Revisit Unravelled Linearization with Erhart (quasi-)Polynomial

Yansong Feng[1,2], Yiming Gao[3], Honggang Hu[3], Abderrahmane Nitaj[4], Yanbin Pan[1,2], and Mengce Zheng[5]

[1] State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China
[2] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, China
{fengyansong,panyanbin}@amss.ac.cn
[3] School of Cyber Science and Technology, University of Science and Technology of China
qw1234567@mail.ustc.edu.cn, hghu2005@ustc.edu.cn
[4] Zhejiang Wanli University, Ningbo, China
mczheng@zwu.edu.cn
[5] LMNO, University of Caen Normandy, Caen, France
abderrahmane.nitaj@unicaen.fr

Abstract. We study lattice constructions arising from Coppersmith's method combined with the Unravelled Linearization technique introduced by Herrmann and May (ASIACRYPT 2009) for solving structured polynomial equations, which can yield improved asymptotic bounds. This work contributes in two aspects, theoretical and practical.

Theoretical contribution. While Unravelled Linearization, introduced can lead to improved asymptotic bounds, computing these bounds is technically delicate. Previous works typically assume that the lattice dimension is a polynomial function of the scaling parameter m and therefore rely on Lagrange interpolation to derive asymptotic bounds. We show that this assumption does not hold in general. In particular, the interpolation approach used in Herrmann and May (ASIACRYPT 2009) and in `cuso` (EUROCRYPT 2025) may yield incorrect results: in the former case, the exponant in the determinate may be a quasi-polynomial instead of polynomial, while in the latter it becomes polynomial only beyond a certain threshold. To address this issue, we present a rigorous analysis based on Ehrhart theory for computing asymptotic bounds. As applications, we improve five cryptanalytic results, including attacks on linear congruential generators, quadratic generators, the subset-sum pseudorandom generator, and a recent partial-key attack on isogenies in the Pòke setting. In the latter case, we reduce the required leakage of most significant bits from 85.29% to 79.81%, and further to 79.08% in certain special cases.

Practical contribution. Asymptotic bounds alone are insufficient for practical attacks, since one must also determine an appropriate lattice dimension. To avoid trivial guessing of the lattice dimension from small

to large, we introduce an estimator, DimOracle, based on Ehrhart theory. Our approach simultaneously estimates the lattice dimension and determinant via the associated Ehrhart (quasi-)polynomials. Due to Barvinok's algorithm, any fixed number of leading coefficients of these (quasi-)polynomial can be computed in polynomial time by reducing the problem to volume computations of faces of the Newton polytope. Using these coefficients, DimOracle provides accurate predictions of the required lattice size in practice. We implement DimOracle and demonstrate its effectiveness through experimental results.

Keywords: Additive combinatorics, Coppersmith's method, automated cryptanalysis, Ehrhart theory, lattice-based cryptanalysis

1 Introduction

Coppersmith's method is a central tool in lattice-based cryptanalysis. It was introduced for attacking RSA [11, 12] and has since been applied in many settings, including post-quantum problems such as the Commutative Isogeny Hidden Number Problem [16, 28, 29, 31], fixed-degree isogeny [1, 7], and level isogeny with hints [13]. Moreover, for equations with additional algebraic structure, Unravelled Linearization [18] provides several advantages, including improved asymptotic bounds [18], simpler lattice constructions [19], and lower lattice dimensions [19]. The main idea is to aggregate monomials with small coefficients into a new auxiliary variable and perform back-substitution at a later stage.

However, computing asymptotic bounds under Unravelled Linearization is substantially more delicate. The bounds depend on the lattice dimension and on the exponent structure of the determinant, both of which are functions of parameters such as the scaling parameter m. Some prior works assume that these quantities are polynomial in m and recover them via interpolation from small values of m [18, 29].

Recent work has used Ehrhart theory to describe lattice constructions without Unravelled Linearization. For instance, [16] and [29] apply Ehrhart polynomials to derive rigorous or heuristic bounds. More precisely, for the classical Jochemsz–May Basic strategy, the lattice dimension equals the number of integer points in a lattice polytope associated with the target polynomial, which is known to be a polynomial in m by Ehrhart's theorem [14]. In contrast, once Unravelled Linearization is introduced, the structure of the counting region changes and the analysis becomes more subtle.

The earliest work on Unravelled Linearization [18] also assumed that the relevant quantities are polynomial in m and recovered them by interpolation. Our analysis shows that in their setting the exponent of the determinant is in fact a quasi-polynomial in m, rather than a polynomial. The reason is that it equals the number of lattice points in a rational polytope, which is known to yield a quasi-polynomial counting function [10, 14, 32]. A simple example is the number of integers in the interval $[0, \lfloor m/2 \rfloor]$, which equals $m/2$ when m is even

and $(m-1)/2$ when m is odd. Therefore, interpolation must take the period of the quasi-polynomial into account. In [18], interpolation was performed at $m = 1, 2, 3, 4$, implicitly assuming period 1, which should be 2. Due to the geometry of the construction, the correct period depends on the denominators of the vertices, and m should be chosen accordingly (for example, as multiples of those denominators).

We also show that even in the simplest Unravelled Linearization setting, the lattice dimension does not behave polynomially in m until m exceeds a certain threshold. Thus, interpolation starting at $m = 1$ may lead to incorrect asymptotic bounds, as in heuristic approaches such as cuso.

We also consider other settings and analyze the corresponding asymptotic bounds. As applications, we improve the best-known asymptotic bounds in five representative scenarios; see Table 1. We further explain why the small private-exponent bound in [29] approaches $1 - \sqrt{2}/2$ but does not attain it exactly.

Table 1. Comparison of asymptotic bounds between previous works and DimOracle.

Setting	Previous Required Leakage	Our Result
LCG (a unknown, consecutive values)	80% ([34, Thm 2])	75%
LCG (a unknown, non-consecutive values)	83.33% ([34, Thm 4])	80%
Quadratic Generator (a, b unknown, consecutive values)	90.91% ([34, Thm 6])	90%
Subset-Sum PRG	73.68% ([9, Sec 5])	71.43%
LIPH (Unknown Degree)	85.29% ([13, Thm 4.3])	79.81% (79.08% for "small" r ⋆)

⋆ Given accessible torsion points $(P, Q) \in E[N]$ and $(P', Q') = \Gamma \cdot (\phi(P), \phi(Q))^\top$ for some $\Gamma \in \mathrm{GL}(N, 2)$, the Weil pairing yields a *known* value $r \equiv \deg(\phi) \det(\Gamma) \bmod N$, which is "small" in the sense that $r < N^{0.7712}$.

In practice, asymptotic bounds alone are insufficient: one must choose a concrete lattice dimension for a given instance. Based on our asymptotic analysis, we propose DimOracle, a dimension estimator that outputs the lattice dimension required in Coppersmith's method. To make the estimator efficient, we introduce algorithms for computing Ehrhart (quasi-)polynomials (or their leading coefficients) in the relevant parameter regimes. We implement DimOracle and experimentally demonstrate its efficiency and correctness. To our knowledge, it is the first dimension estimator that does not rely on heuristic assumptions about the dimension and determinant exponent.

Technique overview We briefly explain the core idea behind our dimension analysis in the simplest case, where all nonlinear monomials of f have relatively small coefficients and every variable x_j, for $1 \le j \le k$, appears in the support of f_{ul}. This overview emphasizes the role of inclusion–exclusion and the threshold condition $m \ge \deg(f)$.

Unravelled Linearization. Let $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$ be monic, and let $\mathrm{LM}(f)$ denote its leading monomial under a fixed monomial order. Formally, let

$\mathcal{I} \subseteq \mathbb{N}^k$ index the nonlinear monomials whose coefficients are small. We rewrite

$$f(x_1, \ldots, x_k) = \underbrace{\mathrm{LM}(f) + \sum_{(i_1,\ldots,i_k)\in\mathcal{I}} \alpha_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}}_{=:u} + \sum_{j=1}^{k} \alpha_j x_j$$
$$= u + \sum_{j=1}^{k} \alpha_j x_j =: f_{\mathrm{ul}}(u, x_1, \ldots, x_k).$$

All nonlinear terms are aggregated into the auxiliary variable u, so that f_{ul} is linear in $(u, x_1, \ldots, x_k)$.

Fix a scaling parameter $m \in \mathbb{N}$. The initial monomial set is

$$\mathcal{M}_{\mathrm{init}} = \{u^{i_0} x_1^{i_1} \cdots x_k^{i_k} : i_0 + \cdots + i_k \le m\},$$

which corresponds to the integer lattice points in the dilated simplex

$$mN_{f_{\mathrm{ul}}} = \{(i_0, \ldots, i_k) \in \mathbb{R}_{\ge 0}^{k+1} : i_0 + \cdots + i_k \le m\}.$$

Here $N_{f_{\mathrm{ul}}}$ denotes the Newton polytope of f_{ul}, and $E_{N_{f_{\mathrm{ul}}}}(m)$ denotes its Ehrhart polynomial, i.e., the number of integer points in $mN_{f_{\mathrm{ul}}}$.

For each monomial $\lambda = u^{i_0} x_1^{i_1} \cdots x_k^{i_k}$, we construct

$$g_\lambda = \frac{\lambda}{u^{i_0}} f_{\mathrm{ul}}^{i_0} M^{m-i_0},$$

and then perform back-substitution by replacing each occurrence of $\mathrm{LM}(f)$ with

$$u - \sum_{(i_1,\ldots,i_k)\in\mathcal{I}} \alpha_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}.$$

The lattice dimension $\dim(\mathcal{L})$ equals the number of distinct monomials that remain after this back-substitution step.

Step 1: Initial monomial count.

