Functional Decomposition of Multivariate Polynomials: Revisit and New Improvements

Dong-Jie Guo, Qun-Xiong Zheng, Zhong-Xiao Wang and Xiao-Xin Zhao

Abstract

The Functional Decomposition Problem (FDP) involves expressing a given set of multivariate polynomials as a composition of simpler polynomials. Traditional methods, such as Faugère-Perret's $\mathrm{Algo}_{\mathrm{FDP}}$ and its generalized variant **MultiComPoly**, rely on Gröbner basis computations on ideals generated from derivatives of composed polynomials $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$, where $\boldsymbol{f}$ and $\boldsymbol{g}$ are called left-factor and right-factor of $\boldsymbol{h}$, respectively. The computational cost of these methods increases significantly with both the number of variables and the degrees of the component polynomials in $\boldsymbol{f}$ and $\boldsymbol{g}$, and their existing complexity estimates are not sufficiently precise. This paper presents two algorithmic improvements to FDP. First, we replace Gröbner basis computation with Gauss–Jordan elimination (GJE) to convert the coefficient matrix into its reduced row-echelon form (RREF), offering a clearer formulation of a key step in **MultiComPoly**. The resulting algorithm, named **RREFComPoly**, integrates this change. Additionally, by using exact binomials in place of original binomial approximations and refining the estimation of a critical parameter, we achieve a tighter complexity bound than that of **MultiComPoly**. Our second and more impactful contribution, **PartComPoly**, inverts the conventional FDP workflow. Instead of directly recovering the vector space spanned by the component polynomials of $\boldsymbol{g}$, **PartComPoly** first uses a localization strategy to recover $\boldsymbol{f}$ and partial information of $\boldsymbol{g}$ with **RREFComPoly**, and then iteratively reconstructs $\boldsymbol{g}$ by solving a series of linear systems derived from the obtained $\boldsymbol{f}$ and partial information of $\boldsymbol{g}$. This inversion dramatically reduces computational complexity and expands the solvable domain of FDP, making previously intractable instances – such as those which were claimed to be not computationally exploitable in [1, page 175] – computationally tractable for the first time. Our experiments have confirmed the correctness and validity of both algorithms **RREFComPoly** and **PartComPoly**.

Index Terms

Functional Decomposition Problem (FDP), $2\mathrm{R}/2\mathrm{R}^{-}$ schemes, **MultiComPoly**, Gaussian-Jordan elimination (GJE), Reduced Row-Echelon Form (RREF), **RREFComPoly**, localization strategy, **PartComPoly**.

I. Introduction

The Functional Decomposition Problem (FDP) for multivariate polynomials (introduced in Subsection II-B) is not only a classical problem in computer algebra [2], [3], [4], [5], [6], but also has applications in computer aided geometry [7], signal processing [8], [9] and cryptography [10], [11] for instance. The decomposition of univariate polynomials is thoroughly investigated both algorithmically and theoretically [2], [3], [4], [12], [13], [14], [15]. This maturity is evidenced by the incorporation of univariate decomposition as standard functionality in major computer algebra systems (for instance, **compoly** of Maple). However, for general multivariate decomposition, the situation is different and probably more complicated. Unlike the univariate setting – where Ritt's Theorem [12], [14], provides foundational structure – no equivalent theoretical framework exists for multivariate polynomials. An early overview of FDP can be found in the Ph.D. thesis of Dickerson [16]. Building on univariate foundations, von zur Gathen, Gutiérrez and Rubio [5] systematically studied three restricted variants of FDP: uni-multivariate, multi-univariate, and single-variable decompositions. Their work provided both practical algorithms and theoretical insight for these structured cases. The general FDP for multivariate polynomials remained intractable and has been proved NP-hard by Dickerson [16].

Recent advances in the decomposition of general multivariate polynomials are motivated by cryptographic applications. In 1997, Patarin and Goubin proposed two-round schemes $2\mathrm{R}$ (introduced in Subsection II-C), where the public key can be represented as the composition of two sets of n quadratic polynomials [10]. The security of these schemes is based on the

This work was supported by the National Key Research and Development Program of China (No. 2024YFB4504700) and the National Natural Science Foundation of China (No. 12371526, No. 62202494).

Dong-Jie Guo, Qun-Xiong Zheng, Zhong-Xiao Wang and Xiao-Xin Zhao are with the School of Cyber Science and Technology, Information Engineering University, Zhengzhou 450001, China (e-mails: djie_guo@163.com; qunxiong_zheng@163.com; zhongxiao_wang@126.com; zhaoxiaoxin46@126.com) (Corresponding authors: Qun-Xiong Zheng and Zhong-Xiao Wang).

difficulty of decomposing the public key into two sets of n quadratic polynomials. However, this kind of FDP for multivariate polynomials is vulnerable to attack. In 1999, Ye, Dai and Lam developed an efficient method based on differentiation and homogenization to decompose (if such a decomposition exists) a set of n polynomials of degree four into two sets of n quadratic polynomials, which rendered the $2\mathrm{R}$ schemes widely regarded as weak [17] [18]. To thwart this attack, the $2\mathrm{R}^-$ signature schemes were proposed, which drop some polynomials of an original $2\mathrm{R}$ public key [11]. This adjustment transformed the public key from an injective mapping to a many-to-one mapping, thereby rendering it applicable only to signature scenarios. In 2006, Faugère and Perret combined the differentiation and homogenization-based method with the Gröbner basis method (specifically, F_5 algorithm [19]) to propose a method to attack $2\mathrm{R}/2\mathrm{R}^-$ schemes, which they called $\mathrm{Algo}_{\mathrm{FDP}}$ [20]. In particular, they successfully solved FDP instances used in $2\mathrm{R}^-$ schemes, solving most of the challenges proposed in [11] within hours. Building on this work, Faugère and Perret introduced an extended algorithm called **MultiComPoly**, designed to decompose multivariate polynomials of arbitrary, but the same degree (i.e. all component polynomials in the left-factor have the same degree, and likewise for the right-factor) [21], [22]. Moreover, they prove that the algorithm works correctly for generic decomposable instances in the special cases where the degree of the left-factor is 2 or 3, and the degree of the right-factor is 2 in [23]. Further progress was made in 2012 when Zhao, Feng and Gao addressed a conjecture posed by Ye, Dai and Lam in [17], proving that the correct decomposition factors for a set of polynomials could indeed be computed from its right-factor space [24].

As far as we know, **MultiComPoly** is the only effective algorithm for decomposing general multivariate polynomials. When the degree of the left-factor is higher than two, they solved FDP by using high order partial derivatives [22] in **MultiComPoly**. However, in 2010, Zhao and Feng observed that **MultiComPoly** would fail practically if the right-factor polynomials were of higher degrees, such as degree three [1]. Moreover, the method also exhibits prohibitive computational complexity, which grows rapidly with both the number of variables and the degrees of the component polynomials in $\boldsymbol{f}$ and $\boldsymbol{g}$ — a behavior captured by the complexity estimate established in [22].

Our contributions in this paper are twofold:

(i) First, we propose a clearer version of **MultiComPoly** described by REFF, called RREFComPoly for convenience, and provide a more precise complexity estimate compared to **MultiComPoly**. The main idea of **RREFComPoly** is to replace the computation of Gröbner basis with a single call of Gauss-Jordan elimination (GJE) when recovering the linear space spanned by the component polynomials of $\boldsymbol{g}$. Moreover, we replace the traditional approximation of binomials in the complexity analysis of **MultiComPoly** with exact binomials and refine the estimate for a crucial parameter δ (see Subsection IV-B), which has a significant impact on computational complexity. These refinements enable **RREFComPoly** to achieve a sharper complexity bound than **MultiComPoly**.

(ii) Second, and most importantly, we propose the **PartComPoly** algorithm which employs a localization strategy and inverts the conventional FDP workflow to significantly reduce computational complexity. Instead of prioritizing recovery of the linear space spanned by the component polynomials of $\boldsymbol{g}$, **PartComPoly** first assigns partial variables of $\boldsymbol{h}$ to 0 and then computes the left-factor $\boldsymbol{f}$ and partial information of $\boldsymbol{g}$ with **RREFComPoly**. Second, it iteratively reconstructs the right-factor $\boldsymbol{g}$ by solving a series of linear systems derived from the obtained $\boldsymbol{f}$ and partial information of $\boldsymbol{g}$. This strategy not only dramatically reduces computational complexity, but also extends its applicability to a larger class of FDP instances, making previously intractable instances – such as those which were claimed to be not computationally exploitable in [1] – computationally tractable for the first time.

Moreover, we prove the correctness of **RREFComPoly** and **PartComPoly** in the sense of the Zariski topology. We also performed extensive experiments to verify the correctness and performance of our newly proposed algorithms; for details, see VI.

The rest of this paper is organized as follows. Section II introduces some necessary preliminary knowledge, including definitions and lemmas essential to understand the subsequent sections. Section III revisits the **MultiComPoly** algorithm. Section IV provides a detailed introduction to our proposed RREF-based algorithm — RREFComPoly. Section V gives the main contribution of this paper, the **PartComPoly** algorithm, detailing its principle and process. Section VI provides experimental results and analysis. Section VII concludes this paper and discusses potential future work.

II. PRELIMINARIES

A. Gröbner Basis

We first give a brief introduction to the theory of Gröbner bases. For more details, refer to [25].

Let $\mathbb{K}$ be a field and let $\mathbb{K}[x_1, x_2, \ldots, x_n]$ be the polynomial ring over $\mathbb{K}$ with indeterminates $x_1, x_2, \ldots, x_n$. A product of the form $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ is called a monomial in $x_1, x_2, \ldots, x_n$, where all exponents $\alpha_1, \alpha_2, \ldots, \alpha_n$ are nonnegative integers. The (total) degree of this monomial, denoted by $\deg(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n})$, is the sum $\alpha_1 + \alpha_2 + \cdots + \alpha_n$. To deal with polynomials in $\mathbb{K}[x_1, x_2, \ldots, x_n]$, we need to first determine the order on monomials. The computation of Gröbner bases is closely related to the monomial orders: different orders may yield different Gröbner bases, and the efficiency of computing a Gröbner basis is highly dependent on the order. One of the most prominent monomial orders in practice is the graded reverse lex (grevlex) order, which is defined as follows.

Definition 1. *(Graded Reverse Lex Order) [25] Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n), \boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, where $\mathbb{N}$ is the set of nonnegative integers. We say $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \prec x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$, if $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, or $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ and the right-most nonzero entry of $\boldsymbol{\alpha} - \boldsymbol{\beta}$ is positive.*

Throughout this paper, we only consider the grevlex order. Moreover, we denote by $\boldsymbol{x}^{\boldsymbol{\alpha_i}}$ the monomial $x_1^{\alpha_{i_1}} x_2^{\alpha_{i_2}} \cdots x_n^{\alpha_{i_n}}$, where $\boldsymbol{\alpha_i} = (\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n}) \in \mathbb{N}^n$. Let f be a nonzero polynomial in $\mathbb{K}[x_1, \ldots, x_n]$. Then f can be uniquely expressed as $f = \sum_{i=1}^w c_{\boldsymbol{\alpha_i}} \boldsymbol{x}^{\boldsymbol{\alpha_i}}$ for some positive integer w, where $c_{\boldsymbol{\alpha_i}} \in \mathbb{K} \setminus \{0\}$ and $\boldsymbol{x}^{\boldsymbol{\alpha_w}} \prec \cdots \prec \boldsymbol{x}^{\boldsymbol{\alpha_2}} \prec \boldsymbol{x}^{\boldsymbol{\alpha_1}}$. We call $\boldsymbol{x}^{\boldsymbol{\alpha_1}}$ the leading monomial of f, denoted by $\mathrm{LM}(f) = \boldsymbol{x}^{\boldsymbol{\alpha_1}}$; $c_{\boldsymbol{\alpha_1}} \boldsymbol{x}^{\boldsymbol{\alpha_1}}$ the leading term of f, denoted by $\mathrm{LT}(f) = c_{\boldsymbol{\alpha_1}} \boldsymbol{x}^{\boldsymbol{\alpha_1}}$; $c_{\boldsymbol{\alpha_1}}$ the leading coefficient of f, denoted by $\mathrm{LC}(f) = c_{\boldsymbol{\alpha_1}}$. The (total) degree of f is $\deg(f) = \max\{\deg(\boldsymbol{x}^{\boldsymbol{\alpha_i}}) : 1 \le i \le w\}$. A polynomial f is called a homogeneous polynomial if all monomials of f have the same degree.

The grevlex order naturally induces an order for polynomials in $\mathbb{K}[x_1, x_2, \ldots, x_n]$. More precisely, for two polynomials $f = \sum_{i=1}^w c_{\boldsymbol{\alpha_i}} \boldsymbol{x}^{\boldsymbol{\alpha_i}}, g = \sum_{i=1}^s c_{\boldsymbol{\beta_i}} \boldsymbol{x}^{\boldsymbol{\beta_i}} \in \mathbb{K}[x_1, x_2, \ldots, x_n]$, we say that $f \prec' g$ if there exists a positive integer k such that $\boldsymbol{x}^{\boldsymbol{\alpha_i}} = \boldsymbol{x}^{\boldsymbol{\beta_i}}$ for $1 \le i < k$ but $\boldsymbol{x}^{\boldsymbol{\alpha_k}} \prec \boldsymbol{x}^{\boldsymbol{\beta_k}}$, or $w < s$ and $\boldsymbol{x}^{\boldsymbol{\alpha_i}} = \boldsymbol{x}^{\boldsymbol{\beta_i}}$ for $1 \le i \le w$.

For any subset S of $\mathbb{K}[x_1, x_2, \ldots, x_n]$, let us denote $\mathrm{LM}(S) = \{\mathrm{LM}(f) : f \in S\}$ and $\langle \mathrm{LM}(S) \rangle$ the ideal generated by the elements of $\mathrm{LM}(S)$. Then the definition of Gröbner bases can be given as follows.

Definition 2. *[25] Let I be a nonzero ideal of $\mathbb{K}[x_1, x_2, \ldots, x_n]$. A finite subset $G = \{g_1, g_2, \ldots, g_t\}$ of I is said to be a Gröbner basis of I if $0 \notin G$ and $\langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_t) \rangle = \langle \mathrm{LM}(I) \rangle$. Moreover, a Gröbner basis G is said to be reduced if every $g \in G$ is monic and no monomial of g is divisible by any of $\mathrm{LM}(G \setminus \{g\})$.*

It is well-known that for any nonzero ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ and any fixed monomial order, there exists a unique reduced Gröbner basis. Informally, a Gröbner basis G of an ideal I is a set of generators of I with "good properties". One of "good properties" is that any polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ yields a unique remainder modulo G (called the normal form of f modulo G). Another is that for any $f \in I$, the normal form of f modulo G is 0. Each of them can be used to define a Gröbner basis, and some other equivalent definitions can be found in [26].

Gröbner bases are a fundamental tool to study algebraic systems, which provides an algorithmic solution for several problems related to polynomial systems. Traditionally, Buchberger's algorithms [27] have served as the historic method for computing Gröbner bases. However, in recent years, more efficient algorithms have been introduced. To date, the F_5 algorithm [19] is recognized as the most effective one for computing Gröbner bases.

A Gröbner basis w.r.t. grevlex order has several interesting properties such as Lemmas 1 and 2.

Lemma 1. *[28] Let I be a nonzero ideal of $\mathbb{K}[x_1, x_2, \ldots, x_n]$, $d = \min\{\deg(f) : f \in I \setminus \{0\}\}$ and let G be a Gröbner basis of I w.r.t. grevlex order. If we denote by $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$ the vector space spanned by the polynomials $g_1, g_2, \ldots, g_n$ over $\mathbb{K}$, i.e., $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n) = \{\sum_{i=1}^n c_i g_i : c_i \in \mathbb{K}\}$, then we have*

$$\mathrm{Span}_{\mathbb{K}}(g \in G : \deg(g) = d) = \{g \in I : \deg(g) = d\}.$$

Lemma 2. *[20] Let $f \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ be a nonzero homogeneous polynomial, $\mathrm{LM}(f)$ the leading monomial of f and m a positive integer. Then we have*

$$x_n^m \mid f \quad \textit{if and only if} \quad x_n^m \mid \mathrm{LM}(f).$$

We recall the quotient of ideals which will be used frequently in Section III.

Definition 3. *[25] Let I and J be two nonzero ideals in $\mathbb{K}[x_1, x_2, \ldots, x_n]$. The **ideal quotient** of I by J, denoted by $I : J$, is the set $I : J = \{f \in \mathbb{K}[x_1, x_2, \ldots, x_n] : fg \in I \text{ for all } g \in J\}$.*

B. Functional Decomposition Problem (FDP)

In this subsection, we will briefly review Functional Decomposition Problem (FDP) [16] [18], which is not only of mathematical interest, but also serves a foundation to the security of 2R and 2R$^-$ schemes.

Let u, m, n be three positive integers and let $\boldsymbol{h} = (h_1, h_2, \ldots, h_u) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u$. We say that

$$(\boldsymbol{f} = (f_1, f_2, \ldots, f_u), \boldsymbol{g} = (g_1, g_2, \ldots, g_m)) \in \mathbb{K}[x_1, x_2, \ldots, x_m]^u \times \mathbb{K}[x_1, x_2 \ldots, x_n]^m$$

is a decomposition of $\boldsymbol{h} = (h_1, h_2 \ldots, h_u)$ if $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$, or equivalently,

$$(h_1, h_2, \ldots, h_u) = (f_1(g_1, g_2, \ldots, g_m), f_2(g_1, g_2, \ldots, g_m), \ldots, f_u(g_1, g_2, \ldots, g_m)).$$

In the case of $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$, $\boldsymbol{h}$ is called the composition of $\boldsymbol{f}$ and $\boldsymbol{g}$, whereas $\boldsymbol{f}$ and $\boldsymbol{g}$ are called the left-factor and the right-factor of $\boldsymbol{h}$, respectively. The decomposition of $\boldsymbol{h}$ is not unique. Indeed, for any $m \times m$ invertible matrix A over $\mathbb{K}$, it is clear that $\boldsymbol{g'} = (g'_1, g'_2, \ldots, g'_m) = (g_1, g_2, \ldots, g_m)A$ and $\boldsymbol{f'} = (f'_1, f'_2, \ldots, f'_u) = (f_1((x_1, x_2, \ldots, x_m)A^{-1}), f_2((x_1, x_2, \ldots, x_m)A^{-1}), \ldots, f_u((x_1, x_2, \ldots, x_m)A^{-1}))$ also satisfy $\boldsymbol{h} = \boldsymbol{f'} \circ \boldsymbol{g'}$ if $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$. Two decompositions $(\boldsymbol{f}, \boldsymbol{g})$ and $(\boldsymbol{f'}, \boldsymbol{g'})$ of $\boldsymbol{h}$ are called affine equivalent if there exists an invertible matrix A over $\mathbb{K}$ such that $\boldsymbol{g'} = \boldsymbol{g} \cdot A$.

It is worth noting that for any given $\boldsymbol{h} = (h_1, h_2, \ldots, h_u) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u$, there are some trivial decompositions. For example, $(\boldsymbol{f} = \boldsymbol{h}, \boldsymbol{g} = (x_1, x_2, \ldots, x_n, 0, \ldots, 0))$ and its affine equivalent decompositions if $m \geq n$; or $(\boldsymbol{f} = (x_1, x_2, \ldots, x_u), \boldsymbol{g} = (h_1, h_2, \ldots, h_u, 0, \ldots, 0))$ and its affine equivalent decompositions if $m \geq u$. A decomposition $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$ is called nontrivial if there exist f_i and g_j such that $\deg(f_i), \deg(g_j) > 1$. The so-called FDP is that given $\boldsymbol{h} = (h_1, h_2, \ldots, h_u) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u$, to find $\boldsymbol{f}$ and $\boldsymbol{g}$ (if exist) such that $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$ is a nontrivial decomposition.

As in [22], **this paper focuses on a restricted version of FDP, called FDP$_{\mathrm{H}}(\boldsymbol{h}, d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$**, which is described in detail as follows.

FDP$_{\mathrm{H}}(\boldsymbol{h}, d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$

Input: homogeneous polynomials $\boldsymbol{h} = (h_1, h_2, \ldots, h_u) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u$ with $\deg(h_1) = \deg(h_2) = \cdots = \deg(h_u)$, $u \leq n$, and two integers $d_{\boldsymbol{f}}, d_{\boldsymbol{g}} > 1$.

