*, we factor the (unique) univariate polynomial f in the (minimal) `LEX` Gröbner basis. The polynomial f has the *last* `LEX` variable as indeterminate. This means that factoring f only recovers partial solutions for the last variable. If needed, partial solutions for this variable are back-substituted into the other equations until a full solution is obtained, which might incur some additional costs. In general, we have $\deg(f) \leq d_{\mathcal{I}}$.

However, for ideals in shape position, factoring f recovers the values for the other variables at once; see Definition 4. In this case, we know that $\deg(f) = d_{\mathcal{I}}$. We note that our algebraic models for Anemoi lead to ideals in shape position. Hence, in this case, the key parameter for estimating the runtime complexity of step *(3)* is $d_{\mathcal{I}}$. As above, we directly use the bound

$$\mathcal{C}_{\mathrm{FAC}}(d_{\mathcal{I}}) = {d_{\mathcal{I}}}^{1.815}. \tag{11}$$

The Value of the Linear Algebra Constant $\boldsymbol{\omega}$. In the context of algebraic cryptanalysis, the linear algebra constant ω often (tacitly) carries a double meaning. On the one hand, it serves as the ordinary linear algebra exponent for dense matrix multiplication with $\omega \approx 2.37$. On the other hand, it is also used to account for the special structure in the (Macaulay) matrices built during step *(1)* and *(2)* [FP22; FM11]. This double meaning complicates the matter of choosing a concrete value for ω, especially when arguing about a secure number of rounds and/or the purported complexity of an attack.

In general, choosing a lower value for ω can be seen as a conservative choice for a designer and an aggressive one for an attacker – and vice-versa. A common choice in the literature, for both viewpoints, is $\omega = 2$ [ACG+19b; FP22; AAB+20; BGL20a; BBC+23; RST23; GKR+22a; GKR+21; ARS+15; GKL+22; GHR+23; GLR+20a]. There exists also a claim for $\omega = 1$ [BGL20b]. In the literal meaning of ω, i.e., as the linear algebra exponent, such choices might appear unrealistic. Implicitly, however, these choices aim to account for better-performing algorithms when dealing with structured matrices (such as sparse matrices) and use ω as a shortcut for this aim.

In our analysis of Anemoi, we orientate ourselves by the choice $\omega = 2$. Considering that our algebraic model of Anemoi yields an ideal in shape position, this choice seems to be justified. Indeed, in the literature, it is the shape position assumption that underlies fast algorithms for, e.g., step *(2)* [FGH+14; FM11]. Nonetheless, we see the topic of a more detailed analysis of solving algorithms for step *(1)* and *(2)* as an interesting and important open problem. Possibly, this helps to make more informed choices about the value of ω.

3.3 Multihomogeneous Bézout

There exists a more general version of Bézout's theorem for so-called *multihomogeneous* equation systems [MS87; Wam92; Sha13].

Definition 7 (Multihomogeneous polynomial). *A polynomial f in $n+m$ variables is called* m-homogeneous of multidegree $\operatorname{mdeg}(f) = (d_1, \dots, d_m) \in \mathbb{Z}^m_{\geq 0}$ *if there exists a partition of the variable set X into m sets*

$$X_j = \left\{x_{j,0}, x_{j,1}, \dots, x_{j,n_j}\right\} \quad \textit{with} \quad |X_j| = n_j + 1, \quad \sum_{j=1}^{m} n_j = n$$

such that f is homogeneous of degree d_j with respect to the variables in the set X_j for all $1 \leq j \leq m$. In particular, f can be written in the form

$$f = \sum_{\substack{\alpha_j \in \mathbb{Z}^{n_j+1}_{\geq 0} \ s.t. \\ |\alpha_j| = d_j,\ j=1,\dots,m}} a_{\alpha_1,\dots,\alpha_m} \cdot X_1^{\alpha_1} \cdot \dots \cdot X_m^{\alpha_m} \ \in \ \mathbb{F}\left[X_1, \dots, X_m\right],$$

where we use the simplified notation $X_j^{\alpha_j}$ for the monomial $x_{j,0}^{\alpha_{j,0}} \cdot x_{j,1}^{\alpha_{j,1}} \cdot \ldots \cdot x_{j,n_j}^{\alpha_{j,n_j}}$, $|\alpha_j| = \alpha_{j,0} + \dots + \alpha_{j,n_j}$ for the total degree of $X_j^{\alpha_j}$, and $\mathbb{F}\left[X_1, \dots, X_m\right]$ for the polynomial ring in all $n+m$ variables $X_1 \uplus \ldots \uplus X_m$.

Theorem 5 (Multihomogeneous Bézout's Theorem). *Let $\mathbb{F}$ be algebraically closed and let $f_1, \ldots, f_n \in \mathbb{F}[X_1, \ldots, X_m]$ be m-homogeneous polynomials in $n+m$ variables of multidegrees* $\operatorname{mdeg}(f_i) = (d_{i,1}, \ldots, d_{i,m}) \in \mathbb{Z}^m_{\geq 0}$*, where $|X_j| = n_j + 1$. If the number of solutions in the multiprojective product space $\mathbb{P}^{n_1}(\mathbb{F}) \times \cdots \times \mathbb{P}^{n_m}(\mathbb{F})$ is finite, then the number of solutions (counted with multiplicities) is given by the coefficient of the monomial $t_1^{n_1} \cdots t_1^{n_m}$ in the product of linear forms $d_{i,1}t_1 + \cdots + d_{i,m}t_m$, that is,*

$$\text{MHB} := [t_1^{n_1} \cdots t_m^{n_m}] \prod_{i=1}^{n} \sum_{j=1}^{m} d_{i,j} t_j .$$

Similar to the classical Bézout bound (cf. Theorem 4), the multihomogeneous version of Bézout's theorem can be used to bound the number of solutions to a polynomial equation system. This is achieved by fixing a partition of the variable set and homogenizing with respect to each set in the partition. To see this, let $f \in \mathbb{F}[x_1, \ldots, x_n]$. Partition the n variables into m groups, where $|X_j| = n_j$ for $1 \leq j \leq m$. Let d_j be the total degree of $f \in \mathbb{F}[X_j]$ for all $1 \leq j \leq m$. For every group j, we introduce a homogenization variable $x_{j,0}$. The *multihomogenization* f^{MH} of f, i.e.,

$$f^{\text{MH}} := \left(\prod_{j=1}^{m} x_{j,0}^{d_j} \right) \cdot f\left(\frac{X_1}{x_{1,0}^{n_1}}, \ldots, \frac{X_m}{x_{m,0}^{n_m}} \right),$$

is an m-homogeneous polynomial in $n+m$ variables of multidegree $(d_1, \ldots, d_m)$, where the variable set is partitioned into distinct sets $X_j \cup \{x_{j,0}\}$ of size $n_j + 1$ for $1 \leq j \leq m$. Here, we used the notation

$$\frac{X_j}{x_{j,0}^{n_j}} = \left\{ \frac{x_{j,1}}{x_{j,0}}, \ldots, \frac{x_{j,n_j}}{x_{j,0}} \right\}$$

to abbreviate the replacement of every $x \in X_j$ by $\frac{x}{x_{j,0}}$. Setting $x_{j,0} = 1$ for every $1 \leq j \leq m$ recovers f.

In this context, a multiprojective point $[\mathbf{x}_1 ; \ldots ; \mathbf{x}_m] \in \mathbb{P}^{n_1}(\mathbb{F}) \times \cdots \times \mathbb{P}^{n_m}(\mathbb{F})$ is called *finite* if $x_{j,0} \neq 0$ for all $1 \leq j \leq m$. Otherwise, it is called a *point at infinity*.

Theorem 6 (Multihomogeneous Bézout bound). *Let $\mathcal{I} = \langle f_1, \ldots, f_n \rangle$ be a zero-dimensional ideal in $\mathbb{F}[x_1, \ldots, x_n]$ and let $\mathcal{Z} = \{X_1, \ldots, X_m\}$ be a partition of the variable set with $|X_j| = n_j$. Denote by $d_{i,j}$ the total degree of f_i with respect to the variables in the set X_j for $1 \leq i \leq n$, $1 \leq j \leq m$. Then*

$$d_{\mathcal{I}} \overset{(Thm.2)}{=} \sum_{P \in V_{\overline{\mathbb{F}}}(\mathcal{I})} m_P \leq \text{MHB}. \tag{12}$$

For large systems, computing the multihomogeneous Bézout bound for a given variable set partition directly from the definition might be expensive.

[Wam92] presented a recursive formula that operates solely on the degrees without performing polynomial multiplications. Since this recursive approach is instrumental to prove the multihomogeneous Bézout bound of a system with respect to a particular variable set partition (cf. Appendix E), it is summarized in Appendix A.

The following example of a polynomial equation system in three variables shows that the multihomogeneous Bézout bound can be smaller or larger than the classical[7] Bézout bound, depending on the variable set partition.

Example 2 (Multihomogeneous Bézout bound). Consider f_1, f_2, f_3 from Example 1 with $\mathcal{I} = \langle f_1, f_2, f_3 \rangle \subset \mathbb{Q}[x_1, x_2, x_3]$ zero-dimensional ($d_{\mathcal{I}} = 4$), where

$$f_1 = x_1 x_2^2 + x_1 x_3^2 - x_2, \qquad f_2 = x_2 + 1, \qquad f_3 = x_1 x_2^2 + 2 x_2 x_3^2 - 2 x_3 + 1.$$

Depending on the chosen variable set partition, the corresponding multihomogeneous Bézout bound might be smaller, equal, or greater than the classical one $\textsc{b} = 9$ (cf. Example 1). The results for the five different partitions of $\{x_1, x_2, x_3\}$ are summarized in Table 2. We see that for the partition $\mathcal{Z} = \{\{x_1\}, \{x_2\}, \{x_3\}\}$, the multihomogeneous Bézout bound corresponds exactly to the quotient space dimension $d_{\mathcal{I}}$. For $\mathcal{Z} = \{\{x_1, x_2\}, \{x_3\}\}$, the resulting multihomogeneous Bézout bound is above the classical one. Finally, note that partitioning the variable set into only $m = 1$ set always recovers the classical Bézout bound from Theorem 4.

To enhance comprehension of the definition of multihomogeneity, we illustratively show the multihomogenization with respect to $\mathcal{Z} = \{\{x_1, x_2\}, \{x_3\}\}$. Introducing the $m = |Z| = 2$ homogeneous coordinates $x_{1,0}$ and $x_{2,0}$ yields

$$\begin{aligned} f_1^{\mathrm{MH}} &= x_1^1 x_2^2 \cdot x_{2,0}^2 + x_1^1 x_{1,0}^2 \cdot x_3^2 - x_2^1 x_{1,0}^2 \cdot x_{2,0}^2, \\ f_2^{\mathrm{MH}} &= x_2^1 + x_{1,0}^1, \\ f_3^{\mathrm{MH}} &= x_1^1 x_2^2 \cdot x_{2,0}^2 + 2 \cdot x_2^1 x_{1,0}^2 \cdot x_3^2 - 2 \cdot x_{1,0}^3 \cdot x_2^1 x_{2,0}{}^1 + x_{1,0}^3 \cdot x_{2,0}^2, \end{aligned}$$

where $\operatorname{multideg}(f_1^{\mathrm{MH}}) = \operatorname{multideg}(f_3^{\mathrm{MH}}) = (3, 2)$ and $\operatorname{multideg}(f_2^{\mathrm{MH}}) = (1, 0)$.

Table 2. Variable set partitions for a set of three variables and resulting multihomogeneous Bézout bound for the polynomial equation system in Example 2.

Partition $\mathcal{Z}$	Multihomogeneous Bézout bound (cf. Theorem 6)
$\{\{x_1, x_2, x_3\}\}$	$9 \ = [t_1^3]\ (3t_1)(1t_1)(3t_1)$
$\{\{x_1\}, \{x_2, x_3\}\}$	$5 \ = [t_1^1 \cdot t_2^2]\ (1t_1 + 2t_2)(0t_1 + 1t_2)(1t_1 + 3t_2)$
$\{\{x_1, x_2\}, \{x_3\}\}$	$12 = [t_1^2 \cdot t_2^1]\ (3t_1 + 2t_2)(1t_1 + 0t_2) \cdot (3t_1 + 2t_2)$
$\{\{x_1, x_3\}, \{x_2\}\}$	$6 \ = [t_1^2 \cdot t_2^1]\ (3t_1 + 2t_2)(0t_1 + 1t_2)(2t_1 + 2t_2)$
$\{\{x_1\}, \{x_2\}, \{x_3\}\}$	$4 \ = [t_1^1 \cdot t_2^1 \cdot t_3^1]\ (t_1 + 2t_2 + 2t_3)(0t_1 + 1t_2 + 0t_3)(1t_1 + 2t_2 + 2t_3)$

[7] We refer to the Bézout bound from Theorem 4 as *classical* in order to distinguish it from the multihomogeneous one clearly.

Minimal Multihomogeneous Bézout Bound. The multihomogeneous Bézout bound can yield a better bound to the number of (affine) solutions than the classical bound given by Bézout's theorem. In particular, the minimal multihomogeneous Bézout bound is at least as good as the classical Bézout bound since the "trivial" partition into a single set recovers the latter. Thus, among all partitions, we would like to find the one that yields the *smallest* multihomogeneous Bézout bound. Let $f_1, \dots, f_n \in \mathbb{F}[x_1, \dots, x_n]$ and let B_X denote the set of all partitions of the variable set $X = \{x_1, \dots, x_n\}$. Our goal is to solve the following minimization problem:

$$\min_{\mathcal{Z} \in B_X} \left[\prod_{j=1}^{|\mathcal{Z}|} t_j^{|X_j|} \right] \prod_{i=1}^{n} \sum_{j=1}^{|\mathcal{Z}|} d_{i,j} t_j. \tag{13}$$

In particular, if $\mathcal{I} = \langle f_1, \dots, f_n \rangle$ is a zero-dimensional ideal in $\mathbb{F}[x_1, \dots, x_n]$ and if MHB denotes the *minimal* multihomogeneous Bézout bound of the polynomial equation system $f_1 = \dots = f_n = 0$, then

$$d_{\mathcal{I}} \leq \textsc{mhb} \leq \textsc{b}. \tag{14}$$

Note that the search space increases exponentially with the number of variables. In general, finding the *minimal multihomogeneous Bézout* number, and thus an optimal variable set partition, is NP-hard (cf. [MM07]). Therefore, we apply a *heuristic* approach in four steps.