Ignoring back-substitution, we have

$$\#\mathcal{M}_{\mathrm{init}} = E_{N_{f_{\mathrm{ul}}}}(m),$$

which is a polynomial in m of degree $k+1$.

Step 2: Effect of back-substitution.

Write

$$\mathrm{LM}(f) = \prod_{j\in\mathcal{J}_0} x_j^{\alpha_j},$$

and define

$$\mathcal{J}_0 = \{j : x_j \text{ divides } \mathrm{LM}(f)\}.$$

Back-substitution eliminates all monomials divided $\mathrm{LM}(f)$, i.e, all exponent vectors satisfying

$$i_j \geq \alpha_j \quad \text{for all } j \in \mathcal{J}_0.$$

Therefore,

$$\dim(\mathcal{L}) = \#\mathcal{M}_{\text{init}} - \#\{\mu \in \mathcal{M}_{\text{init}} : \mathrm{LM}(f) \text{ divides } \mu\}.$$

Step 3: Inclusion–exclusion.

For $j \in \mathcal{J}_0$, let

$$P_j^c = \{(i_0, \ldots, i_k) \in mN_{f_{\text{ul}}} \cap \mathbb{Z}^{k+1} : i_j \geq \alpha_j\},$$

and for any nonempty $\mathcal{J} \subseteq \mathcal{J}_0$, define

$$P_{\mathcal{J}} = \{(i_0, \ldots, i_k) \in mN_{f_{\text{ul}}} \cap \mathbb{Z}^{k+1} : i_j < \alpha_j \ \forall j \in \mathcal{J}\}.$$

Thus, we have

$$\{\mu \in \mathcal{M}_{\text{init}} : \mathrm{LM}(f) \text{ divides } \mu\} = \bigcap_{j \in \mathcal{J}_0} P_j^c.$$

Applying inclusion–exclusion yields

$$\dim(\mathcal{L}) = \sum_{\emptyset \neq \mathcal{J} \subseteq \mathcal{J}_0} (-1)^{\#\mathcal{J}+1} \#P_{\mathcal{J}}.$$

For any nonempty $\mathcal{J} \subseteq \mathcal{J}_0$, the quantity $\#P_{\mathcal{J}}$ becomes polynomial in m once $m \geq \deg(f)$. Indeed, recall that

$$mN_{f_{\text{ul}}} = \{(i_0, \ldots, i_k) \in \mathbb{R}_{\geq 0}^{k+1} : i_0 + \cdots + i_k \leq m\}.$$

Fix $\mathcal{J}$ with $\#\mathcal{J} = r$. For each choice of exponents $i_j = \ell_j$ with $0 \leq \ell_j < \alpha_j$ for $j \in \mathcal{J}$, the remaining coordinates satisfy

$$\sum_{j \notin \mathcal{J}} i_j \leq m - \sum_{j \in \mathcal{J}} \ell_j.$$

Thus the remaining variables range over the lattice points in a dilation of the standard simplex of dimension $k+1-r$. When $m \geq \deg(f)$, the shift by $\sum_{j \in \mathcal{J}} \ell_j$ does not affect the leading behavior, and $\#P_{\mathcal{J}}$ is a polynomial in m of degree $k+1-r$ (see Lemma 14).

Consequently, once $m \geq \deg(f)$, each $\#P_{\mathcal{J}}$ stabilizes to an Ehrhart polynomial. Therefore, $\dim(\mathcal{L})$ itself becomes a polynomial in m of degree k, and its leading coefficient equals $\deg(f)/k!$ (see Theorem 1).

Using the same inclusion–exclusion framework, we can analyze the determinant exponent in an analogous way. This yields the following asymptotic bound (Corollary 1):

Suppose $f \in \mathbb{Z}[x_1, \ldots, x_k]$ and, after aggregation, the resulting polynomial f_{ul} has degree 1. Then all roots $(x_1, \ldots, x_k)$ of f satisfying $x_j < X$ can be found in polynomial time if

$$X < M^{\frac{1}{\deg(f)+k-1}}.$$

More detailed analysis of this setting is provided in Section 4.2. We further investigate more general cases of Unravelled Linearization in Section 4.

Roadmap Section 2 provides the background on Coppersmith's method and Ehrhart theory. Section 3 reformulates the Jochemsz–May Strategy in the Ehrhart framework and explains how to compute the lattice dimension and determinant via Ehrhart (quasi-)polynomials. Section 4 develops a geometric perspective on Unravelled Linearization and presents our analysis of asymptotic bounds together with applications. Section 5 introduces DimOracle. Section 6 concludes the paper.

2 Preliminaries

We use $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ to denote the set of non-negative integers, the ring of integers, the field of rational numbers, and the field of real numbers, respectively. We use little-o notation $o(\cdot)$ and big-O notation $O(\cdot)$ to denote asymptotic upper bounds for functions. For a vector $\mathbf{u} = (u_1, \ldots, u_k)$, we denote its Euclidean norm by $\|\mathbf{u}\|_2 = \left(\sum_{i=1}^{k} u_i^2\right)^{1/2}$ and its infinity norm by $\|\mathbf{u}\|_\infty = \max_i |u_i|$. We write

$$\mathbf{e}_j^{(k)} = \underbrace{(0, \ldots, 1, \ldots, 0)}_{\text{the } j\text{-th position is } 1} \in \mathbb{Z}^k$$

for the j-th unit vector in $\mathbb{Z}^k$, and

$$\mathbf{0}^{(k)} = \underbrace{(0, \ldots, 0)}_{\text{all entries are } 0} \in \mathbb{Z}^k$$

for the origin vector. The cardinality of a set S is denoted by $\#S$.

2.1 Polynomials

Let $x_1, \ldots, x_k$ be k variables. Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ be a polynomial. Then f can be written as

$$f(x_1, \ldots, x_k) = \sum_{i_1, \ldots, i_k \in \mathbb{N}} \alpha_{i_1, \ldots, i_k} x_1^{i_1} \cdots x_k^{i_k}.$$

A monomial $x_1^{i_1} \cdots x_k^{i_k}$ is said to appear in f if its coefficient $\alpha_{i_1, \ldots, i_k} \neq 0$. The set of all monomials of f is denoted by $\mathrm{supp}(f)$. The total degree of f is defined as

$$\deg(f) := \max_{\alpha_{i_1, \ldots, i_k} \neq 0} (i_1 + \cdots + i_k).$$

The following definitions fix notation for multivariate polynomials.

Definition 1 (Monomial order). Let $\mathcal{M}$ be the set of all monomials in a polynomial ring. A monomial order on $\mathcal{M}$ is a total order $\prec$ satisfying:

1. $1 \prec \lambda$ for every $\lambda \in \mathcal{M} \setminus \{1\}$.
2. If $\lambda_1 \prec \lambda_2$, then $\lambda\lambda_1 \prec \lambda\lambda_2$ for every $\lambda \in \mathcal{M}$.

Throughout this work, we consider two polynomial rings. The first is $\mathbb{Z}[x_1, \ldots, x_k]$, equipped with the degree-lexicographic order (deglex). The second is $\mathbb{Z}[u, x_1, \ldots, x_k]$, equipped with the lexicographic order (lex) satisfying

$$u \succ x_1 \succ \cdots \succ x_k.$$

For example, in $\mathbb{Z}[x_1, x_2]$ with deglex order, we have

$$x_1^2 \succ x_1 x_2 \succ x_2^2 \succ x_1 \succ x_2 \succ 1,$$

while in $\mathbb{Z}[u, x_1]$ with lex order,

$$u^2 \succ u x_1 \succ x_1^3 \succ x_1^2 \succ x_1 \succ 1.$$

If $\prec$ is a monomial order, the leading monomial of a polynomial f is the unique monomial λ of f such that $\lambda' \prec \lambda$ for every other monomial λ' of f. We denote the leading monomial and leading coefficient of f by $\mathrm{LM}(f)$ and $\mathrm{LC}(f)$, respectively. The leading term of f is

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

If $\mathrm{LC}(f) = 1$, we say that f is monic.

For a polynomial f, define

$$A_f := \{(i_1, \ldots, i_k) : x_1^{i_1} \cdots x_k^{i_k} \text{ is a monomial of } f\}$$

to represent the support of f as lattice points. We write $\mathrm{conv}(\cdot)$ for the convex hull. For a finite set $A \subset \mathbb{Z}^k$, $\mathrm{conv}(A)$ denotes its convex hull.

Definition 2 (Newton polytope). Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$. The Newton polytope of f is

$$N_f := \mathrm{conv}(A_f).$$

For $A, B \subset \mathbb{R}^k$, their Minkowski sum is

$$A + B := \{a + b : a \in A,\ b \in B\}.$$

For $A \subset \mathbb{R}^k$ and $m \in \mathbb{N}$, define

$$mA := \underbrace{A + \cdots + A}_{m \text{ times}}.$$

The Newton polytope satisfies the following property.

Lemma 1. *For all $f_1, f_2 \in \mathbb{Z}[x_1, \ldots, x_k]$,*

$$N_{f_1 f_2} = N_{f_1} + N_{f_2}.$$

2.2 Lattices

A lattice is a discrete additive subgroup of $\mathbb{R}^m$ for some $m \in \mathbb{N}$.

Definition 3 (Lattice). Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^m$ be linearly independent with $n \leq m$. The lattice spanned by them is

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} a_i \mathbf{v}_i : a_i \in \mathbb{Z} \right\}.$$

The integer n is the rank of $\mathcal{L}$ and m its dimension. We say $\mathcal{L}$ is full-rank if $n = m$.