Output: homogeneous polynomials $(\boldsymbol{f} = (f_1, f_2, \ldots, f_u), \boldsymbol{g} = (g_1, g_2, \ldots, g_n)) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u \times \mathbb{K}[x_1, x_2, \ldots, x_n]^n$ (if exist) with $\deg(f_1) = \deg(f_2) = \cdots = \deg(f_u) = d_{\boldsymbol{f}}$ and $\deg(g_1) = \deg(g_2) = \cdots = \deg(g_n) = d_{\boldsymbol{g}}$ such that $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$. The output, if exists, of FDP$_{\mathrm{H}}(\boldsymbol{h}, d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$ is called a $(d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$-decomposition of $\boldsymbol{h}$.

C. The 2R and 2R$^-$ schemes

2R schemes (2R stands for 2 rounds) were introduced by Patarin and Goubin in [10]. The private key of 2R schemes consists of: three affine bijections α, β, γ: $\mathbb{K}^n \to \mathbb{K}^n$ and two bijections ψ, ϕ: $\mathbb{K}^n \to \mathbb{K}^n$ given by n quadratic multivariate polynomials, where $\mathbb{K}$ is a finite field with q elements. Quadratic multivariate polynomials are usually chosen from given S-boxes, triangular functions, or combinations of them, which can be easily inverted [10]. The public key of 2R schemes consists of: the field $\mathbb{K}$ and the n polynomials $\boldsymbol{h} = (h_1, h_2, \ldots, h_n) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^n$ corresponding to the composition of mappings $\alpha \circ \psi \circ \beta \circ \phi \circ \gamma$. Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ be a plaintext and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ the corresponding ciphertext. Then we have

$$\boldsymbol{y} = (y_1, y_2, \ldots, y_n) = (h_1(x_1, x_2, \ldots, x_n), \ldots, h_n(x_1, x_2, \ldots, x_n)) = \alpha \circ \psi \circ \beta \circ \phi \circ \gamma(x_1, x_2, \ldots, x_n).$$

If only u of these $h_1, h_2, \ldots, h_n$ are given with $1 \leq u < n$, then the 2R schemes become the 2R$^-$ schemes. Since the mappings corresponding to the 2R$^-$ schemes are many-to-one mappings, the 2R$^-$ schemes can only be used for signature, but not for encryption.

D. Zhao-Feng schemes

In response to decomposition attacks like **MultiComPoly** against 2R and 2R$^-$ schemes, Zhao and Feng proposed an enhanced design by replacing the original map ϕ with a bijection given by n cubic multivariate polynomials [1]. These polynomials are usually chosen from invertible components such as cubic S-boxes, cubic C^* maps, role exchange of C^*'s private and public keys, or cubic Feistel maps. To control the size of the public key, three key techniques are adopted: reducing the number of cubic terms in ϕ, restricting C^*-based branches to at most 8 bits, and utilizing simpler affine maps (see [1] for more details).

Consequently, the public key polynomials $\boldsymbol{h} = (h_1, h_2, \ldots, h_n) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^n$ in the Zhao-Feng schemes—which correspond to the mapping composition $\alpha \circ \psi \circ \beta \circ \phi \circ \gamma$ —achieve a degree of 6.

The authors argue that the public key polynomials of these enhanced schemes cannot be effectively decomposed using **MultiComPoly** [1]. In fact, when the higher-order partial derivatives of $\boldsymbol{h}$ lie in the ideal $\langle g_j : 1 \leq j \leq n \rangle$, **MultiComPoly** could employ these derivatives to recover the right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$. In these schemes, however, the last two terms (called noise terms) in the identity

$$\frac{\partial^2 h_i}{\partial x_m \partial x_j} = \sum a_{k,l} \left(\frac{\partial^2 g_k}{\partial x_m \partial x_j} g_l + \frac{\partial^2 g_l}{\partial x_m \partial x_j} g_k + \frac{\partial g_l}{\partial x_m} \cdot \frac{\partial g_k}{\partial x_j} + \frac{\partial g_k}{\partial x_m} \cdot \frac{\partial g_l}{\partial x_j} \right), 1 \leq i \leq u, 1 \leq m \leq j \leq n,$$

prevent the second-order partial derivatives from belonging to this ideal. The same holds for the higher-order partial derivatives. As a result, **MultiComPoly** is forced to rely solely on the first-order partial derivatives of $\boldsymbol{h}$ to build the Macaulay matrix associated with the ideal $\left\langle \frac{\partial h_i}{\partial x_j} : 1 \leq i \leq u, 1 \leq j \leq n \right\rangle$ in order to recover the right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$. Although the resulting Macaulay matrix remains sparse, its number of rows grows prohibitively large, rendering the attack computationally infeasible. Specifically, for parameters[1] in the range $39 \leq n \leq 101$ and $n - 20 \leq u \leq n - 4$, the number of rows (denoted as Row) of the Macaulay matrix in **MultiComPoly** range from $2^{33.3}$ to $2^{64.8}$. Since Row is already unacceptably large and, to make things worse for an attacker, at least $O(Row^2)$ operations are needed to compute the row echelon form of this matrix. The authors therefore conclude that the matrix, even vulnerable in theory, is not computationally exploitable in practice. More details can be found in [1, page 175].

E. Reduced Row-Echelon Form (RREF) of matrices

Since we will use the RREF of matrices to build algorithms for the decomposition of multivariate polynomials, we will briefly review the fundamental concept of RREF, which is formally defined as follows.

Definition 4. *[29] A matrix is of RREF if it meets all of the following conditions:*

1. *If there is a row where every entry is zero, then this row lies below any other row that contains a nonzero entry.*
2. *The leftmost nonzero entry of a row is equal to 1.*
3. *The leftmost nonzero entry of a row is the only nonzero entry in its column.*
4. *Consider two different nonzero leftmost entries, one located in row i, column j and the other located in row s, column t. If $s > i$, then $t > j$.*

III. REVISIT OF THE MULTICOMPOLY ALGORITHM

Let $\boldsymbol{h} = (h_1, h_2, \ldots, h_u) = \boldsymbol{f} \circ \boldsymbol{g} = (f_1(g_1, g_2, \ldots, g_n), f_2(g_1, g_2, \ldots, g_n), \ldots, f_u(g_1, g_2, \ldots, g_n)) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u$, where u, n are integers satisfying $1 \leq u \leq n$ and $f_i, g_j \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ are homogeneous polynomials with $\deg(f_i) = d_{\boldsymbol{f}} \geq 2, \deg(g_j) = d_{\boldsymbol{g}} \geq 2$ for all $1 \leq i \leq u$ and all $1 \leq j \leq n$. Inspired by [17], Faugère and Perret proposed an algorithm called $\mathrm{Algo}_{\mathrm{FDP}}$ in 2006, specifically designed to solve FDP for quadratic polynomials $\boldsymbol{f}$ and $\boldsymbol{g}$ [20]. The algorithm consists of three steps: first, it constructs an ideal $\partial I_h = \left\langle \frac{\partial h_i}{\partial x_j} : 1 \leq i \leq u, 1 \leq j \leq n \right\rangle$ of $\mathbb{K}[x_1, x_2, \ldots, x_n]$ using the partial derivatives of the known polynomials $h_1, h_2, \ldots, h_u$; second, it employs Gröbner bases techniques to extract the right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$ from ∂I_h, which is the most difficult step of this algorithm; finally, it recovers the left-factor polynomials by solving a linear system derived from a basis of the right-factor space. Subsequently, they refined and extended $\mathrm{Algo}_{\mathrm{FDP}}$, generalizing the decomposition from the case where $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ to a more general scenario where $d_{\boldsymbol{f}}$ and $d_{\boldsymbol{g}}$ are of arbitrary degree [21], [22]. This generalized algorithm was named **MultiComPoly** [22]. The core idea of **MultiComPoly** lies in replacing partial derivatives with higher-order partial derivatives. In this section, we present a comprehensive revisit of the fundamental principles underlying **MultiComPoly**, thereby establishing the theoretical foundation for the development of our new algorithms.

A commonly used method for directly computing the RREF of a matrix is the Gaussian-Jordan elimination (GJE) which is readily available in most Linear Algebra textbooks such as [29]. The classic algorithms to transform an $m \times n$ matrix with $m < n$ into its RREF can be implemented with complexity $O(m^2 n)$ [29] [30]. Over the finite field $\mathbb{F}_q$, however, the complexity can be further refined to $O(m^2 n / \log_q m)$ [31]. Regardless of the actual sequence of row operations used to produce it, each matrix has precisely one unique RREF [29].

[1]In [1], the indexing of polynomials h_i starts from 0, so the value of n here is exactly one greater than that reported in [1].

A. The homogenization of FDP

For any $f \in \mathbb{K}[x_1, x_2, \ldots, x_n]$, its homogenization, denoted by f^*, is defined by

$$f^*(x_0, x_1, x_2, \ldots, x_n) = x_0^{\deg(f)} f(x_1/x_0, x_2/x_0, \ldots, x_n/x_0),$$

where x_0 is a new variable. Furthermore, for a vector of multivariate polynomials $\boldsymbol{f} = (f_1, f_2, \ldots, f_u) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u$, its homogenization, denoted by $\boldsymbol{f}^*$, is defined by

$$\boldsymbol{f}^* = (x_0^{\deg(\boldsymbol{f})}, x_0^{\deg(\boldsymbol{f})-\deg(f_1)} f_1^*, x_0^{\deg(\boldsymbol{f})-\deg(f_2)} f_2^*, \ldots, x_0^{\deg(\boldsymbol{f})-\deg(f_u)} f_u^*),$$

where $\deg(\boldsymbol{f}) = \max\limits_{1 \le i \le u} \deg(f_i)$. Then it can be seen that each component function of $\boldsymbol{f}^*$ is a sum of homogeneous monomial of degree $\deg(\boldsymbol{f})$. Conversely, $\boldsymbol{f}$ can be easily obtained from $\boldsymbol{f}^*$ as follows

$$\boldsymbol{f} = (f_1^*(1, x_1, \ldots, x_n), f_2^*(1, x_1, \ldots, x_n), \ldots, f_u^*(1, x_1, \ldots, x_n)).$$

Lemma 3. *[17] Let $\boldsymbol{f} = (f_1, f_2, \ldots, f_u) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u$ and $\boldsymbol{g} = (g_1, g_2, \ldots, g_n) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^n$ be two vectors of multivariate polynomials. Then $(\boldsymbol{f} \circ \boldsymbol{g})^* = \boldsymbol{f}^* \circ \boldsymbol{g}^*$.*

By Lemma 3, if $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$, then $\boldsymbol{h}^* = \boldsymbol{f}^* \circ \boldsymbol{g}^*$. Therefore, to obtain a decomposition of $\boldsymbol{h}$, one can first homogenizes $\boldsymbol{h}$ to obtain $\boldsymbol{h}^*$, then decompose $\boldsymbol{h}^*$ to obtain $\boldsymbol{f}^*$ and $\boldsymbol{g}^*$, and finally dehomogenizes $\boldsymbol{f}^*$ and $\boldsymbol{g}^*$ to get $\boldsymbol{f}$ and $\boldsymbol{g}$. Based on this fact, unless otherwise specified, this paper always assumes that **$\boldsymbol{f}$ and $\boldsymbol{g}$ are two vectors of homogeneous polynomials**.

B. Compute a decomposition of $\boldsymbol{h}$ if $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$ is known

The core of **MultiComPoly** lies in recovering the correct right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$, as this enables the computation of a decomposition of $\boldsymbol{h}$. In this subsection, our focus will be on demonstrating how to efficiently compute a decomposition of $\boldsymbol{h}$ from $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$. In the next subsection, we will detail the methodology for recovering $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$.

We note that the original **MultiComPoly** algorithm requires that $g_1, g_2, \ldots, g_n$ are linearly independent over $\mathbb{K}$, since otherwise the algorithm will return "Fail". On one hand, from a random point of view, $g_1, g_2, \ldots, g_n$ tend to be linearly independent over $\mathbb{K}$. On the other hand, the decomposition of linearly dependent cases can be reduced to that of linearly independent cases. In fact, let $\{g_{k_1}, g_{k_2}, \ldots, g_{k_l}\}$ be a maximal linearly independent subset of $\{g_1, g_2, \ldots, g_n\}$, where $1 \le l \le n$ and $1 \le k_1 < k_2 < \cdots < k_l \le n$. Then there exists an $l \times n$ matrix A over $\mathbb{K}$ such that

$$(g_1, g_2, \ldots, g_n) = (g_{k_1}, g_{k_2}, \ldots, g_{k_l})A.$$

Let $\boldsymbol{g}' = (g_{k_1}, g_{k_2}, \ldots, g_{k_l})$ and $\boldsymbol{f}' = (f_1', f_2', \ldots, f_u')$, where

$$f_i' = f_i((x_1, x_2, \ldots, x_l)A), i = 1, 2, \ldots, u.$$

Then it is clear that $\boldsymbol{h} = \boldsymbol{f}' \circ \boldsymbol{g}'$ satisfying that $g_{k_1}, g_{k_2}, \ldots, g_{k_l}$ are linearly independent over $\mathbb{K}$. Thus, without loss of generality, **we can assume that $g_1, g_2, \ldots, g_n$ are linearly independent over $\mathbb{K}$.**

Given a basis $(g_1', g_2', \ldots, g_n')$ of $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$, there exists an $n \times n$ invertible matrix B over $\mathbb{K}$ such that $(g_1', g_2', \ldots, g_n') = (g_1, g_2, \ldots, g_n)B$. Then one can derive the following equalities:

$$h_i = f_i'(g_1', g_2', \ldots, g_n') \text{ for } 1 \le i \le u, \tag{1}$$

where $\boldsymbol{f}' = (f_1', f_2', \ldots, f_u') = (f_1((x_1, x_2, \ldots, x_n)B^{-1}), f_2((x_1, x_2, \ldots, x_n)B^{-1}), \ldots, f_u((x_1, x_2, \ldots, x_n)B^{-1}))$. Comparing the coefficients of h_i and the right-most parts of Equalities (1), one can obtain a linear system of $u \cdot \binom{n+d_{\boldsymbol{h}}-1}{d_{\boldsymbol{h}}}$ equations in $u \cdot \binom{n+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}$ unknown coefficients of $f_1', f_2', \ldots, f_u'$. Since $d_{\boldsymbol{h}} = d_{\boldsymbol{f}} \cdot d_{\boldsymbol{g}}$ and $d_{\boldsymbol{f}}, d_{\boldsymbol{g}} > 1$, the number of equations in the linear system significantly exceeds the number of variables. In general, the linear system will have a unique solution, leading to a nontrivial decomposition for $\boldsymbol{h}$. Conversely, if there is no solution for this system, it implies that $\boldsymbol{h}$ is undecomposable for the given right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$. The computational complexity of solving the linear system is $O(U^\omega)$, where $U = u \cdot \binom{n+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}$ and ω is the linear algebra exponent[2].

[2]From a practical point-of-view, the best achievable result for ω is given by Strassen's algorithm [32], where $\omega = 2.807$. Throughout this paper, we always take $\omega = 2.807$.

C. Compute the right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$

In this subsection, we will first review how to compute the right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$ from $\boldsymbol{h}$, and then present the complete algorithm of **MultiComPoly** for solving $\mathbf{FDP}_{\mathrm{H}}(\boldsymbol{h}, d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$.

For $1 \le i \le u$, let

$$f_i = \sum_{1 \le k_1 \le k_2 \le \cdots \le k_{d_{\boldsymbol{f}}} \le n} f^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}} x_{k_1} x_{k_2} \cdots x_{k_{d_{\boldsymbol{f}}}},$$

where $f^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}} \in \mathbb{K}$ are the coefficients of f_i. It follows that

$$h_i = \sum_{1 \le k_1 \le k_2 \le \cdots \le k_{d_{\boldsymbol{f}}} \le n} f^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}} g_{k_1} g_{k_2} \cdots g_{k_{d_{\boldsymbol{f}}}},$$

and so the $(d_{\boldsymbol{f}}-1)$-th partial derivative of h_i is given by

$$\frac{\partial^{(d_{\boldsymbol{f}}-1)} h_i}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} = \sum_{1 \le k_1 \le k_2 \le \cdots \le k_{d_{\boldsymbol{f}}} \le n} f^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}} \left(\frac{\partial^{(d_{\boldsymbol{f}}-1)} g_{k_1} g_{k_2} \cdots g_{k_{d_{\boldsymbol{f}}-1}}}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} g_{k_{d_{\boldsymbol{f}}}} + \cdots + \frac{\partial^{(d_{\boldsymbol{f}}-1)} g_{k_2} g_{k_3} \cdots g_{k_{d_{\boldsymbol{f}}}}}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} g_{k_1} \right)$$

for $1 \le i \le u$ and $1 \le j_1 \le j_2 \le \cdots \le j_{d_{\boldsymbol{f}}-1} \le n$.

It is important to note that

$$\frac{\partial^{(d_{\boldsymbol{f}}-1)} g_{k_1} g_{k_2} \cdots g_{k_{d_{\boldsymbol{f}}-1}}}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}}, \ldots, \frac{\partial^{(d_{\boldsymbol{f}}-1)} g_{k_2} g_{k_3} \cdots g_{k_{d_{\boldsymbol{f}}}}}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}}$$

are all of degree $(d_{\boldsymbol{f}}-1)(d_{\boldsymbol{g}}-1)$. Let $d = (d_{\boldsymbol{f}}-1)(d_{\boldsymbol{g}}-1)$, and let

$$\tilde{F} = \left\{ \frac{\partial^{(d_{\boldsymbol{f}}-1)} h_i}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} : 1 \le i \le u, 1 \le j_1 \le j_2 \le \ldots \le j_{d_{\boldsymbol{f}}-1} \le n \right\},$$

$$F = \left\{ \boldsymbol{x}^{\boldsymbol{\alpha}} g_k : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(d), 1 \le k \le n \right\},$$

where $M_n(d)$ is the set of all monomials of degree d in $\mathbb{K}[x_1, x_2, \ldots, x_n]$. It is clear that $\tilde{V} = \mathrm{Span}_{\mathbb{K}}\left(\tilde{F}\right)$ is a subspace of $V = \mathrm{Span}_{\mathbb{K}}(F)$. If $\dim(\tilde{V}) = |F|$, since $\dim(\tilde{V}) \le \dim(V) \le |F|$, it immediately follows that $\tilde{V} = V$, and so

$$x_n^d g_k \in F \subseteq V = \tilde{V} \subseteq \partial^{(d_{\boldsymbol{f}}-1)} I_h \text{ for } 1 \le k \le n,$$

where $\partial^{(d_{\boldsymbol{f}}-1)} I_h = \left\langle \frac{\partial^{(d_{\boldsymbol{f}}-1)} h_i}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} : 1 \le i \le u, 1 \le j_1 \le j_2 \le \ldots \le j_{d_{\boldsymbol{f}}-1} \le n \right\rangle$. When $\dim(\tilde{V}) < |F|$, Faugère and Perret enlarged $\tilde{F}$ by multiplying its elements with degree δ monomials, where δ is a nonnegative integer. Specifically, let

$$\tilde{F}_\delta = \left\{ \boldsymbol{x}^{\boldsymbol{\alpha}} \frac{\partial^{(d_{\boldsymbol{f}}-1)} h_i}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(\delta), 1 \le i \le u, 1 \le j_1 \le j_2 \le \ldots \le j_{d_{\boldsymbol{f}}-1} \le n \right\},$$

$$F_\delta = \left\{ \boldsymbol{x}^{\boldsymbol{\alpha}} g_k : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(\delta + d), 1 \le k \le n \right\}.$$

Then $\tilde{V}_\delta = \mathrm{Span}_{\mathbb{K}}\left(\tilde{F}_\delta\right)$ is a subspace of $V_\delta = \mathrm{Span}_{\mathbb{K}}(F_\delta)$. Since

$$\frac{|\tilde{F}_\delta|}{|F_\delta|} = \frac{|\tilde{F}| \cdot |M_n(\delta)|}{n \cdot |M_n(\delta + d)|} = \frac{|\tilde{F}|}{n} \cdot \frac{\binom{n+\delta-1}{\delta}}{\binom{n+\delta+d-1}{\delta+d}},$$

it is clear that $|\tilde{F}|/n$ significantly exceeds 1 and $\binom{n+\delta-1}{\delta}/\binom{n+\delta+d-1}{\delta+d}$ monotonically approaches 1 as δ increases, and so $|\tilde{F}_\delta| \ge |F_\delta|$ holds for sufficiently large δ. In particular, if $\dim(\tilde{V}_\delta) = |F_\delta|$ for some δ, then $V_\delta = \tilde{V}_\delta$ follows immediately, implying that

$$x_n^{d+\delta} g_k \in F_\delta \subseteq V_\delta = \tilde{V}_\delta \subseteq \partial^{(d_{\boldsymbol{f}}-1)} I_h \text{ for } 1 \le k \le n.$$

Therefore, we arrive at the following Theorem 1, which forms the algorithmic foundation for **MultiComPoly**.