1. Compute the multihomogeneous Bézout bound for all different variable set partitions for the round reduced instances and identify the optimal partition(s).
2. Find a pattern in this partition(s), that is, variable groupings that consistently reappear when increasing the number of rounds N.
3. Extrapolate (one of) the "optimal" partition pattern(s) to the general case for arbitrary $N \geq 1$.
4. Given an "optimal" partition pattern, derive an explicit formula for the multihomogeneous Bézout bound dependent on the number of rounds N.

This strategy seems appropriate, as variables and equations modeling round-based primitives are typically generated in a very structured way, thus likely maintaining the properties of a particular variable set partition. While there is no proof that the selected "optimal" partition pattern consistently yields *the* minimal multihomogenous Bézout bound, it still yields a bound at least as good as the classical Bézout bound.

4 Algebraic Cryptanalysis of Anemoi

This section presents our security analysis of Anemoi [BBC+23] over prime fields. Section 4.1 recaps the essentials of the Anemoi design, Sections 4.2 to 4.4 follow the attack and analysis methodology described in Section 3.1.

4.1 Design Description

Anemoi [BBC+23] is a family of permutations that can be used as a building block for arithmetization-friendly hash functions. In particular, the designers suggest two modes of operation: the sponge mode, to turn the permutation into a hash function, and a mode of operation called Jive to turn the permutation into a compression function.

By design, Anemoi operates over $\mathbb{F}_q^{2\ell}$, for $\ell \in \mathbb{N}$, and either $q = p$ is an odd prime or $q = 2^n$, for n odd and $\log_2 q \geq 10$. When used in a sponge construction, the designers argue that for sufficiently large fields, choosing $\ell = 1$ is enough [BBC+23, Section 5.3] to reach the security goals. We thus restrict the discussion to this special case.

Each round of the Anemoi permutation is designed similarly to a substitution-permutation network (SPN). Let $x_{r-1}, y_{r-1} \in \mathbb{F}_q$ denote the two inputs to the round function R_r in the r-th round. The following operations are performed:

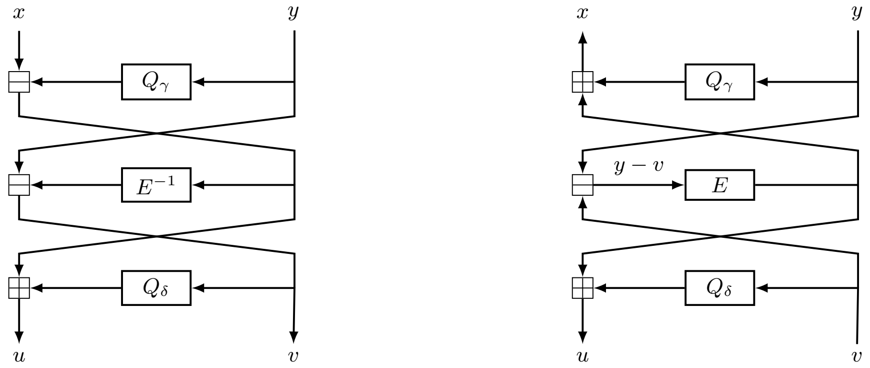
1. *Addition of round constants*: Add round constant vector $\begin{bmatrix} c_r \ d_r \end{bmatrix}^T \in \mathbb{F}_q^2$ to the input vector $\begin{bmatrix} x_{r-1} \ y_{r-1} \end{bmatrix}^T \in \mathbb{F}_q^2$.
2. *Linear layer*: The Pseudo-Hadamard transform $H \in \mathbb{F}_q^{2\times 2}$ is applied to the result vector of the round constant addition, that is,
$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_{r-1} + c_r \\ y_{r-1} + d_r \end{bmatrix} .$$
3. *Nonlinear layer / S-Box*: Let $Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$, $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ be low-degree polynomials and let $E : \mathbb{F}_q \to \mathbb{F}_q$ be a low degree power map inducing a permutation on $\mathbb{F}_q$, that is, $E(x) = x^\alpha$ with appropriate small $\alpha \geq 3$. The nonlinear layer is given by a 3-round Feistel network with Q_γ, E^{-1} and Q_δ as round functions. It is denoted by $\mathcal{H} : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ and called *open* Flystel (cf. Figure 1a). Note that $E^{-1}(x) = x^{\frac{1}{\alpha}}$ is of high degree, where $\frac{1}{\alpha}$ denotes the inverse of α modulo $q-1$. The corresponding counterpart $\mathcal{V} : \mathbb{F}_q^2 \to \mathbb{F}_q^2$, called *closed* Flystel, is defined such that verifying that $(u, v) = \mathcal{H}(x, y)$ is equivalent to verifying that $(x, u) = \mathcal{V}(y, v)$. In particular,
$$\begin{bmatrix} u \\ v \end{bmatrix} = \mathcal{H}(x, y) \quad \Longleftrightarrow \quad \begin{bmatrix} x \\ u \end{bmatrix} = \begin{bmatrix} Q_\gamma(y) + E(y - v) \\ Q_\delta(v) + E(y - v) \end{bmatrix} =: \mathcal{V}(y, v). \tag{15}$$
See also Figure 1b. The degrees of Q_δ and Q_γ differ depending on the characteristic of $\mathbb{F}_q$:
$$Q_\gamma = \begin{cases} \beta x^2 + \gamma & \text{for } q = p \text{ odd} \\ \beta x^3 + \gamma & \text{for } q = 2^n \end{cases} \qquad Q_\delta = \begin{cases} \beta x^2 + \delta & \text{for } q = p \text{ odd} \\ \beta x^3 + \delta & \text{for } q = 2^n \end{cases} \tag{16}$$
In practice, $\beta = g$, $\gamma = 0$, and $\delta = g^{-1}$, where g is a generator of the multiplicative subgroup of the field $\mathbb{F}_q$.

After performing N rounds, the linear layer is again applied to the last round output. That is, for $x_0, y_0 \in \mathbb{F}_q$, the Anemoi permutation of the inputs is given by the function

$$\text{Anemoi}_{q,\alpha}(x_0, y_0) = H \circ \mathrm{R}_N \circ \cdots \circ \mathrm{R}_1(x_0, y_0) = (x_{N+1}, y_{N+1}), \tag{17}$$

where for $1 \leq r \leq N$ the round function R_r is given by

$$\mathrm{R}_r(x_{r-1}, y_{r-1}) = \mathcal{H} \circ H(x_{r-1} + c_r, y_{r-1} + d_r). \tag{18}$$



(a) Evaluation $(u, v) = \mathcal{H}(x, y)$.

(b) Verification $(x, u) = \mathcal{V}(y, v)$.

Fig. 1. Flystel evaluation (high-degree) and verification (low-degree).

4.2 Algebraic Model

The security of cryptographic permutations used in sponge mode is connected to the difficulty of solving the CICO problem. For $\ell = 1$, that is,

$$\text{Anemoi} : \mathbb{F}_q^2 \to \mathbb{F}_q^2,$$

[BBC+23] suggest fixing the first input and the first output element of the permutation. This yields the following CICO problem:

Definition 8 (CICO problem for Anemoi, $\ell = 1$). *The task is to find* $y_{\text{in}}, y_{\text{out}} \in \mathbb{F}_q$ *such that* $\text{Anemoi}\,(0, y_{\text{in}}) = (0, y_{\text{out}})$.

[BBC+23] present two different models for Anemoi under the above CICO constraints, $\mathcal{F}_{\text{CICO}}$ and $\mathcal{P}_{\text{CICO}}$. The security analysis of Anemoi in [BBC+23] is based on the easier model, $\mathcal{F}_{\text{CICO}}$. In this section, we recap both models for the special case $\ell = 1$ and elaborate on $\mathcal{P}_{\text{CICO}}$ for the prime field case since our security analysis is based on this more complicated model. In particular, we provide a more detailed analysis of the polynomial equations and the evolution of their degrees. To visually distinguish variables and functions, the former are highlighted below.

Model 1: $\mathcal{F}_{\mathbf{CICO}}$. Let x_0, y_0 model the input to the Anemoi permutation and let x_r, y_r model the output of the r-th round function (cf. Equation (18)), for $1 \leq r \leq N$. The verification property of the Flystel construction, given in Equation (15), yields a straightforward model that uses two equations for each round. See Table 3 for the model details.[8]

Model 2: $\mathcal{P}_{\mathbf{CICO}}$. Let x_0, y_0 model the input to the Anemoi permutation and let s_r model the output of the high-degree polynomial $E^{-1}(x) = x^{\frac{1}{\alpha}}$ in the open Flystel $\mathcal{H}$ (cf. Figure 1a) in the r-th round R_r, for $1 \leq r \leq N$. We define the following functions for every round $1 \leq r \leq N$:

1. Let x_{r-1}, y_{r-1} be the inputs to R_r. The outputs of the linear layer, and thus the inputs to the S-box $\mathcal{H}$, are given by the functions f_r, g_r, where
$$\begin{bmatrix} f_r(x_{r-1}, y_{r-1}) \\ g_r(x_{r-1}, y_{r-1}) \end{bmatrix} \coloneqq \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_{r-1} + c_r \\ y_{r-1} + d_r \end{bmatrix} = \begin{bmatrix} 2x_{r-1} + y_{r-1} + 2c_r + d_r \\ x_{r-1} + y_{r-1} + c_r + d_r \end{bmatrix}.$$
2. Let f_r, g_r be the inputs to the S-box $\mathcal{H}$ in the r-th round. Its outputs are the functions x_r, y_r, where
$$\begin{bmatrix} x_r \\ y_r \end{bmatrix} \coloneqq \mathcal{H}(f_r, g_r) = \begin{bmatrix} f_r - Q_\gamma(g_r) + Q_\delta(g_r - s_r) \\ g_r - s_r \end{bmatrix} \tag{19}$$

Clearly, $f_r, g_r \in \mathbb{F}_p[x_0, y_0, s_1, \ldots, s_{r-1}]$ and $x_r, y_r \in \mathbb{F}_p[x_0, y_0, s_1, \ldots, s_r]$ for $1 \leq r \leq N$. Applying the CICO input constraint from Definition 8, that is, fixing $x_0 = 0$, we get $f_r, g_r \in \mathbb{F}_p[y_0, s_1, \ldots, s_{r-1}]$ and $x_r, y_r \in \mathbb{F}_p[y_0, s_1, \ldots, s_r]$. Using the definition of the variable s_r, that is,

$$s_r = E^{-1}(f_r - Q_\gamma(g_r)) \qquad \iff \qquad E(s_r) = f_r - Q_\gamma(g_r),$$

every round $1 \leq r \leq N$ can be modeled using a single equation

$$p_r \coloneqq E(s_r) + Q_\gamma(g_r) - f_r = 0, \tag{20}$$

where $p_r \in \mathbb{F}_p[y_0, s_1, \ldots, s_r]$. After the last round, the linear layer is applied once more. The CICO output constraint is thus modeled via

$$x_{N+1} \coloneqq 2x_N + y_N + 2c_{N+1} + d_{N+1} = 0, \tag{21}$$

where x_N, y_N as in Equation (19), and $x_{N+1} \in \mathbb{F}_p[y_0, s_1, \ldots, s_N]$.

Model 2 ($\mathcal{P}_{\mathbf{CICO}}$ for $\ell = 1$) *An algebraic model of the permutation* Anemoi : $\mathbb{F}_q^{2\ell} \to \mathbb{F}_q^{2\ell}$ *for the special case* $\ell = 1$ *under the* CICO *constraints in Definition 8 is given by the system*

$$\mathcal{P}_{\mathrm{CICO}} = \{p_1, \ldots, p_N, x_{N+1}\} \subset \mathbb{F}_p[y_0, s_1, \ldots, s_N],$$

where p_r *as in Equation* (20) *and* x_{N+1} *as in Equation* (21). *In particular, this system contains* $n_e(N) = N+1$ *equations in* $n_v(N) = N+1$ *variables.*

[8] It seems that [BBC+23] ignore the final linear layer in the algebraic models.

$\mathcal{P}_{\text{CICO}}$ for $q = p$ odd prime. Finally, we inspect the polynomial degrees of the equations in $\mathcal{P}_{\text{CICO}}$ for the special case $q = p$ odd prime, for which $\deg(Q_\gamma) = \deg(Q_\delta) = 2$ (cf. Equation (16)). First note that the leading terms of $Q_\gamma(g_r)$ and $Q_\delta(g_r - s_r)$ cancel in the equation for x_r in Equation (19), i.e.,

$$\begin{aligned} x_r &= f_r - Q_\gamma(g_r) + Q_\delta(g_r - s_r) = f_r - (\beta g_r^2 + \gamma) + (\beta(g_r - s_r)^2 + \delta) \\ &= f_r - \beta g_r^2 - \gamma + \beta g_r^2 - 2\beta g_r s_r + {s_r}^2 + \delta = f_r - 2\beta g_r s_r + {s_r}^2 - \gamma + \delta. \end{aligned}$$

Since $f_r, g_r \in \mathbb{F}_p[y_0, s_1, \ldots, s_{r-1}]$ with $\deg(f_r) = \deg(g_r)$, we get the following degrees for the polynomials x_r and y_r:

$$\begin{aligned} \deg(x_r) &= \max\left\{\deg(f_r), \deg(g_r s_r), \deg\left({s_r}^2\right)\right\} = \deg(g_r) + 1, \\ \deg(y_r) &= \max\left\{\deg(g_r), \deg(s_r)\right\} = \deg(g_r). \end{aligned}$$

The degrees of the polynomials f_r and g_r depend on those of x_{r-1} and y_{r-1}:

$$\deg(g_r) = \max\left\{\deg(x_{r-1}), \deg(y_{r-1})\right\} = \deg(g_{r-1}) + 1 = r,$$

where the last equation follows from $\deg(g_1) = 1$. Finally, we arrive at the following degrees for the equations in the polynomial system $\mathcal{P}_{\text{CICO}}$:

$$\deg(p_r) = \max\left\{\alpha, \deg(Q_\gamma) \cdot \deg(g_r), \deg(f_r)\right\} = \max\{\alpha, 2r\}, \tag{22}$$

$$\deg(x_{N+1}) = \max\left\{\deg(x_N), \deg(y_N)\right\} = \deg(g_N) + 1 = N + 1. \tag{23}$$

Table 3. Algebraic models for Anemoi : $\mathbb{F}_q^{2\ell} \to \mathbb{F}_q^{2\ell}$ for the special case $\ell = 1$, $q = p$ being an odd prime, and applied CICO constraints as in Definition 8.