A lattice can be represented by a basis matrix $\mathbf{B} \in \mathbb{R}^{n \times m}$ whose rows are the basis vectors. Its determinant is

$$\det(\mathcal{L}) = \sqrt{\det(\mathbf{B}\mathbf{B}^t)}.$$

If $\mathcal{L}$ is full-rank, then $\det(\mathcal{L}) = |\det(\mathbf{B})|$.

Definition 4 (Shortest Vector Problem (SVP)). Given a lattice $\mathcal{L}$, the SVP asks for a nonzero $\mathbf{v} \in \mathcal{L}$ minimizing $\|\mathbf{v}\|_2$.

The SVP is NP-hard under randomized reductions [2]. The LLL algorithm [23] computes in polynomial time a relatively short vector.

Lemma 2 (LLL basis reduction). *Let $\mathcal{L} \subseteq \mathbb{Z}^n$ be a lattice. The LLL algorithm computes in polynomial time a basis $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ such that*

$$\|\mathbf{v}_i\|_2 \leq 2^{\frac{n(n-1)}{4(n+1-i)}} \det(\mathcal{L})^{1/(n+1-i)}$$

for all $i = 1, \ldots, n$.

2.3 Ehrhart theory

Ehrhart theory studies the relationship between convex polytopes and the number of lattice points in their dilates. Let $N \subset \mathbb{R}^k$ be a lattice polytope of affine rank d. Its Ehrhart function is

$$E_N(m) = \#(mN \cap \mathbb{Z}^k),$$

for $m \in \mathbb{N}$. For a polynomial function ϕ, define the weighted counting function

$$E_N(m, \phi) = \sum_{\mathbf{x} \in mN \cap \mathbb{Z}^k} \phi(\mathbf{x}).$$

Then $E_N(m) = E_N(m, 1)$.

If N is integral, then $E_N(m)$ is a polynomial of degree d. If N is rational, then $E_N(m)$ is a quasi-polynomial. See, e.g., [10, 14, 32].

Definition 5. Let $N \subseteq \mathbb{R}^k$ be an integral convex polytope with affine hull $\mathrm{aff}(N)$. The relative volume $\mathrm{Vol}(N)$ is the Euclidean volume measured with respect to the lattice $\mathbb{Z}^k \cap \mathrm{aff}(N)$.

Lemma 3 ([33, Cor. 4.6.11 and Prop. 4.6.13]). *Let $N \subseteq \mathbb{R}^k$ be an integral convex polytope of affine rank d. Then $E_N(m)$ is a polynomial of degree d whose leading coefficient equals* $\mathrm{Vol}(N)$.

Lemma 4. *If $N \subseteq \mathbb{R}^k$ is full-rank and integral, then $E_N(m)$ has degree k and leading coefficient equal to the Euclidean volume of N.*

Lemma 5 ([10, Prop. 4.1]). *Let $N \subseteq \mathbb{R}^k$ be a full-rank integral convex polytope and ϕ a homogeneous polynomial. Then $E_N(m, \phi)$ is a polynomial of degree $k + \deg(\phi)$ whose leading coefficient equals $\int_N \phi$.*

Lemma 6 ([6, Thm. 3.23]). *Let $N \subseteq \mathbb{R}^k$ be a rational convex polytope of affine rank d. Then $E_N(m)$ is a quasi-polynomial of degree d.*

The sum of a homogeneous polynomial function ϕ over a rational polytope N satisfies a similar property, as stated in the introduction of [3].

Lemma 7. *Let $N \subseteq \mathbb{R}^k$ be a rational convex polytope of affine rank d. Then $E_N(m, \phi)$ is a quasi-polynomial of degree $d + \deg(\phi)$.*

We will use Lemma 5 in the case of multiple polytopes, which can be directly obtained from the Ehrhart theorem, as proposed by Brion and Vergne [10].

Lemma 8. *Suppose $N_1, \ldots, N_n$ are integer convex polytopes with vertices in $\mathbb{Z}^k$ and ϕ be any homogeneous polynomial function, then the following counting function:*

$$\sum_{\delta \in (\sum_{i=1}^{n} m_i N_i) \cap \mathbb{Z}^k} \phi(\delta)$$

is a polynomial of $m_1, \ldots, m_n$.

2.4 Coppersmith's method and the Jochemsz–May strategy

Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ have a small root $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{Z}^k$ modulo M, meaning $|u_i| < X_i$. Coppersmith's method constructs a lattice $\mathcal{L}$ from polynomials sharing the same root modulo M^m, e.g.,

$$g_{[i_1,\ldots,i_k]} = x_1^{i_1} \cdots x_k^{i_k} f^\ell M^{m-\ell}, \quad \ell = 0, \ldots, m.$$

Using LLL and the following lemma, we obtain polynomials vanishing at $\mathbf{u}$ over $\mathbb{Z}$.

Lemma 9 (Howgrave-Graham [20]). *Let $g \in \mathbb{Z}[x_1, \ldots, x_k]$ have at most ω monomials. If $g(\mathbf{u}) \equiv 0 \bmod M$ and $\|g(x_1 X_1, \ldots, x_k X_k)\| < M/\sqrt{\omega}$, then $g(\mathbf{u}) = 0$ over $\mathbb{Z}$.*

To obtain k polynomials vanishing at $\mathbf{u}$ over $\mathbb{Z}$, we require

$$2^{\frac{\dim(\mathcal{L})(\dim(\mathcal{L})-1)}{4(\dim(\mathcal{L})+1-i)}} \det(\mathcal{L})^{\frac{1}{\dim(\mathcal{L})+1-i}} \leq \frac{M^m}{\sqrt{\dim(\mathcal{L})}} \tag{1}$$

for $i = 1, \ldots, k$.

We usually assume the ideal generated by these k polynomials being zero-dimensional, allowing us to compute the small root $\mathbf{u}$ by Gröbner basis. The following Assumtion 1 is widely used in many works [17, 24–28].

Assumption 1. *The ideal generated by the polynomials obtained from Coppersmith's method is zero-dimensional.*

Regarding asymptotic bounds, we derive bounds on X_j from the behavior as $m \to \infty$. Specifically, we assume that m is large and absorb lower-order factors; in particular, we use the determinant condition $\det(\mathcal{L}) \leq M^{m \dim(\mathcal{L})}$. Writing

$$\det(\mathcal{L}) = X_1^{p_1} \cdots X_k^{p_k} M^{p_M},$$

The Jochemsz–May strategy. Jochemsz and May [21] proposed selecting shifts to minimize $\det(\mathcal{L})$. They define

$$J_\ell = \{\lambda \in \mathrm{supp}(f^m) : \lambda/\mathrm{LM}(f)^\ell \in \mathrm{supp}(f^{m-\ell})\}$$

and use

$$g_{[i_1,\ldots,i_k]} = \frac{x_1^{i_1} \cdots x_k^{i_k}}{\mathrm{LM}(f)^\ell} f^\ell M^{m-\ell}, \tag{2}$$

for $x_1^{i_1} \cdots x_k^{i_k} \in J_\ell \setminus J_{\ell+1}$.

Extra shifts in a variable x_{j_0} can be incorporated by replacing J_ℓ with

$$\bigcup_{0 \leq j \leq t} \{x_{j_0}^j \lambda : \lambda \in \mathrm{supp}(f^m),\ \lambda/\mathrm{LM}(f)^\ell \in \mathrm{supp}(f^{m-\ell})\}.$$

Recent works [28, 29] study automated selection of shift polynomials, including for systems of equations. While effective in practice, computing rigorous asymptotic bounds remains challenging, and current approaches rely on heuristics.

3 Coppersmith's Method with Ehrhart Theory

In this section, we introduce Ehrhart theory to approximate the dimension and determinant of the lattice arising in Coppersmith's method. In Section 3.1, we first recall an Ehrhart-theoretic strategy that was independently proposed in an early draft of Feng et al. [15] (October 2024) and in [29]. Since both the early draft of Feng et al. [15] and [29] consider only the case of a single polytope, as in Lemmas 4 and 5, we extend their approach to multiple polytopes in order to compute the dimension and determinant for the Extended strategy using Lemma 8. Finally, observing that the resulting lattice dimension and determinant can be interpreted as Ehrhart (quasi-)polynomials associated with the target polynomial equation, we apply algorithms for computing Ehrhart polynomials to approximate these quantities in Section 3.2, following Barvinok's approach [4].

3.1 The Jochemsz–May strategy with Ehrhart theory

For simplicity, we assume throughout this subsection that f is monic. Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ be a polynomial with a small root $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{Z}^k$ modulo an integer M, and let the leading monomial of f correspond to the exponent vector $\boldsymbol{\alpha}_f \in \mathbb{Z}^k$. Here, a small root means that $|u_j| < X_j$ for known bounds X_j, for $j = 1, \ldots, k$. We focus on selecting a basis for the lattice used in Coppersmith's method.

Basic Strategy. The Basic Strategy proceeds as follows.

Compute the dilated polytope mN_f for an integer m and define

$$S_\ell = \ell\boldsymbol{\alpha}_f + (m - \ell)N_f,$$

so that $S_m \subset \cdots \subset S_0$.

For each integer point $\mathbf{i} = (i_1, \ldots, i_k) \in mN_f \cap \mathbb{Z}^k$, determine the unique ℓ such that $\mathbf{i} \in S_\ell$ but $\mathbf{i} \notin S_{\ell+1}$. We then construct

$$g_{\mathbf{i}}(x_1, \ldots, x_k) = \frac{x_1^{i_1} \cdots x_k^{i_k}}{\mathrm{LM}(f)^\ell} f^\ell M^{m-\ell}.$$

The coefficient vectors of all polynomials $g_{[i_1,\ldots,i_k]}(x_1X_1, \ldots, x_kX_k)$ form a basis of the lattice.

To analyze the dimension and determinant of $\mathcal{L}$, we use Definition 6 proposed in [28].