Theorem 1. *[22] Let $\tilde{F}_\delta, F_\delta, \tilde{V}_\delta$ and V_δ be defined as above, and let*

$$\partial^{(d_{\boldsymbol{f}}-1)} I_h = \left\langle \frac{\partial^{(d_{\boldsymbol{f}}-1)} h_i}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} : 1 \le i \le u, 1 \le j_1 \le j_2 \le \ldots \le j_{d_{\boldsymbol{f}}-1} \le n \right\rangle.$$

If $\dim(\tilde{V}_\delta) = |F_\delta|$*, then*

$$x_n^{\delta+d} g_k \in \partial^{(d_{\boldsymbol{f}}-1)} I_h \text{ for } 1 \le k \le n. \tag{2}$$

Based on Theorem 1, the correct right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$ can be recovered as follows. If $x_n^{\delta+d} g_k \in \partial^{(d_{\boldsymbol{f}}-1)} I_h$ for $1 \le k \le n$, then $g_k \in \partial^{(d_{\boldsymbol{f}}-1)} I_h : \left\langle x_n^{\delta+d} \right\rangle$ for $1 \le k \le n$, where $\left\langle x_n^{\delta+d} \right\rangle$ is the ideal generated by $x_n^{\delta+d}$. Let $I = \partial^{(d_{\boldsymbol{f}}-1)} I_h : \left\langle x_n^{\delta+d} \right\rangle$ and G the reduced Gröbner basis of I w.r.t. the grevlex order. The authors of [22] observe that (without proof) the minimal degree[3] of a nonzero polynomial in the ideal I is $d_{\boldsymbol{g}}$, then it follows from Lemma 1 that

$$\mathrm{Span}_{\mathbb{K}}\left(g \in G : \deg(g) = d_{\boldsymbol{g}}\right) = \mathrm{Span}_{\mathbb{K}}\left(g \in I : \deg(g) = d_{\boldsymbol{g}}\right),$$

and so $g_k \in \mathrm{Span}_{\mathbb{K}}(g \in G : \deg(g) = d_{\boldsymbol{g}})$ for $1 \le k \le n$, or equivalently,

$$\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n) \subseteq \mathrm{Span}_{\mathbb{K}}\left(g \in G : \deg(g) = d_{\boldsymbol{g}}\right).$$

Furthermore, if $\dim\left(\mathrm{Span}_{\mathbb{K}}(g \in G : \deg(g) = d_{\boldsymbol{g}})\right) = n$, then the desired result is obtained, that is,

$$\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n) = \mathrm{Span}_{\mathbb{K}}\left(g \in G : \deg(g) = d_{\boldsymbol{g}}\right).$$

In [22], the value of δ in Theorem 1 is set to be the smallest value of δ satisfying $|\tilde{F}_\delta| \ge |F_\delta|$, or equivalently, satisfying the inequality

$$u \cdot \binom{n + d_{\boldsymbol{f}} - 2}{d_{\boldsymbol{f}} - 1} \binom{n + \delta - 1}{\delta} \ge n \binom{n + \delta + d - 1}{\delta + d}.$$

For instance, $\delta = \left\lceil \frac{n-u}{u-1} \right\rceil$ [4] if $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$.

Remark 1. *We note that the condition "*$\dim(\tilde{V}_\delta) = |F_\delta|$*" of Theorem 1 will never hold if* $\delta + d \ge d_{\boldsymbol{g}}$*. This is due to the fact that, in this case, the polynomials in* F_δ *are linearly dependent over* $\mathbb{K}$*, leading to* $\dim(\tilde{V}_\delta) \le \dim(V_\delta) < |F_\delta|$*. More precisely, consider the two polynomials* $g_i = \sum_{1 \le j \le |M_n(d_{\boldsymbol{g}})|} c_{i,j} \boldsymbol{x}^{\boldsymbol{\alpha}_j}$ *for* $i = 1, 2$*, where* $c_{i,j} \in \mathbb{K}$ *and* $M_n(d_{\boldsymbol{g}}) = \{\boldsymbol{x}^{\boldsymbol{\alpha}_1}, \boldsymbol{x}^{\boldsymbol{\alpha}_2}, \cdots, \boldsymbol{x}^{\boldsymbol{\alpha}_{|M_n(d_{\boldsymbol{g}})|}}\}$*. Since* $\boldsymbol{x}^{\boldsymbol{\alpha}_j} \in M_n(d_{\boldsymbol{g}})$*, it is clear that* $x_1^{\delta+d-d_{\boldsymbol{g}}} \boldsymbol{x}^{\boldsymbol{\alpha}_j} \in M_n(\delta + d)$ *for* $1 \le j \le |M_n(d_{\boldsymbol{g}})|$*, and so*

$$x_1^{\delta+d-d_{\boldsymbol{g}}} \boldsymbol{x}^{\boldsymbol{\alpha}_j} g_1, x_1^{\delta+d-d_{\boldsymbol{g}}} \boldsymbol{x}^{\boldsymbol{\alpha}_j} g_2 \in F_\delta \quad \text{for} \quad 1 \le j \le |M_n(d_{\boldsymbol{g}})|.$$

However, we have the following identity:

$$\sum_{1 \le j \le |M_n(d_{\boldsymbol{g}})|} c_{1,j} x_1^{\delta+d-d_{\boldsymbol{g}}} \boldsymbol{x}^{\boldsymbol{\alpha}_j} g_2 - \sum_{1 \le j \le |M_n(d_{\boldsymbol{g}})|} c_{2,j} x_1^{\delta+d-d_{\boldsymbol{g}}} \boldsymbol{x}^{\boldsymbol{\alpha}_j} g_1 = x_1^{\delta+d-d_{\boldsymbol{g}}} g_1 g_2 - x_1^{\delta+d-d_{\boldsymbol{g}}} g_2 g_1 = 0,$$

which implies that the polynomials in F_δ *are linearly dependent over* $\mathbb{K}$*. In fact, the condition "*$\dim(\tilde{V}_\delta) = |F_\delta|$*" of Theorem 1 can be relaxed to the condition "*$\dim(\tilde{V}_\delta) = \dim(V_\delta)$*", just as we do in Section IV.*

Finally, the pseudo-code representation of **MultiComPoly** can be described as follows [22].

Algorithm 1 MultiComPoly

Input: Integers $d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, s$ with $d_{\boldsymbol{f}}, d_{\boldsymbol{g}} > 1$ and $1 \le u, s \le n$, homogeneous monic polynomials $h_1, h_2, \ldots, h_u$ of the same degree $d_{\boldsymbol{h}}$

Output: Fail, or homogeneous monic polynomials $\boldsymbol{f}' = (f_1', f_2', \ldots, f_u'), \boldsymbol{g}' = (g_1', g_2', \ldots, g_n')$ of degree $d_{\boldsymbol{f}}$ and $d_{\boldsymbol{g}}$ respectively such that $\boldsymbol{h} = \boldsymbol{f}' \circ \boldsymbol{g}'$

1: $d \leftarrow (d_{\boldsymbol{f}} - 1)(d_{\boldsymbol{g}} - 1)$

2: $\delta \leftarrow \min\left\{\delta' \ge 0 : u\binom{n+d_{\boldsymbol{f}}-2}{d_{\boldsymbol{f}}-1}\binom{n+\delta'-1}{\delta'} \ge n\binom{n+\delta'+d-1}{\delta'+d}\right\}$

3: $G_\delta \leftarrow$ a reduced Gröbner basis of the ideal $\partial^{(d_{\boldsymbol{f}}-1)} I_h : \left\langle x_n^{\delta+d} \right\rangle$ w.r.t. the grevlex order

4: **if** $\dim\left(\mathrm{Span}_{\mathbb{K}}(g \in G_\delta : \deg(g) = d_{\boldsymbol{g}})\right) \ne n$ **then**

5: **return** Fail

6: **end if**

7: Let $g_1', g_2', \ldots, g_n'$ be a basis of $\mathrm{Span}_{\mathbb{K}}(g \in G_\delta : \deg(g) = d_{\boldsymbol{g}})$

---

[3] If $\partial^{(d_{\boldsymbol{f}}-1)} I_h$ is replaced with a smaller ideal $\left\langle \tilde{F}_\delta \right\rangle$, then the minimal degree becomes evident. Indeed, since $x_n^{\delta+d} g_i \in V_\delta = \tilde{V}_\delta \subseteq \left\langle \tilde{F}_\delta \right\rangle$ and every polynomial in $\tilde{F}_\delta$ has degree $\delta + d + d_{\boldsymbol{g}}$, it follows immediately that the minimal degree of a nonzero polynomial in the ideal $\left\langle \tilde{F}_\delta \right\rangle : \left\langle x_n^{\delta+d} \right\rangle$ is $d_{\boldsymbol{g}}$.

[4] In [22], the value of δ is given by $\delta = \left\lceil \frac{n-1}{u-1} \right\rceil$, whereas a simple calculation suggests it should be $\delta = \left\lceil \frac{n-u}{u-1} \right\rceil$. This discrepancy appears to be a typographical error in the original text.

Solve a system of linear equations derived from Equalities (1) to obatin $\boldsymbol{f}'$
if $\boldsymbol{f}' = \emptyset$ **then**
    return Fail
end if
return $\boldsymbol{f}'$ and $\boldsymbol{g}'$

The computational complexity of **MultiComPoly** is estimated to be $O(n^{3\delta+3d+3d_{\boldsymbol{g}}})$ field operations [22]. Specifically, for $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$, the complexity is $O(n^{3\delta+9})$. When $d_{\boldsymbol{f}} = 2$ and $d_{\boldsymbol{g}} = 3$, the complexity increases to $O(n^{3\delta+15})$, while for $d_{\boldsymbol{f}} = 3$ and $d_{\boldsymbol{g}} = 2$, it becomes $O(n^{3\delta+12})$.

IV. AN RREF-BASED ALGORITHM FOR FDP

As shown in Section III, FDP's core task is to recover the correct right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$. **MultiComPoly** achieves this by computing a reduced Gröbner Basis of the ideal $\partial^{(d_{\boldsymbol{f}}-1)} I_h : \left\langle x_n^{\delta+d} \right\rangle$ w.r.t. the grevlex order. From an algorithmic point of view, this reduces to compute the row echelon form of a Macaulay matrix. This section reveals an intriguing observation: by applying Gauss-Jordan elimination (GJE) to transform the coefficient matrix associated with the polynomial set $\tilde{F}_\delta$ (defined in Theorem 1) into its RREF, we can correctly recover this space. This provides a more explicit description of computing the right-factor space. We have integrated this approach into **MultiComPoly** and call the obtained algorithm **RREFComPoly**. Furthermore, for cases where $\delta \geq d_{\boldsymbol{g}} - d$, **RREFComPoly** delivers a more precise estimate of the parameter δ by establishing a tighter upper bound on $\dim(V_\delta)$. This refinement, combined with the use of exact binomials (as opposed to the traditional approximation in **MultiComPoly**), yields a sharper and more reliable complexity bound. Together, these refinements provide better guidance for both practical experimentation and theoretical analysis, and lay the necessary groundwork for our subsequent introduction of **PartComPoly**.

Since the **RREFComPoly** algorithm is a component of the **PartComPoly** algorithm, which will be introduced in the next section, to facilitate a consistent presentation, we consider the case where the number s of variables is less than or equal to the number n of right-factor polynomials in this section, that is, we consider the FDP where $\boldsymbol{h} = (h_1, h_2, \ldots, h_u) = \boldsymbol{f} \circ \boldsymbol{g} = (f_1(g_1, g_2, \ldots, g_n), f_2(g_1, g_2, \ldots, g_n), \ldots, f_u(g_1, g_2, \ldots, g_n)) \in \mathbb{K}[x_1, x_2, \ldots, x_s]^u$ with $0 < s \leq n$.

A. Compute the right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$

In this subsection, we will focus on how to recover the correct right-factor space $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$. Once we have obtained a basis of $\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$, similar to Subsection III-B, we can get a decomposition of $\boldsymbol{h}$ by solving a linear system of $u \cdot \binom{s+d_{\boldsymbol{h}}-1}{d_{\boldsymbol{h}}}$ equations in $u \cdot \binom{n+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}$ unknown coefficients.

Before giving the main result of this subsection, we first introduce the definition of the coefficient matrix associated with a given set of polynomials. For a nonnegative integer δ, let

$$\tilde{F}_\delta = \left\{ \boldsymbol{x}^{\boldsymbol{\alpha}} \frac{\partial^{(d_{\boldsymbol{f}}-1)} h_i}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(\delta), 1 \leq i \leq u, 1 \leq j_1 \leq j_2 \leq \ldots \leq j_{d_{\boldsymbol{f}}-1} \leq s \right\},$$

where $M_n(\delta)$ is the set of all monomials of degree δ in $\mathbb{K}[x_1, x_2, \ldots, x_s]$. If we write

$$\tilde{F}_\delta = \left\{ p_1(x_1, x_2, \ldots, x_s), p_2(x_1, x_2, \ldots, x_s), \ldots, p_{|\tilde{F}_\delta|}(x_1, x_2, \ldots, x_s) \right\},$$

$$M_n(d_\delta) = \{\boldsymbol{x}^{\alpha_1}, \boldsymbol{x}^{\alpha_2}, \ldots, \boldsymbol{x}^{\alpha_{|M_n(d_\delta)|}}\} = \left\{ x_1^{d_\delta}, x_2 x_1^{d_\delta - 1}, x_3 x_1^{d_\delta - 1}, \ldots, x_s^{d_\delta} \right\},$$

where $d_\delta = \delta + (d_{\boldsymbol{f}} - 1)(d_{\boldsymbol{g}} - 1) + d_{\boldsymbol{g}}$ and the monomials in $M_n(d_\delta)$ are sorted in descending order w.r.t. the grevlex order, then the coefficient matrix C associated with $\tilde{F}_\delta$ is the $|\tilde{F}_\delta| \times |M_n(d_\delta)|$ matrix whose (i, j) entry is the coefficient of $\boldsymbol{x}^{\alpha_j}$ in $p_i(x_1, x_2, \cdots, x_s)$.

Now we present the main result of this section which serves as the theoretical basis for the **RREFComPoly** algorithm.

Theorem 2. *Let $\tilde{F}_\delta$ be defined as above, $\tilde{V}_\delta = \mathrm{Span}_{\mathbb{K}}(\tilde{F}_\delta)$, and C the matrix associated with $\tilde{F}_\delta$. Let $C^* = (c^*_{i,j})_{|\tilde{F}_\delta| \times |M_n(d_\delta)|}$ be the RREF of C and r the rank of C^*. Let $d = (d_{\boldsymbol{f}} - 1)(d_{\boldsymbol{g}} - 1)$, $F_\delta = \{\boldsymbol{x}^{\boldsymbol{\alpha}} g_k : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(\delta + d), 1 \leq k \leq n\}$, and $V_\delta = \mathrm{Span}_{\mathbb{K}}(F_\delta)$. If $\dim(\tilde{V}_\delta) = \dim(V_\delta)$ and t is the largest positive integer such that $x_s^{\delta+d} \mid \mathrm{LM}(\hat{g}_j)$ for $t \leq j \leq r$ but*

$x_s^{\delta+d} \nmid \mathrm{LM}(\hat{g}_{t-1})$, *where* $\hat{g}_j = c_{j,1}^* x_1^{d_\delta} + c_{j,2}^* x_2 x_1^{d_\delta - 1} + \cdots + c_{j,|M_n(d_\delta)|}^* x_s^{d_\delta}$ *is the polynomial corresponding to the* j*-th row of* C^* *for* $1 \le j \le r$*, then*

$$\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n) \subseteq \mathrm{Span}_{\mathbb{K}}(\hat{g}_j / x_s^{\delta+d} : t \le j \le r).$$

Proof. To prove Theorem 2, it suffices to show that $x_s^{\delta+d} g_i \in \mathrm{Span}_{\mathbb{K}}(\hat{g}_j : t \le j \le r)$ for $1 \le i \le n$. We note that $\tilde{V}_\delta \subseteq V_\delta$, and so it follows from $\dim(\tilde{V}_\delta) = \dim(V_\delta)$ that $V_\delta = \tilde{V}_\delta = \mathrm{Span}_{\mathbb{K}}(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_r)$. By the definition of V_δ, we have $x_s^{\delta+d} g_i \in V_\delta$, and thus $x_s^{\delta+d} g_i$ can be expressed as $x_s^{\delta+d} g_i = \sum_{1 \le j \le r} b_j \hat{g}_j$, where $b_j \in \mathbb{K}$ for $1 \le j \le r$. To complete the proof, we need to show that $b_j = 0$ for $1 \le j \le t-1$. Suppose, on the contrary, that there is a smallest integer j^* with $1 \le j^* \le t-1$ such that $b_{j^*} \ne 0$. Since the columns of C^* are arranged in descending grevlex order, together with the definition of RREF, it follows that $\mathrm{LM}(x_s^{\delta+d} g_i) = \mathrm{LM}(\hat{g}_{j^*})$, and so

$$x_s^{\delta+d} \mid \mathrm{LM}(\hat{g}_{j^*}). \tag{3}$$

Moreover, it is clear that

$$\mathrm{LM}(\hat{g}_i) \prec \mathrm{LM}(\hat{g}_j) \text{ if and only if } i > j. \tag{4}$$

However, since $x_s^{\delta+d} \nmid \mathrm{LM}(\hat{g}_{t-1})$, it follows that $x_s^{\delta+d} \nmid \mathrm{LM}(\hat{g}_{j^*})$ (since otherwise the homogeneity of the monomials implies that $\mathrm{LM}(\hat{g}_{j^*}) \prec \mathrm{LM}(\hat{g}_{t-1})$, which contradicts (4)), a contradiction to (3). □

Since by assumption $g_1, g_2, \ldots, g_n$ are linearly independent over $\mathbb{K}$, we have $\dim(\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)) = n$. Consequently, by Theorem 2, we have $\dim(\mathrm{Span}_{\mathbb{K}}(\hat{g}_j / x_s^{\delta+d} : t \le j \le r)) \ge n$, which implies that $t \le r - n + 1$.

Case 1: If $t = r - n + 1$, then it immediately follows that

$$\mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n) = \mathrm{Span}_{\mathbb{K}}(\hat{g}_j / x_n^{\delta+d} : r - n + 1 \le j \le r).$$

Case 2: If $t < r - n + 1$, then there exists a nonzero polynomial

$$\hat{g} \in V_\delta - \mathrm{Span}_{\mathbb{K}}(x_s^{\delta+d} g_1, x_s^{\delta+d} g_2, \ldots, x_s^{\delta+d} g_n)$$

such that $x_s^{\delta+d} \mid \hat{g}$. However, for randomly generated $\boldsymbol{g}$, this scenario is highly improbable, as confirmed by our experiments.

B. Analysis of the parameter δ

We note that the condition "$\dim(\tilde{V}_\delta) = \dim(V_\delta)$" in Theorem 2 cannot be directly verified in practice because V_δ is unknown. To address this, we instead estimate the smallest value of δ such that this equality holds with high probability. As the algorithm's time complexity exhibits a direct dependence on the parameter δ, an accurate estimation of δ can not only optimize the computational efficiency of the algorithm, but also provides more precise experimental guidance. Since $\dim(\tilde{V}_\delta)$ is known or equals $|\tilde{F}_\delta|$ with a high probability, our approach focuses on deriving a reliable upper bound estimate for $\dim(V_\delta)$.

It is clear that $\dim(V_\delta) \le |F_\delta|$, and thus it is natural to use $|F_\delta|$ as an upper bound for estimating $\dim(V_\delta)$. This upper bound is sharp when $\delta < d_{\boldsymbol{g}} - d$, but becomes less tight for $\delta \ge d_{\boldsymbol{g}} - d$. Specifically, when $\delta = d_{\boldsymbol{g}} - d$, we have the following lemma.

Lemma 4. *If* $\delta = d_{\boldsymbol{g}} - d$*, then* $\dim(V_\delta) \le n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right)$.

Proof. We assume, without loss of generality, that the coefficient matrix associated with $g_1, g_2, \ldots, g_n$ is in RREF (otherwise, the following proof remains valid by instead considering a linearly equivalent system $g_1', g_2', \ldots, g_n'$ whose coefficient matrix is in RREF).