			Variables		**Equations**	
Model	n_v	n_e	*Variable*	*Indices*	*Degree*	*Number*
$\mathcal{F}_{\text{CICO}}$	$2N$	$2N$	x_r	$0 < r < N$	α	N
			y_r	$0 \leq r \leq N$	α	N
$\mathcal{P}_{\text{CICO}}$	$N+1$	$N+1$	y_r	$r = 0$	$\max\{2r, \alpha\}$	N
			s_r	$1 \leq r \leq N$	$N+1$	1

Table 3 summarizes the two algebraic models for Anemoi over a prime field for the special case $\ell = 1$. $\mathcal{F}_{\text{CICO}}$ maintains a constant degree for its polynomials, albeit at the expense of an augmented variable and equation count. In contrast, $\mathcal{P}_{\text{CICO}}$ requires only about half the number of variables and equations, yet the polynomial degrees exhibit linear growth beyond a certain number of rounds. In the subsequent sections, we establish that $\mathcal{P}_{\text{CICO}}$ demonstrates superior timing results for small round numbers. Moreover, the reduced variable count notably influences the complexity estimations.

4.3 Experimental Results

In the following, we experimentally compare the runtime of Gröbner basis attacks on Anemoi using the two models $\mathcal{F}_{\text{CICO}}$ and $\mathcal{P}_{\text{CICO}}$ and elaborate further on the latter. The presented results were achieved for Anemoi over $\mathbb{F}_p$ with a small prime $p = 2^{16} + 1$. All experiments are conducted on a machine with an Intel Xeon E5-2630 v3 @ 2.40GHz (32 cores) and $378GB$ RAM under Debian 11 using Magma V2.26-2.

Runtime comparison of $\mathcal{F}_{\text{CICO}}$ and $\mathcal{P}_{\text{CICO}}$. Practical timing results for both algebraical models are shown in Figure 2 (for $\alpha = 3$) and Appendix B (for $\alpha \in \{5, 7, 11\}$). We found that the variable ordering significantly impacts the runtime of the Gröbner basis step by exhaustive testing. In particular, while the ordering used[9] by [BBC+23] for $\mathcal{F}_{\text{CICO}}$ seems well suited, we identified a more efficient one for $\mathcal{P}_{\text{CICO}}$. For comparison, the experimental results for a bad variable ordering for $\mathcal{F}_{\text{CICO}}$ are also shown.

1. Variable orderings for $\mathcal{F}_{\text{CICO}}$:
   (a) Original: $x_1 > x_2 > \cdots > x_{N-1} > y_0 > y_1 > \cdots > y_N$
   (b) Bad: $x_1 < x_2 < \cdots < x_{N-1} < y_0 < y_1 < \cdots < y_N$
2. Variable orderings for $\mathcal{P}_{\text{CICO}}$:
   (a) Original: $y_0 > s_1 > \cdots > s_N$
   (b) Good: $y_0 > s_N > \cdots > s_1$

During the experiments, we found that both ideals $\langle \mathcal{F}_{\text{CICO}} \rangle$ and $\langle \mathcal{P}_{\text{CICO}} \rangle$ were always in shape position (cf. Definition 4), having the same reduced `LEX` Gröbner basis. This means that both algebraic models of Anemoi exhibit a strong algebraic structure which might be further exploited with dedicated algorithms [BND22]. We also observed that the cost for the final factoring step *(3)* in a Gröbner basis attack was negligible, see Table 4. Hence, our comparison focuses on steps *(1)* and *(2)*.

For both models, the FGLM step takes longer than the GB step in the Gröbner basis attack. The FGLM performance is approximately the same for both models, regardless of the variable ordering. Moreover, the GB step could be performed for more rounds. However, with the new variable ordering, $\mathcal{P}_{\text{CICO}}$ seems to outperform $\mathcal{F}_{\text{CICO}}$ in the GB step. Therefore, we concentrate on the more complex and so far less analyzed model $\mathcal{P}_{\text{CICO}}$.

Experimental results for $\mathcal{P}_{\text{CICO}}$. Table 4 shows the experimental results for $\mathcal{P}_{\text{CICO}}$ with the new variable ordering (2b). Regarding *execution time*, the FGLM step is the most involved part of the Gröbner basis attack. On the other hand, regarding the *complexities* $\mathcal{C}_{\text{GB}}$ and $\mathcal{C}_{\text{FGLM}}$ derived from the *experimentally observed* solving degree d_{solv} and quotient space dimension $d_{\mathcal{I}}$, respectively, the former seems to grow slightly faster.

[9] The used variable ordering is not stated explicitly in [BBC+23] and was deduced from the polynomial ring notation, that is, $\mathbb{F}[x_1, x_2, \ldots, x_{N-1}, y_0, \ldots, y_N]$ and $\mathbb{F}[y_0, s_1, \ldots, s_N]$ for the models $\mathcal{F}_{\text{CICO}}$ and $\mathcal{P}_{\text{CICO}}$, respectively.

[10] Out of memory.

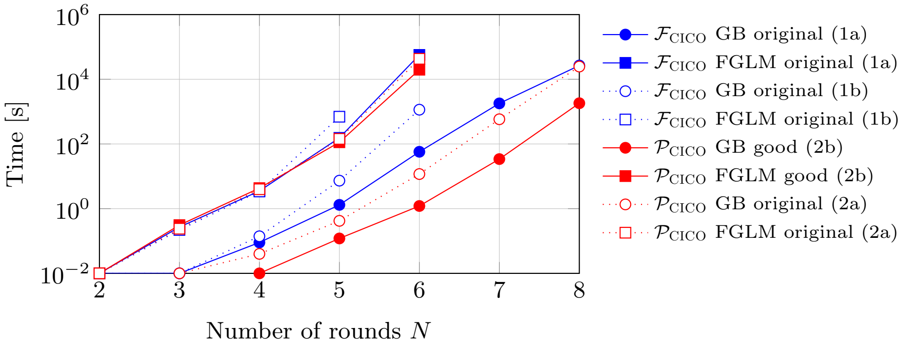


Fig. 2. Runtime results for the *(1) GB* and *(2) FGLM* steps in the Gröbner basis attack on $\mathcal{F}_{\text{CICO}}$ and $\mathcal{P}_{\text{CICO}}$ over the prime field $\mathbb{F}_p$ for different variable orderings, with $p = 2^{16} + 1$ and $\alpha = 3$.

Table 4. Gröbner basis attack to solve the algebraic system $\mathcal{P}_{\text{CICO}} \subset \mathbb{F}_p\,[y_0, s_N, \ldots, s_1]$, where $p = 2^{16} + 1$ and $y_0 > s_N > \cdots > s_1$, for different values of α. The complexities $\mathcal{C}_{\text{GB}}$ and $\mathcal{C}_{\text{FGLM}}$ are derived using d_{solv} and $d_{\mathcal{I}}$ from the experiments, for $\omega = 2$.

			Gröbner basis			Basis conversion			Elim.
α	N	$d_{\max}$	T_{DRL} [s]	d_{solv}	$\mathcal{C}_{\text{GB}}$ [bits]	T_{FGLM} [s]	$d_{\mathcal{I}}$	$\mathcal{C}_{\text{FGLM}}$ [bits]	T_{ELIM} [s]
3	2	4	0.00	7	10	0.01	25	10	0.0
	3	6	0.00	8	14	0.11	125	15	0.01
	4	8	0.01	11	21	1.85	625	20	0.01
	5	10	0.12	13	26	73.55	3125	25	0.1
	6	12	1.21	15	31	17728.47	15625	30	0.93
	7	14	34.09	17	37				
	8	16	1818.47	21	44				
5	2	5	0.00	10	12	0.00	49	12	0.0
	3	6	0.03	13	19	0.84	343	18	0.0
	4	8	0.85	17	26	67.56	2401	24	0.08
	5	10	11.72	20	32	27327.94	16807	30	0.74
	6	12	377.07	26	41				
	7	14	11837.27	28	46				
7	2	7	0.00	13	14	0.10	81	14	0.0
	3	7	0.19	17	21	3.64	729	21	0.01
	4	8	28.13	22	29	733.23	6561	27	0.22
	5	10	9469.04	28	37		59049[10]		
11	2	11	0.02	21	17	0.25	169	16	0.0
	3	11	3.21	24	24	32.30	2197	24	0.06
	4	11	2618.12	32	33	44074.20	28561	31	1.69

Since the overall complexity of a Gröbner basis attack is determined by the dominant step (cf. Section 3.2), we extrapolate the observed metrics to gain insight for larger round numbers. Note that this might introduce a heuristic gap whose impact is unclear. Our results for the *estimated complexities* of step *(1)* and step *(2)* of the Gröbner basis attack are shown in Figure 3.

We derive the following *conjectured formulae* for the solving degree d_{solv} and the quotient space dimension $d_{\mathcal{I}}$ from the results of our experiments in Table 4. The formulae for d_{solv} are derived from performing linear regression on the observed data points. We mention the following caveat: even if the linear regression is a good fit for the observed data points, extrapolating this trend necessarily introduces a heuristic gap. An estimate derived from a certain (small) amount of actual data points does, in general, not guarantee a good approximation for large-scale variants.

Conjecture 1 (Solving degree d_{solv}). The solving degree for the `DRL` Gröbner basis computation in dependence of the round number N for $\mathcal{I} = \langle \mathcal{P}_{\text{CICO}} \rangle \subset \mathbb{F}_p\left[y_0, s_N, \ldots, s_1\right]$ is approximately given by

$$d_{\text{solv}} \approx \begin{cases} 2.2857 \cdot N + 1.7143 & \text{for } \alpha = 3, \\ 3.7714 \cdot N + 2.0286 & \text{for } \alpha = 5, \\ 5 \cdot N + 2.5 & \text{for } \alpha = 7, \\ 5.5 \cdot N + 9.1667 & \text{for } \alpha = 11. \end{cases} \tag{24}$$

Conjecture 2 (Quotient space dimension $d_{\mathcal{I}}$). The dimension of the quotient space $\mathbb{F}_p\left[y_0, s_N, \ldots, s_1\right]/\mathcal{I}$ in dependence of the round number N for $\mathcal{I} = \langle \mathcal{P}_{\text{CICO}} \rangle$ and $\alpha \in \{3, 5, 7, 11\}$ is given by

$$d_{\mathcal{I}} = (\alpha + 2)^N. \tag{25}$$

We note that the formula for $d_{\mathcal{I}}$ exactly matches the observed values, thus justifying a high level of confidence in the conjecture. Moreover, [BBC+23] observe the same quotient space dimension for $\mathcal{F}_{\text{CICO}}$ and thus arrive at the same conjecture.

Figure 3 shows the estimated complexities for the *(1) GB* and *(2) FGLM* step over the number of rounds N. $\mathcal{C}_{\text{GB}}$ is derived using d_{solv} from Conjecture 1 (cf. Equation (6)), and $\mathcal{C}_{\text{FGLM}}$ is derived using $d_{\mathcal{I}}$ from Conjecture 2 (cf. Equation (9)). For all inspected values of α, $\mathcal{C}_{\text{GB}}$ seems to grow faster than $\mathcal{C}_{\text{FGLM}}$, albeit closest for $\alpha = 11$.

In summary, the *runtime results* indicate that the *(2) FGLM* step is more challenging compared to the *(1) GB* step, contrary to the *estimated complexities* which suggest the opposite. Moreover, using conjectured metrics for the complexity estimates introduces an unclear heuristic gap, potentially leading to over- or underestimation. Finally, relying on asymptotic complexity bounds for derivation may overlook factors that vary based on the specific problem, introducing potential limitations to the analysis.

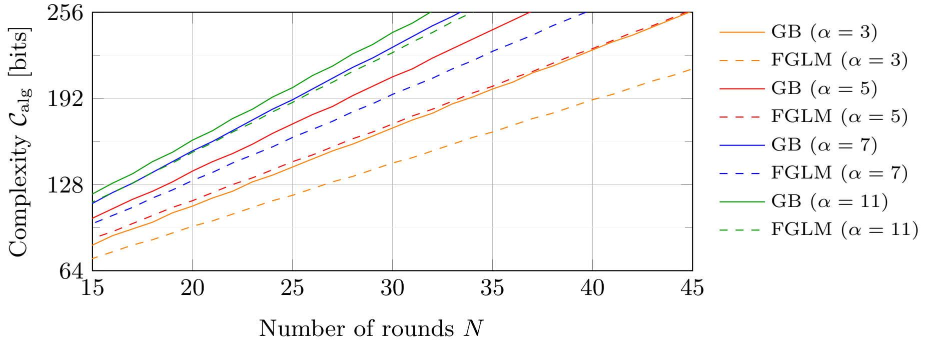


Fig. 3. Estimated complexities for the *(1) GB* and *(2) FGLM* steps in the Gröbner basis attack on $\mathcal{P}_{\text{CICO}} \subset \mathbb{F}_p\left[y_0, s_N, \ldots, s_1\right]$, for $\omega = 2$.