Definition 6. Let $\mathcal{M}$ be a finite set of monomials and let $\prec$ be a monomial order on $\mathcal{M}$. A set of polynomials G is called $(\mathcal{M}, \prec)$-suitable if:

1. Every $g \in G$ is supported on $\mathcal{M}$.
2. For every $\lambda \in \mathcal{M}$, there exists a unique $g \in G$ whose leading monomial (with respect to $\prec$) is λ.

Suppose G is a set of polynomials such that every $g \in G$ shares the same small root as f. If G is $(\mathcal{M}, \prec)$-suitable, then the coefficient vectors of all $g(x_1X_1, \ldots, x_kX_k)$ for $g \in G$ form a basis of $\mathcal{L}$, and

$$\begin{aligned} \dim(\mathcal{L}) &= \#\mathcal{M}, \\ \det(\mathcal{L}) &= \prod_{g \in G} \mathrm{LM}(g(x_1X_1, \ldots, x_kX_k)). \end{aligned}$$

If we take

$$\mathcal{M} = \{x_1^{i_1} \cdots x_k^{i_k} : (i_1, \ldots, i_k) \in mN_f \cap \mathbb{Z}^k\},$$

then the set $\{g_{\mathbf{i}}\}$ is $(\mathcal{M}, \prec)$-suitable. Hence

$$\dim(\mathcal{L}) = \sum_{(i_1,\ldots,i_k) \in mN_f \cap \mathbb{Z}^k} 1 = E_{N_f}(m).$$

Write

$$\det(\mathcal{L}) = X_1^{p_1} \cdots X_k^{p_k} M^{p_M}.$$

Since f is monic,

$$\begin{aligned} p_j &= \sum_{(i_1,\ldots,i_k)\in mN_f \cap \mathbb{Z}^k} i_j, \quad j = 1,\ldots,k, \\ p_M &= \sum_{\mathbf{i}} (m - \ell_{\mathbf{i}}), \end{aligned}$$

where $\ell_{\mathbf{i}}$ is the index associated with $\mathbf{i}$. As shown in [15], the exponents can be expressed as

$$\begin{cases} p_j = E_{N_f}(m, x_j), \quad j = 1,\ldots,k, \\ p_M = (m+1)E_{N_f}(m) - E_{\mathrm{conv}(\widetilde{A}_f)}(m), \end{cases}$$

where

$$\widetilde{A}_f := \{(i_1,\ldots,i_k,1) : (i_1,\ldots,i_k) \in A_f\} \cup \{(\alpha^{(1)},\ldots,\alpha^{(k)},0)\}.$$

Remark 1. *For certain polynomial equations, the asymptotic bounds derived from the Basic Strategy can be improved by adding unit vectors to A_f. For example, consider*

$$f(x_1,x_2,x_3) = x_1^2 x_2 + x_3^2 + \alpha_{1,2,0} x_1 x_2^2 + \alpha_{1,1,0} x_1 x_2 + \alpha_{0,0,1} x_3 + \alpha_{0,0,0},$$

with coefficients $\alpha_{i_1,i_2,i_3} \in \mathbb{Z}$. Under Assumption 1, the Basic Strategy finds all roots (x_1,x_2,x_3) with $|x_j| < X$ in polynomial time if $X < M^{1/8-\varepsilon}$. If we replace A_f with

$$\overline{A}_f := A_f \cup \{\mathbf{e}_j^{(k)} : 1 \le j \le k\} \cup \{\mathbf{0}^{(k)}\},$$

the bound improves from $M^{1/8}$ to $M^{5/36}$.

Extended strategy. Let $E_{j_0} := \{\mathbf{0}^{(k)}, \mathbf{e}_{j_0}^{(k)}\}$. We describe the Extended Strategy using x_{j_0}.

Compute $mN_f + tE_{j_0}$ for integers m, t, and define

$$S_\ell = \ell \boldsymbol{\alpha}_f + (m-\ell)N_f + t\,\mathrm{conv}(E_{j_0}),$$

so that $S_m \subset \cdots \subset S_0$.

For each $\mathbf{i} \in (mN_f + t\,\mathrm{conv}(E_{j_0})) \cap \mathbb{Z}^k$, determine the unique ℓ such that $\mathbf{i} \in S_\ell$ but not in $S_{\ell+1}$, and define

$$g_{\mathbf{i}} = \frac{x_1^{i_1} \cdots x_k^{i_k}}{\mathrm{LM}(f)^\ell} f^\ell M^{m-\ell}.$$

The coefficient vectors of $g_{[i_1,\ldots,i_k]}(x_1X_1,\ldots,x_kX_k)$ form a basis of $\mathcal{L}$.

Write

$$\det(\mathcal{L}) = X_1^{p_1} \cdots X_k^{p_k} M^{p_M}.$$

Assume

$$\dim(\mathcal{L}) = \sum_{i=0}^{k} a_i m^{k+1-i} t^i,$$

and

$$\det(\mathcal{L}) = \prod_{j=1}^{k} X_j^{\sum_{i=0}^{k+1} b_i^{(j)} m^{k+1-i} t^i} \cdot M^{\sum_{i=0}^{k+1} c_i m^{k+1-i} t^i}.$$

The coefficients are determined by solving, for $\delta = 0, \ldots, k+1$,

$$\begin{cases} \displaystyle\sum_{i=0}^{k} a_i \delta^i = E_{N_f + \delta \operatorname{conv}(E_{j_0})}(m), \\ \displaystyle\sum_{i=0}^{k+1} b_i^{(j)} \delta^i = E_{N_f + \delta \operatorname{conv}(E_{j_0})}(m, x_j), \\ \displaystyle\sum_{i=0}^{k+1} c_i \delta^i = (m+1) E_{N_f + \delta \operatorname{conv}(E_{j_0})}(m) - E_{\operatorname{conv}(\widetilde{A}_f) + \delta \operatorname{conv}(\widetilde{E}_{j_0})}(m), \end{cases}$$

where

$$\widetilde{A}_f = \{(i_1, \ldots, i_k, 1) : (i_1, \ldots, i_k) \in A_f\} \cup \{(\alpha^{(1)}, \ldots, \alpha^{(k)}, 0)\} \subseteq \mathbb{Z}^{k+1},$$

and

$$\widetilde{E}_{j_0} = \{\mathbf{0}^{(k+1)}, \mathbf{e}_{j_0}^{(k+1)}\} \subseteq \mathbb{Z}^{k+1}.$$

3.2 Approximating the dimension and determinant via volumes of faces

In practice, asymptotic bounds alone are insufficient. For example, for a 1024-bit RSA modulus, Coppersmith's classical result states that if 256 most significant bits of p are leaked, then the modulus can be factored in polynomial time. From a practical perspective, however, one must also choose an explicit lattice dimension. If 260 MSBs are leaked, how large should the lattice dimension be? Thus, computing the Ehrhart polynomials involved in the dimension and determinate plays a important role.

Let $N \subset \mathbb{R}^k$ be a k-dimensional lattice polytope. Its Ehrhart polynomial

$$E_N(m) = \#(mN \cap \mathbb{Z}^k)$$

can be written as

$$E_N(m) = c_k m^k + c_{k-1} m^{k-1} + \cdots + c_0.$$

We recall a classical result of Ehrhart and Macdonald for computing the second leading coefficient.

Lemma 10.

$$c_{k-1} = \frac{1}{2} \sum_{F} \mathrm{Vol}_{k-1}(F),$$

where the sum ranges over all $(k-1)$*-dimensional facets* F *of* N*, and* $\mathrm{Vol}_{k-1}(F)$ *denotes the* $(k-1)$*-dimensional normalized lattice volume of* F *with respect to the induced lattice* $\mathbb{Z}^k \cap \mathrm{aff}(F)$*.*

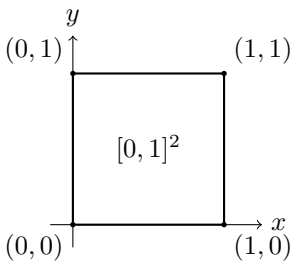
Example 1 (The unit square). Let $N = [0,1]^2 \subset \mathbb{R}^2$. Then

$$E_N(m) = \#\big(mN \cap \mathbb{Z}^2\big) = \#\big([0,m]^2 \cap \mathbb{Z}^2\big) = (m+1)^2 = m^2 + 2m + 1.$$

The facets of N are its four edges, each having $(k-1) = 1$ dimensional normalized lattice volume equal to 1. Hence

$$c_1 = \frac{1}{2} \sum_{F} \mathrm{Vol}_1(F) = \frac{1}{2} \cdot 4 = 2,$$

which matches the coefficient of m in $E_N(m) = m^2 + 2m + 1$.



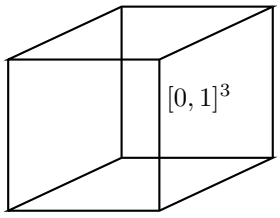
Example 2 (The unit cube). Let $N = [0,1]^3 \subset \mathbb{R}^3$. Then

$$E_N(m) = \#\big(mN \cap \mathbb{Z}^3\big) = \#\big([0,m]^3 \cap \mathbb{Z}^3\big) = (m+1)^3 = m^3 + 3m^2 + 3m + 1.$$

The facets of N are its six square faces, each having $(k-1) = 2$ dimensional normalized lattice area equal to 1. Hence

$$c_2 = \frac{1}{2} \sum_{F} \mathrm{Vol}_2(F) = \frac{1}{2} \cdot 6 = 3,$$

which matches the coefficient of m^2 in $E_N(m) = m^3 + 3m^2 + 3m + 1$.



To compute additional coefficients c_j, one may use Barvinok's algorithm [4].