For $1 \le k \le n$, let $G_k' = G_k'' \cup \{g_i g_k : 1 \le i \le n\}$ and $F_\delta' = \bigcup_{k=1}^n G_k'$, where

$$G_k'' = \{\boldsymbol{x}^{\boldsymbol{\alpha}} g_k : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(\delta + d) \setminus \{\mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_n)\}\}.$$

To prove Lemma 4, it suffices to show that

$$V_\delta = \mathrm{Span}_{\mathbb{K}}(F_\delta') \text{ and } |F_\delta'| \le n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right).$$

For $1 \le k \le n$, let $G_k = \{\boldsymbol{x}^{\boldsymbol{\alpha}} g_k : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(\delta + d)\}$. Then it is clear that $\mathrm{Span}_{\mathbb{K}}(G_k') \subseteq \mathrm{Span}_{\mathbb{K}}(G_k)$. On the other hand, since for each $1 \le i \le n$ we have $g_i - \mathrm{LM}(g_i) \in \mathrm{Span}_{\mathbb{K}}\left(M_n(\delta + d) \setminus \{\mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_n)\}\right)$, it follows that

$$(g_i - \mathrm{LM}(g_i)) g_k \in \mathrm{Span}_{\mathbb{K}}(G_k'').$$

Consequently, $\mathrm{LM}(g_i)g_k \in \mathrm{Span}_{\mathbb{K}}(G'_k)$ for $1 \le i \le n$, which implies that $\mathrm{Span}_{\mathbb{K}}(G_k) \subseteq \mathrm{Span}_{\mathbb{K}}(G'_k)$. Therefore, we have $\mathrm{Span}_{\mathbb{K}}(G_k) = \mathrm{Span}_{\mathbb{K}}(G'_k)$, and thus $V_\delta = \mathrm{Span}_{\mathbb{K}}(F_\delta) = \mathrm{Span}_{\mathbb{K}}(\bigcup_{k=1}^n G_k) = \mathrm{Span}_{\mathbb{K}}(\bigcup_{k=1}^n G'_k) = \mathrm{Span}_{\mathbb{K}}(F'_\delta)$.

To complete the proof, we need to show that $|F'_\delta| \le n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right)$. Since $\mathrm{LM}(g_i) \ne \mathrm{LM}(g_j)$ if $i \ne j$, we have

$$|G''_k| = \binom{s+\delta+d-1}{\delta+d} - n.$$

Let $G_g = \{g_i g_k : 1 \le i \le n, 1 \le k \le n\}$. It is clear that $|G_g| = \binom{n+1}{2}$, and so

$$|F'_\delta| \le n|G''_k| + |G_g| = n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right).$$

□

For the case where $\delta > d_{\boldsymbol{g}} - d$, establishing a tight upper bound on $\dim(V_\delta)$ is challenging; nevertheless, we can obtain an approximate estimate[5] of $\dim(V_\delta)$, that is,

$$\dim(V_\delta) \approx n \cdot \binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right)\binom{s+\delta+d-d_{\boldsymbol{g}}-1}{\delta+d-d_{\boldsymbol{g}}}.$$

To see this, we similarly define the following two sets:

$$G''_k = \left\{\boldsymbol{x}^{\boldsymbol{\alpha}} g_k : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(\delta+d), \boldsymbol{x}^{\boldsymbol{\alpha}} \ne \boldsymbol{x}^{\boldsymbol{\beta}}\mathrm{LM}(g_i) \text{ for all } \boldsymbol{x}^{\boldsymbol{\beta}} \in M_n(\delta+d-d_{\boldsymbol{g}}) \text{ and all } 1 \le i \le n\right\}.$$

and $G_g = \left\{\boldsymbol{x}^{\boldsymbol{\beta}} g_i g_k : \boldsymbol{x}^{\boldsymbol{\beta}} \in M_n(\delta+d-d_{\boldsymbol{g}}), 1 \le i,k \le n\right\}$. Then it is clear that $|G_g| = \binom{n+1}{2}\binom{s+\delta+d-d_{\boldsymbol{g}}-1}{\delta+d-d_{\boldsymbol{g}}}$. However, in contrast to the case when $\delta = d_{\boldsymbol{g}} - d$, we cannot ensure that $\boldsymbol{x}^{\boldsymbol{\beta_1}}\mathrm{LM}(g_i) \ne \boldsymbol{x}^{\boldsymbol{\beta_2}}\mathrm{LM}(g_j)$ for $i \ne j$, where $\boldsymbol{x}^{\boldsymbol{\beta_1}}, \boldsymbol{x}^{\boldsymbol{\beta_2}} \in M_n(\delta+d-d_{\boldsymbol{g}})$. Consequently, we cannot calculate $|G''_k|$ exactly but can estimate its approximate value

$$|G''_k| \approx \binom{s+\delta+d-1}{\delta+d} - n\binom{s+\delta+d-d_{\boldsymbol{g}}-1}{\delta+d-d_{\boldsymbol{g}}},$$

and so

$$|F'_\delta| \le n|G''_k| + |G_g| \approx n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right)\binom{s+\delta+d-d_{\boldsymbol{g}}-1}{\delta+d-d_{\boldsymbol{g}}}.$$

Therefore, in our algorithm, the value of δ is selected as the smallest integer δ satisfying

$$|\tilde{F}_\delta| \ge n\binom{s+\delta+d-1}{\delta+d}$$

when $\delta < d_{\boldsymbol{g}} - d$ or

$$|\tilde{F}_\delta| \ge n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right)\binom{s+\delta+d-d_{\boldsymbol{g}}-1}{\delta+d-d_{\boldsymbol{g}}}$$

when $\delta \ge d_{\boldsymbol{g}} - d$, where $|\tilde{F}_\delta| = u\binom{s+d_{\boldsymbol{f}}-2}{d_{\boldsymbol{f}}-1}\binom{s+\delta-1}{\delta}$. However, if the selected δ satisfies either

$$n\binom{s+\delta+d-1}{\delta+d} \ge \binom{s+\delta+d+d_{\boldsymbol{g}}-1}{\delta+d+d_{\boldsymbol{g}}}$$

when $\delta < d_{\boldsymbol{g}} - d$, or

$$n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right)\binom{s+\delta+d-d_{\boldsymbol{g}}-1}{\delta+d-d_{\boldsymbol{g}}} \ge \binom{s+\delta+d+d_{\boldsymbol{g}}-1}{\delta+d+d_{\boldsymbol{g}}}$$

when $\delta \ge d_{\boldsymbol{g}} - d$, then the algorithm terminates and returns "Fail". This is due to the fact that, under these conditions, we have $M_n(\delta+d+d_{\boldsymbol{g}}) \subset V_\delta = \tilde{V}_\delta$, implying that every homogeneous polynomial of degree $\delta+d+d_{\boldsymbol{g}}$ in $\mathbb{K}[x_1, x_2, \ldots, x_s]$ belongs to $\tilde{V}_\delta$. As a result, the RREF C^* of the coefficient matrix C associated with $\tilde{F}_\delta$ is an identity matrix. This leads to $t = r - \binom{n+d_{\boldsymbol{g}}-1}{d_{\boldsymbol{g}}} + 1 < r - n + 1$ and consequently

$$\mathrm{Span}_{\mathbb{K}}(\hat{g}_j / x_s^{\delta+d} : t \le j \le r) = \mathrm{Span}_{\mathbb{K}}(M_n(d_{\boldsymbol{g}})) \ne \mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n).$$

Based on the preceding analysis, we present the ***δ*-Estimate** algorithm for estimating the value of δ as follows.

[5]In practice, this approximation proves adequate for our purposes. Specifically, it yields a reliable estimate for the value of δ. Experimental results show strong agreement between this estimate and the smallest δ for which both **MultiComPoly** and **RREFComPoly** successfully return a solution. For detailed numerical comparisons, see Tables III and IV.

Algorithm 2 $\boldsymbol{\delta}$**-Estimate**

Input: Integers $d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, s$ with $d_{\boldsymbol{f}}, d_{\boldsymbol{g}} > 1$ and $1 \leq u, s \leq n$

$d \leftarrow (d_{\boldsymbol{f}} - 1)(d_{\boldsymbol{g}} - 1)$
$\delta \leftarrow 0$
while $\delta \geq 0$ **do**
  if $\delta < d_{\boldsymbol{g}} - d$ **then**
    if $n\binom{s+\delta+d-1}{\delta+d} \geq \binom{s+\delta+d+d_{\boldsymbol{g}}-1}{\delta+\delta+d_{\boldsymbol{g}}}$ **then**
      Return -1
    end if
    if $u\binom{s+d_{\boldsymbol{f}}-2}{d_{\boldsymbol{f}}-1}\binom{s+\delta-1}{\delta} \geq n\binom{s+\delta+d-1}{\delta+d}$ **then**
      Return δ
    end if
  end if
  if $\delta \geq d_{\boldsymbol{g}} - d$ **then**
    if $n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right)\binom{s+\delta+d-d_{\boldsymbol{g}}-1}{\delta+d-d_{\boldsymbol{g}}} \geq \binom{s+\delta+d+d_{\boldsymbol{g}}-1}{\delta+\delta+d_{\boldsymbol{g}}}$ **then**
      Return -1
    end if
    if $u\binom{s+d_{\boldsymbol{f}}-2}{d_{\boldsymbol{f}}-1}\binom{s+\delta-1}{\delta} \geq n\binom{s+\delta+d-1}{\delta+d} - \left(n^2 - \binom{n+1}{2}\right)\binom{s+\delta+d-d_{\boldsymbol{g}}-1}{\delta+d-d_{\boldsymbol{g}}}$ **then**
      Return δ
    end if
  end if
  $\delta \leftarrow \delta + 1$
end while
return δ

*C. The **RREFComPoly** algorithm*

The pseudo-code representation of **RREFComPoly** is as follows.

Algorithm 3 RREFComPoly

Input: Integers $d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, s$ with $d_{\boldsymbol{f}}, d_{\boldsymbol{g}} > 1$ and $1 \leq u, s \leq n$, homogeneous monic polynomials $h_1, h_2, \ldots, h_u \in \mathbb{K}[x_1, x_2, \ldots, x_s]$ of the same degree $d_{\boldsymbol{h}}$

Output: Fail, or homogeneous monic polynomials $\boldsymbol{f}' = (f_1', f_2', \ldots, f_u')$ and $\boldsymbol{g}' = (g_1', g_2', \ldots, g_n')$ of degree $d_{\boldsymbol{f}}$ and $d_{\boldsymbol{g}}$, respectively, such that $\boldsymbol{h} = \boldsymbol{f}' \circ \boldsymbol{g}'$

$d \leftarrow (d_{\boldsymbol{f}} - 1)(d_{\boldsymbol{g}} - 1)$
$\delta \leftarrow \boldsymbol{\delta}$**-Estimate**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, s)$
if $\delta < 0$ **then**
  Return Fail
end if
$\tilde{F}_\delta \leftarrow \left\{ \boldsymbol{x}^{\boldsymbol{\alpha}} \frac{\partial^{(d_{\boldsymbol{f}}-1)} h_i}{\partial x_{j_1} \partial x_{j_2} \cdots \partial x_{j_{d_{\boldsymbol{f}}-1}}} : \boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n(\delta), 1 \leq i \leq u, 1 \leq j_1 \leq j_2 \leq \ldots \leq j_{d_{\boldsymbol{f}}-1} \leq s \right\}$
$C \leftarrow$ the coefficient matrix associated with $\tilde{F}_\delta$
Compute the RREF C^* of C
Let t be the largest integer such that $x_n^{\delta+d} \mid \mathrm{LM}(\hat{g}_j)$ for $t \leq j \leq r$ but $x_n^{\delta+d} \nmid \mathrm{LM}(\hat{g}_{t-1})$, where $\hat{g}_j$ is the polynomial corresponding to the j-th row of C^* for $1 \leq j \leq r$ and r is the rank of C^*
if $t \neq r - n + 1$ **then**
  Return Fail
end if
$g_i' \leftarrow \frac{\hat{g}_{t+i-1}}{x_n^{\delta+d}}$ for $1 \leq i \leq n$
Solve a system of linear equations to obtain $\boldsymbol{f}'$
if $\boldsymbol{f}' = \emptyset$ **then**
  Return Fail
end if
return $\boldsymbol{f}', \boldsymbol{g}'$

For the matrix C, which has $H = u\binom{s+d_{\boldsymbol{f}}-2}{d_{\boldsymbol{f}}-1}\binom{s+\delta-1}{\delta}$ rows and $J = \binom{s+\delta+d+d_{\boldsymbol{g}}-1}{\delta+d+d_{\boldsymbol{g}}}$ columns, the complexity of computing its RREF is $O(H^2 J/\log_q H)$. Additionally, the complexity of solving the system of linear equations to obtain $\boldsymbol{f}'$ is $O(U^\omega)$, where $U = u \cdot \binom{s+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}$. Therefore, the overall complexity of the **RREFComPoly** algorithm is $O(\max(H^2 J/\log_q H, U^\omega))$ field operations.

*D. The correctness of **RREFComPoly***

In this subsection, we prove the correctness of **RREFComPoly**. Our proof follows the framework of [23], which established that **MultiComPoly** returns a unique normal form decomposition of $\boldsymbol{h}$ for generic monic instances of $\mathbf{FDP}_{\mathrm{H}}(\boldsymbol{h}, d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$ with $d_{\boldsymbol{f}} \in \{2, 3\}$ and $d_{\boldsymbol{g}} = 2$. Recall that in [23], the authors introduced the concept of "normal form": a decomposition $(\boldsymbol{f}, \boldsymbol{g})$ of homogeneous monic polynomials $\boldsymbol{h}$ is said to be in normal form if both $(f_1, f_2, \ldots, f_u)$ and $(g_1, g_2, \ldots, g_n)$ are homogeneous and monic, and $(g_1, g_2, \ldots, g_n)$ constitutes a $d_{\boldsymbol{g}}$-Gröbner basis w.r.t. the grevlex order. Here, a $d_{\boldsymbol{g}}$-Gröbner basis is a subset up to degree $d_{\boldsymbol{g}}$ of a reduced Gröbner basis, under the default ordering $g_n \prec g_{n-1} \prec \cdots \prec g_1$. It is worth noting that the coefficient matrix associated with a $d_{\boldsymbol{g}}$-Gröbner basis w.r.t. the grevlex order must be in RREF. **MultiComPoly** actually returns a normal form decomposition, see [23, Section 2] for more details. A generic homogeneous monic polynomial of degree d in $\mathbb{K}[x_1, x_2, \ldots, x_s]$ can be expressed as $\sum_{i_1+i_2\cdots+i_n=d} a_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, where the coefficients $a_{i_1,i_2,\ldots,i_n}$ are indeterminate serving as formal parameters (except for the leading coefficient which is fixed as 1). An instance of $\mathbf{FDP}_{\mathrm{H}}(\boldsymbol{h}, d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$ is called generic monic if $\boldsymbol{f}$ and $\boldsymbol{g}$ are both generic homogeneous monic polynomials.

We note that **RREFComPoly** in fact returns a normal form decomposition. More precisely, let $(\boldsymbol{f}', \boldsymbol{g}')$ be the output of **RREFComPoly**. Then it is clear that $\boldsymbol{h} = \boldsymbol{f}' \circ \boldsymbol{g}'$, where $\boldsymbol{f}'$ and $\boldsymbol{g}'$ are both homogeneous and monic, and the coefficient matrix associated with $\boldsymbol{g}'$ is in RREF. To verify that $(\boldsymbol{f}', \boldsymbol{g}')$ is indeed a normal form decomposition of $\boldsymbol{h}$, it suffices to show that $\boldsymbol{g}'$ constitutes a $d_{\boldsymbol{g}}$-Gröbner basis of the ideal $I = \langle g_1', g_2', \ldots, g_n' \rangle$ w.r.t. the grevlex order. In fact, let G be a reduced Gröbner basis of the ideal I w.r.t. the grevlex order. Since $d_{\boldsymbol{g}} = \min\{\deg(g) : g \in I \setminus \{0\}\}$, it follows from Lemma 1 that

$$\mathrm{Span}_{\mathbb{K}}(g \in G : \deg(g) = d_{\boldsymbol{g}}) = \{g \in I : \deg(g) = d_{\boldsymbol{g}}\} = \mathrm{Span}_{\mathbb{K}}(g_1', g_2', \ldots, g_n').$$

The set $\{g \in G : \deg(g) = d_{\boldsymbol{g}}\}$ is the $d_{\boldsymbol{g}}$-Gröbner basis w.r.t. the grevlex order of G, and so its matrice is also in RREF. Since the coefficient matrices of both spanning sets are in RREF, it follows that

$$\{g \in G : \deg(g) = d_{\boldsymbol{g}}\} = \{g_1', g_2', \ldots, g_n'\},$$

which implies that $\boldsymbol{g}'$ constitutes a $d_{\boldsymbol{g}}$-Gröbner basis of the ideal I. This observation leads to an alternative definition of "normal form" as follows.

Definition 5. *Let*

$$\boldsymbol{h} = (h_1, h_2, \ldots, h_u) = \boldsymbol{f} \circ \boldsymbol{g} = (f_1(g_1, g_2, \ldots, g_n), f_2(g_1, g_2, \ldots, g_n), \ldots, f_u(g_1, g_2, \ldots, g_n)) \in \mathbb{K}[x_1, x_2, \ldots, x_s]^u$$

with $s, n, u > 0$, where $h_1, h_2, \ldots, h_u$ are homogeneous monic polynomials whose leading coefficients w.r.t. the grevlex order are 1. A $(d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$-decomposition $(\boldsymbol{f}, \boldsymbol{g})$ of $\boldsymbol{h}$ is said to be in normal form if both $(f_1, f_2, \ldots, f_u)$ and $(g_1, g_2, \ldots, g_n)$ are homogeneous and monic, and the coefficient matrix w.r.t. the grevlex order associated with $(g_1, g_2, \ldots, g_n)$ is in RREF.

As pointed out in Subsection II-B, the decomposition of $\boldsymbol{h}$ is not unique, as there exist many affine equivalent decompositions. However, if a decomposition $(\boldsymbol{f}, \boldsymbol{g})$ is affine equivalent to another decomposition $(\boldsymbol{f}', \boldsymbol{g}')$ of $\boldsymbol{h}$, then both are affine equivalent to a decomposition in normal form. **Consequently, without loss of generality, we will always assume that $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$, where $(\boldsymbol{f}, \boldsymbol{g})$ is already in normal form for the rest of this paper.**

Before proceeding, we introduce some notation. For integers $n \geq 1$ and $d_{\boldsymbol{f}} \geq 2$, let

$$P_{u,n,d_{\boldsymbol{f}}} = \{\boldsymbol{f} = (f_1, f_2, \ldots, f_u) \in \mathbb{K}[x_1, x_2, \ldots, x_n]^u : f_i \text{ is homogeneous monic of degree } d_{\boldsymbol{f}} \text{ for } 1 \leq i \leq u\}.$$

Moreover, for integers $s \geq 1$ and $d_{\boldsymbol{g}} \geq 2$, let

$$Q_{n,s,d_{\boldsymbol{g}}} = \{\boldsymbol{g} = (g_1, g_2, \ldots, g_n) \in P_{n,s,d_{\boldsymbol{g}}} : \text{the coefficient matrix associated with } \boldsymbol{g} \text{ w.r.t. the grevlex order is in RREF}\}.$$

The composition map is then defined as

$$\begin{aligned} \eta_{u,n,d_{\boldsymbol{f}},s,d_{\boldsymbol{g}}} \colon P_{u,n,d_{\boldsymbol{f}}} \times Q_{n,s,d_{\boldsymbol{g}}} &\longrightarrow P_{u,s,d_{\boldsymbol{f}} \cdot d_{\boldsymbol{g}}} \\ (\boldsymbol{f}, \boldsymbol{g}) &\longmapsto \boldsymbol{f} \circ \boldsymbol{g} \end{aligned}$$

and the set of all decomposable polynomials is denoted by $U_{u,n,s,d_{\boldsymbol{f}},d_{\boldsymbol{g}}} = \mathrm{Im}(\eta_{u,n,d_{\boldsymbol{f}},s,d_{\boldsymbol{g}}})$. It is worth noting that for any $\boldsymbol{h} \in U_{u,n,s,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$, there exists a decomposition $(\boldsymbol{f},\boldsymbol{g})$ which is a normal form of $\boldsymbol{h}$.

To prove the correctness of **RREFComPoly**, given a polynomial vector $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g} \in U_{u,n,s,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$, we need to show that **RREFComPoly** returns the unique normal form decomposition $(\boldsymbol{f},\boldsymbol{g})$ of $\boldsymbol{h}$. Following the approach of [23], we next prove that the condition

$$\mathrm{Span}_{\mathbb{K}}(\hat{g}_j/x_n^{\delta+d} : t \le j \le r) = \mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$$

is a generic property in the sense of the Zariski topology, which will be used in the proof of Theorem 3.