4.4 Security Analysis

This section states the classical Bézout bound and the multihomogeneous Bézout bound for $\mathcal{P}_{\text{CICO}}$, bounding the number of solutions. Proofs can be found in the appendix. Subsequently, we provide the derivations to obtain a lower bound on the number of rounds necessary to reach a security level of s bits using the conjectured metrics, as well as the theoretical Bézout bounds. The results are compared to those provided in [BBC+23].

Bounding the number of solutions. As the degrees of the polynomials in $\mathcal{P}_{\text{CICO}}$ depend on the choice of $\alpha > 0$ and the number of rounds N, we a priori fix the following notation:

$$r_\alpha \coloneqq \min\left\{r \in \mathbb{N} \,:\, 2r \geq \alpha\right\}. \tag{26}$$

In other words, r_α is the first round number such that $2r \geq \alpha$. For $p_r \in \mathcal{P}_{\text{CICO}}$ (cf. Model 2) this means that

$$\deg\left(p_r\right) = \begin{cases} \alpha & \text{for} \quad 1 \leq r < r_\alpha, \\ 2r & \text{for} \quad r_\alpha \leq r \leq N. \end{cases}$$

For $\alpha = 3, 5, 7, 11$, we get $r_\alpha = 2, 3, 4, 6$, respectively. The value r_α plays an important role in the formulas for the classical and the multihomogeneous Bézout bound.

Theorem 7 (Classical Bézout bound for $\mathcal{P}_{\text{CICO}}$). *Let $N \geq r_\alpha$. The Bézout bound for $\mathcal{P}_{\text{CICO}}$ is given by*

$$\text{B} = \alpha^{r_\alpha - 1} \cdot 2^{N - r_\alpha + 1} \cdot \frac{(N+1)!}{(r_\alpha - 1)!}. \tag{27}$$

A proof of Theorem 7 is given in Appendix D.

Table 5. "Optimal" variable set partition for $\mathcal{P}_{\text{CICO}}$ minimizing the multihomogeneous Bézout bound (cf. Theorem 8) derived using the heuristic approach described in Section 3.3. The exhaustive search was performed for up to 8 rounds.

α	r_α	Optimal partition for $1 \leq N < r_\alpha$	Optimal partition for $N \geq r_\alpha$
3	2	$\{\{y_0, s_1\}\}$	$\{\{y_0, s_1, \ldots, s_{r_\alpha}\}, \{s_{r_\alpha+1}\}, \ldots, \{s_N\}\}$
5	3	$\{\{y_0\}, \{s_1\}\}$, but $\{\{y_0, s_1, s_2\}\}$	$\{\{y_0, s_1, \ldots, s_{r_\alpha}\}, \{s_{r_\alpha+1}\}, \ldots, \{s_N\}\}$
7	4	$\{\{y_0\}, \{s_1\}, \ldots, \{s_N\}\}$	$\{\{y_0, s_1, \ldots, s_{r_\alpha}\}, \{s_{r_\alpha+1}\}, \ldots, \{s_N\}\}$
11	6	$\{\{y_0\}, \{s_1\}, \ldots, \{s_N\}\}$	$\{\{y_0\}, \{s_1\}, \ldots, \{s_N\}\}$

Theorem 8 (Multihomogeneous Bézout bound for $\mathcal{P}_{\text{CICO}}$). *Let $N \geq r_\alpha$. For $\alpha \in \{3, 5, 7, 11\}$, the multihomogeneous Bézout bound for $\mathcal{P}_{\text{CICO}}$ with respect to the variable set partition as in Table 5 is given by*

$$\textsc{mhb} = \tau_\alpha \cdot (\alpha + 4)^{N - r_\alpha}, \tag{28}$$

where $\tau_\alpha = 2r_\alpha \cdot \alpha^{r_\alpha - 1} \cdot (r_\alpha + 1)$ for $\alpha \in \{3, 5, 7\}$ and $\tau_\alpha = (\alpha + 4)^{r_\alpha}$ for $\alpha = 11$. In particular,

$$\tau_3 = 2^2 \cdot 3^2 = (\alpha + 3)^{r_\alpha}, \qquad \tau_5 = 2^3 \cdot 3 \cdot 5^2 \approx (\alpha + 3.43)^{r_\alpha},$$
$$\tau_7 = 2^3 \cdot 5 \cdot 7^3 \approx (\alpha + 3.82)^{r_\alpha}, \qquad \tau_{11} = 3^6 \cdot 5^6 = (\alpha + 4)^{r_\alpha}.$$

A proof of Theorem 8 for $\alpha \in \{3, 5, 7\}$ is given in Appendix E.

Note that the classical Bézout bound is larger and grows much faster than the experimental quotient space dimension $d_{\mathcal{I}}$ (cf. Conjecture 2) and the multihomogeneous Bézout bound. Summarizing our results, we get the following bounds on the number of solutions to the algebraic system $\mathcal{P}_{\text{CICO}}$ for $\alpha \in \{3, 5, 7, 11\}$.

Conjecture 3. For the algebraic model $\mathcal{P}_{\text{CICO}}$ of Anemoi : $\mathbb{F}_p^2 \to \mathbb{F}_p^2$, the following relationship holds between the quotient space dimension $d_{\mathcal{I}}$, the number $D(N)$ of solutions to the system (over the algebraic closure, counted with multiplicities), the (minimal) multihomogeneous Bézout bound mhb, and the classical Bézout bound b, for $\alpha \in \{3, 5, 7, 11\}$:

$$d_{\mathcal{I}} = D(N) < \textsc{mhb} < \textsc{b}, \tag{29}$$

where $d_{\mathcal{I}}$ as in Conjecture 2, mhb as in Theorem 8 and b as in Theorem 7.

In our case, the classical Bézout bound is not a good approximation to the number of solutions. We remark that models yielding $D(N) = \textsc{mhb}$ might exist. However, none have been found so far.

Minimum number of rounds. In [BBC+23], a lower bound N^* on the number of rounds needed to reach a certain security level s is derived from the (conjectured) algebraic complexity of the potentially most expensive step in the

Gröbner basis attack, plus some security margin. In particular, the designers considered the easier algebraic model $\mathcal{F}_{\text{CICO}}$, and N^* is defined as

$$N^* = \max\left\{8, \underbrace{\min(5, 1+\ell)}_{\text{(a) security margin}} + \underbrace{2 + \min\left\{N \in \mathbb{N} : \mathcal{C}_{\text{alg}(N)} \geq 2^s\right\}}_{\text{(b) to prevent algebraic attacks}}\right\}, \tag{30}$$

where $\mathcal{C}_{\text{alg}} = \mathcal{C}_{\text{GB}}$ with a conjectured lower bound on the solving degree d_{solv} derived from the experiments and a conservative choice of $\omega = 2$ for the linear algebra constant (cf. [BBC+23, Sections 5.2 & 6.6.2]). An additional security margin of two rounds was added in (b) to account for the second model, $\mathcal{P}_{\text{CICO}}$. In the following, we argue that this margin might not be sufficient to provide the targeted security level by analyzing the algebraic complexity with respect to the more complex model $\mathcal{P}_{\text{CICO}}$.

As discussed in Section 4.3, given the estimated complexities, the *(1) GB* step seems to dominate the overall complexity of the Gröbner basis attack on $\mathcal{P}_{\text{CICO}}$. However, the experimental runtime results suggest the opposite. Thus, we compare the suggested round numbers from [BBC+23], *without* additional security margin (a), to

$$\min\left\{N \in \mathbb{N} : \mathcal{C}_{\text{alg}(N)} \geq 2^s\right\} \tag{31}$$

for $\mathcal{C}_{\text{alg}} \in \{\mathcal{C}_{\text{GB}}, \mathcal{C}_{\text{FGLM}}\}$ in (E) the experimental world and (T) the theoretical world. Tables 6 and 7 state our results for a security level of $s = 128$ and $s = 256$ bits, respectively. If the derived round number is above the suggested one for both the *(1)* GB and the *(2)* FGLM steps, the respective line is highlighted.

Table 6. Lower bounds on the minimum number of rounds needed to reach a security level of $s = 128$ bits derived from $\mathcal{C}_{\text{alg}} \in \{\mathcal{C}_{\text{GB}}, \mathcal{C}_{\text{FGLM}}\}$ using $\mathcal{P}_{\text{CICO}} \subset \mathbb{F}_p\left[y_0, s_N, \ldots, s_1\right]$, with $\omega = 2$ fixed. Round number suggestions from [BBC+23] as in Equation (30)(b), *without* additional security margin (a). Results in the (E) experimental world are derived from d_{solv}, $d_{\mathcal{I}}$ as in Conjectures 1 and 2, results in the (T) theoretical world are derived from B and MHB as in Theorems 7 and 8.

Model	$\mathcal{F}_{\text{CICO}}$	$\mathcal{P}_{\text{CICO}}$			
World	*Experimental*	*Experimental*		*Theoretical*	
α	[BBC+23]	$\mathcal{C}_{\text{GB}}(d_{\text{solv}})$	$\mathcal{C}_{\text{FGLM}}(d_{\mathcal{I}})$	$\mathcal{C}_{\text{FGLM}}(\text{MHB})$	$\mathcal{C}_{\text{FGLM}}(\text{B})$
3	19	23 (+21.05%)	27 (+42.11%)	23 (+21.05%)	16
5	19	19	22 (+15.79%)	20 (+5.26%)	16
7	18	17	20 (+11.11%)	18	15
11	17	16	17	16	15

According to our analysis for $\omega = 2$, for some values of α, an adjustment in the round number for Anemoi (over prime fields) might be necessary to achieve the desired security level. Specifically, for $\alpha = 3$ and $s = 128$, our analysis across three out of four worlds in both step *(1)* and step *(2)* indicates

Table 7. Lower bounds on the minimum number of rounds needed to reach a security level of $s = 256$ bits derived from $\mathcal{C}_{\text{alg}} \in \{\mathcal{C}_{\text{GB}}, \mathcal{C}_{\text{FGLM}}\}$ using $\mathcal{P}_{\text{CICO}} \subset \mathbb{F}_p[y_0, s_N, \ldots, s_1]$, with $\omega = 2$ fixed. Round number suggestions from [BBC+23] as in Equation (30)(b), *without* additional security margin (a). Results in the (E) experimental world are derived from d_{solv}, $d_{\mathcal{I}}$ as in Conjectures 1 and 2, results in the (T) theoretical world are derived from B and MHB as in Theorems 7 and 8.

Model	$\mathcal{F}_{\text{CICO}}$	$\mathcal{P}_{\text{CICO}}$			
Dimension	*Experimental*	*Experimental*		*Theoretical*	
α	[BBC+23]	$\mathcal{C}_{\text{GB}}(d_{\text{solv}})$	$\mathcal{C}_{\text{FGLM}}(d_{\mathcal{I}})$	$\mathcal{C}_{\text{FGLM}}(\text{MHB})$	$\mathcal{C}_{\text{FGLM}}(\text{B})$
3	35	45 (+28.57%)	54 (+54.29%)	45 (+28.57%)	28
5	35	37 (+5.71%)	45 (+28.57%)	40 (+14.29%)	27
7	34	34	40 (+17.65%)	37 (+8.82%)	27
11	33	32	34 (+3.03%)	33	27

a recommended increase in round numbers ranging from approximately 21% to 42%. This increase becomes more pronounced for $s = 256$, ranging from 28.57% to 54.29%. Furthermore, for $\alpha = 5$ and $s = 256$, an increase of 5.71% to 28.57% is advised to reach the targeted security level. Finally, even with the addition of an extra security margin (a), equivalent to two additional rounds as per designer suggestions (cf. Equation (30)), our results still advocate for an increase in the round number in the case $\alpha = 3$.

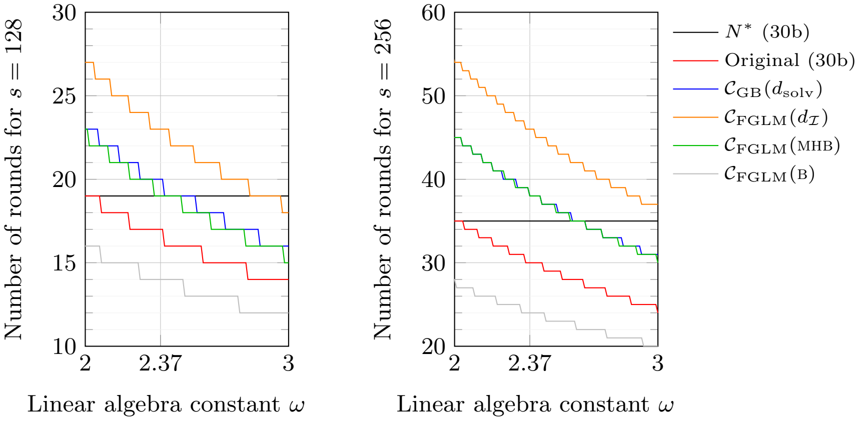
The dominance of the *(1) GB* step over the *(2) FGLM* step, as claimed in [BBC+23], remains unclear. As experimental runtime results indicate the opposite, considering higher round numbers derived from $\mathcal{C}_{\text{FGLM}}$ might be prudent. Notably, the highest round number suggestions are derived from the (E) experimental world. In the (T) theoretical world, outcomes derived from the classical Bézout bound underestimate the round numbers, as it provides only a loose upper bound for the number of solutions and, consequently, the quotient space dimension. Furthermore, our findings emphasize the importance of employing more precise upper bounds, like those provided by the multihomogeneous Bézout bound, to enhance the quality of theoretical results.