Lemma 11. *The computation of any fixed number of highest-degree coefficients of the Ehrhart polynomial of an integral polytope can be reduced in polynomial time to the computation of volumes of its faces.*

Therefore, we can obtain accurate approximations of $\dim(\mathcal{L})$ and $\det(\mathcal{L})$, and then apply (1) to determine the lattice dimension required in practice.

Based on this insight, we introduce an estimator, DimOracle, which predicts the required lattice size in practical settings. We implement DimOracle and demonstrate its effectiveness through experimental results in Section 5.

4 A geometric perspective for Unravelled Linearization

We first introduce Unravelled Linearization from the perspective of Newton polytopes in Section 4.1. Our ultimate goal is to compute asymptotic bounds for arbitrary polynomial equations. We begin with a simpler setting based on the Basic Strategy in Section 4.2, and then focus on the general case in Section 4.3. Moreover, we analyze a special case in Section 4.4 before presenting the Extended Strategy in Section 4.5. Finally, leveraging our analysis of asymptotic bounds, we demonstrate improvements to several cryptanalytic results in Section 4.6.

4.1 Unravelled Linearization with Newton polytopes

Benefits of Unravelled Linearization. Unravelled Linearization provides several advantages, including improved asymptotic bounds [18], simpler lattice constructions [19], and lower lattice dimensions [19].

Let $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$. Suppose that all nonlinear monomials of f have relatively small coefficients. We aggregate these monomials into a new auxiliary variable. Specifically, we introduce a variable u representing the sum of the selected monomials and denote the resulting polynomial by f_{ul}. In many cryptanalytic applications, the resulting polynomial is linear in the new variables. In this work, we assume that f is monic, so that its leading coefficient is small.

Regarding monomial orders, we assume $x_k \prec \cdots \prec x_1 \prec u$. We use $\prec_{\mathsf{deglex}}$ in the ring $\mathbb{Z}[x_1, \ldots, x_k]$ and $\prec_{\mathsf{lex}}$ in $\mathbb{Z}[u, x_1, \ldots, x_k]$. Thus, $\mathrm{LM}(f)$ is taken with respect to $\prec_{\mathsf{deglex}}$, while the leading monomials of f_{ul} and related polynomials are taken with respect to $\prec_{\mathsf{lex}}$.

Formally, let $\mathcal{I} \subseteq \mathbb{N}^k$ index the monomials with small coefficients. We write

$$\begin{aligned} f(x_1, \ldots, x_k) &= \underbrace{\mathrm{LM}(f) + \sum_{(i_1,\ldots,i_k)\in\mathcal{I}} \alpha_{i_1,\ldots,i_k}\, x_1^{i_1} \cdots x_k^{i_k}}_{=:\,u} + \sum_{j\in\mathcal{J}} \alpha_j\, x_j \\ &= u + \sum_{j\in\mathcal{J}} \alpha_j\, x_j =: f_{\mathrm{ul}}(u, x_1, \ldots, x_k). \end{aligned}$$

In earlier works, all nonlinear terms are aggregated into u, so that f_{ul} is linear [5,18,19]. More recently, `cuso` [29] considers a generalized version allowing more flexible relations. In this paper, we primarily focus on the case where f_{ul} is linear, which suffices for most cryptanalytic applications, but we also discuss situations where f_{ul} is not linear in Section 4.3.

We now describe how to apply Unravelled Linearization in the Basic and Extended Strategies [5, 18, 19].

Basic Strategy. Fix an integer m. Compute the dilated polytope $mN_{f_{\mathrm{ul}}}$ and define the initial monomial set

$$\mathcal{M}_{\mathrm{init}} = \{u^{i_0}x_1^{i_1}\cdots x_k^{i_k} : (i_0,\ldots,i_k) \in mN_{f_{\mathrm{ul}}} \cap \mathbb{Z}^{k+1}\}.$$

Define

$$S_\ell = \ell\mathbf{e}_1^{(k+1)} + (m-\ell)N_{f_{\mathrm{ul}}},$$

so that $S_m \subset \cdots \subset S_0$. For each integer point $\mathbf{i} = (i_0, i_1, \ldots, i_k) \in mN_{f_{\mathrm{ul}}} \cap \mathbb{Z}^{k+1}$, determine the unique ℓ such that $\mathbf{i} \in S_\ell$ but $\mathbf{i} \notin S_{\ell+1}$.

We construct

$$h_{i_0,\ldots,i_k}(u,x_1,\ldots,x_k) = \frac{u^{i_0}x_1^{i_1}\cdots x_k^{i_k}}{u^\ell} f_{\mathrm{ul}}^\ell M^{m-\ell}.$$

The main difference from the standard strategy is the additional back-substitution step. For each $h_{i_0,\ldots,i_k}$, we replace every occurrence of $\mathrm{LM}(f)$ by

$$u - \sum_{(i_1,\ldots,i_k)\in\mathcal{I}} \alpha_{i_1,\ldots,i_k}\, x_1^{i_1}\cdots x_k^{i_k},$$

and denote the resulting polynomial by $g_{i_0,\ldots,i_k}(u,x_1,\ldots,x_k)$.

We then define

$$\mathcal{M} = \bigcup_{g_{i_0,\ldots,i_k}} \mathrm{supp}(g_{i_0,\ldots,i_k}).$$

If several polynomials in $\{g_{i_0,\ldots,i_k}\}$ share the same leading monomial, we keep the one with smallest leading coefficient and discard the others; denote the resulting set by G_1. Define

$$G_2 = \{\tau M^m : \tau \in \mathcal{M} \setminus \{\mathrm{LM}(g) : g \in G_1\}\}.$$

Finally, let $G = G_1 \cup G_2$ and use the coefficient vectors of

$$\{g(uU, x_1X_1, \ldots, x_kX_k) : g \in G\}$$

as a basis of the lattice.

Remark 2. *Each $h_{i_0,\ldots,i_k}$ has a distinct leading monomial. However, after back-substitution, distinct $h_{i_0,\ldots,i_k}$ may yield polynomials with the same leading monomial. For example, let*

$$f(x_1,x_2,x_3) = x_1^2 - x_2x_3 + \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3,$$

and define $u = x_1^2 - x_2x_3$*, so that* $f_{\mathrm{ul}}(u, x_1, x_2, x_3) = u + \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3$*. For* $m = 3$*, the monomials* ux_1^2 *and* ux_2x_3 *yield*

$$h_{1,2,0,0} = x_1^2(u + \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3)M^2,$$

and

$$h_{1,0,1,1} = ux_2x_3M^3.$$

Their leading monomials are ux_1^2 *and* ux_2x_3*, respectively. After back-substitution,*

$$g_{1,2,0,0} = (u + x_2x_3)(u + \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3)M^2,$$

whose leading monomial is ux_2x_3*, identical to that of* $g_{1,0,1,1}$*.*

Remark 3. *The purpose of introducing* G_2 *is to ensure that* G *is* $(\mathcal{M}, \prec_{\mathsf{lex}})$*-suitable.*

Extended Strategy. For the Extended Strategy, we instead use

$$\mathcal{M}_{\mathrm{init}} = \{u^{i_0}x_1^{i_1} \cdots x_k^{i_k} : (i_0, \ldots, i_k) \in mN_{f_{\mathrm{ul}}} + t\mathrm{conv}(\mathbf{0}^{(k+1)}, \mathbf{e}_{j_0}^{(k+1)}\}.$$

The introduction of additional monomials makes the analysis more complicated. Consider the Small Private Exponent Attack [8, 19]. Let

$$f(x_1, x_2) = x_1x_2 + \alpha_{1,0}x_1 + 1 \bmod e,$$

and set $u = x_1x_2 + 1$. Then $f_{\mathrm{ul}} = u + \alpha_{1,0}x_1$, and under the Basic Strategy,

$$\mathcal{M}_{\mathrm{init}} = \{u^{i_0}x_1^{i_1} : 0 \le i_0 + i_1 \le m\}.$$

In this case, no back-substitution is required. However, under the Extended Strategy we additionally consider monomials $u^{i_0}x_1^{i_1}x_2^{i_2}$ with $i_2 \le t$, and for these monomials back-substitution becomes necessary. We return to this special case later in Section 4.5.

4.2 Start with $\mathbf{rank}(\boldsymbol{A}_{\boldsymbol{f}_{\mathbf{ul}}}) = \boldsymbol{k} + \mathbf{1}$

We begin with a simpler case in which every variable x_j, for $1 \le j \le k$, appears in the support of f_{ul}. Thus,

$$f_{\mathrm{ul}}(u, x_1, \ldots, x_k) = u + \sum_{j=1}^{k} \alpha_j x_j.$$

We derive asymptotic bounds in this setting based on the following observation.

Lemma 12.

$$\mathcal{M} = \mathcal{M}_{\mathrm{init}} \setminus \{\mu \in \mathcal{M}_{\mathrm{init}} : \mathrm{LM}(f) \textit{ divides } \mu\}.$$

Proof. In this case,

$$\mathcal{M}_{\text{init}} = \{u^{i_0} x_1^{i_1} \cdots x_k^{i_k} : 0 \le i_0 + \cdots + i_k \le m\}.$$

Every $\lambda \in \mathcal{M}_{\text{init}}$ can be written as $\lambda = \text{LM}(f)^\ell \tau$ where $\text{LM}(f)$ does not divide τ. After back-substitution, each occurrence of $\text{LM}(f)$ is replaced by

$$u - \sum_{(i_1,\ldots,i_k)\in\mathcal{I}} \alpha_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}.$$

Hence:

1. $\mathcal{M} \subseteq \mathcal{M}_{\text{init}}$;
2. if $\text{LM}(f)$ does not divide λ, then $\lambda \in \mathcal{M}$;
3. if $\text{LM}(f)$ divides λ, then $\lambda \notin \mathcal{M}$.