Definition 6. *Let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$, and let*

$$\overline{P}_{u,n,d_{\boldsymbol{f}}} \times \overline{Q}_{n,s,d_{\boldsymbol{g}}} \subset \overline{\mathbb{K}}[y_1,\ldots,y_n]^u \times \overline{\mathbb{K}}[x_1,\ldots,x_s]^n$$

be the parameter set of $((f_1,\ldots,f_u),(g_1,\ldots,g_n))$. A property is called generic if the subset of $\overline{P}_{u,n,d_{\boldsymbol{f}}} \times \overline{Q}_{n,s,d_{\boldsymbol{g}}}$ satisfying it is a non-empty Zariski-open set; equivalently, the property holds for all elements of $\overline{P}_{u,n,d_{\boldsymbol{f}}} \times \overline{Q}_{n,s,d_{\boldsymbol{g}}}$ except an algebraic subset of codimension one.

To establish that a given property is generic, it suffices to verify the following two points.

1. Show that the set of points where the property fails is the zero of a system of polynomial equations. This ensures that its complement (the set where the property holds) is Zariski-open.
2. Prove that this Zariski-open subset is non-empty by providing at least one explicit example, defined over the ground field $\mathbb{K}$, for which the property holds.

To prove the main result of this section, we first give a necessary lemmas.

Lemma 5. *Given $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g} \in U_{u,n,s,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$, $\mathrm{Span}_{\mathbb{K}}(\hat{g}_j/x_n^{\delta+d} : t \le j \le r) = \mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$ is a generic property in the cases where $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ and $\gcd(q,2) = 1$; or $d_{\boldsymbol{f}} = 2, d_{\boldsymbol{g}} = 3$, and the characteristic of $\mathbb{K}$ is larger than $n+5$.*

Proof. By Lemma 9 (see Appendix A), the set of all coefficients (serving as formal parameters) of $\boldsymbol{f}$ and $\boldsymbol{g}$ for which $\mathrm{Span}_{\mathbb{K}}(\hat{g}_j/x_s^{\delta+d} : t \le j \le r) = \mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$ holds forms a Zariski-open set. To finish the proof, it remains to show that this set is non-empty. For the cases where $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ and $\gcd(q,2) = 1$; or $d_{\boldsymbol{f}} = 2, d_{\boldsymbol{g}} = 3$, and the characteristic of $\mathbb{K}$ is larger than $n+5$, the explicit examples provided in [23] demonstrate that this Zariski-open set is indeed non-empty. □

Now we give the main result of this subsection, which is stated formally in Theorem 3 below.

Theorem 3. *Let n, u, s and $U_{u,n,s,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$ be defined as above, and let δ, d, r, t and $\hat{g}_j$ be defined in Theorem 2. Given $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g} \in U_{u,n,s,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$,* **RREFComPoly** *generically returns a normal form decomposition $(\boldsymbol{f},\boldsymbol{g})$ of $\boldsymbol{h}$ in the cases where $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ and $\gcd(q,2) = 1$; or $d_{\boldsymbol{f}} = 2, d_{\boldsymbol{g}} = 3$, and the characteristic of $\mathbb{K}$ is larger than $n+5$. Furthermore, the normal form decomposition of $\boldsymbol{h}$ is generically unique.*

Proof. It immediately follows from Lemma 5 that $\mathrm{Span}_{\mathbb{K}}\{\hat{g}_j/x_n^{\delta+d} : t \le j \le r\} = \mathrm{Span}_{\mathbb{K}}\{g_1, g_2, \ldots, g_n\}$ holds generically. Since both $\{g_1, g_2, \ldots, g_n\}$ and $\{\hat{g}_j/x_s^{\delta+d} : r-n+1 \le j \le r\}$ form bases of the same vector space and their respective coefficient matrices under the grevlex order are in RREF, it follows that

$$g_i = \hat{g}_{r-n+i}/x_s^{\delta+d} \text{ for } 1 \le i \le n$$

hold generically. As conjectured in [23], once the right factor is known, the linear system to recover the left factor becomes overdetermined if $u \cdot \binom{s+d_{\boldsymbol{h}}-1}{d_{\boldsymbol{h}}} \ge u \cdot \binom{n+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}$. Consequently, $\boldsymbol{f}$ can be uniquely determined from $(g_1, g_2, \ldots, g_n)$ by solving the corresponding overdetermined linear system.

To finish the proof, it suffices to show that the right-factor whose coefficient matrix is in RREF w.r.t. the grevlex order is generically unique. Let $\boldsymbol{g}'$ be a right-factor of $\boldsymbol{h}$ whose coefficient matrix is in RREF. Then $\mathrm{Span}_{\mathbb{K}}\{\hat{g}_j/x_n^{\delta+d} : t \le j \le r\} = \mathrm{Span}_{\mathbb{K}}\{g'_1, g'_2, \ldots, g'_n\}$ also holds generically. This implies that $\mathrm{Span}_{\mathbb{K}}\{g_1, g_2, \ldots, g_n\} = \mathrm{Span}_{\mathbb{K}}\{g'_1, g'_2, \ldots, g'_n\}$ holds generically. Since the coefficient matrices of both spanning sets are in RREF, it follows that $g_i = g'_i$ for $1 \le i \le n$ generically. □

V. A NEW ALGORITHM FOR FDP BASED ON LOCALIZATION STRATEGY

Building on the foundation of the **RREFComPoly** algorithm, this section presents the most significant contribution of this paper. To the best of our knowledge, existing algorithms for solving FDP—relying on differentiation and homogenization—typically adopt a two-stage procedure: (1) computing the right-factor space, followed by (2) recovering the left-factor by solving a linear system derived from a basis of the right-factor space. In contrast, we propose a novel approach that inverts this conventional methodology. First, we use a localization strategy to recover the left-factor by the **RREFComPoly** algorithm. Second, we recover the right-factor through an iterative solution process, where at each iteration we construct and solve a system of linear equations derived from the left-factor and local information of the right-factor. Using this strategy, we develop a new algorithm, **PartComPoly**, which significantly reduces computation complexity compared to **MultiComPoly** and **RREFComPoly**. Beyond efficiency gains, our new algorithm extends the solvable scope of FDP, making intractable instances — such as those which were claimed to be not computationally exploitable in [1] – computationally tractable for the first time.

Throughout this section, we always assume that

$$\boldsymbol{h} = (h_1, h_2, \ldots, h_u) = \boldsymbol{f} \circ \boldsymbol{g} = (f_1(g_1, g_2, \ldots, g_n), f_2(g_1, g_2, \ldots, g_n), \ldots, f_u(g_1, g_2, \ldots, g_n)),$$

where u, n are integers satisfying $1 \leq u \leq n$ and $f_i, g_j \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ are homogeneous monic polynomials with the coefficient matrix associated with $\boldsymbol{g}$ w.r.t. the grevlex order is in RREF and $\deg(f_i) = d_{\boldsymbol{f}} \geq 2, \deg(g_j) = d_{\boldsymbol{g}} \geq 2$ for all $1 \leq i \leq u$ and all $1 \leq j \leq n$. It is worth noting that $(\boldsymbol{f}, \boldsymbol{g})$ is a normal form decomposition of $\boldsymbol{h}$.

A. Compute the left-factor with a localization strategy

We begin by presenting an intriguing observation, stated formally in Lemma 6 below, which is obviously true.

Lemma 6. *Let $\boldsymbol{h}, \boldsymbol{f}, \boldsymbol{g}$ be defined as above. Then for any integer s with $1 \leq s \leq n$, we have*

$$(h_1^{(s)}, h_2^{(s)}, \ldots, h_u^{(s)}) = (f_1(g_1^{(s)}, g_2^{(s)}, \ldots, g_n^{(s)}), f_2(g_1^{(s)}, g_2^{(s)}, \ldots, g_n^{(s)}), \ldots, f_u(g_1^{(s)}, g_2^{(s)}, \ldots, g_n^{(s)})), \tag{5}$$

where $h_i^{(s)} = h_i(x_1, x_2, \ldots, x_s, 0, \ldots, 0)$ for $1 \leq i \leq u$ and $g_j^{(s)} = g_j(x_1, x_2, \ldots, x_s, 0, \ldots, 0)$ for $1 \leq j \leq n$.

Remark 2. *In fact, Lemma 6 remains valid when we fix any s variables $x_{k_1}, x_{k_2}, \ldots, x_{k_s}$ while setting the remaining $n - s$ variables to zero, where $1 \leq k_1 < k_2 < \cdots < k_s \leq n$. However, this is essentially equivalent to the original Lemma 6, as it can be reduced to the original case via the variable substitution $y_1 = x_{k_1}, y_2 = x_{k_2}, \ldots, y_s = x_{k_s}$.*

Remark 3. *We note that the coefficient matrix associated with $g_1^{(s)}, g_2^{(s)}, \ldots, g_n^{(s)}$ is still in RREF, since it is a submatrix formed by the first $\binom{s+d_{\boldsymbol{g}}-1}{d_{\boldsymbol{g}}}$ columns of the coefficient matrix associated with $g_1, g_2, \ldots, g_n$.*

By Lemma 6, if $\boldsymbol{f} = (f_1, f_2, \ldots, f_u)$ and $\boldsymbol{g} = (g_1, g_2, \ldots, g_n)$ form a $(d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$-decomposition of $\boldsymbol{h}$, then $\boldsymbol{f} = (f_1, f_2, \ldots, f_u)$ and $\boldsymbol{g}^{(s)} = (g_1^{(s)}, g_2^{(s)}, \ldots, g_n^{(s)})$ also yield a $(d_{\boldsymbol{f}}, d_{\boldsymbol{g}})$-decomposition of $\boldsymbol{h}^{(s)} = (h_1^{(s)}, h_2^{(s)}, \ldots, h_u^{(s)})$. To compute $\boldsymbol{f}$ and $\boldsymbol{g}$, we adopt a two-step approach:

1. Selecting the parameter s. We choose the smallest integer s such that the **RREFCompoly** succeeds on input $\boldsymbol{h}^{(s)} = (h_1^{(s)}, h_2^{(s)}, \ldots, h_u^{(s)})$, returing $\boldsymbol{f}$ and $\boldsymbol{g}^{(s)}$ rather than "Fail".
2. Recovering $\boldsymbol{g}$. We first compute $\boldsymbol{g}^{(s+1)}$ from $\boldsymbol{f}$ and $\boldsymbol{g}^{(s)}$, then $\boldsymbol{g}^{(s+2)}$ from $\boldsymbol{f}$ and $\boldsymbol{g}^{(s+1)}$, and continue this iterative process until we finally recover $\boldsymbol{g}$ from $\boldsymbol{f}$ and $\boldsymbol{g}^{(n-1)}$.

In this subsection, we detail our strategy to determine the parameter s. The subsequent subsection will address the computation of $\boldsymbol{g}$ from $\boldsymbol{g}^{(s)}$ and $\boldsymbol{f}$.

Although smaller values of s might seem advantageous for computing $\boldsymbol{f}$ and $\boldsymbol{g}^{(s)}$ efficiently, they may prevent the **RREFCompoly** algorithm from producing correct outputs $\boldsymbol{f}$ and $\boldsymbol{g}^{(s)}$. To balance correctness and computational efficiency, the selection of s must satisfy three key conditions:

1. Nonnegative δ Estimate: The $\boldsymbol{\delta}$-Estimate algorithm must return $\delta \geq 0$ to ensure the correctness of **RREFCompoly**'s computation.
2. Computational Efficiency: Since δ significantly impacts the computational complexity of **RREFCompoly**, we require $\boldsymbol{\delta}$-**Estimate**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, s) \leq \boldsymbol{\delta}$-**Estimate**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, n)$ to maintain reasonable efficiency.

3. Uniqueness of Solution: Given $\boldsymbol{g}^{(s)}$, $\boldsymbol{f}$ is determined by solving a linear system of $u \cdot \binom{s+d_{\boldsymbol{h}}-1}{d_{\boldsymbol{h}}}$ equations in $u \cdot \binom{n+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}$ unknown coefficients derived from $\boldsymbol{h}^{(s)} = \boldsymbol{f} \circ \boldsymbol{g}^{(s)}$. To guarantee a unique solution, we require $\binom{s+d_{\boldsymbol{h}}-1}{d_{\boldsymbol{h}}} \geq \binom{n+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}$.

Therefore, the parameter s must satisfy the following conditions simultaneously:

$$0 \leq \boldsymbol{\delta}\text{-Estimate}(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, s) \leq \boldsymbol{\delta}\text{-Estimate}(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, n) \text{ and } \binom{s+d_{\boldsymbol{h}}-1}{d_{\boldsymbol{h}}} \geq \binom{n+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}. \tag{6}$$

B. Compute $\boldsymbol{g}$ from $\boldsymbol{f}$ and $\boldsymbol{g}^{(s)}$

In this subsection, we will introduce how to compute $\boldsymbol{g}$ from $\boldsymbol{g}^{(s)}$ and $\boldsymbol{f}$. We first give a necessary lemma.

Lemma 7. *Let $n, u, d_{\boldsymbol{h}}, d_{\boldsymbol{g}}$ be defined as above and let s be an integer with $1 \leq s < n$. If $\binom{s+d_{\boldsymbol{h}}-2}{d_{\boldsymbol{h}}-1} / \binom{s+d_{\boldsymbol{g}}-2}{d_{\boldsymbol{g}}-1} \geq n/u$, then*

$$\binom{s+d_{\boldsymbol{h}}-a-2}{d_{\boldsymbol{h}}-a-1} / \binom{s+d_{\boldsymbol{g}}-a-2}{d_{\boldsymbol{g}}-a-1} \geq n/u \text{ for all } 0 < a < d_{\boldsymbol{g}}.$$

Proof. Since $d_{\boldsymbol{h}} > d_{\boldsymbol{g}}$, it follows that

$$\frac{\binom{s+d_{\boldsymbol{h}}-a-2}{d_{\boldsymbol{h}}-a-1} / \binom{s+d_{\boldsymbol{g}}-a-2}{d_{\boldsymbol{g}}-a-1}}{\binom{s+d_{\boldsymbol{h}}-a-1}{d_{\boldsymbol{h}}-a} / \binom{s+d_{\boldsymbol{g}}-a-1}{d_{\boldsymbol{g}}-a}} = \frac{(d_{\boldsymbol{g}}-a+s-1)(d_{\boldsymbol{h}}-a)}{(d_{\boldsymbol{h}}-a+s-1)(d_{\boldsymbol{g}}-a)} = \frac{1+\frac{s-1}{d_{\boldsymbol{g}}-a}}{1+\frac{s-1}{d_{\boldsymbol{h}}-a}} \geq 1 \text{ for all } 0 \leq a < d_{\boldsymbol{g}},$$

and so the ratio $\binom{s+d_{\boldsymbol{h}}-a-2}{d_{\boldsymbol{h}}-a-1} / \binom{s+d_{\boldsymbol{g}}-a-2}{d_{\boldsymbol{g}}-a-1}$ is monotonically increasing in a over the range $0 \leq a < d_{\boldsymbol{g}}$. Consequently,

$$\binom{s+d_{\boldsymbol{h}}-a-2}{d_{\boldsymbol{h}}-a-1} / \binom{s+d_{\boldsymbol{g}}-a-2}{d_{\boldsymbol{g}}-a-1} \geq \binom{s+d_{\boldsymbol{h}}-2}{d_{\boldsymbol{h}}-1} / \binom{s+d_{\boldsymbol{g}}-2}{d_{\boldsymbol{g}}-1} \geq n/u \text{ for all } 0 < a < d_{\boldsymbol{g}}.$$

□

Now we give the main result of this subsection, which is stated formally in Theorem 4 below.

Theorem 4. *Let $n, u, \boldsymbol{h}, \boldsymbol{f}, \boldsymbol{g}, d_{\boldsymbol{h}}, d_{\boldsymbol{f}}, d_{\boldsymbol{g}}$ be defined as above and let s be an integer with $1 \leq s < n$ such that $\binom{s+d_{\boldsymbol{h}}-2}{d_{\boldsymbol{h}}-1} / \binom{s+d_{\boldsymbol{g}}-2}{d_{\boldsymbol{g}}-1} \geq n/u$. For $1 \leq j \leq n$ and $1 \leq l \leq u$, let*

$$g_j^{(s+1)} = g_j(x_1, x_2, \ldots, x_s, x_{s+1}, 0, \ldots, 0) = \sum_{0 \leq i \leq d_{\boldsymbol{g}}} D_{i,j} x_{s+1}^i,$$

$$h_l^{(s+1)} = h_l(x_1, x_2, \ldots, x_s, x_{s+1}, 0, \ldots, 0) = \sum_{0 \leq k \leq d_{\boldsymbol{h}}} H_{k,l} x_{s+1}^k,$$

where $D_{i,j}, H_{k,l} \in \mathbb{K}[x_1, x_2, \ldots, x_s]$ with $\deg(D_{i,j}) = d_{\boldsymbol{g}} - i$ for $0 \leq i \leq d_{\boldsymbol{g}}$ and $\deg(H_{k,l}) = d_{\boldsymbol{h}} - k$ for $0 \leq k \leq d_{\boldsymbol{h}}$(we note that $D_{0,j} = g_j^{(s)}$). If $\boldsymbol{h}$ and $\boldsymbol{f}$ are known, and there exists an integer a with $0 \leq a < d_{\boldsymbol{g}}$ such that all $D_{i,j}$ are known for $0 \leq i \leq a$ and $1 \leq j \leq n$, then $D_{a+1,1}, D_{a+1,2}, \ldots, D_{a+1,n}$ can be determined by solving a linear system consisting of $u \cdot \binom{s+d_{\boldsymbol{h}}-a-2}{d_{\boldsymbol{h}}-a-1}$ equations with $n \cdot \binom{s+d_{\boldsymbol{g}}-a-2}{d_{\boldsymbol{g}}-a-1}$ unknowns.

Proof. For $1 \leq l \leq u$, let

$$f_l(x_1, x_2, \ldots, x_n) = \sum_{1 \leq k_1 \leq k_2 \leq \cdots \leq k_{d_{\boldsymbol{f}}} \leq n} f^{(l)}_{k_1, k_2, \ldots, k_{d_{\boldsymbol{f}}}} x_{k_1} x_{k_2} \cdots x_{k_{d_{\boldsymbol{f}}}},$$

where $f^{(l)}_{k_1, k_2, \ldots, k_{d_{\boldsymbol{f}}}} \in \mathbb{K}$ is the coefficient of f_l. Then we have

$$h_l^{(s+1)} = \sum_{1 \leq k_1 \leq k_2 \leq \cdots \leq k_{d_{\boldsymbol{f}}} \leq n} f^{(l)}_{k_1, k_2, \ldots, k_{d_{\boldsymbol{f}}}} g_{k_1}^{(s+1)} g_{k_2}^{(s+1)} \cdots g_{k_{d_{\boldsymbol{f}}}}^{(s+1)},$$

or equivalently

$$\sum_{0 \leq k \leq d_{\boldsymbol{h}}} H_{k,l} x_{s+1}^k = \sum_{1 \leq k_1 \leq k_2 \leq \cdots \leq k_{d_{\boldsymbol{f}}} \leq n} f^{(l)}_{k_1, k_2, \ldots, k_{d_{\boldsymbol{f}}}} \left(\sum_{0 \leq i_1 \leq d_{\boldsymbol{g}}} D_{i_1, k_1} x_{s+1}^{i_1} \sum_{0 \leq i_2 \leq d_{\boldsymbol{g}}} D_{i_2, k_2} x_{s+1}^{i_2} \cdots \sum_{0 \leq i_{d_{\boldsymbol{f}}} \leq d_{\boldsymbol{g}}} D_{i_{d_{\boldsymbol{f}}}, k_{d_{\boldsymbol{f}}}} x_{s+1}^{i_{d_{\boldsymbol{f}}}} \right),$$

and so we obtain

$$H_{k,l} = \sum_{1\le k_1\le k_2\le\cdots\le k_{d_{\boldsymbol{f}}}\le n} f^{(l)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}} \sum_{\substack{i_1+i_2+\cdots+i_{d_{\boldsymbol{f}}}=k\\ 0\le i_1,i_2,\ldots,i_{d_{\boldsymbol{f}}}\le d_{\boldsymbol{g}}}} \left(D_{i_1,k_1}D_{i_2,k_2}\cdots D_{i_{d_{\boldsymbol{f}}},k_{d_{\boldsymbol{f}}}}\right) \text{ for } 0\le k\le d_{\boldsymbol{h}} \text{ and } 1\le l\le u.$$

In particular, for the case $k = a+1$, we have

$$\begin{aligned}&\sum_{1\le k_1\le k_2\le\cdots\le k_{d_{\boldsymbol{f}}}\le n} f^{(l)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}} \left(D_{a+1,k_1}D_{0,k_2}\cdots D_{0,k_{d_{\boldsymbol{f}}}} + D_{0,k_1}D_{a+1,k_2}\cdots D_{0,k_{d_{\boldsymbol{f}}}} + \cdots + D_{0,k_1}D_{0,k_2}\cdots D_{a+1,k_{d_{\boldsymbol{f}}}}\right)\\ &= H_{a+1,l} - \sum_{1\le k_1\le k_2\le\cdots\le k_{d_{\boldsymbol{f}}}\le n} f^{(l)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}} \sum_{\substack{i_1+i_2+\cdots+i_{d_{\boldsymbol{f}}}=a+1\\ 0\le i_1,i_2,\ldots,i_{d_{\boldsymbol{f}}}\le a}} \left(D_{i_1,k_1}D_{i_2,k_2}\cdots D_{i_{d_{\boldsymbol{f}}},k_{d_{\boldsymbol{f}}}}\right) \text{ for } 1\le l\le u.\end{aligned} \tag{7}$$

By assumptions, all quantities in Equalities (7) are known except for $D_{a+1,1}, D_{a+1,2}, \ldots, D_{a+1,n}$. For each $1\le j\le n$, the number of unknown coefficients in $D_{a+1,j}$ is $\binom{s+d_{\boldsymbol{g}}-a-2}{d_{\boldsymbol{g}}-a-1}$, while for each $1\le l\le u$, the number of (known) coefficients in $H_{a+1,l}$ is $\binom{s+d_{\boldsymbol{h}}-a-2}{d_{\boldsymbol{h}}-a-1}$. By comparing the coefficients on both sides of Equalities (7), a linear system consisting of $u\cdot\binom{s+d_{\boldsymbol{h}}-a-2}{d_{\boldsymbol{h}}-a-1}$ equations with $n\cdot\binom{s+d_{\boldsymbol{g}}-a-2}{d_{\boldsymbol{g}}-a-1}$ unknowns is obtained.