It is important to underline the difference in the nature of the metrics used in the formulas for the algebraic complexity once more. While d_{solv} and $d_{\mathcal{I}}$ are conjectured values extrapolated from the *experiments*, the Bézout bounds B and MHB are purely *theoretical*. In the case of $\mathcal{P}_{\text{CICO}}$, it was, for example, relatively straightforward to identify a potential formula for $d_{\mathcal{I}}$. In contrast, the formulas for d_{solv} arose through regression on only a few data points (cf. Section 4.3). As there is no actual proof that the conjectured metrics are indeed correct, theoretical upper bounds can help to increase confidence in the results, at the cost of potentially overestimating the true complexity and thus underestimating N^*. For the *(2) FGML* step, the results derived from the classical Bézout bound give a relatively small lower bound N^* on the minimum number of rounds needed to reach s-bit security (cf. Tables 6 and 7 and Figure 4). Using the multihomogeneous Bézout bound, more realistic values in comparison to the classical Bézout bound could be achieved for N^* while providing the confidence of an actual proof. Thus, any round number N below this bound is *proven to be insufficient* to reach the targeted security level in the *(2) FGLM* step, under the assumption that asymptotic constants can be ignored.

In the previous discussion, we fixed the value of the linear algebra constant to $\omega = 2$. While this choice is generally considered conservative from a designer's perspective, it might seem rather aggressive for an attacker. Even though we think this choice is still suitable due to the internal structures of the polynomial systems (cf. Section 3.2), we conclude our analysis considering a more flexible choice of ω. Figure 4 compares the derived round numbers for $2 \leq \omega \leq 3$ in the case $\alpha = 3$ (see Appendix C when $\alpha \in \{5, 7, 11\}$). We state the following observations, comparing the suggested round number N^* (*without* including the additional security margin (a)) with our results for $\omega = 2.37$:

- For a security level of $s = 128$ bits, our analysis suggests at least 20 rounds (+5.26%) instead of 19.
- For a security level of $s = 256$ bits, our analysis suggests at least 38 rounds (+8.57%) instead of 35.

Including the additional security margin (a) of two rounds, in the case of $s = 256$, we still suggest at least 38 rounds instead of 37 (+2.7%).



(a) $s = 128$.

(b) $s = 256$.

Fig. 4. Lower bounds on the minimum number of rounds needed to reach a security level of s bits derived from $\mathcal{C}_{\mathrm{alg}} \in \{\mathcal{C}_{\mathrm{GB}}, \mathcal{C}_{\mathrm{FGLM}}\}$ using $\mathcal{P}_{\mathrm{CICO}} \subset \mathbb{F}_p[y_0, s_N, \ldots, s_1]$ with $\alpha = 3$. The red line indicates the results of the original analysis in [BBC+23], adapted to $2 \leq \omega \leq 3$, and N^* highlights the suggested round number as in Equation (30)(b), both *without* additional security margin (a). Results in the (E) experimental world derived from d_{solv} and $d_{\mathcal{I}}$ as in Conjectures 1 and 2, results in the (T) theoretical world derived from B and MHB as in Theorems 7 and 8.

As discussed in Section 3.2, a very aggressive choice would be $\omega = 1$, accounting for algorithms exploiting structure in the polynomial equation system. In this case, the number of rounds would need to be increased significantly. For example, for $\alpha = 3$, we arrive at a minimum of 44 rounds (+109.52%) for $s = 128$ and 89 rounds (+191.89%) for $s = 256$ in comparison to the original suggestions (including the additional security margin (a)).

Besides simply increasing the number of rounds, another strategy to address the newly identified vulnerabilities is to select a larger exponent for Q_δ and Q_γ. Specifically, if $\deg(Q_\delta) = \deg(Q_\gamma) > 2$, the polynomial degrees in $\mathcal{P}_{\text{CICO}}$ will demonstrate exponential growth instead of solely linear growth. The practical performance influence of the two approaches might depend on the concrete use case.

Acknowledgments. This work was partially funded by the CONFIDENTIAL-6G EU project (Grant No: 101096435). We express our sincere gratitude to Clémence Bouvier, Fredrik Meisingseth, and Markus Schofnegger for their valuable feedback during the intermediate stages of our work. Further, we want to acknowledge Markus Schofnegger's idea of the $\mathcal{P}_{\text{CICO}}$ model provided to us in January 2023. Additionally, we appreciate the engagement and discussions with our colleagues from the ALPSY research retreat at Obergurgel.

References

[AAB+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. "Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols". In: *IACR Transactions on Symmetric Cryptology* 2020.3 (2020), pp. 1–45. DOI: `10.13154/tosc.v2020.i3.1-45` (cit. on pp. 4, 10, 11, 14).

[AC09] Martin R. Albrecht and Carlos Cid. "Algebraic Techniques in Differential Cryptanalysis". In: *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*. Ed. by Orr Dunkelman. Vol. 5665. Lecture Notes in Computer Science. Springer, 2009, pp. 193–208. DOI: `10.1007/978-3-642-03317-9\_12` (cit. on p. 1).

[ACG+19a] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, et al. "Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC". In: *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11923. Lecture Notes in Computer Science. Springer, 2019, pp. 371–397. DOI: `10.1007/978-3-030-34618-8\_13` (cit. on p. 1).

[ACG+19b] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, et al. "Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC". In: *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III.* Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11923. Lecture Notes in Computer Science. Springer, 2019, pp. 371–397. DOI: `10.1007/978-3-030-34618-8_13` (cit. on pp. 11, 14).

[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: *ASIACRYPT 2016.* Vol. 10031. LNCS. 2016, pp. 191–219 (cit. on p. 4).

[ARS+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. "Ciphers for MPC and FHE". In: *Advances in Cryptology - EUROCRYPT 2015.* Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9056. Lecture Notes in Computer Science. Springer, 2015, pp. 430–454. DOI: `10.1007/978-3-662-46800-5_17` (cit. on p. 14).

[Bar04] Magali Bardet. "Étude des Systèmes Algébriques Surdéterminés. Applications aux Codes Correcteurs et à la Cryptographie". PhD thesis. Pierre and Marie Curie University, Paris, France, 2004 (cit. on p. 2).

[BBC+23] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, et al. "New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode". In: *CRYPTO 2023.* Vol. 14083. LNCS. 2023, pp. 507–539 (cit. on pp. 2–4, 14, 17–20, 22, 24–29, 41, 42).

[BCP23] Clémence Bouvier, Anne Canteaut, and Léo Perrin. "On the algebraic degree of iterated power functions". In: *Des. Codes Cryptogr.* 91.3 (2023), pp. 997–1033. DOI: `10.1007/S10623-022-01136-X` (cit. on p. 1).

[BDP+11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. *The KECCAK reference.* `https://keccak.team/files/Keccak-reference-3.0.pdf`. 2011 (cit. on p. 10).

[Ber71] Elwyn R. Berlekamp. "Factoring Polynomials over Large Finite Fields". In: *Symposium on Symbolic and Algebraic Manipulation - SYMSAC 1971.* Ed. by Stanley R. Petrick, Jean E. Sammet, Robert G. Tobey, and Joel Moses. ACM, 1971, p. 223. DOI: `10.1145/800204.806290` (cit. on p. 13).

[BFS15a] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. "On the Complexity of the F5 Gröbner Basis Algorithm". In: *Journal of Symbolic Computation* 70 (2015), pp. 49–70 (cit. on p. 12).

[BFS15b] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. "On the complexity of the F5 Gröbner basis algorithm". In: *Journal of Symbolic Computation* 70 (2015), pp. 49–70. ISSN: 0747-7171. DOI: `https://doi.org/10.1016/j.jsc.2014.09.025` (cit. on p. 11).

[BGL20a] Eli Ben-Sasson, Lior Goldberg, and David Levit. "STARK Friendly Hash - Survey and Recommendation". In: *IACR Cryptology ePrint Archive* (2020), p. 948 (cit. on pp. 3, 13, 14).

[BGL20b] Eli Ben-Sasson, Lior Goldberg, and David Levit. *STARK Friendly Hash – Survey and Recommendation*. Cryptology ePrint Archive, Paper 2020/948. `https://eprint.iacr.org/2020/948`. 2020 (cit. on p. 14).

[BMM+94] Eberhard Becker, Teo Mora, Maria Grazia Marinari, and Carlo Traverso. "The Shape of the Shape Lemma". In: *International Symposium on Symbolic and Algebraic Computation - ISSAC 1994*. Ed. by Malcolm A. H. MacCallum. ACM, 1994, pp. 129–133. DOI: `10.1145/190347.190382` (cit. on p. 7).

[BND22] Jérémy Berthomieu, Vincent Neiger, and Mohab Safey El Din. "Faster Change of Order Algorithm for Gröbner Bases under Shape and Stability Assumptions". In: *ISSAC '22: International Symposium on Symbolic and Algebraic Computation*. Ed. by Marc Moreno Maza and Lihong Zhi. ACM, 2022, pp. 409–418. DOI: `10.1145/3476446.3535484` (cit. on pp. 7, 22).

[BPW06] Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann. "A Zero-Dimensional Gröbner Basis for AES-128". In: *Fast Software Encryption - FSE 2006*. Ed. by Matthew J. B. Robshaw. Vol. 4047. Lecture Notes in Computer Science. Springer, 2006, pp. 78–88. DOI: `10.1007/11799313_6` (cit. on p. 10).

[CL05] Carlos Cid and Gaëtan Leurent. "An Analysis of the XSL Algorithm". In: *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings*. Ed. by Bimal K. Roy. Vol. 3788. Lecture Notes in Computer Science. Springer, 2005, pp. 333–352. DOI: `10.1007/11593447\_18` (cit. on p. 1).

[CLO15] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra*. 4th ed. Springer, 2015. DOI: `10.1007/978-3-319-16721-3` (cit. on pp. 5, 6).

[CMR05] Carlos Cid, Sean Murphy, and Matthew J. B. Robshaw. "Small Scale Variants of the AES". In: *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers*. Ed. by Henri Gilbert and Helena Handschuh. Vol. 3557. Lecture Notes in Computer Science. Springer, 2005, pp. 145–162. DOI: `10.1007/11502760\_10` (cit. on pp. 1, 10).

[CP02] Nicolas T. Courtois and Josef Pieprzyk. "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". In: *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings.* Ed. by Yuliang Zheng. Vol. 2501. Lecture Notes in Computer Science. Springer, 2002, pp. 267–287. DOI: `10.1007/3-540-36178-2\_17` (cit. on p. 1).

[CZ81] David Cantor and Hans Zassenhaus. "A New Algorithm for Factoring Polynomials over Finite Fields". In: *Mathematics of Computation* 36.154 (1981), pp. 587–592 (cit. on p. 13).

[DGG+21] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters. "Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields". In: *EUROCRYPT 2021.* Vol. 12697. LNCS. 2021, pp. 3–34 (cit. on p. 4).

[DGH+23] Christoph Dobraunig, Lorenzo Grassi, Lukas Helminger, Christian Rechberger, Markus Schofnegger, and Roman Walch. "Pasta: A Case for Hybrid Homomorphic Encryption". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.3 (2023), pp. 30–73 (cit. on p. 4).

[EGL+20] Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, et al. "An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC". In: *ASIACRYPT 2020.* Vol. 12491. LNCS. 2020, pp. 477–506 (cit. on p. 1).

[Fau99] Jean-Charles Faugère. "A New Efficient Algorithm for Computing Gröbner Bases (F4)". In: *Journal of Pure and Applied Algebra* 139 (1999), pp. 61–88. DOI: `10.1016/S0022-4049(99)00005-5` (cit. on pp. 2, 12).

[FGH+14] 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. Kobe, Japan: Association for Computing Machinery, 2014, pp. 170–177. ISBN: 9781450325011. DOI: `10.1145/2608628.2608669` (cit. on p. 14).

[FGL+93] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. "Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering". In: *Journal of Symbolic Computation* 16.4 (1993), pp. 329–344. DOI: `10.1006/jsco.1993.1051` (cit. on pp. 2, 13).

[FM11] Jean-Charles Faugère and Chenqi Mou. "Fast Algorithm for Change of Ordering of Zero-Dimensional Gröbner bases with Sparse Multiplication Matrices". In: June 2011, pp. 115–122. DOI: 10.1145/1993886.1993908 (cit. on pp. 7, 14).

[FP22] Jean-Charles Faugère and Ludovic Perret. *Algebraic Attacks against STARK-Friendly Ciphers.* 2022 (cit. on pp. 1, 12, 14).

[Gen07] Giulio Genovese. "Improving the algorithms of Berlekamp and Niederreiter for Factoring Polynomials over Finite Fields". In: *Journal of Symbolic Computatation* 42.1-2 (2007), pp. 159–177. DOI: 10.1016/j.jsc.2006.02.007 (cit. on p. 13).

[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: *Advances in Cryptology - CRYPTO 2023.* Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. Lecture Notes in Computer Science. Springer, 2023, pp. 573–606. DOI: 10.1007/978-3-031-38548-3_19 (cit. on pp. 4, 14).

[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: *SIGSAC Computer and Communications Security - CCS 2022.* Ed. by Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi. ACM, 2022, pp. 1323–1335. DOI: 10.1145/3548606.3560686 (cit. on p. 14).

[GKR+21] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. "Poseidon: A New Hash Function for Zero-Knowledge Proof Systems". In: *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021.* Ed. by Michael Bailey and Rachel Greenstadt. USENIX Association, 2021, pp. 519–535 (cit. on pp. 4, 11, 14).

[GKR+22a] Lorenzo Grassi, Dmitry Khovratovich, Sondre Rønjom, and Markus Schofnegger. "The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over $GF(p)^n$: Preimage Attack on Full Grendel". In: *IACR Transactions on Symmetric Cryptolology* 2022.1 (2022), pp. 5–37. DOI: 10.46586/tosc.v2022.i1.5-37 (cit. on p. 14).

[GKR+22b] Lorenzo Grassi, Dmitry Khovratovich, Sondre Rønjom, and Markus Schofnegger. "The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over Fnp Preimage Attack on Full Grendel". In: *IACR Trans. Symmetric Cryptol.* 2022.1 (2022), pp. 5–37. DOI: 10.46586/TOSC.V2022.I1.5-37 (cit. on pp. 1, 11).