This proves the claim. □

Thus,

$$\dim(\mathcal{L}) = \#\mathcal{M} = \#\mathcal{M}_{\text{init}} - \#\{\mu \in \mathcal{M}_{\text{init}} : \text{LM}(f) \text{ divides } \mu\}.$$

By inclusion–exclusion, we obtain the following.

Lemma 13. *Let $\mathcal{J}_0 = \{j : x_j \text{ divides } \text{LM}(f)\}$. For any nonempty $\mathcal{J} \subseteq \mathcal{J}_0$, define*

$$P_{\mathcal{J}} = \{(i_0, \ldots, i_k) \in mN_{f_{\text{ul}}} \cap \mathbb{Z}^{k+1} : i_j < \alpha_j \ \forall j \in \mathcal{J}\}.$$

Then

$$\dim(\mathcal{L}) = \sum_{\emptyset \neq \mathcal{J} \subseteq \mathcal{J}_0} (-1)^{\#\mathcal{J}+1} \#P_{\mathcal{J}}.$$

Proof. Let P_j^c denote the complement of P_j in $mN_{f_{\text{ul}}} \cap \mathbb{Z}^{k+1}$:

$$P_j^c = \{(i_0, \ldots, i_k) : i_j \ge \alpha_j\}.$$

Then

$$\{\mu \in \mathcal{M}_{\text{init}} : \text{LM}(f) \text{ divides } \mu\} = \bigcap_{j\in\mathcal{J}_0} P_j^c.$$

Hence

$$\mathcal{M} = \left(\bigcap_{j\in\mathcal{J}_0} P_j^c\right)^c = \bigcup_{j\in\mathcal{J}_0} P_j,$$

and the result follows by inclusion–exclusion. □

Lemma 14. *For any nonempty $\mathcal{J} \subseteq \mathcal{J}_0$, the quantity $\#P_{\mathcal{J}}$ is a polynomial in m of degree $k + 1 - \#\mathcal{J}$ when $m \ge \deg(f)$.*

Proof. We have

$$mN_{f_{\mathrm{ul}}} = \{(i_0, \ldots, i_k) \in \mathbb{R}^{k+1}_{\geq 0} : i_0 + \cdots + i_k \leq m\}.$$

Fix $\mathcal{J}$ with $\#\mathcal{J} = r$. For each choice of $i_j = \ell_j$ with $0 \leq \ell_j < \alpha_j$ for $j \in \mathcal{J}$, the remaining coordinates satisfy

$$\sum_{j \notin \mathcal{J}} i_j \leq m - \sum_{j \in \mathcal{J}} \ell_j.$$

Thus they range over the lattice points in a dilation of the standard simplex in dimension $k+1-r$. Since $m \geq \deg(f)$, the count is a polynomial in m of degree $k+1-r$. □

Theorem 1. *For $m \geq \deg(f)$, $\dim(\mathcal{L})$ is a polynomial in m of degree k. Its leading coefficient equals $\deg(f)/k!$.*

Proof. By Lemma 13 and Lemma 14, the highest-degree terms arise from $\#\mathcal{J} = 1$. Each such term contributes $\alpha_j/k!$, and summing over $j \in \mathcal{J}_0$ yields

$$\frac{\sum_{j \in \mathcal{J}_0} \alpha_j}{k!} = \frac{\deg(f)}{k!}.$$

□

Write $\det(\mathcal{L}) = U^{p_0} X_1^{p_1} \cdots X_k^{p_k} M^{p_M}$, we obtain the following results on p_j and p_M based on similar analysis.

Theorem 2. *For $m \geq \deg(f)$, each p_j for $j = 0, \ldots, k$ is a polynomial in m of degree $k+1$. Moreover,*

$$\lim_{m \to \infty} \frac{p_j(m)}{m^{k+1}} = \begin{cases} \dfrac{\deg(f)}{(k+1)!}, & j = 0, \\ \dfrac{\deg(f) - \alpha_j}{(k+1)!}, & j = 1, \ldots, k. \end{cases}$$

Theorem 3. *For $m \geq \deg(f)$, p_M is a polynomial in m of degree $k+1$. Its leading coefficient equals $\frac{k \deg(f)}{(k+1)!}$.*

4.3 The Basic Strategy

In the previous section, we showed how to compute asymptotic bounds when f_{ul} has degree 1 and $\mathrm{rank}(A_{f_{\mathrm{ul}}}) = k+1$. We now consider the case where f_{ul} has degree 1 but $\mathrm{rank}(A_{f_{\mathrm{ul}}}) \leq k$. Using the idea of adding unit vectors from Remark 1, we derive asymptotic bounds in Theorem 4. We then generalize the argument to $\deg(f_{\mathrm{ul}}) > 1$ in Theorem 5.

Theorem 4. *Suppose that after linearization, f_{ul} has degree 1. Then we can find all roots $(x_1, \ldots, x_k)$ satisfying $x_j < X_j$ if*

$$\prod_{j=1}^{k} X_j^{\alpha_j \deg(f)+\deg(f)-\alpha_j} < M^{\deg(f)}.$$

Corollary 1. *Suppose that after linearization, f_{ul} has degree 1. Then we can find all roots $(x_1, \ldots, x_k)$ satisfying $x_j < X$ if*

$$X < M^{\frac{1}{\deg(f)+k-1}}.$$

Proof. Set $X_1 = \cdots = X_k = X$ in Theorem 4. □

Proof of Theorem 4

Adding unit vectors. For general f, it is difficult to analyze the resulting set G, and in particular the contribution of G_2. Recall from Remark 1 that adding unit vectors can sometimes yield better asymptotic bounds. We adapt the same idea to Unravelled Linearization. Informally, adding unit vectors increases the proportion of low-degree monomials and can therefore improve the asymptotic bounds. A rigorous characterization of when adding unit vectors improves the bounds remains open.

We proceed as follows.

Compute

$$\bar{A}_{f_{\mathrm{ul}}} = A_{f_{\mathrm{ul}}} \cup \{\mathbf{e}_j^{(k+1)} : 1 \le j \le k+1\} \cup \{\mathbf{0}^{(k+1)}\},$$

and let $\bar{N}_{f_{\mathrm{ul}}} := \mathrm{conv}(\bar{A}_{f_{\mathrm{ul}}})$.

Fix an integer m, compute the dilated polytope $m\bar{N}_{f_{\mathrm{ul}}}$, and define the initial monomial set

$$\mathcal{M}_{\mathrm{init}} = \{u^{i_0} x_1^{i_1} \cdots x_k^{i_k} : (i_0, \ldots, i_k) \in m\bar{N}_{f_{\mathrm{ul}}} \cap \mathbb{Z}^{k+1}\}.$$

Define

$$S_\ell = \ell \mathbf{e}_1^{(k+1)} + (m-\ell)\bar{N}_{f_{\mathrm{ul}}},$$

so that $S_m \subset \cdots \subset S_0$. For each integer point $\mathbf{i} = (i_0, i_1, \ldots, i_k) \in m\bar{N}_{f_{\mathrm{ul}}} \cap \mathbb{Z}^{k+1}$, determine the unique ℓ such that $\mathbf{i} \in S_\ell$ but $\mathbf{i} \notin S_{\ell+1}$.

We construct

$$h_{i_0,\ldots,i_k}(u, x_1, \ldots, x_k) = \frac{u^{i_0} x_1^{i_1} \cdots x_k^{i_k}}{u^\ell} f_{\mathrm{ul}}^\ell M^{m-\ell}.$$

For each $h_{i_0,\ldots,i_k}$, we replace every occurrence of $\mathrm{LM}(f)$ with

$$u - \sum_{(i_1,\ldots,i_k)\in\mathcal{I}} \alpha_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k},$$

and denote the resulting polynomial by $g_{i_0,\ldots,i_k}(u, x_1, \ldots, x_k)$.

Next define

$$\mathcal{M} = \bigcup_{g_{i_0,\ldots,i_k}} \mathrm{supp}(g_{i_0,\ldots,i_k}).$$

Among the set $\{g_{i_0,\ldots,i_k} : u^{i_0} x_1^{i_1} \cdots x_k^{i_k} \in \mathcal{M}\}$, if several polynomials share the same leading monomial, we keep the one with the smallest leading coefficient and discard the others; denote the resulting set by G_1. Define

$$G_2 = \{\tau M^m : \tau \in \mathcal{M} \setminus \{\mathrm{LM}(g) : g \in G_1\}\}.$$

Let $G = G_1 \cup G_2$, and form the lattice basis from the coefficient vectors of

$$\{g(uU, x_1X_1, \ldots, x_kX_k) : g \in G\}.$$

Even after adding unit vectors, the resulting set G remains $(\mathcal{M}, \prec)$-suitable. This yields the stated asymptotic condition

$$\prod_{j=1}^{k} X_j^{\alpha_j \deg(f)+\deg(f)-\alpha_j} < M^{\deg(f)}.$$

We also consider the generalized case $\deg(f_{\mathrm{ul}}) > 1$. We apply the same idea, but now add

$$\bigcup_{i_1+\cdots+i_k \le \deg(f_{\mathrm{ul}})} \{(0, i_1, \ldots, i_k)\}.$$

Theorem 5. *Suppose that after linearization, f_{ul} has degree $d' \ge 1$. Then we can find all roots $(x_1, \ldots, x_k)$ satisfying $x_j < X_j$ if*

$$\prod_{j=1}^{k} X_j^{\alpha_j \deg(f)+\deg(f_{\mathrm{ul}})\deg(f)-\alpha_j} < M^{\deg(f)}.$$

4.4 The Basic Strategy: a special case

Assume that every variable x_j, for $1 \le j \le k$, appears in the support of f, and that all nonlinear terms are aggregated into u. We consider the special case where there exists an index $j_0 \in \{1, \ldots, k\}$ such that the coefficient c of the linear term x_{j_0} is sufficiently small and is therefore also aggregated into u.