Since $\binom{s+d_{\boldsymbol{h}}-2}{d_{\boldsymbol{h}}-1}/\binom{s+d_{\boldsymbol{g}}-2}{d_{\boldsymbol{g}}-1} \ge n/u$, by Lemma 7, the number of equations in the linear system is not less than the number of unknowns. Consequently, the above linear system typically admits a unique solution, allowing us to determine $D_{a+1,1}, D_{a+1,2}, \ldots, D_{a+1,n}$ uniquely. □

According to Theorem 4, we begin by computing $(D_{1,1}, D_{1,2}, \ldots, D_{1,n})$ using $\boldsymbol{f}$ and $\boldsymbol{g}^{(s)} = (D_{0,1}, D_{0,2}, \ldots, D_{0,n})$, then $(D_{2,1}, D_{2,2}, \ldots, D_{2,n})$ using $\boldsymbol{f}$ and the previously obtained $(D_{1,1}, D_{1,2}, \ldots, D_{1,n})$, and continue this iterative process until we finally recover $\boldsymbol{g}^{(s+1)}$. Subsequently, we can compute $\boldsymbol{g}^{(s+2)}$ from $\boldsymbol{f}$ and $\boldsymbol{g}^{(s+1)}$ and continue this iterative process until we finally recover $\boldsymbol{g} = \boldsymbol{g}^{(n)}$.

*C. The **PartComPoly** algorithm*

Having introduced the key components, we now present the complete **PartComPoly** algorithm in its entirety. The following pseudo-code provides a formal representation of the algorithm.

Algorithm 4 PartComPoly

Input: Integers $d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u$ with $d_{\boldsymbol{f}}, d_{\boldsymbol{g}} > 1$ and $1\le u\le n$, homogeneous monic polynomials $h_1, h_2, \ldots, h_u$ of the same degree $d_{\boldsymbol{h}}$

Output: Fail, or homogeneous monic polynomials $\boldsymbol{f} = (f_1, f_2, \ldots, f_u), \boldsymbol{g} = (g_1, g_2, \ldots, g_n)$ of degree $d_{\boldsymbol{f}}$ and $d_{\boldsymbol{g}}$ respectively such that $\boldsymbol{h} = \boldsymbol{f}\circ\boldsymbol{g}$

$s \leftarrow \min\left\{s' \ge 0 : \binom{s'+d_{\boldsymbol{h}}-1}{d_{\boldsymbol{h}}} \ge \binom{n+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}, \binom{s'+d_{\boldsymbol{h}}-2}{d_{\boldsymbol{h}}-1}/\binom{s'+d_{\boldsymbol{g}}-2}{d_{\boldsymbol{g}}-1} \ge n/u\right\}$
$\delta_n \leftarrow$ **$\boldsymbol{\delta}$-Estimate**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, n)$
while $s\le n$ **do**
    $\delta \leftarrow$ **$\boldsymbol{\delta}$-Estimate**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, s)$
    if $0\le\delta\le\delta_n$ **then**
        break
    end if
    $s \leftarrow s+1$
end while
if $s > n$ **then**
    Return Fail
end if
$h_j^{(s)} \leftarrow h_j(x_1, x_2, \ldots, x_s, 0, \ldots, 0)$ for $1\le j\le n$
$\boldsymbol{f} = (f_1, f_2, \ldots, f_u), \boldsymbol{g}^{(s)} = (g_1^{(s)}, g_2^{(s)}, \ldots, g_n^{(s)}) \leftarrow$ **RREFComPoly**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, s, h_1^{(s)}, h_2^{(s)}, \ldots, h_u^{(s)})$
while $s < n$ **do**
    $a \leftarrow 0$
    $D_{0,j} \leftarrow g_j^{(s)}$ for $1\le j\le n$
    while $a < d_{\boldsymbol{g}}$ **do**

Solve the linear system derived from equations (5) to obtain $D_{a+1,1}, D_{a+1,2}, \ldots, D_{a+1,n}$
$a \leftarrow a+1$
end while
$\boldsymbol{g}^{(s+1)} = (g_1^{(s+1)}, g_2^{(s+1)}, \ldots, g_n^{(s+1)}) \leftarrow \left(\sum_{0\le i_1\le d_{\boldsymbol{g}}} D_{i_1,1}x_{s+1}^{i_1}, \sum_{0\le i_2\le d_{\boldsymbol{g}}} D_{i_2,2}x_{s+1}^{i_2}, \ldots, \sum_{0\le i_n\le d_{\boldsymbol{g}}} D_{i_n,n}x_{s+1}^{i_n}\right)$
$s \leftarrow s+1$
end while
return $\boldsymbol{f}$ and $\boldsymbol{g} = \boldsymbol{g}^{(n)}$

The complexity of computing $\boldsymbol{f}$, $\boldsymbol{g}^{(s)}$ through **RREFComPoly** is estimated as $O(\max(H^2J/\log_q H, U^\omega))$, where

$$H = u\binom{s+d_{\boldsymbol{f}}-2}{d_{\boldsymbol{f}}-1}\binom{s+\delta-1}{\delta}, J = \binom{s+\delta+d+d_{\boldsymbol{g}}-1}{\delta+d+d_{\boldsymbol{g}}} \text{ and } U = u\cdot\binom{s+d_{\boldsymbol{f}}-1}{d_{\boldsymbol{f}}}$$

with $d = (d_{\boldsymbol{f}}-1)(d_{\boldsymbol{g}}-1)$. Additionally, the complexity of solving the linear system derived from Equations (5) is $O(E_{s,a}^\omega)$, where $E_{s,a} = n\binom{s+d_{\boldsymbol{g}}-a-2}{d_{\boldsymbol{g}}-a-1}$. Consequently, the overall complexity of computing $\boldsymbol{g}$ from $\boldsymbol{f}$ and $\boldsymbol{g}^{(s)}$ is $O(\sum_{s\le s'<n}\sum_{0\le a<d_{\boldsymbol{g}}} E_{s',a}^\omega)$. In summary, the **PartComPoly** algorithm has an overall complexity of

$$O(\max(H^2J/\log_q H, U^\omega, \sum_{s\le s'<n}\sum_{0\le a<d_{\boldsymbol{g}}} E_{s',a}^\omega))$$

field operations.

Next, we present a comparative evaluation between our new algorithm, **RREFComPoly** and **MultiComPoly** in attacking some instances described in Subsection II-D, focusing on the dimensions of the resulting matrices and the computational complexity. Table I provides the comparison between **MultiComPoly**, **RREFComPoly** and **PartComPoly**, where the degree $d_{\boldsymbol{f}}$ is equal to 2 and $d_{\boldsymbol{g}}$ is equal to 3, with the prime modulus q fixed at 2.

Table I: Comparative analysis of computational complexity, where
- n: the number of variables;
- u: the number of polynomial components of $\boldsymbol{h}$;
- δ_{old}: the smallest δ satisfying $|\tilde{F}_\delta| \ge |F_\delta|$;
- δ_{new}: the value of δ return by $\boldsymbol{\delta}$**-Estimate**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, n)$;
- δ_{Part}: the value assigned to δ in **PartComPoly**;
- s: the value assigned to s in **PartComPoly**;
- R_{RREF}/C_{RREF}: the number of rows/columns of C in **RREFComPoly**;
- R_{Part}/C_{Part}: the number of rows/columns of C in **PartComPoly**;
- O_{Multi}: the estimated complexity of **MultiComPoly**;
- O_{RREF}: the estimated complexity of **RREFComPoly**;
- O_{Part}: the estimated complexity of **PartComPoly**.

n	u	δ_{old}	δ_{new}	s	δ_{Part}	R_{RREF}/C_{RREF}	R_{Part}/C_{Part}	$O_{Multi}{}^*$	O_{RREF}	O_{Part}
39	19	10	9	21	6	$2^{39.9}/2^{40.7}$	$2^{26.5}/2^{26.3}$	$2^{237.8}$	$2^{115.1}$	$2^{74.5}$
39	23	9	8	20	5	$2^{37.8}/2^{38.8}$	$2^{24.2}/2^{24.3}$	$2^{222.0}$	$2^{109.1}$	$2^{68.1}$
39	27	8	8	20	5	$2^{38.0}/2^{38.8}$	$2^{24.5}/2^{24.3}$	$2^{206.1}$	$2^{109.5}$	$2^{68.5}$
39	31	7	7	18	4	$2^{35.7}/2^{36.8}$	$2^{21.7}/2^{21.6}$	$2^{190.3}$	$2^{103.0}$	$2^{60.5}$
39	35	7	6	18	4	$2^{33.2}/2^{34.8}$	$2^{21.8}/2^{21.6}$	$2^{190.3}$	$2^{96.0}$	$2^{60.8}$
48	28	10	9	23	6	$2^{43.2}/2^{44.4}$	$2^{27.9}/2^{27.5}$	$2^{251.3}$	$2^{125.3}$	$2^{78.4}$
48	32	9	9	22	5	$2^{43.4}/2^{44.4}$	$2^{25.5}/2^{25.4}$	$2^{234.6}$	$2^{125.7}$	$2^{71.7}$
48	36	8	8	22	5	$2^{40.9}/2^{42.2}$	$2^{25.6}/2^{25.4}$	$2^{217.8}$	$2^{118.7}$	$2^{72.0}$
48	40	8	7	20	4	$2^{38.3}/2^{40.0}$	$2^{22.8}/2^{22.7}$	$2^{217.8}$	$2^{111.4}$	$2^{63.7}$
48	44	7	7	20	4	$2^{38.4}/2^{40.0}$	$2^{22.9}/2^{22.7}$	$2^{201.1}$	$2^{111.7}$	$2^{64.0}$
57	37	10	9	25	6	$2^{45.9}/2^{47.5}$	$2^{29.0}/2^{28.6}$	$2^{262.5}$	$2^{133.8}$	$2^{81.8}$
57	41	9	9	24	5	$2^{46.1}/2^{47.5}$	$2^{26.5}/2^{26.5}$	$2^{245.0}$	$2^{134.1}$	$2^{74.8}$
57	45	9	8	24	5	$2^{43.4}/2^{45.1}$	$2^{26.7}/2^{26.5}$	$2^{245.0}$	$2^{126.4}$	$2^{75.1}$
57	49	8	8	24	5	$2^{43.5}/2^{45.1}$	$2^{26.8}/2^{26.5}$	$2^{227.5}$	$2^{126.7}$	$2^{75.3}$
57	53	8	8	22	4	$2^{43.6}/2^{45.1}$	$2^{23.8}/2^{23.8}$	$2^{227.5}$	$2^{126.9}$	$2^{66.8}$
66	46	10	10	25	5	$2^{51.2}/2^{52.6}$	$2^{27.0}/2^{27.0}$	$2^{272.0}$	$2^{149.2}$	$2^{76.3}$
66	50	10	9	25	5	$2^{48.4}/2^{50.1}$	$2^{27.1}/2^{27.0}$	$2^{272.0}$	$2^{141.3}$	$2^{76.5}$

66	54	9	9	25	5	$2^{48.5}/2^{50.1}$	$2^{27.3}/2^{27.0}$	$2^{253.9}$	$2^{141.5}$	$2^{76.7}$
66	58	9	9	23	4	$2^{48.6}/2^{50.1}$	$2^{24.2}/2^{24.3}$	$2^{253.9}$	$2^{141.7}$	$2^{68.2}$
66	62	8	8	23	4	$2^{45.6}/2^{47.6}$	$2^{24.3}/2^{24.3}$	$2^{235.7}$	$2^{133.4}$	$2^{68.4}$
75	55	11	10	27	5	$2^{53.3}/2^{55.1}$	$2^{27.9}/2^{27.9}$	$2^{299.0}$	$2^{156.0}$	$2^{78.9}$
75	59	10	10	27	5	$2^{53.4}/2^{55.1}$	$2^{28.0}/2^{27.9}$	$2^{280.3}$	$2^{156.2}$	$2^{79.1}$
75	63	10	9	27	5	$2^{50.5}/2^{52.5}$	$2^{28.1}/2^{27.9}$	$2^{280.3}$	$2^{147.8}$	$2^{79.3}$
75	67	9	9	27	5	$2^{50.6}/2^{52.5}$	$2^{28.2}/2^{27.9}$	$2^{261.6}$	$2^{148.0}$	$2^{79.5}$
75	71	9	9	27	5	$2^{50.6}/2^{52.5}$	$2^{28.3}/2^{27.9}$	$2^{261.6}$	$2^{148.1}$	$2^{79.7}$
84	64	11	10	28	5	$2^{55.3}/2^{57.3}$	$2^{28.4}/2^{28.4}$	$2^{306.8}$	$2^{162.1}$	$2^{80.4}$
84	68	10	10	28	5	$2^{55.4}/2^{57.3}$	$2^{28.5}/2^{28.4}$	$2^{287.7}$	$2^{162.3}$	$2^{80.6}$
84	72	10	10	28	5	$2^{55.4}/2^{57.3}$	$2^{28.6}/2^{28.4}$	$2^{287.7}$	$2^{162.4}$	$2^{80.7}$
84	76	10	9	28	5	$2^{52.3}/2^{54.6}$	$2^{28.7}/2^{28.4}$	$2^{287.7}$	$2^{153.5}$	$2^{80.9}$
84	80	9	9	28	5	$2^{52.4}/2^{54.6}$	$2^{28.7}/2^{28.4}$	$2^{268.5}$	$2^{153.7}$	$2^{81.0}$
93	73	11	11	29	5	$2^{60.2}/2^{62.1}$	$2^{28.9}/2^{28.8}$	$2^{313.9}$	$2^{176.7}$	$2^{81.8}$
93	77	11	10	29	5	$2^{57.1}/2^{59.4}$	$2^{29.0}/2^{28.8}$	$2^{313.9}$	$2^{167.7}$	$2^{81.9}$
93	81	11	10	29	5	$2^{57.2}/2^{59.4}$	$2^{29.1}/2^{28.8}$	$2^{313.9}$	$2^{167.9}$	$2^{82.1}$
93	85	10	10	29	5	$2^{57.2}/2^{59.4}$	$2^{29.1}/2^{28.8}$	$2^{294.3}$	$2^{168.0}$	$2^{82.2}$
93	89	10	10	29	5	$2^{57.3}/2^{59.4}$	$2^{29.2}/2^{28.8}$	$2^{294.3}$	$2^{168.1}$	$2^{82.3}$
101	81	12	11	31	5	$2^{61.7}/2^{63.9}$	$2^{29.6}/2^{29.7}$	$2^{339.6}$	$2^{181.5}$	$2^{84.0}$
101	85	11	11	31	5	$2^{61.8}/2^{63.9}$	$2^{29.7}/2^{29.7}$	$2^{319.6}$	$2^{181.6}$	$2^{84.1}$
101	89	11	11	31	5	$2^{61.9}/2^{63.9}$	$2^{29.7}/2^{29.7}$	$2^{319.6}$	$2^{181.7}$	$2^{84.2}$
101	93	11	10	31	5	$2^{58.6}/2^{61.1}$	$2^{29.8}/2^{29.7}$	$2^{319.6}$	$2^{172.4}$	$2^{84.4}$
101	97	10	10	31	5	$2^{58.7}/2^{61.1}$	$2^{29.9}/2^{29.7}$	$2^{299.6}$	$2^{172.5}$	$2^{84.5}$

* The computational complexity of **MultiComPoly** is estimated using a binomial approximation, which causes both the parameter δ and the complexity to be overstated. In practice, however, the actual complexity is far lower than this initial estimate suggests.

A comparison of R_{RREF}/C_{RREF} and R_{Part}/C_{Part} in Table I reveals that when $d_{\boldsymbol{f}} = 2$ and $d_{\boldsymbol{g}} = 3$, the coefficient matrix C in **RREFComPoly** undergoes dramatic expansion as n increases, while **PartComPoly** maintains significantly smaller matrix dimensions. This dimensional reduction directly translates to computational efficiency: as shown by comparing O_{Multi}, O_{RREF} and O_{Part}, **PartComPoly** achieves a dramatic complexity reduction over **RREFComPoly**, while the latter already represents a tighter complexity than **MultiComPoly**.

*D. The correctness of **PartComPoly***

In this subsection, we prove the correctness of **PartComPoly**. We first give a necessary lemma.

Lemma 8. *Let* $\gcd(q, 2) = 1$*, and let* $n \geq 6, u = n, s = n - 1$*. Consider* $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$*, where*

$$\boldsymbol{f} = (f_1, f_2, \ldots, f_n), \boldsymbol{g} = (g_1, g_2, \ldots, g_n)$$

with

$$f_1 = (x_1 + x_3 + x_5 + x_6 + \cdots + x_n)^2, f_i = x_i(x_1 + x_3 + x_5 + x_6 + \cdots + x_n), 2 \leq i \leq n,$$

$$g_1 = x_1^2, g_2 = x_1x_2, g_3 = x_2^2, g_4 = x_2x_3, g_i = x_{i-2}^2, 5 \leq i \leq n-1, g_n = x_{n-2}^2 + x_{n-1}^2 + x_n^2.$$

Then we have

$$\mathrm{Span}_{\mathbb{K}}(\hat{g}_j/x_n : t \leq j \leq r) = \mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n), \tag{8}$$

$$\mathrm{Span}_{\mathbb{K}}({\hat{g}_j}^{(s)}/x_s : t_s \leq j \leq r_s) = \mathrm{Span}_{\mathbb{K}}(g_1^{(s)}, g_2^{(s)}, \ldots, g_n^{(s)}). \tag{9}$$

Proof. Let C and C_s be the coefficient matrices associated with $\{\partial h_i/\partial x_j : 1 \leq i \leq n, 1 \leq j \leq n\}$ and $\{\partial h_i^{(s)}/\partial x_j : 1 \leq i \leq n, 1 \leq j \leq s\}$. Let $C^* = (c_{i,j}^*)_{n^2 \times |M_n(3)|}$ be the RREF of C and C_s^* be the RREF of C_s, with $\mathrm{rank}(C^*) = r$ and $\mathrm{rank}(C_s^*) = r_s$. Let t be the largest positive integer such that $x_n \mid \mathrm{LM}(\hat{g}_k)$ for $t \leq k \leq r$ but $x_n \nmid \mathrm{LM}(\hat{g}_{t-1})$, where $\hat{g}_k = c_{k,1}^* x_1^3 + c_{k,2}^* x_2 x_1^2 + \cdots + c_{k,|M_n(3)|}^* x_n^3$ is the polynomial corresponding to the k-th row of C^* for $1 \leq k \leq r$. Analogously, let t_s be the largest positive integer such that $x_s \mid \mathrm{LM}({\hat{g}_k}^{(s)})$ for $t_s \leq k \leq r_s$ but $x_s \nmid \mathrm{LM}(\hat{g}_{t_s-1}^{(s)})$.

In Subsection IV-B, it is proved that (8) holds provided that

$$\mathrm{Span}_{\mathbb{K}}(\partial h_i/\partial x_j : 1 \le i \le n, 1 \le j \le n) = \mathrm{Span}_{\mathbb{K}}(x_j g_i : 1 \le i \le n, 1 \le j \le n)$$

and $t = r - n + 1$ and (9) holds provided that

$$\mathrm{Span}_{\mathbb{K}}(\partial h_i^{(s)}/\partial x_j : 1 \le i \le n, 1 \le j \le s) = \mathrm{Span}_{\mathbb{K}}(x_j g_i^{(s)} : 1 \le i \le n, 1 \le j \le s)$$

and $t_s = r_s - n + 1$.