[GLR+20a] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. "On a Generalization of Substitution Permutation Networks: The HADES Design Strategy". In: *Advances in Cryptology - EUROCRYPT 2020*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. Lecture Notes in Computer Science. Springer, 2020, pp. 674–704. DOI: `10.1007/978-3-030-45724-2_23` (cit. on p. 14).

[GLR+20b] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. "On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy". In: *39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings*. Vol. 12105. Lecture Notes in Computer Science. Springer, 2020. DOI: `10.1007/978-3-030-45724-2_23` (cit. on p. 4).

[GØS+23] Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, and Roman Walch. "From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications". In: *EUROCRYPT (4)*. Vol. 14007. Lecture Notes in Computer Science. Springer, 2023, pp. 255–286 (cit. on p. 4).

[HKC+20] Jincheol Ha, Seongkwang Kim, Wonseok Choi, Jooyoung Lee, Dukjae Moon, Hyojin Yoon, et al. "Masta: An HE-Friendly Cipher Using Modular Arithmetic". In: *IEEE Access* 8 (2020), pp. 194741–194751 (cit. on p. 4).

[HKL+22] Jincheol Ha, Seongkwang Kim, ByeongHak Lee, Jooyoung Lee, and Mincheol Son. "Rubato: Noisy Ciphers for Approximate Homomorphic Encryption". In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part I*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13275. Lecture Notes in Computer Science. Springer, 2022, pp. 581–610. DOI: `10.1007/978-3-031-06944-4\_20` (cit. on p. 4).

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Berlin: Springer, 2000. DOI: `10.1007/978-3-540-70628-1` (cit. on pp. 5, 7).

[KR05] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*. Berlin: Springer, 2005. DOI: `10.1007/3-540-28296-3` (cit. on p. 5).

[KS98] Erich L. Kaltofen and Victor Shoup. "Subquadratic-Time Factoring of Polynomials over Finite Fields". In: *Mathematics of Computation* 67.223 (1998), pp. 1179–1197. DOI: `10.1090/S0025-5718-98-00944-2` (cit. on pp. 2, 13).

[KU11] Kiran S. Kedlaya and Christopher Umans. "Fast Polynomial Factorization and Modular Composition". In: *SIAM Journal on Computing* 40.6 (2011), pp. 1767–1802. DOI: `10.1137/08073408X` (cit. on p. 13).

[Laz79] Daniel Lazard. “Systems of Algebraic Equations”. In: *International Symposium on Symbolic and Algebraic Computation - EUROSAM 1979*. Ed. by Edward W. Ng. Vol. 72. Lecture Notes in Computer Science. Springer, 1979, pp. 88–94 (cit. on p. 12).

[Laz83] Daniel Lazard. “Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations”. In: *European Conference on Computer Algebra - EUROCAL 1983*. Ed. by J. A. van Hulzen. Vol. 162. Lecture Notes in Computer Science. Springer, 1983, pp. 146–156 (cit. on p. 12).

[LP19] Chaoyun Li and Bart Preneel. “Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree”. In: *Selected Areas in Cryptography - SAC 2019 - 26th International Conference, Waterloo, ON, Canada, August 12-16, 2019, Revised Selected Papers*. Ed. by Kenneth G. Paterson and Douglas Stebila. Vol. 11959. Lecture Notes in Computer Science. Springer, 2019, pp. 171–193. DOI: `10.1007/978-3-030-38471-5\_8` (cit. on p. 1).

[MM07] Gregorio Malajovich and Klaus Meer. “Computing Minimal Multi-Homogeneous Bezout Numbers Is Hard”. In: *Theory of Computing Systems* 40.4 (2007), pp. 553–570. DOI: `10.1007/s00224-006-1322-y` (cit. on p. 17).

[MS87] Alexander Morgan and Andrew Sommese. “A homotopy for solving general polynomial systems that respects m-homogeneous structures”. In: *Applied Mathematics and Computation* 24.2 (1987), pp. 101–113. ISSN: 0096-3003. DOI: `10.1016/0096-3003(87)90063-4` (cit. on p. 14).

[MW83] D.W. Masser and Gisbert Wüstholz. “Fields of Large Transcendence Degree Generated by Values of Elliptic Functions.” In: *Inventiones mathematicae* 72 (1983), pp. 407–464 (cit. on p. 9).

[RAS20] Arnab Roy, Elena Andreeva, and Jan Ferdinand Sauer. “Interpolation Cryptanalysis of Unbalanced Feistel Networks with Low Degree Round Functions”. In: *Selected Areas in Cryptography - SAC 2020 - 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers*. Ed. by Orr Dunkelman, Michael J. Jacobson Jr., and Colin O’Flynn. Vol. 12804. Lecture Notes in Computer Science. Springer, 2020, pp. 273–300. DOI: `10.1007/978-3-030-81652-0\_11` (cit. on p. 1).

[RST23] Arnab Roy, Matthias Johann Steiner, and Stefano Trevisani. “Arion: Arithmetization-Oriented Permutation and Hashing from Generalized Triangular Dynamical Systems”. In: *CoRR* abs/2303.04639 (2023) (cit. on pp. 4, 14).

[Sha13] Igor R. Shafarevich. *Basic Algebraic Geometry 1. Varieties in Projective Space*. 3rd ed. Springer, 2013. ISBN: 978-3-642-37955-0. DOI: `10.1007/978-3-642-37956-7` (cit. on pp. 7, 14).

[SKP+07] Makoto Sugita, Mitsuru Kawazoe, Ludovic Perret, and Hideki Imai. "Algebraic Cryptanalysis of 58-Round SHA-1". In: *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*. Ed. by Alex Biryukov. Vol. 4593. Lecture Notes in Computer Science. Springer, 2007, pp. 349–365. DOI: `10.1007/978-3-540-74619-5\_22` (cit. on p. 1).

[Spa12] Pierre-Jean Spaenlehauer. "Solving Multi-Homogeneous and Determinantal Systems: Algorithms, Complexity, Applications." PhD thesis. Pierre and Marie Curie University, Paris, France, 2012 (cit. on p. 12).

[Vas07] Oleg Nikolaevich Vasilenko. *Number-Theoretic Algorithms in Cryptography*. Vol. 232. Translations of Mathematical Monographs. American Mathematical Society, 2007. DOI: `10.1090/mmono/232` (cit. on p. 13).

[Wam92] Charles W. Wampler. "Bezout number calculations for multi-homo-geneous polynomial systems". In: *Applied Mathematics and Computation* 51.2 (1992), pp. 143–157. ISSN: 0096-3003. DOI: `10.1016/0096-3003(92)90070-H` (cit. on pp. 3, 14, 16, 38).

A Row Expansion Algorithm

The *Row Expansion Algorithm*, presented by Wampler in 1992 [Wam92], is an algorithm to compute the multihomogeneous Bézout bound of a polynomial equation system defined by $f_1, \ldots, f_n \in \mathbb{F}[x_1, \ldots, x_n]$ for a particular variable set partition $\mathcal{Z} = \{X_1, \ldots, X_m\}$ with $|X_j| = n_j$ solely from the total degrees $d_{i,j}$ of f_i with respect to the variables in X_j, for $1 \le i \le n$, $1 \le j \le m$. For simplicity, those degrees are summarized in a *degree matrix* $D = (d_{i,j}) \in \mathbb{Z}_{\ge 0}^{n \times m}$. Note that D remains the same for the multihomogenized system in $n + m$ variables with the multihomogenization variables added to the according variable sets in $\mathcal{Z}$, that is, $|X_j| = n_j + 1$.

Theorem 9 (Row expansion algorithm). *Given the degree matrix $D \in \mathbb{Z}_{\ge 0}^{n \times m}$ of a system of n multihomogeneous polynomials $f_1, \ldots, f_n$ in $n + m$ variables with respect to some variable set partition $\mathcal{Z} = \{X_1, \ldots, X_m\}$ with $|X_j| = n_j + 1$. Let $K = [n_1, \ldots, n_m]$ and define*

$$b(D, K, i) \coloneqq \sum_{\substack{j=1 \\ n_j \neq 0}}^{m} d_{i,j} \cdot b(D, M(K, j), i + 1),$$

where $M(K, j)$ is constructed by decrementing the j-th entry of K by 1. Then the multihomogeneous Bézout number with respect to $\mathcal{Z}$ is given by $b(D, K, 1)$.

As the proof for the multihomogeneous Bézout bounds for Anemoi in Appendix E follows the idea of this algorithm, we briefly sketch its correctness proof below. A concrete example, elaborating on Example 2 from Section 3.3, is given at the end of this section.

Proof (Proof Sketch). The multihomogeneous Bézout bound is given by the coefficient of $t_1^{n_1} \cdot \cdots \cdot t_m^{n_m}$ in the product of linear forms, that is,

$$[t_1^{n_1} \cdot \cdots \cdot t_m^{n_m}] \prod_{i=1}^{n} \sum_{j=1}^{m} d_{i,j} t_j.$$

In other words, given the degree matrix D, an element in the i-th row and j-th column may additively contribute to $[t_1^{n_1} \cdot \cdots \cdot t_m^{n_m}]$ with $d_{i,j}$, if selected.

We start with the first row and have m possibilities to choose any of the m columns. Assume we picked the j_1-th column, that is, we picked the value d_{1,j_1}. Now, in the second row, we have to pick another column. Since we already picked column j_1 in the first step, the remaining number of selections for the j_1-th column is $n_j - 1$. This is equivalent to solving the original problem on the minor corresponding to d_{1,j_1}. That is, we operate on the degree matrix $\tilde{D} \in \mathbb{Z}_{\ge 0}^{(n-1) \times m}$, where $\tilde{D}$ is obtained by deleting the first row of D, and $\tilde{K}$, where $\tilde{K}$ is obtained by decrementing the j_1-th entry of K by one. In practice, it is more convenient to leave the matrix D unchanged and pass the next row index to the subroutine.

Now assume that for some row i, we are given the matrices D and K as inputs and that we obtained the solutions to all minor problems, denoted by $b(D, M(K, j), i+1)$ for $1 \leq j \leq m$ where $n_j \neq 0$ in this step, and $\tilde{K} = M(K, j)$ was constructed by decrementing the j-th entry of K by 1. Then

$$b(D, K, i) = \sum_{\substack{j=1 \\ n_j \neq 0}}^{m} d_{i,j} \cdot b(D, M(K, j), i+1).$$

The process is repeated until D has no unseen rows left, or equivalently, after reaching a recursion depth of $n+1$. In this case, $b(D, M(K, j), n+1)$ shall return the empty product, that is, 1, to the previous minor. □

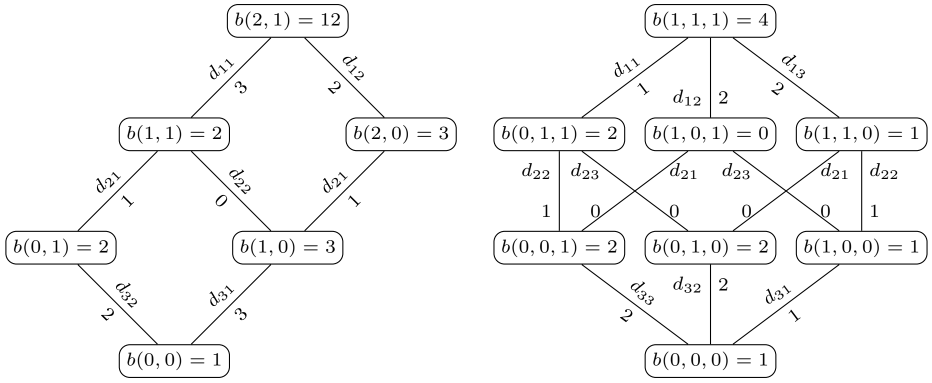
Example 3. Consider $f_1, f_2, f_3 \in \mathbb{Q}[x_1, x_2, x_3]$ as in Example 2, that is,

$$f_1 = x_1x_2^2 + x_1x_3^2 - x_2, \qquad f_2 = x_2 + 1, \qquad f_3 = x_1x_2^2 + 2x_2x_3^2 - 2x_3 + 1.$$

Table 8 states the degree matrices arising from the five different variable set partitions of $\{x_1, x_2, x_3\}$. Figure 5 visualizes the steps of the row expansion algorithm for the partitions yielding the maximal and the minimal multihomogeneous Bézout bound.

Table 8. Variable set partitions for a set of three variables and resulting multihomogeneous Bézout bound, partiton set size vector K and degree matrix D for the polynomial equation system in Example 3.

$\mathcal{Z}$	$\{\{x_1, x_2, x_3\}\}$	$\{\{x_1\}, \{x_2, x_3\}\}$	$\{\{x_1, x_2\}, \{x_3\}\}$	$\{\{x_1, x_3\}, \{x_2\}\}$	$\{\{x_1\}, \{x_2\}, \{x_3\}\}$
MHB	9	5	12	6	4
K	$\begin{bmatrix}3\end{bmatrix}$	$\begin{bmatrix}1 & 2\end{bmatrix}$	$\begin{bmatrix}2 & 1\end{bmatrix}$	$\begin{bmatrix}2 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1 & 1\end{bmatrix}$
D	$\begin{bmatrix}3\\1\\3\end{bmatrix}$	$\begin{bmatrix}1 & 2\\0 & 1\\1 & 3\end{bmatrix}$	$\begin{bmatrix}3 & 2\\1 & 0\\3 & 2\end{bmatrix}$	$\begin{bmatrix}3 & 2\\0 & 1\\2 & 2\end{bmatrix}$	$\begin{bmatrix}1 & 2 & 2\\0 & 1 & 0\\1 & 2 & 2\end{bmatrix}$



(a) $\mathcal{Z} = \{\{x_1, x_2\}, \{x_3\}\}$

(b) $\mathcal{Z} = \{\{x_1\}, \{x_2\}, \{x_3\}\}$

Fig. 5. Visualization of the steps of the row expansion algorithm.