The key difference from the previous case is that we don't add the unit vector corresponding to x_{j_0} in $\mathcal{M}_{\mathrm{init}}$, even though x_{j_0} no longer appears in the support of f_{ul}. Then

$$f_{\mathrm{ul}}(u, x_1, \ldots, x_k) = u + \sum_{j \ne j_0} \alpha_j x_j,$$

and

$$\mathcal{M}_{\mathrm{init}} = \left\{ u^{i_0} \prod_{\substack{1 \le j \le k \\ j \ne j_0}} x_j^{i_j} : 0 \le i_0 + \sum_{\substack{1 \le j \le k \\ j \ne j_0}} i_j \le m \right\}.$$

When $\mathrm{rank}(A_{f_{\mathrm{ul}}}) \le k$, the behavior differs substantially. For example, the Power Generator in Section 4 of [18] and the Pollard generator in Section 4.1 of [5] consider

$$f(x_1, x_2) = x_1^2 - x_2 + \alpha_{1,0}x_1 + \alpha_{0,0},$$

and use $u = x_1^2 - x_2$ for Unravelled Linearization.

We analyze the dimension and determinant of the lattice after applying Unravelled Linearization.

Define a map $\phi_{\mathrm{LM}(f)}$ on monomials by

$$\phi_{\mathrm{LM}(f)}(\lambda) = \max\{r \ge 0 : \mathrm{LM}(f)^r \mid \lambda\}.$$

Lemma 15. *With*

$$\mathcal{M}_{\mathrm{init}} = \left\{ u^{i_0} \prod_{\substack{1\le j\le k\\ j\ne j_0}} x_j^{i_j} \,:\, 0 \le i_0 + \sum_{\substack{1\le j\le k\\ j\ne j_0}} i_j \le m \right\},$$

the resulting monomial set satisfies

$$\mathcal{M} = \left\{ \frac{\lambda \cdot x_{j_0}^{\phi_{\mathrm{LM}(f)}(\lambda)}}{\mathrm{LM}(f)^{\phi_{\mathrm{LM}(f)}(\lambda)}} : \lambda \in \mathcal{M}_{\mathrm{init}} \right\},$$

that is, each occurrence of $\mathrm{LM}(f)$ *is replaced by* x_{j_0}.

Proof. By construction, $\phi_{\mathrm{LM}(f)}(\lambda)$ counts the maximal power of $\mathrm{LM}(f)$ dividing λ. In the back-substitution step, each factor $\mathrm{LM}(f)$ is replaced by a linear expression whose leading monomial is x_{j_0} with respect to $\prec_{\mathsf{lex}}$. Consequently, replacing $\mathrm{LM}(f)^{\phi_{\mathrm{LM}(f)}(\lambda)}$ by $x_{j_0}^{\phi_{\mathrm{LM}(f)}(\lambda)}$ yields exactly the set of leading monomials appearing after back-substitution. This proves the claimed description of $\mathcal{M}$. □

Theorem 6.

$$\dim(\mathcal{L}) = E_{N_{f_{\mathrm{ul}}}}(m),$$

which is a polynomial in m *of degree* k. *Its leading coefficient equals* $1/k!$.

Proof. Replacing every occurrence of $\mathrm{LM}(f)$ by x_{j_0} preserves the number of monomials. Hence $\#\mathcal{M} = \#(mN_{f_{\mathrm{ul}}} \cap \mathbb{Z}^{k+1}) = E_{N_{f_{\mathrm{ul}}}}(m)$, and the result follows from Ehrhart theory. □

Since each occurrence of $\mathrm{LM}(f)$ is replaced by x_{j_0}, we must account for the number of such occurrences.

Lemma 16.

$$\sum_{\lambda\in\mathcal{M}_{\mathrm{init}}} \phi_{\mathrm{LM}(f)}(\lambda) = E_{N^*}(m) - E_{N_{f_{\mathrm{ul}}}}(m),$$

where N^* is the polytope

$$N^* = \left\{ (x_0,\dots,x_k,y) \in \mathbb{R}^{k+2} : \begin{array}{l} (x_0,\dots,x_k,y) \in \operatorname{conv}\Big(\mathbf{0}^{(k+2)}, \mathbf{e}_1^{(k+2)}, \dots, \mathbf{e}_{k+2}^{(k+2)}, \\ \qquad \Big(0, \frac{\alpha_1}{\deg(f)}, \dots, \frac{\alpha_k}{\deg(f)}, \frac{1}{\deg(f)}\Big)\Big), \\ x_{j_0} = 0 \end{array} \right\}.$$

Proof. See Appendix B. □

Theorem 7.

$$p_j(m) = \begin{cases} E_{N_{f_{\mathrm{ul}}}}(m,u), & j = 0, \\ E_{N^*}(m) - E_{N_{f_{\mathrm{ul}}}}(m), & j = j_0, \\ E_{N_{f_{\mathrm{ul}}}}(m,x_j) - \alpha_j\big(E_{N^*}(m) - E_{N_{f_{\mathrm{ul}}}}(m)\big), & j \neq j_0. \end{cases}$$

Since N^* is rational when $\deg(f) > 1$, some p_j may be quasi-polynomials. Moreover,

$$\lim_{m\to\infty} \frac{p_j(m)}{m^{k+1}} = \begin{cases} \dfrac{1}{(k+1)!}, & j = 0, \\ \dfrac{1}{\deg(f)(k+1)!}, & j = j_0, \\ \dfrac{\deg(f) - \alpha_j}{\deg(f)(k+1)!}, & j \neq j_0. \end{cases}$$

Proof. The exponent p_j is obtained by subtracting the total number of occurrences of $\mathrm{LM}(f)$, given by Lemma 16, from the corresponding weighted Ehrhart sums. The asymptotic limits follow from the leading coefficients of the associated (quasi-)polynomials. □

Theorem 8.

$$p_M = (m+1)E_{N_{f_{\mathrm{ul}}}}(m) - E_{\operatorname{conv}(\widetilde{A}_{f_{\mathrm{ul}}})}(m),$$

which is a polynomial in m of degree $k+1$. Its leading coefficient equals $k/(k+1)!$.

Proof. Replacing occurrences of $\mathrm{LM}(f)$ by x_{j_0} does not affect the total exponent of M. The formula follows from the same determinant computation as in the full-rank case. □

4.5 Extended Strategy

We again start from the simplest setting in which all nonlinear monomials of f have relatively small coefficients and every variable x_j, for $1 \le j \le k$, appears in the support of f_{ul}. In this case, the same structural property as in Lemma 12 holds, and the monomial elimination induced by back-substitution can be analyzed in exactly the same way. Consequently, the lattice dimension and determinant exponents can be derived via the same inclusion–exclusion and Ehrhart-theoretic arguments.

We further consider a generalization of the small private-exponent attack [8, 19]. In this setting, the constant term is sufficiently small and can be aggregated into the auxiliary variable u. Applying the same geometric analysis yields the asymptotic bound obtained in [22], thus recovering their result within our unified framework.

Moreover, the asymptotic bound derived in [29] is strictly smaller than $1-\sqrt{2}/2$. The author conjectures that this gap is caused by the irrationality of $\sqrt{2}$. This naturally raises the question of whether cuso can attain the bound $1-\sqrt{2}/2$, and under what conditions. We confirm that the gap indeed arises from the irrationality of $\sqrt{2}$, and we prove that the bound $1-\sqrt{2}/2$ is achieved asymptotically as the parameter k_{pre} tends to infinity. For details on cuso, see [29].

Specifically, let

$$t_{\mathrm{pre}} = \left\lfloor (\sqrt{2}-1)k_{\mathrm{pre}} \right\rfloor$$

and take

$$\mathcal{M}_{\mathrm{vert}} = \{1,\ x^{k_{\mathrm{pre}}},\ x^{k_{\mathrm{pre}}}y^{k_{\mathrm{pre}}},\ x^{k_{\mathrm{pre}}}y^{k_{\mathrm{pre}}+t_{\mathrm{pre}}}\}$$

as the input monomials. Then

$$\begin{aligned}
\dim &= \frac{1}{2}k_{\mathrm{pre}}(k_{\mathrm{pre}}+t_{\mathrm{pre}}),\\
p_1 &= \frac{1}{3}k_{\mathrm{pre}}^2(k_{\mathrm{pre}}+t_{\mathrm{pre}}),\\
p_2 &= \frac{1}{6}k_{\mathrm{pre}}(k_{\mathrm{pre}}+t_{\mathrm{pre}})^2,\\
p_{\mathcal{F}} &= \frac{1}{2}k_{\mathrm{pre}}^2(k_{\mathrm{pre}}+t_{\mathrm{pre}}) - \frac{1}{6}k_{\mathrm{pre}}^3 - \frac{1}{3}k_{\mathrm{pre}}^2 t_{\mathrm{pre}}.
\end{aligned}$$