It can be verified that

$$h_1 = (g_1 + g_3 + g_5 + g_6 + \cdots + g_n)^2 = (x_1^2 + x_2^2 + \cdots + x_n^2)^2,$$
$$h_1^{(s)} = (g_1^{(s)} + g_3^{(s)} + g_5^{(s)} + g_6^{(s)} + \cdots + g_n^{(s)})^2 = (x_1^2 + x_2^2 + \cdots + x_{n-1}^2)^2,$$
$$h_i = g_i(g_1 + g_3 + g_5 + g_6 + \cdots + g_n) = g_i \cdot (x_1^2 + x_2^2 + \cdots + x_n^2),$$
$$h_i^{(s)} = g_i^{(s)}(g_1^{(s)} + g_3^{(s)} + g_5^{(s)} + g_6^{(s)} + \cdots + g_n^{(s)}) = g_i^{(s)} \cdot (x_1^2 + x_2^2 + \cdots + x_{n-1}^2), 1 \le i \le n,$$

with $s = n - 1$. The partial derivatives of $\boldsymbol{h}$ are given by

$$\partial h_1/\partial x_j = 4x_j(g_1 + g_3 + g_5 + g_6 + \cdots + g_n), 1 \le j \le n,$$
$$\partial h_i/\partial x_j = \partial g_i/\partial x_j \cdot (g_1 + g_3 + g_5 + g_6 + \cdots + g_n) + 2x_j g_i, 2 \le i \le n, 1 \le j \le n.$$

Similarly,

$$\partial h_1^{(s)}/\partial x_j = 4x_j(g_1^{(s)} + g_3^{(s)} + g_5^{(s)} + g_6^{(s)} + \cdots + g_n^{(s)}), 1 \le j \le n-1,$$
$$\partial h_i^{(s)}/\partial x_j = \partial g_i^{(s)}/\partial x_j \cdot (g_1^{(s)} + g_3^{(s)} + g_5^{(s)} + g_6^{(s)} + \cdots + g_n^{(s)}) + 2x_j g_i^{(s)}, 2 \le i \le n, 1 \le j \le n-1.$$

It follows immediately that

$$\begin{aligned}
&\mathrm{Span}_{\mathbb{K}}(\partial h_i/\partial x_j : 1 \le i \le n, 1 \le j \le n)\\
&= \mathrm{Span}_{\mathbb{K}}(x_j(g_1 + g_3 + g_5 + g_6 + \cdots + g_n) : 1 \le j \le n) + \mathrm{Span}_{\mathbb{K}}(x_j g_i : 2 \le i \le n, 1 \le j \le n)\\
&= \mathrm{Span}_{\mathbb{K}}(x_j g_1 : 1 \le j \le n) + \mathrm{Span}_{\mathbb{K}}(x_j g_i : 2 \le i \le n, 1 \le j \le n)\\
&= \mathrm{Span}_{\mathbb{K}}(x_j g_i : 1 \le i \le n, 1 \le j \le n).
\end{aligned}$$

Similarly, we also have

$$\mathrm{Span}_{\mathbb{K}}(\partial h_i^{(s)}/\partial x_j : 1 \le i \le n, 1 \le j \le n-1) = \mathrm{Span}_{\mathbb{K}}(x_j g_i^{(s)} : 1 \le i \le n, 1 \le j \le n-1).$$

Since for $1 \le j \le n-1$ we have

$$x_j g_1^{(s)} = x_j g_1 = x_j x_1^2,$$
$$x_j g_2^{(s)} = x_j g_2 = x_j x_1 x_2,$$
$$x_j g_3^{(s)} = x_j g_3 = x_j x_2^2,$$
$$x_j g_4^{(s)} = x_j g_4 = x_j x_2 x_3,$$
$$x_j g_i^{(s)} = x_j g_i = x_j x_{i-2}^2 \text{ for } 5 \le i \le n-1,$$
$$x_j g_n^{(s)} = x_j(x_{n-2}^2 + x_{n-1}^2), x_j g_n = x_j(x_{n-2}^2 + x_{n-1}^2 + x_n^2)$$

and the leading monomial $x_{n-1}x_{n-2}^2$ of $x_{n-1}g_n$ is the minimal leading monomial of $\mathrm{Span}_{\mathbb{K}}(x_j g_i : 1 \le i \le n, 1 \le j \le n-1)$ w.r.t. the grevlex order. It follows that for any $g \in \mathrm{Span}_{\mathbb{K}}(x_j g_i : 1 \le i \le n, 1 \le j \le n-1)$, $x_n \nmid \mathrm{LM}(g)$, and so $x_n \nmid g$ by Lemma 2. Similarly, the leading monomial x_{n-2}^3 of $x_{n-2}g_n$ is the minimal leading monomial of $\mathrm{Span}_{\mathbb{K}}(x_j g_i : 1 \le i \le n, 1 \le j \le n-2)$, and so $x_{n-1} \nmid g^{(s)}$ for any $g^{(s)} \in \mathrm{Span}_{\mathbb{K}}(x_j g_i^{(s)} : 1 \le i \le n, 1 \le j \le n-2)$. It is obvious that $\dim(\mathrm{Span}_{\mathbb{K}}(x_n g_i : 1 \le i \le n)) = n$ and $\dim(\mathrm{Span}_{\mathbb{K}}(x_{n-1} g_i^{(s)} : 1 \le i \le n)) = n$. Then it follows immediately that $t = r - n + 1$ and $t_s = r_s - n + 1$. □

Now we given the main result of this subsection, which is stated formally in Theorem 5 below.

Theorem 5. *Let n, u and $U_{u,n,n,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$ be as in Subsection IV-D, and let δ, d, r, t and $\hat{g}_j$ be as in Theorem 2. Given $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g} \in U_{u,n,n,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$,* **PartComPoly** *generically returns a normal form decomposition $(\boldsymbol{f}, \boldsymbol{g})$ of $\boldsymbol{h}$ in the case where $n \ge 6, d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ and $\gcd(q, 2) = 1$. Furthermore, the normal form decomposition of $\boldsymbol{h}$ is generically unique.*

Proof. Let s be the index selected in **PartComPoly**. We first prove that the set of coefficients (serving as formal parameters) of $\boldsymbol{f}$ and $\boldsymbol{g}$ satisfying both

$$\mathrm{Span}_{\mathbb{K}}(\hat{g}_j/x_n^{\delta+d} : t \le j \le r) = \mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n) \tag{10}$$

and

$$\mathrm{Span}_{\mathbb{K}}(\hat{g}_j{}^{(s)}/x_s^{\delta_s+d} : t_s \le j \le r_s) = \mathrm{Span}_{\mathbb{K}}(g_1^{(s)}, g_2^{(s)}, \ldots, g_n^{(s)}) \tag{11}$$

is Zariski-open. Indeed, by Lemma 9 (see Appendix A), the sets of coefficients of $\boldsymbol{f}$ and $\boldsymbol{g}$ for which (10) fails and for which (11) fails are each Zariski-closed. Since a finite union of Zariski-closed sets remains Zariski-closed, the set of coefficients violating (10) or (11) is also Zariski-closed. Its complement — the set of coefficients satisfying both (10) and (11) — is therefore Zariski-open. Furthermore, by Lemma 8, this open set is non-empty when $n \ge 6, d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ and $\gcd(q, 2) = 1$. Consequently, the simultaneous holding of (10) and (11) is a generic property.

On the one hand, by Theorem 3, $(\boldsymbol{f}, \boldsymbol{g})$ is the unique normal form decomposition of $\boldsymbol{h}$. On the other hand, during the execution of **PartComPoly**, the subroutine **RREFComPoly** returns a unique normal form decomposition of $\boldsymbol{h}^{(s)} = (h_1^{(s)}, h_2^{(s)}, \ldots, h_u^{(s)})$. It is obvious that $(\boldsymbol{f}, \boldsymbol{g}^{(s)})$ is a normal form decomposition of $\boldsymbol{h}^{(s)}$. Since the normal form decomposition of $\boldsymbol{h}^{(s)}$ is unique, the output of the subroutine **RREFComPoly** must coincide with the pair $(\boldsymbol{f}, \boldsymbol{g}^{(s)})$. Once $(\boldsymbol{f}, \boldsymbol{g}^{(s)})$ is obtained, it follows from the argument in Subsection V-B, the complete vector $\boldsymbol{g}$ can be uniquely recovered from $\boldsymbol{f}$ and $\boldsymbol{g}^{(s)}$ by solving overdetermined linear systems, provided that $\binom{s+d_{\boldsymbol{h}}-2}{d_{\boldsymbol{h}}-1} / \binom{s+d_{\boldsymbol{g}}-2}{d_{\boldsymbol{g}}-1} \ge n/u$. Therefore, in the case where $n \ge 6, d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ and $\gcd(q, 2) = 1$, **PartComPoly** generically returns the unique decomposition $(\boldsymbol{f}, \boldsymbol{g})$ of $\boldsymbol{h}$. □

Remark 4. *Although Theorem 5 is established in the case where $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ and $\gcd(q, 2) = 1$, it is expected to extend to the cases where $(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}) = (2, 3)$ and $(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}) = (2, 4)$. A direct proof for this extension is not straightforward: constructing an explicit instance to verify the non-emptiness of the Zariski-open set is less intuitive than in the case where $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ with $\gcd(q, 2) = 1$, and the value of δ varies with n, which complicates the construction. Nevertheless, we have conducted extensive experiments by generating numerous random instances of $\boldsymbol{FDP}_H(\boldsymbol{h}, 2, 3)$ and $\boldsymbol{FDP}_H(\boldsymbol{h}, 2, 4)$. In all experiments, the algorithm returned a unique normal form decomposition of $\boldsymbol{h}$ (see Subsection VI-B). This consistent empirical evidence suggests that the theorem should remain valid for $(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}) = (2, 3)$ and $(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}) = (2, 4)$.*

VI. Experimental Results

The computational environment used in our experiments is detailed in Table II. The source code is available at https://pastebin.com/qcC9YCFr.

Table II: Specifications of the computational environment utilized in our experiments

Resource	Specifications
Operating System	Windows 10
CPU	Intel(R) Xeon(R) W-2255 CPU @ 3.70GHz 3696 MHz
GPU	NVIDIA Quadro RTX 4000
RAM	160GB

Our experiments were performed using SageMath 9.2, where the RREF of a matrix was computed through the built-in ".echelon_form()" function.

A. Attack the $2\mathrm{R}$ and $2\mathrm{R}^-$ schemes

Table III compares the actual computational time of three algorithms—**MultiComPoly**, **RREFComPoly**, and **PartComPoly**—when $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$ and the prime modulus q is fixed at 65521.

Table III: Performance comparison of **MultiComPoly**, **RREFComPoly**, and **PartComPoly** algorithms, where
- n: the number of variables;
- u: the number of polynomial components of $\boldsymbol{h}$;
- δ_{old}: the smallest δ satisfying $|\tilde{F}_\delta| \geq |F_\delta|$;
- δ_{Multi}: the smallest δ for which **MultiComPoly** returns a solution;
- δ_{new}: the value of δ return by $\boldsymbol{\delta}$**-Estimate**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, n)$;
- δ_{RREF}: the smallest δ for which **RREFComPoly** returns a solution;
- s: the value assigned to s in **PartComPoly**;
- δ_{Part}: the value assigned to δ in **PartComPoly**;
- T_{Multi}: the actual running time (in seconds) of **MultiComPoly**;
- T_{RREF}: the actual running time (in seconds) of **RREFComPoly**;
- T_{Part}: the actual running time (in seconds) of **PartComPoly**.

n	u	δ_{old}	δ_{Multi}	δ_{new}	δ_{RREF}	s	δ_{Part}	T_{Multi}*	T_{RREF}	T_{Part}
8	8	0	0	0	0	7	0	0.0	0.0	0.0
8	4	2	1	1	1	8	1	0.0	0.4	0.4
8	3	2	2	2	2	8	2	0.3	0.7	0.7
8	2	6	3	3	3	8	3	1.9	2.6	2.6
10	5	2	1	1	1	9	1	0.2	1.3	0.9
10	4	2	2	2	2	9	2	3.2	3.5	1.6
10	3	4	3	3	3	10	3	21.4	29.3	29.3
10	2	8	4	4	4	10	3	180.8	191.8	191.8
12	12	0	0	0	0	9	0	0.1	0.2	0.2
12	7	1	1	1	1	10	1	0.9	1.5	1.7
12	6	2	1	1	1	10	1	0.9	2.1	1.5
12	5	2	2	2	2	11	2	20.5	16.7	10.8
12	4	3	2	2	2	11	2	25.2	13.1	8.8
12	3	5	3	3	3	11	3	414	188.9	83.5
20	20	0	0	0	0	10	0	1.6	4.2	4.6
20	15	1	1	1	1	13	1	55.2	45.3	10.4
20	10	2	1	1	1	13	1	78.6	55.6	8.9
24	24	0	0	0	0	13	0	4.9	8.3	9.6
24	12	2	1	1	1	14	1	376.1	226.0	19.3
30	15	2	1	1	1	14	1	2910.5	1516.9	61.7
32	32	0	0	0	0	14	0	31.3	24.5	25.6
32	22	1	1	1	1	17	1	3287.9	2002.1	106.4
32	16	2	1	1	1	17	1	4667.9	3143.2	97.5
36	21	1	1	1	1	18	1	13427.4	4997.0	181.7
36	18	1	/	1	1	18	1	/	10997.0	178.3
40	40	0	/	0	0	16	0	/	435.6	325.6
40	20	2	/	1	1	19	1	/	14482.3	427.0
50	50	0	/	0	0	18	0	/	874.0	663.7
50	25	1	/	1	1	21	1	/	16492.1	1762.2
60	60	0	/	0	0	19	0	/	1160.7	946.6
60	30	1	/	1	1	24	1	/	23722.1	6413.8
64	64	0	/	0	0	20	0	/	2213.8	1899.3

* Since SageMath does not include an implementation of the F_5 algorithm, and its built-in F_4 algorithm takes significantly longer time to solve these instances compared to the times reported in [21], we adopt the solving times from [21] as T_{Multi}.

The comparative analysis of δ_{old}, δ_{Multi}, δ_{new} and δ_{RREF} in Table III reveals that when $\delta_{old} \geq d_{\boldsymbol{g}} - d = 1$, δ_{old} frequently exceeds δ_{Multi}, δ_{new} and δ_{RREF}. Representative examples include:

- For $n = 8$, $u = 2$: $\delta_{old} = 6$ (vs. $\delta_{Multi} = \delta_{new} = \delta_{RREF} = 3$)
- For $n = 10$, $u = 3$: $\delta_{old} = 4$ (vs. $\delta_{Multi} = \delta_{new} = \delta_{RREF} = 3$)
- For $n = 10$, $u = 2$: $\delta_{old} = 8$ (vs. $\delta_{Multi} = \delta_{new} = \delta_{RREF} = 4$)

- For $n = 12$, $u = 3$: $\delta_{old} = 5$ (vs. $\delta_{Multi} = \delta_{new} = \delta_{RREF} = 3$)

In particular, the equality $\delta_{Multi} = \delta_{new} = \delta_{RREF}$ holds in all test cases, experimentally confirming the accuracy of the estimation of δ in **RREFComPoly** for the case $d_{\boldsymbol{f}} = d_{\boldsymbol{g}} = 2$. When $n = u$ or when n is relatively small (e.g., $n = 8$ or 10), the performance of **MultiComPoly**, **RREFComPoly**, and **PartComPoly** shows no significant differences. However, a comparison of T_{Multi}, T_{RREF}, and T_{Part} indicates that as n increases and u decreases, T_{Part} becomes markedly smaller than both T_{RREF} and T_{Multi}, demonstrating the clear advantage of **PartComPoly** for instances where $u < n$. Furthermore, as will be shown later, when $d_{\boldsymbol{g}} > 2$, **PartComPoly** significantly outperforms both **MultiComPoly** and **RREFCompoly**.

B. Attack Zhao-Feng schemes

Table IV compares the actual computational time between **RREFComPoly** and **PartComPoly** for the cases where $d_{\boldsymbol{f}} = 2$ and $d_{\boldsymbol{g}} \in \{3, 4\}$.

Table IV: Comparative analysis of computational complexity and execution time, where
- n: the number of variables;
- $d_{\boldsymbol{g}}$: the degree of homogeneous polynomials in $\boldsymbol{g}$;
- q: the prime modulus;
- u: the number of polynomial components of $\boldsymbol{h}$;
- δ_{RREF}: the value of δ return by $\boldsymbol{\delta}$**-Estimate**$(d_{\boldsymbol{f}}, d_{\boldsymbol{g}}, n, u, n)$;
- δ_{Part}: the value assigned to δ in **PartComPoly**;
- s: the value assigned to s in **PartComPoly**;
- R_{RREF}/C_{RREF}: the number of rows/columns of the matrix C in **RREFComPoly**;
- R_{Part}/C_{Part}: the number of rows/columns of the matrix C in **PartComPoly**;
- O_{RREF}: the bit-level complexity estimate of **RREFComPoly**, i.e., its arithmetic complexity multiplied by $\log_2(q)$;
- O_{Part}: the bit-level complexity estimate of **PartComPoly**, i.e., its arithmetic complexity multiplied by $\log_2(q)$;
- T_{RREF}: the actual running time (in seconds) of **RREFComPoly**;
- T_{Part}: the actual running time (in seconds) of **PartComPoly**.

n	$d_{\boldsymbol{g}}$	q	u	δ_{RREF}	s	δ_{Part}	R_{RREF}/C_{RREF}	R_{Part}/C_{Part}	O_{RREF}	O_{Part}	T_{RREF}	T_{Part}
8	3	65521	8	3	7	2	$2^{12.9}/2^{12.7}$	$2^{10.6}/2^{10.7}$	$2^{38.8}$	$2^{32.6}$	59.5	4.1
8	3	65521	6	3	7	3	$2^{12.5}/2^{12.7}$	$2^{11.8}/2^{11.6}$	$2^{38.0}$	$2^{35.6}$	44.2	11.2
10	3	65521	10	3	8	3	$2^{14.4}/2^{14.6}$	$2^{13.2}/2^{12.7}$	$2^{43.6}$	$2^{39.4}$	1057.7	80.2
10	3	65521	8	3	8	3	$2^{14.1}/2^{14.6}$	$2^{12.9}/2^{12.7}$	$2^{43.0}$	$2^{38.8}$	802.0	62.1
11	3	65521	11	3	9	3	$2^{15.1}/2^{15.4}$	$2^{14.0}/2^{13.7}$	$2^{45.7}$	$2^{41.8}$	4005.1	324.8
11	3	65521	6	5	9	4	$2^{17.6}/2^{17.5}$	$2^{14.7}/2^{14.6}$	$2^{52.5}$	$2^{44.1}$	234510.4*	1159.4
12	3	65521	12	3	9	3	$2^{15.7}/2^{16.2}$	$2^{14.1}/2^{13.7}$	$2^{47.5}$	$2^{42.1}$	14987.5	364.4
12	3	65521	10	4	9	3	$2^{17.3}/2^{17.4}$	$2^{13.9}/2^{13.7}$	$2^{51.9}$	$2^{41.6}$	182974.3*	323.7
8	4	65521	8	5	7	4	$2^{15.6}/2^{15.6}$	$2^{13.5}/2^{13.6}$	$2^{46.9}$	$2^{40.9}$	6541.7	233.7
10	4	65521	10	6	8	5	$2^{18.9}/2^{18.9}$	$2^{16.0}/2^{15.6}$	$2^{56.5}$	$2^{47.5}$	/	10120.9
10	4	65521	8	6	8	5	$2^{18.6}/2^{18.9}$	$2^{15.6}/2^{15.6}$	$2^{55.9}$	$2^{46.9}$	/	8340.5
14	3	2	14	4	10	3	$2^{18.8}/2^{18.9}$	$2^{14.9}/2^{14.6}$	$2^{52.4}$	$2^{40.5}$	61234.5*	94.8
14	3	2	12	4	10	3	$2^{18.6}/2^{18.9}$	$2^{14.7}/2^{14.6}$	$2^{52.5}$	$2^{40.6}$	66708.9*	80.5
16	3	2	16	4	11	3	$2^{19.9}/2^{20.3}$	$2^{15.6}/2^{15.4}$	$2^{55.8}$	$2^{42.7}$	/	261.4
18	3	2	18	4	12	3	$2^{20.9}/2^{21.6}$	$2^{16.3}/2^{16.2}$	$2^{59.0}$	$2^{44.7}$	/	811
18	3	2	16	4	12	3	$2^{20.7}/2^{21.6}$	$2^{16.1}/2^{16.2}$	$2^{59.2}$	$2^{44.4}$	/	721.2
20	3	2	20	4	12	3	$2^{21.8}/2^{22.7}$	$2^{16.4}/2^{16.2}$	$2^{61.8}$	$2^{45.0}$	/	816.3
24	3	2	24	4	13	3	$2^{25.8}/2^{26.5}$	$2^{17.1}/2^{16.9}$	$2^{73.3}$	$2^{47.1}$	/	2801.4
26	3	2	26	5	14	3	$2^{26.5}/2^{27.5}$	$2^{17.6}/2^{17.6}$	$2^{75.8}$	$2^{48.8}$	/	6248.3
28	3	2	28	5	14	3	$2^{27.2}/2^{28.4}$	$2^{17.7}/2^{17.6}$	$2^{78.1}$	$2^{49.0}$	/	6662.6
30	3	2	30	5	15	3	$2^{27.9}/2^{29.2}$	$2^{18.2}/2^{18.3}$	$2^{80.2}$	$2^{50.5}$	/	15459.5

20	3	2	16	5	13	4	$2^{23.7}/2^{24.3}$	$2^{18.5}/2^{18.2}$	$2^{67.1}$	$2^{51.0}$	/	19017.9
21	3	2	17	5	14	4	$2^{24.2}/2^{24.8}$	$2^{19.1}/2^{18.9}$	$2^{68.6}$	$2^{52.9}$	/	84103.3*
24	3	2	20	5	14	4	$2^{25.5}/2^{26.5}$	$2^{19.3}/2^{18.9}$	$2^{72.8}$	$2^{53.3}$	/	107703.6*
27	3	2	23	6	15	4	$2^{29.1}/2^{29.7}$	$2^{20.0}/2^{19.6}$	$2^{82.9}$	$2^{55.3}$	/	455423.3*
30	3	2	26	6	16	4	$2^{30.2}/2^{31.1}$	$2^{20.6}/2^{20.3}$	$2^{86.7}$	$2^{57.2}$	/	1553522.7*
11	4	2	11	6	9	5	$2^{19.9}/2^{20.1}$	$2^{17.0}/2^{16.9}$	$2^{55.6}$	$2^{46.8}$	/	1938.6
12	4	2	12	6	9	5	$2^{20.8}/2^{21.3}$	$2^{17.1}/2^{16.9}$	$2^{58.4}$	$2^{47.0}$	/	2211.4

* Execution times marked with an asterisk (*) were performed on a high-memory server (1.6 TB RAM, Windows 11 Operating System, Intel(R) Xeon(R) Gold 6342 CPU @ 2.80GHz CPU, NVIDIA A100-SXM4-80GB GPU) to meet their high memory requirements.