B Experimental results for $\alpha \in \{5, 7, 11\}$

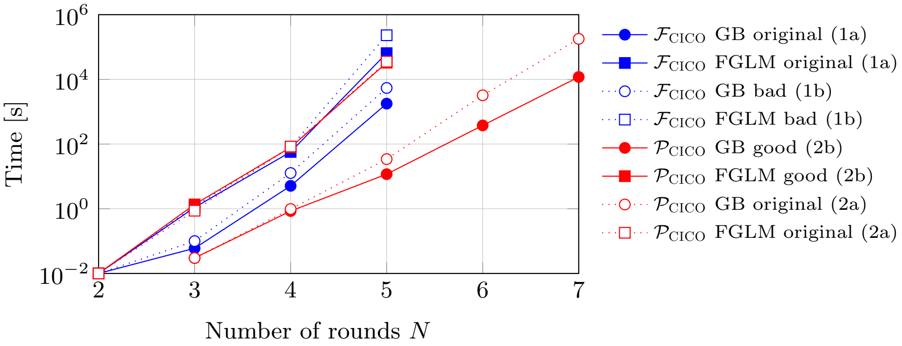


Fig. 6. Runtime results for the *(1) GB* and *(2) FGLM* steps in the Gröbner basis attack on $\mathcal{F}_{\text{CICO}}$ and $\mathcal{P}_{\text{CICO}}$ over the prime field $\mathbb{F}_p$ for different variable orderings, with $p = 2^{16} + 1$ and $\alpha = 5$.

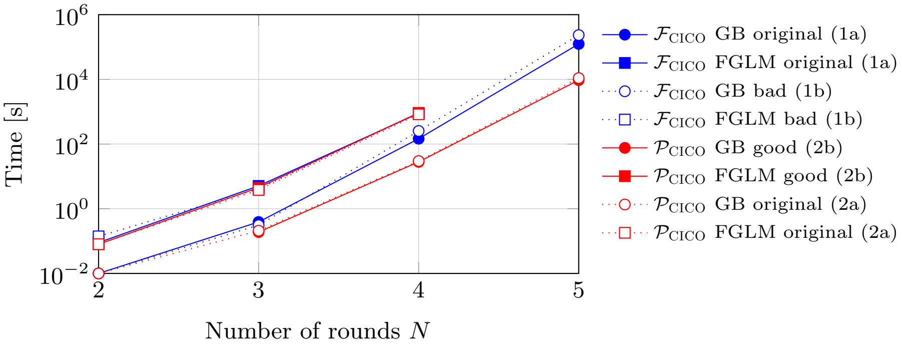


Fig. 7. Runtime results for the *(1) GB* and *(2) FGLM* steps in the Gröbner basis attack on $\mathcal{F}_{\text{CICO}}$ and $\mathcal{P}_{\text{CICO}}$ over the prime field $\mathbb{F}_p$ for different variable orderings, with $p = 2^{16} + 1$ and $\alpha = 7$.

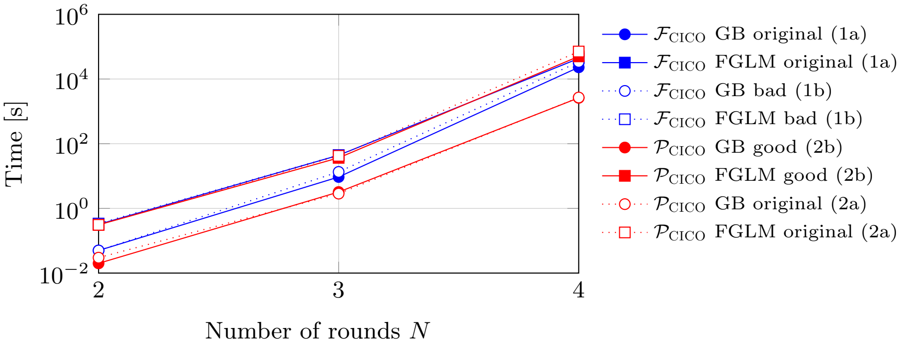


Fig. 8. Runtime results for the *(1) GB* and *(2) FGLM* steps in the Gröbner basis attack on $\mathcal{F}_{\text{CICO}}$ and $\mathcal{P}_{\text{CICO}}$ over the prime field $\mathbb{F}_p$ for different variable orderings, with $p = 2^{16} + 1$ and $\alpha = 11$.

C Minimum number of rounds for $\alpha \in \{5, 7, 11\}$

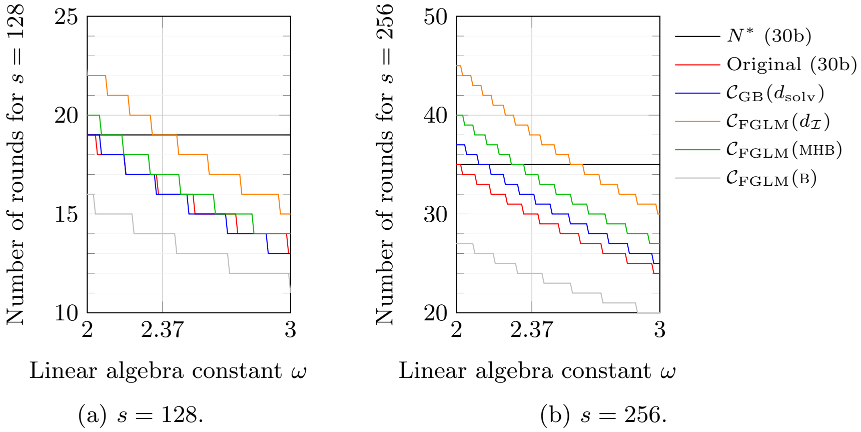
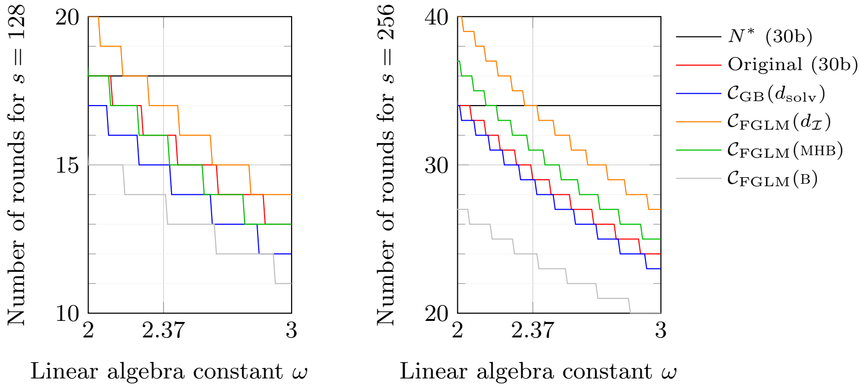


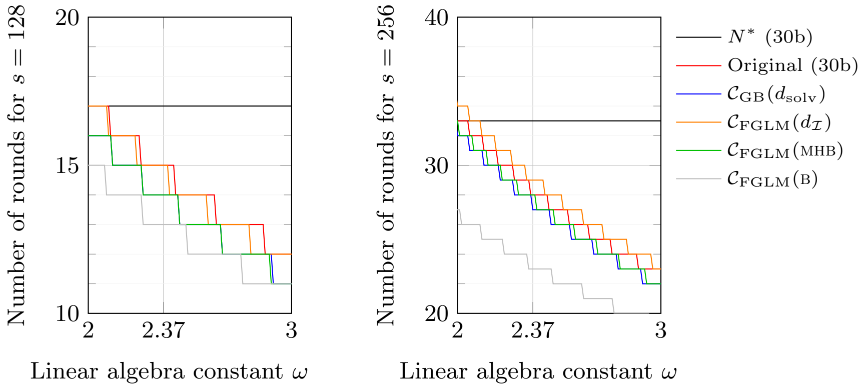
Fig. 9. Lower bounds on the minimum number of rounds needed to reach a security level of s bits derived from $\mathcal{C}_{\text{alg}} \in \{\mathcal{C}_{\text{GB}}, \mathcal{C}_{\text{FGLM}}\}$ using $\mathcal{P}_{\text{CICO}} \subset \mathbb{F}_p[y_0, s_N, \ldots, s_1]$ with $\alpha = 5$. The red line indicates the results of the original analysis in [BBC+23], adapted to $2 \leq \omega \leq 3$, and N^* highlights the suggested round number as in Equation (30)(b), both *without* additional security margin (a). Results in the (E) experimental world derived from d_{solv} and $d_{\mathcal{I}}$ as in Conjectures 1 and 2, results in the (T) theoretical world derived from B and MHB as in Theorems 7 and 8.



(a) $s = 128$.

(b) $s = 256$.

Fig. 10. Lower bounds on the minimum number of rounds needed to reach a security level of s bits derived from $\mathcal{C}_{\mathrm{alg}} \in \{\mathcal{C}_{\mathrm{GB}}, \mathcal{C}_{\mathrm{FGLM}}\}$ using $\mathcal{P}_{\mathrm{CICO}} \subset \mathbb{F}_p[y_0, s_N, \ldots, s_1]$ with $\alpha = 7$. The red line indicates the results of the original analysis in [BBC+23], adapted to $2 \leq \omega \leq 3$, and N^* highlights the suggested round number as in Equation (30)(b), both *without* additional security margin (a). Results in the (E) experimental world derived from d_{solv} and $d_{\mathcal{I}}$ as in Conjectures 1 and 2, results in the (T) theoretical world derived from B and MHB as in Theorems 7 and 8.



(a) $s = 128$.

(b) $s = 256$.

Fig. 11. Lower bounds on the minimum number of rounds needed to reach a security level of s bits derived from $\mathcal{C}_{\mathrm{alg}} \in \{\mathcal{C}_{\mathrm{GB}}, \mathcal{C}_{\mathrm{FGLM}}\}$ using $\mathcal{P}_{\mathrm{CICO}} \subset \mathbb{F}_p[y_0, s_N, \ldots, s_1]$ with $\alpha = 11$. The red line indicates the results of the original analysis in [BBC+23], adapted to $2 \leq \omega \leq 3$, and N^* highlights the suggested round number as in Equation (30)(b), both *without* additional security margin (a). Results in the (E) experimental world derived from d_{solv} and $d_{\mathcal{I}}$ as in Conjectures 1 and 2, results in the (T) theoretical world derived from B and MHB as in Theorems 7 and 8.

D Proof Theorem 7 (Bézout bound)

Proof. Let $N \geq r_\alpha$. $\mathcal{P}_{\text{CICO}}$ is a polynomial equation system in $n_v = N+1$ variables and $n_e = N+1$ equations, thereof 1 of degree $\max\{2r, \alpha\}$ for each $1 \leq r \leq N$, and 1 of degree $N+1$. By Theorem 4, the number of solutions to the polynomial equation system is bounded from above by

$$\begin{aligned} \mathrm{B} &= (N+1) \cdot \prod_{r=1}^{N} \max\{2r, \alpha\} = (N+1) \cdot \prod_{r=1}^{r_\alpha - 1} \alpha \cdot \prod_{r=r_\alpha}^{N} 2r \\ &= (N+1) \cdot \alpha^{r_\alpha - 1} \cdot 2^{N - r_\alpha + 1} \prod_{r=r_\alpha}^{N} r = \alpha^{r_\alpha - 1} \cdot 2^{N - r_\alpha + 1} \cdot \frac{(N+1)!}{(r_\alpha - 1)!}. \end{aligned}$$

□

E Proof Theorem 8 (Multihomogeneous Bézout bound)

We proof Theorem 8 for $\alpha \in \{3, 5, 7\}$ by induction using the idea of the *Row Expansion Algorithm*, presented in Appendix A. Concrete degree matrices for a small number of rounds for $\alpha \in \{3, 5, 7, 11\}$ are given in Tables 9 and 10.

Proof. Let $\alpha \in \{3, 5, 7\}$ and $N \geq r_\alpha$. We consider the partition of the variable set $X = \{y_0, s_1, \ldots, s_N\}$ into $m = n_v - r_\alpha = N + 1 - r_\alpha$ sets. In particular, we group the input variables y_0 and the first r_α state variables $s_1, \ldots, s_{r_\alpha}$. The remaining variables form individual groups of size one each:

$$\mathcal{Z} = \{\{y_0, s_1, \ldots, s_{r_\alpha}\}, \{s_{r_\alpha+1}\}, \ldots, \{s_N\}\} = \{X_1, \ldots, X_m\}.$$