As shown in Table IV, the computational times recorded for T_{Part} are substantially shorter than those for T_{RREF} in all comparable rows. Moreover, as n increases or u decreases, **RREFComPoly** frequently encounters memory overflow and fails to complete, while **PartComPoly** maintains tractable demands on both memory and computational time. These empirical results strongly align with our theoretical complexity analysis in Subsection V-C, confirming the clear advantage of **PartComPoly** for instances when $d_{\boldsymbol{g}} \in \{3, 4\}$.

VII. Conclusions

The Functional Decomposition Problem (FDP) for multivariate polynomials is not only of mathematical interest, but also serves a foundation for the security of 2R and 2R$^-$ schemes. In this paper, we examine the evolution of algorithms designed to address FDP, beginning with the foundational algorithm $\mathrm{Algo}_{\mathrm{FDP}}$ of Faugère and Perret for quadratic polynomials and extending to their generalized work, **MultiComPoly**, which handles homogeneous polynomials of arbitrary degrees. Central to these approaches is the construction of ideals derived from partial or higher-order derivatives of composed polynomials $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g}$, followed by Gröbner basis computations to recover the right-factor spaces.

Our work introduces two key advancements to FDP. First, the **RREFComPoly** algorithm refines **MultiComPoly** by replacing Gröbner basis computations with Gauss-Jordan elimination (GJE) on the coefficient matrice associated with the polynomial set $\tilde{F}_\delta$, offering a clearer formulation of computing the right-factor space in **MultiComPoly**. Moreover, the **RREFComPoly** algorithm replaces the traditional approximation of binomials in the complexity analysis of MultiComPoly with exact binomials and refines the estimate for a crucial parameter δ, yielding a tighter complexity bound than that of **MultiComPoly**. The second and more significant contribution is the **PartComPoly** algorithm, which inverts the traditional two-stage FDP methodology. Instead of prioritizing recovery of the right-factor space, **PartComPoly** first localizes and recovers the left-factor polynomials $\boldsymbol{f}$ using **RREFComPoly**, then iteratively reconstructs the right-factor $\boldsymbol{g}$ through solving linear systems derived from $\boldsymbol{f}$ and local information of $\boldsymbol{g}$. This inversion drastically reduces computational complexity, particularly in high-degree regimes ($d_{\boldsymbol{g}} > 2$), where existing methods like **MultiComPoly** and **RREFComPoly** become prohibitively expensive. Most importantly, **PartComPoly** significantly expands the solvable domain of FDP, making previously intractable instances - such as those in [1] - computationally feasible for the first time. Our proposed **PartComPoly** algorithm demonstrates how local information can be leveraged to reduce the complexity of solving FDP. However, whether alternative approaches could achieve further complexity reduction remains an open problem worthy of future investigation.

Acknowledgments

We would like to thank the anonymous reviewers for their helpful suggestions and comments.

Appendix

A. A auxiliary lemma

Lemma 9. *Let n, u, s and $U_{u,n,s,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$ be defined in Subsection IV-D, and let δ, d, r, t and $\hat{g}_j$ be defined in Theorem 2. Given $\boldsymbol{h} = \boldsymbol{f} \circ \boldsymbol{g} \in U_{u,n,s,d_{\boldsymbol{f}},d_{\boldsymbol{g}}}$, the set of coefficients (serving as formal parameters) of $\boldsymbol{f}$ and $\boldsymbol{g}$ violating the property $\mathrm{Span}_{\mathbb{K}}(\hat{g}_j/x_n^{\delta+d} : t \le j \le r) = \mathrm{Span}_{\mathbb{K}}(g_1, g_2, \ldots, g_n)$ is Zariski-closed.*

Proof. Let

$$f_i = \sum_{1\le k_1\le k_2\le\cdots\le k_{d_{\boldsymbol{f}}}\le n} a^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}} x_{k_1}x_{k_2}\cdots x_{k_{d_{\boldsymbol{f}}}} \text{ for } 1\le i\le u, \tag{12}$$

$$g_j = \sum_{1\le l_1\le l_2\le\cdots\le l_{d_{\boldsymbol{g}}}\le s} b^{(j)}_{l_1,l_2,\ldots,l_{d_{\boldsymbol{g}}}} x_{l_1}x_{l_2}\cdots x_{l_{d_{\boldsymbol{g}}}} \text{ for } 1\le j\le n, \tag{13}$$

where the coefficients $a^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}}$ and $b^{(j)}_{l_1,l_2,\ldots,l_{d_{\boldsymbol{g}}}}$ are indeterminate serving as formal parameters (except for the prescribed leading coefficient 1). In Subsection IV-B, it is proved that

$$\mathrm{Span}_{\mathbb{K}}(g_1,g_2,\ldots,g_n) = \mathrm{Span}_{\mathbb{K}}(\hat{g}_j/x_s^{\delta+d} : t\le j\le r)$$

provided that

$$\dim(\tilde{V}_\delta) = \dim(V_\delta), \tag{14}$$

and

$$t = r-n+1. \tag{15}$$

Since a finite union of Zariski-closed sets remains Zariski-closed, it suffices to show that the sets where conditions (14) and (15) fail are Zariski-closed, respectively. **This is achieved by constructing two systems of polynomial equations as follows.**

- The first system will vanish if and only if $\dim(\tilde{V}_\delta)\neq\dim(V_\delta)$.
- When $\dim(\tilde{V}_\delta)=\dim(V_\delta)$, the second system will vanish if and only if $t\neq r-n+1$.

The construction of the first system. Let δ be the smallest integer satisfying $|\tilde{F}_\delta|\ge\dim(V_\delta)$, and let G_δ be a maximal linearly independent subset of F_δ. Recall that each $\boldsymbol{x}^{\boldsymbol{\alpha}}\frac{\partial^{(d_{\boldsymbol{f}}-1)}h_i}{\partial x_{j_1}\partial x_{j_2}\cdots\partial x_{j_{d_{\boldsymbol{f}}-1}}}$ can be linearly expressed by the elements in F_δ, then it can also be linearly expressed by the elements in G_δ. In other words, there is an $|\tilde{F}_\delta|\times\dim(V_\delta)$ matrix A_{G_δ} whose entries are polynomials of degree 1 in the variables $a^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}}$ and of degree $d_{\boldsymbol{f}}-1$ in the variables $b^{(j)}_{l_1,l_2,\ldots,l_{d_{\boldsymbol{g}}}}$ such that

$$\begin{bmatrix} \vdots \\ \vdots \\ \vdots \\ \boldsymbol{x}^{\boldsymbol{\alpha}}\frac{\partial^{(d_{\boldsymbol{f}}-1)}h_i}{\partial x_{j_1}\partial x_{j_2}\cdots\partial x_{j_{d_{\boldsymbol{f}}-1}}} \\ \vdots \\ \vdots \end{bmatrix} = A_{G_\delta}\cdot\begin{bmatrix} \vdots \\ \vdots \\ \vdots \\ \boldsymbol{x}^{\boldsymbol{\alpha'}}g_i \\ \vdots \\ \vdots \end{bmatrix},$$

where $\boldsymbol{x}^{\boldsymbol{\alpha'}}g_i\in G_\delta$. Since $\tilde{V}_\delta\subseteq V_\delta$, it is clear that $\dim(\tilde{V}_\delta)\neq\dim(V_\delta)$ if and only if $\dim(\tilde{V}_\delta)<\dim(V_\delta)$ if and only if every $\dim(V_\delta)\times\dim(V_\delta)$ minor of A_{G_δ} vanishes. Each such vanishing minor yields a polynomial equation of degree $\dim(V_\delta)$ in the variables $a^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}}$ and of degree $(d_{\boldsymbol{f}}-1)\cdot\dim(V_\delta)$ in the variables $b^{(j)}_{l_1,l_2,\ldots,l_{d_{\boldsymbol{g}}}}$. Then the collection of these polynomial equations constitutes a system whose solutions are the set of values of $a^{(i)}_{k_1,k_2,\ldots,k_{d_{\boldsymbol{f}}}}, b^{(j)}_{l_1,l_2,\ldots,l_{d_{\boldsymbol{g}}}}$ violating the conditions (14).

The construction of the second system. When $\dim(\tilde{V}_\delta)=\dim(V_\delta)$, as described in Subsection IV-A, if $t<r-n+1$, there exists a nonzero polynomial

$$\hat{g}\in V_\delta - \mathrm{Span}_{\mathbb{K}}(x_s^{\delta+d}g_1, x_s^{\delta+d}g_2,\ldots,x_s^{\delta+d}g_n) \tag{16}$$

such that $x_s^{\delta+d}\mid\hat{g}$. Under the assumption that $g_1,g_2,\ldots,g_n$ are linearly independent, $x_s^{\delta+d}g_1, x_s^{\delta+d}g_2,\ldots,x_s^{\delta+d}g_n$ are also linearly independent. We can therefore extend $x_s^{\delta+d}g_1, x_s^{\delta+d}g_2,\ldots,x_s^{\delta+d}g_n$ to a basis of V_δ, denoted by $\hat{G}'_\delta$. Let $\hat{G}_\delta = \hat{G}'_\delta - \{x_s^{\delta+d}g_1, x_s^{\delta+d}g_2,\ldots,x_s^{\delta+d}g_n\}$, and let $C_{\hat{G}_\delta}$ be the coefficient matrix associated with $\hat{G}_\delta$ w.r.t the grevlex order, whose elements are polynomials of degree 1 in the variables $b^{(i)}_{l_1,l_2,\ldots,l_{d_{\boldsymbol{g}}}}$. By (16), there exists a polynomial $\hat{g}'\in\mathrm{Span}_{\mathbb{K}}(x_s^{\delta+d}g_1, x_s^{\delta+d}g_2,\ldots,x_s^{\delta+d}g_n)$ such that $\hat{g}+\hat{g}'\in\mathrm{Span}_{\mathbb{K}}(\hat{G}_\delta)$ and $x_s^{\delta+d}\mid\hat{g}+\hat{g}'$, and so $\hat{g}+\hat{g}'$ can be expressed as

$$\hat{g}+\hat{g}' = \hat{a}_1x_1^{d_{\boldsymbol{g}}}x_s^{\delta+d} + \hat{a}_2x_1^{d_{\boldsymbol{g}}-1}x_2x_s^{\delta+d} + \cdots + \hat{a}_{|M_s(d_{\boldsymbol{g}})|}x_s^{\delta+d+d_{\boldsymbol{g}}}.$$

These facts imply the existence of a nonzero coefficient vector $(\hat{b}_1,\hat{b}_2,\ldots,\hat{b}_{|\hat{G}_\delta|})$ such that

$$(\hat{b}_1,\hat{b}_2,\ldots,\hat{b}_{|\hat{G}_\delta|})\cdot C_{\hat{G}_\delta} = (0,\cdots,0,\hat{a}_1,\hat{a}_2,\cdots,\hat{a}_{|M_s(d_{\boldsymbol{g}})|}).$$

Let $C'_{\hat{G}_\delta}$ be the submatrix of $C_{\hat{G}_\delta}$ consisting of its first $|M_s(\delta+d+d_{\boldsymbol{g}})| - |M_s(d_{\boldsymbol{g}})|$ columns. Then we have

$$(\hat{b}_1, \hat{b}_2, \ldots, \hat{b}_{|\hat{G}_\delta|}) \cdot C'_{\hat{G}_\delta} = (0, 0, \cdots, 0).$$

It follows that every $|\hat{G}_\delta| \times |\hat{G}_\delta|$ minor of $C'_{\hat{G}_\delta}$ vanishes. Conversely, it is obvious that if every $|\hat{G}_\delta| \times |\hat{G}_\delta|$ minor of $C'_{\hat{G}_\delta}$ vanishes, then there exists a polynomial $\hat{g} \in \mathrm{Span}_{\mathbb{K}}(\hat{G}_\delta)$ such that $x_s^{\delta+d} \mid \hat{g}$, which implies that $t < r - n + 1$. Each such vanishing minor yields a polynomial equation of degree $|\hat{G}_\delta|$ in the variables $b^{(i)}_{l_1,l_2,\ldots,l_{d_{\boldsymbol{g}}}}$. Then the collection of these polynomial equations constitutes a system whose solutions are the set of values of $b^{(j)}_{l_1,l_2,\ldots,l_{d_{\boldsymbol{g}}}}$ violating the conditions (15). □

REFERENCES

[1] X. F. Zhao and D. G. Feng, "Bypassing the decomposition attacks on two-round multivariate schemes by a practical cubic round," *IET Inf. Secur.*, vol. 4, no. 3, pp. 167–184, 2010.

[2] D. Kozen and S. Landau, "Polynomial decomposition algorithms," *J. Symbol. Comput.*, vol. 7, no. 5, pp. 445–456, 1989.

[3] J. von zur Gathen, "Functional decomposition of polynomials: The tame case," *J. Symbol. Comput.*, vol. 9, no. 3, pp. 281–299, 1990.

[4] J. von zur Gathen, "Functional decomposition of polynomials: The wild case," *J. Symbol. Comput.*, vol. 10, no. 5, pp. 437–452, 1990.

[5] J. von zur Gathen, J. Gutierrez, and R. Rubio, "Multivariate polynomial decomposition," *J. Applicable Algebra Eng. Commun. Comput.*, vol. 14, no. 1, pp. 11–31, 2003.

[6] S. M. Watt, "Functional decomposition of symbolic polynomials," in *Proc. Int. Conf. Comput. Sci. Appl.* IEEE, 2008, pp. 353–362.

[7] E.-W. Chionh, X. S. Gao, and L. Y. Shen, "Inherently improper surface parametric supports," *Computer Aided Geometric Design*, vol. 23, no. 8, pp. 629–639, 2006.

[8] G. Su *et al.*, "Polynomial decomposition algorithms in signal processing," Ph.D. dissertation, Massachusetts Institute of Technology, 2013.

[9] S. Demirtas, G. Su, and A. V. Oppenheim, "Exact and approximate polynomial decomposition methods for signal processing applications," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.* IEEE, 2013, p. 5373–5377.

[10] J. Patarin and L. Goubin, "Asymmetric cryptography with S-Boxes," in *Proc. Int. Conf. Inf. Commun. Secur.* Springer, 1997, pp. 369–380.

[11] L. Goubin and J. Patarin, "Asymmetric cryptography with S-Boxes–Extended Version," 1997. [Online]. Available: http://citeseer.ist.psu.edu/patarin97asymmetric.html.

[12] J. F. Ritt, "Prime and composite polynomials," *Trans. Amer. Math. Soc.*, vol. 23, no. 1, pp. 51–66, 1922.

[13] V. S. Alagar and M. Thanh, "Fast polynomial decomposition algorithms," in *Eur. Conf. Comput. Algebra, Lecture Notes in Computer Science*, vol. 204. Springer, 1985, pp. 150–153.

[14] F. Dorey and G. Whaples, "Prime and composite polynomials," *J. Algebra*, vol. 28, no. 1, pp. 88–101, 1974.

[15] D. R. Barton and R. Zippel, "Polynomial decomposition algorithms," *J. Symbol. Comput.*, vol. 1, no. 2, pp. 159–168, 1985.

[16] M. T. Dickerson, "The functional decomposition of polynomials," Ph.D. dissertation, TR89-1023, Dept. Comp. Sci., Cornell Univ., Ithaca, NY, USA, 1989.

[17] D. F. Ye, K. Y. Lam, and Z. D. Dai, "Cryptanalysis of 2R schemes," in *Advances in Cryptology—CRYPTO 1999, Lecture Notes in Computer Science*. Springer, 1999, pp. 315–325.

[18] D. F. Ye, Z. D. Dai, and K. Y. Lam, "Decomposing attacks on asymmetric cryptography based on mapping compositions," *J. Cryptol.*, vol. 14, no. 2, pp. 137–150, 2001.

[19] J.-C. Faugère, "A new efficient algorithm for computing Gröbner bases without reduction to zero: F_5," in *Proc. Int. Symp. Symbolic Algebraic Computation*. ACM, 2002, pp. 75–83.

[20] J.-C. Faugère and L. Perret, "Cryptanalysis of $2R^-$ schemes," in *Advances in Cryptology - CRYPTO 2006*. Springer, 2006, pp. 357–372.

[21] J.-C. Faugère and L. Perret, "An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography," *J. Symbol. Comput.*, vol. 44, no. 12, pp. 1676–1689, 2009.

[22] J.-C. Faugère and L. Perret, "High order derivatives and decomposition of multivariate polynomials," in *Proc. Int. Symp. Symbolic Algebraic Computation*. ACM, 2009, pp. 207–214.

[23] J.-C. Faugère, J. von zur Gathen, and L. Perret, "Decomposition of generic multivariate polynomials," in *Proc. Int. Symp. Symbolic Algebraic Computation*. ACM, 2010, pp. 131–137.

[24] S. W. Zhao, R. Y. Feng, and X. S. Gao, "On functional decomposition of multivariate polynomials with differentiation and homogenization," *J. Syst. Sci. Complex.*, vol. 25, no. 2, pp. 329–347, 2012.

[25] D. Cox, J. Little, D. O'shea, and M. Sweedler, *Ideals, varieties, and algorithms*. Springer, 1997.

[26] T. Becker, V. Weispfenning, and H. Kredel, *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer, 1993.

[27] B. Buchberger, G. E. Collins, R. Loos, and R. Albrecht, "Computer algebra symbolic and algebraic computation," *ACM SIGSAM Bull.*, vol. 16, no. 4, p. 5, 1982.

[28] G. Ars and J.-C. Faugère, "Algebraic immunities of functions over finite fields," Ph.D. dissertation, INRIA, 2005.

[29] R. A. Beezer, *A first course in linear algebra*. Independent, 2015.

[30] G. Strang, *Linear Algebra and Its Applications 4th ed.* Brooks cole, 2012.

[31] D. Andrén, L. Hellström, and K. Markström, "On the complexity of matrix reduction over finite fields," *Advances in Applied Mathematics*, vol. 39, no. 4, p. 428–452, 2007.

[32] V. Strassen, "Gaussian elimination is not optimal," *Numerische mathematik*, vol. 13, no. 4, pp. 354–356, 1969.