The degree matrix $D_\alpha^{(N)} \in \mathbb{Z}_{\geq 0}^{(N+1)\times(N+1-r_\alpha)}$ is given by

$$D_\alpha^{(N)} = \begin{array}{c|c|c|} & X_1 & X_2 \cdots X_m \\ \hline p_1 & \alpha & \\ \vdots & \vdots & 0 \\ \vdots & \alpha & \\ p_{r_\alpha} & 2r_\alpha & \\ \hline p_{r_\alpha+1} & 2(r_\alpha+1) & \\ \vdots & \vdots & A_\alpha^{(N)} \\ p_N & 2(r_\alpha+1) & \\ \hline x_{N+1} & r_\alpha+1 & 2 \cdot \dots \cdot 2 \end{array}, \qquad A_\alpha^{(N)} = \begin{bmatrix} \alpha & 0 & \cdots & 0 \\ 4 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 4 & \cdots & 4 & \alpha \end{bmatrix}$$

with $A_\alpha^{(N)} \in \mathbb{Z}_{\geq 0}^{(N-r_\alpha)\times(N-r_\alpha)}$. See also Table 9. By Theorem 6, the multihomogeneous Bézout bound with respect to the variable partition $\mathcal{Z}$ is given by the coefficient of $t_1^{r_\alpha+1} \cdot t_2 \cdots t_m$ in the product of linear forms $\mathcal{L}(D_\alpha^{(N)})$, where for simplicity we defined

$$\mathcal{L}(D) := \prod_{i=1}^{n} \sum_{j=1}^{m} d_{i,j} t_j.$$

As the first r_α rows of $D_\alpha^{(N)}$ each only contains one nonzero entry in the column associated to X_1, t_1 will contribute to $\mathcal{L}(D_\alpha^{(N)})$ via these rows with exponent r_α and coefficient $\alpha^{r_\alpha - 1} \cdot 2r_\alpha$. Removing these rows from $D_\alpha^{(N)}$, the exponent of t_1 in $\mathcal{L}(D_\alpha^{(N)})$ has to be lowered by r_α. Let $\tilde{D}_\alpha^{(N)} \in \mathbb{Z}_{\geq 0}^{(N-r_\alpha+1)\times(N-r_\alpha+1)} = \mathbb{Z}_{\geq 0}^{m\times m}$ denote the modified degree matrix, where the first r_α rows of $D_\alpha^{(N)}$ were removed, that is,

$$\tilde{D}_\alpha^{(N)} = \begin{array}{c} \begin{array}{cc} X_1 & \quad X_2 \cdots X_m \end{array} \\ \left[\begin{array}{c|c} 2(r_\alpha+1) & \\ \vdots & A_\alpha^{(N)} \\ 2(r_\alpha+1) & \\ \hline r_\alpha+1 & 2\cdots\cdots 2 \end{array}\right] \end{array} = \begin{array}{c} \begin{array}{cccccc} X_1 & X_2 & \cdots & X_{m-1} & X_m \end{array} \\ \left[\begin{array}{cccccc} 2(r_\alpha+1) & \alpha & 0 & \cdots & 0 & 0 \\ \vdots & 4 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ 2(r_\alpha+1) & 4 & \cdots & 4 & \alpha & 0 \\ 2(r_\alpha+1) & 4 & \cdots & 4 & 4 & \alpha \\ r_\alpha+1 & 2 & \cdots & 2 & 2 & 2 \end{array}\right] \end{array}.$$

Then

$$\left[t_1^{r_\alpha+1} \cdot t_2 \cdots t_m\right] \ \mathcal{L}(D_\alpha^{(N)}) = 2r_\alpha \cdot \alpha^{r_\alpha-1} \cdot [t_1 \cdot t_2 \cdots t_m] \ \mathcal{L}(\tilde{D}_\alpha^{(N)}). \tag{32}$$

For $N = r_\alpha$, that is, $m = 1$, $\mathcal{L}(\tilde{D}_\alpha^{(N)}) = (r_\alpha + 1) \cdot t_1$, and thus

$$\left[t_1^{r_\alpha+1} \cdot t_2 \cdots t_m\right] \ \mathcal{L}(D_\alpha^{(N)}) = 2r_\alpha \cdot \alpha^{r_\alpha-1} \cdot (r_\alpha+1). \tag{33}$$

Let $N > r_\alpha$. There are only two ways in which t_m can enter the product $\mathcal{L}(\tilde{D}_\alpha^{(N)})$. Either via the second last row (with coefficient α) or the last row (with coefficient 2). It is easy to see that

$$\begin{aligned} [t_1 \cdot t_2 \cdots t_m] \ \mathcal{L}(\tilde{D}_\alpha^{(N)}) = \quad & \alpha \cdot [t_1 \cdot t_2 \cdots t_{m-1}] \ \mathcal{L}(\tilde{D}_\alpha^{(N-1)}) \quad + \\ & 2 \cdot [t_1 \cdot t_2 \cdots t_{m-1}] \ \mathcal{L}(B_\alpha^{(N)}), \end{aligned} \tag{34}$$

where $B_\alpha^{(N)} \in \mathbb{Z}_{\geq 0}^{(N-r_\alpha)\times(N-r_\alpha)} = \mathbb{Z}_{\geq 0}^{(m-1)\times(m-1)}$ always takes a form similar to a lower triangular matrix, where the first diagonal (the one above the main diagonal) is filled with α. That is,

$$B_\alpha^{(N)} = \begin{array}{c} \begin{array}{ccccc} X_1 & X_2 & \cdots & & X_{m-1} \end{array} \\ \left[\begin{array}{ccccc} 2(r_\alpha+1) & \alpha & 0 & \cdots & 0 \\ 2(r_\alpha+1) & 4 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ \vdots & \vdots & & \ddots & \alpha \\ 2(r_\alpha+1) & 4 & \cdots & \cdots & 4 \end{array}\right] \end{array} = \begin{array}{c} \begin{array}{cc} X_1 & \quad X_2 \cdots X_{m-1} \end{array} \\ \left[\begin{array}{c|c} 2(r_\alpha+1) & \\ \vdots & A_\alpha^{(N-1)} \\ 2(r_\alpha+1) & \\ \hline 2(r_\alpha+1) & 4\cdots\cdots 4 \end{array}\right] \end{array}.$$

We will prove by induction over N (and thus implicitly m) that for $N > r_\alpha$

(A) $[t_1 \cdot t_2 \cdots t_{m-1}] \ \mathcal{L}(B_\alpha^{(N)}) = 2(r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha-1}$, and

(B) $[t_1 \cdot t_2 \cdots t_m] \ \mathcal{L}(\tilde{D}_\alpha^{(N)}) = (r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha}$.

Inserting these results into (32) concludes the proof:

$$\begin{aligned}\text{MHB} &= \left[t_1^{r_\alpha+1} \cdot t_2 \cdots t_m\right]\ \mathcal{L}(D_\alpha^{(N)}) = 2r_\alpha \cdot \alpha^{r_\alpha-1} \cdot [t_1 \cdot t_2 \cdots t_m]\ \mathcal{L}(\tilde{D}_\alpha^{(N)}) \\ &= 2r_\alpha \cdot \alpha^{r_\alpha-1} \cdot (r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha}.\end{aligned}$$

In particular, $\tau_\alpha = 2r_\alpha \cdot \alpha^{r_\alpha-1} \cdot (r_\alpha+1)$.

Induction proofs:

(A) To show: $[t_1 \cdot t_2 \cdots t_{m-1}]\ \mathcal{L}(B_\alpha^{(N)}) = 2(r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha-1}$, for $N > r_\alpha$.
- *Base case*:
  - For $N = r_\alpha + 1$ ($m = 2$):

$$\begin{aligned}[t_1]\ \mathcal{L}(B_\alpha^{(N)}) &= [t_1]\ (2(r_\alpha+1)t_1 + \alpha t_2) = 2(r_\alpha+1) \\ &= 2(r_\alpha+1) \cdot (\alpha+4)^0 = 2(r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha-1}.\end{aligned}$$

  - For $N = r_\alpha + 2$ ($m = 3$):

$$\begin{aligned}[t_1 \cdot t_2]\ \mathcal{L}(B_\alpha^{(N)}) &= [t_1 \cdot t_2]\,(2(r_\alpha+1)t_1 + \alpha t_2) \cdot (2(r_\alpha+1)t_1 + 4t_2) \\ &= 2(r_\alpha+1) \cdot (\alpha+4)^1 = 2(r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha-1}.\end{aligned}$$

- *Induction hypothesis*: Assume that

$$[t_1 \cdots t_{m-2}]\ \mathcal{L}(B_\alpha^{(N-1)}) = 2(r_\alpha+1) \cdot (\alpha+4)^{(N-1)-r_\alpha-1}.$$

- *Induction step*: ($N-1 \to N$). Given $B_\alpha^{(N)}$, the last column, associated with X_{m-1}, contains only two nonzero entries in the last two rows. Removing one of those rows and the last column from $B_\alpha^{(N)}$ results in $B_\alpha^{(N-1)}$. Thus:

$$\begin{aligned}&[t_1 \cdots t_{m-1}]\ \mathcal{L}(B_\alpha^{(N)}) \\ &\quad= \alpha \cdot [t_1 \cdots t_{m-2}]\ \mathcal{L}(B_\alpha^{(N-1)}) + 4 \cdot [t_1 \cdots t_{m-2}]\ \mathcal{L}(B_\alpha^{(N-1)}) \\ &\quad= (\alpha+4) \cdot [t_1 \cdots t_{m-2}]\ \mathcal{L}(B_\alpha^{(N-1)}) = 2(r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha-1}.\end{aligned}$$

(B) To show: $[t_1 \cdot t_2 \cdots t_m]\ \mathcal{L}(\tilde{D}_\alpha^{(N)}) = (r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha}$, for $N > r_\alpha$.
- *Base case*: For $N = r_\alpha + 1$ ($m = 2$):

$$\begin{aligned}[t_1 \cdot t_2]\ \mathcal{L}(\tilde{D}_\alpha^{(N)}) &= [t_1 \cdot t_2]\ (2(r_\alpha+1)t_1 + \alpha t_2) \cdot ((r_\alpha+1)t_1 + 2t_2) \\ &= (r_\alpha+1) \cdot (\alpha+4)^1 = (r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha}.\end{aligned}$$

- *Induction hypothesis*: Assume that

$$[t_1 \cdot t_2 \cdots t_{m-1}]\ \mathcal{L}(\tilde{D}_\alpha^{(N-1)}) = (r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha-1}.$$

- *Induction step*: ($N-1 \to N$). Combining (34) and the previous result for $[t_1 \cdots t_{m-1}]\ \mathcal{L}(B_\alpha^{(N)})$ yields:

$$\begin{aligned}&[t_1 \cdot t_2 \cdots t_m]\ \mathcal{L}(\tilde{D}_\alpha^{(N)}) \\ &\quad= \alpha \cdot [t_1 \cdot t_2 \cdots t_{m-1}]\ \mathcal{L}(\tilde{D}_\alpha^{(N-1)}) + 2 \cdot [t_1 \cdot t_2 \cdots t_{m-1}]\ \mathcal{L}(B_\alpha^{(N)}) \\ &\quad= \alpha \cdot (r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha-1} + 2 \cdot 2(r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha-1} \\ &\quad= (r_\alpha+1) \cdot (\alpha+4)^{N-r_\alpha}.\end{aligned}$$

□

Table 9. Degree matrices $D_\alpha^{(N)}$ for $N \geq r_\alpha$ and $\alpha \in \{3, 5, 7\}$ with respect to the variable set partition $\{\{y_0, s_1, \ldots, s_{r_\alpha}\}, \{s_{r_\alpha+1}\}, \ldots, \{s_N\}\}$.

$$D_3^{(2)} = \left[\begin{array}{c} 3 \\ 4 \\ \hline\hline 3 \end{array}\right] \qquad D_3^{(3)} = \left[\begin{array}{c|c} 3 & 0 \\ 4 & 0 \\ \hline 6 & 3 \\ \hline 3 & 2 \end{array}\right] \qquad D_3^{(4)} = \left[\begin{array}{c|cc} 3 & 0 & 0 \\ 4 & 0 & 0 \\ \hline 6 & 3 & 0 \\ 6 & 4 & 3 \\ \hline 3 & 2 & 2 \end{array}\right] \qquad D_3^{(5)} = \left[\begin{array}{c|ccc} 3 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 \\ \hline 6 & 3 & 0 & 0 \\ 6 & 4 & 3 & 0 \\ 6 & 4 & 4 & 3 \\ \hline 3 & 2 & 2 & 2 \end{array}\right]$$

$$D_5^{(3)} = \left[\begin{array}{c} 5 \\ 5 \\ 6 \\ \hline\hline 4 \end{array}\right] \qquad D_5^{(4)} = \left[\begin{array}{c|c} 5 & 0 \\ 5 & 0 \\ 6 & 0 \\ \hline 8 & 5 \\ \hline 4 & 2 \end{array}\right] \qquad D_5^{(5)} = \left[\begin{array}{c|cc} 5 & 0 & 0 \\ 5 & 0 & 0 \\ 6 & 0 & 0 \\ \hline 8 & 5 & 0 \\ 8 & 4 & 5 \\ \hline 4 & 2 & 2 \end{array}\right] \qquad D_5^{(6)} = \left[\begin{array}{c|ccc} 5 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 \\ \hline 8 & 5 & 0 & 0 \\ 8 & 4 & 5 & 0 \\ 8 & 4 & 4 & 5 \\ \hline 4 & 2 & 2 & 2 \end{array}\right]$$

$$D_7^{(4)} = \left[\begin{array}{c} 7 \\ 7 \\ 7 \\ 8 \\ \hline\hline 5 \end{array}\right] \qquad D_7^{(5)} = \left[\begin{array}{c|c} 7 & 0 \\ 7 & 0 \\ 7 & 0 \\ 8 & 0 \\ \hline 10 & 7 \\ \hline 5 & 2 \end{array}\right] \qquad D_7^{(6)} = \left[\begin{array}{c|cc} 7 & 0 & 0 \\ 7 & 0 & 0 \\ 7 & 0 & 0 \\ 8 & 0 & 0 \\ \hline 10 & 7 & 0 \\ 10 & 4 & 7 \\ \hline 5 & 2 & 2 \end{array}\right] \qquad D_7^{(7)} = \left[\begin{array}{c|ccc} 7 & 0 & 0 & 0 \\ 7 & 0 & 0 & 0 \\ 7 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 \\ \hline 10 & 7 & 0 & 0 \\ 10 & 4 & 7 & 0 \\ 10 & 4 & 4 & 7 \\ \hline 5 & 2 & 2 & 2 \end{array}\right]$$

Table 10. Degree matrices $D_\alpha^{(N)}$ for $N \geq 1$ and $\alpha = 11$ with respect to the variable set partition $\{\{y_0\}, \{s_1\}, \ldots, \{s_N\}\}$.

$$D_{11}^{(1)} = \left[\begin{array}{c|c} 2 & 11 \\ \hline 1 & 2 \end{array}\right] \qquad D_{11}^{(2)} = \left[\begin{array}{c|cc} 2 & 11 & 0 \\ 2 & 4 & 11 \\ \hline 1 & 2 & 2 \end{array}\right] \qquad D_{11}^{(3)} = \left[\begin{array}{c|ccc} 2 & 11 & 0 & 0 \\ 2 & 4 & 11 & 0 \\ 2 & 4 & 4 & 11 \\ \hline 1 & 2 & 2 & 2 \end{array}\right]$$