Let $\tau_{\mathrm{pre}} = t_{\mathrm{pre}}/k_{\mathrm{pre}}$ and $\tau^* = \sqrt{2}-1$. The corresponding asymptotic bound satisfies

$$\begin{aligned}
\log_e X &= \frac{\frac{1}{6}k_{\mathrm{pre}}^3 + \frac{1}{3}k_{\mathrm{pre}}^2 t_{\mathrm{pre}} - \frac{1}{2}\left(\frac{1}{6}k_{\mathrm{pre}}(k_{\mathrm{pre}}+t_{\mathrm{pre}})^2\right)}{\frac{1}{3}k_{\mathrm{pre}}^2(k_{\mathrm{pre}}+t_{\mathrm{pre}})}\\
&= 1 - \frac{1}{4}\left(1+\tau+\frac{2}{1+\tau}\right)\\
&= 1 - \frac{1}{4}\left(1+\tau^*+\frac{2}{1+\tau^*} + (\tau-\tau^*)\left(1-\frac{1}{\tau\tau^*}\right)\right)\\
&= 1 - \frac{\sqrt{2}}{2} - \frac{1}{4}(\tau-\tau^*)\left(1-\frac{1}{\tau\tau^*}\right).
\end{aligned}$$

Hence,

$$\begin{aligned}\left|\log_e X - \left(1 - \frac{\sqrt{2}}{2}\right)\right| &= \frac{1}{4}\left(1 - \frac{1}{\tau\tau^*}\right)|\tau - \tau^*| \\ &= \frac{1}{4}\left(1 - \frac{1}{\tau\tau^*}\right)\left|\frac{\tau^* k_{\text{pre}} - \lfloor \tau^* k_{\text{pre}} \rfloor}{k_{\text{pre}}}\right| \\ &< \frac{1}{4}\left(1 - \frac{1}{(\sqrt{2}-1)^2}\right)\frac{1}{k_{\text{pre}}}.\end{aligned}$$

Therefore,

$$\lim_{k_{\text{pre}} \to +\infty} \log_e X = 1 - \frac{\sqrt{2}}{2}.$$

4.6 Applications

Next we will show the application of our analysis for asymptotic bounds. In all, we've improved 5 previous results, including the linear congruential generator, the quadratic generator [34], the subset-sum PRG [9] and the partial-key attack on Pòke [13].

Improvement of [34, Theorem 2]. They consider $f(x_1, x_2, x_3) \in \mathbb{Z}[x_1, x_2, x_3]$, which can be written as

$$f(x_1, x_2, x_3) = -x_1 x_3 + x_2^2 + \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_0.$$

Denote $u = x_2^2 - x_1 x_3$, then we have

$$f_{\text{ul}} = u + \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_0.$$

By Theorem 4, we have

$$\prod_{j=1}^{k} X_j^{\alpha_j \deg(f) + \deg(f) - \alpha_j} < M^{\deg(f)}.$$

Then substitute $k = 3, \alpha_1 = \alpha_2 = 1$ and $\alpha_2 = 0$, we have

$$X_1^3 X_2^2 X_3^3 < M^2.$$

Moreover, if we suppose $X_1 = X_2 = X_3 = X$, we have

$$X < M^{1/4}.$$

Improvement of [34, Theorem 4]. They consider $f(x_1, x_2, x_3, x_4) \in \mathbb{Z}[x_1, x_2, x_3, x_4]$, which can be written as

$$f(x_1, x_2, x_3) = x_1x_4 - x_2x_3 + \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3 + \alpha_4x_4 + \alpha_0.$$

Denote $u = x_1x_4 - x_2x_3$, then we have

$$f_{\text{ul}} = u + \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3 + \alpha_4x_4 + \alpha_0.$$

By Theorem 4, we have

$$\prod_{j=1}^{k} X_j^{\alpha_j \deg(f)+\deg(f)-\alpha_j} < M^{\deg(f)}.$$

Then substitute $k = 4, \alpha_1 = \alpha_4 = 1$ and $\alpha_2 = \alpha_3 = 0$, we have

$$X_1^3X_2^2X_3^2X_4^3 < M^2.$$

Moreover, if we suppose $X_1 = X_2 = X_3 = X_4 = X$, we have

$$X < M^{1/5}.$$

Improvement of [34, Theorem 6]. They consider $f(x_1, x_2, x_3, x_4) \in \mathbb{Z}[x_1, x_2, x_3, x_4]$, which can be written as

$$f(x_1, x_2, x_3, x_4) = -x_2^3+x_3^2x_2+x_2^2x_4-x_3^3-x_1^2x_4+x_1^2x_3+\sum_{i_1+i_2+i_3+i_4\le 2} \alpha_{i_1,i_2,i_3,i_4}x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}.$$

Denote $u = -x_2^3 + x_3^2x_2 + x_2^2x_4 - x_3^3 - x_1^2x_4 + x_1^2x_3$, then we have

$$f_{\text{ul}} = u + \sum_{i_1+i_2+i_3+i_4\le 2} \alpha_{i_1,i_2,i_3,i_4}x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}.$$

By Theorem 5, we have

$$\prod_{j=1}^{k} X_j^{\alpha_j \deg(f)+\deg(f_{\text{ul}})\deg(f)-\alpha_j} < M^{\deg(f)}$$

Then substitute $k = 4, \alpha_1 = 2\alpha_3 = 2$ and $\alpha_2 = \alpha_4 = 0$, we have

$$X_1^{10}X_2^6X_3^8X_4^6 < M^3.$$

Moreover, if we suppose $X_1 = X_2 = X_3 = X_4 = X$, we have

$$X < M^{1/10}.$$

Improvement of Subset-Sum Pseudorandom Generator [9, Section 5]. They consider $f(x_1, x_2, x_3) \in \mathbb{Z}[x_1, x_2, x_3]$, which can be written as

$$f(x_1, x_2, x_3) = x_1x_2 - x_3 + \alpha_1x_1 + \alpha_2x_2 + \alpha_0.$$

Denote $u = x_1x_2 - x_3$, then we have

$$f_{\text{ul}} = u + \alpha_1x_1 + \alpha_2x_2 + \alpha_0.$$

Now we compute the dimension and determinate of the lattice by using the theorems in Section 4.4, i.e., computing $\dim(\mathcal{L}), p_0, \ldots, p_k$ and p_M in the following inequaty:

$$U^{p_0}X_1^{p_1} \ldots X_k^{p_k}M^{p_M} < M^{m\dim(\mathcal{L})}. \tag{3}$$

By Theorem 6, we have

$$\lim_{m\to\infty} \frac{\dim(\mathcal{L})}{m^k} = \frac{1}{k!}.$$

And by Theorem 7, we have

$$\lim_{m\to\infty} \frac{p_j(m)}{m^{k+1}} = \begin{cases} \dfrac{1}{(k+1)!}, & \text{for } j = 0, \\ \dfrac{1}{\deg(f)(k+1)!}, & \text{for } j = j_0, \\ \dfrac{\deg(f) - \alpha_j}{\deg(f)(k+1)!}, & \text{for } j = 1, \ldots, k \text{ and } j \neq j_0. \end{cases}$$

Finally, by Theorem 8, we have

$$\lim_{m\to\infty} \frac{p_M}{m^{k+1}} = \frac{k}{(k+1)!}.$$

Then substitute $k = 3$ in (3), we have

$$U^{1/24}X_1^{1/48}X_2^{1/48}X_3^{1/48}M^{1/8} < M^{1/6}$$

Moreover, if we suppose $X_1 = X_2 = X_3 = X$, then we have $U = X^2$, thus we have

$$X < M^{2/7}.$$

Improvement of Leveled Isogeny Problems with Hints over Pòke [13, Theorem 4.3]. In the leveled isogeny setting with hints over Pòke, the authors consider the polynomial equation

$$f(x_1, x_2) = x_1^2x_2 + \alpha_{1,1}x_1x_2 + \alpha_{0,1}x_2 + \alpha_{0,0} \pmod M,$$

with the bound $X_2 = M^{6/17}$.

Applying the result of Section 3 with the Extended Strategy using x_2, we obtain the bound

$$X < M^{\frac{-23+2\sqrt{223}}{34}} \approx M^{0.2020},$$

by choosing

$$t = \frac{-10 + 2\sqrt{223}}{33}\, m \approx 0.6020\, m.$$

Furthermore, if the constant term $\alpha_{0,0}$ is sufficiently small, we can aggregate it via Unravelled Linearization by setting

$$u = x_1^2 x_2 + \alpha_{0,0}.$$

This yields the improved bound

$$X < M^{\frac{32}{153}} \approx M^{0.2092},$$

by taking $t = m$.

The aggregation is valid under the constraint

$$\alpha_{0,0} < X_1^2 X_2 = M^{\frac{118}{153}} \approx M^{0.7712}.$$

In the isogeny notation, given accessible torsion points $(P, Q) \in E[N]$ and $(P', Q') = \Gamma \cdot (\phi(P), \phi(Q))^\top$ for some $\Gamma \in \mathrm{GL}(N, 2)$, the Weil pairing yields a known value

$$r \equiv \deg(\phi) \det(\Gamma) \bmod N.$$

Our condition translates to requiring

$$r < N^{0.7712}.$$

5 A Dimension Estimator for Coppersmith's method

Given explicit formulas for the lattice dimension and determinant exponent, we can determine the minimal lattice dimension required for a successful small-root attack without explicitly constructing the lattice or performing lattice reduction, provided that the target bound lies below the asymptotic threshold, i.e., Equation (1).

When the target bound exceeds the polynomial-time threshold, practical attacks typically require enumerating several most significant bits of one or more variables. Using our precise expressions for the lattice dimension and determinant exponent, together with a standard cost model for lattice reduction (e.g., LLL or BKZ), we design an estimator that automatically identifies feasible parameter choices and effective enumeration strategies. This enables a systematic exploration of the parameter space while minimizing computational overhead.

5.1 Dimension Estimator

We first present a precise estimator in Algorithm 1 that exhaustively searches over $m \le m_{\max}$ and identifies the minimal lattice dimension satisfying the determinant condition.

Algorithm 1: Precise Dimension Estimator

Input: Bounds X, modulus M, maximum multiplier $m_{\max}$, symbolic expressions $\dim(m,t)$, $p_1, \ldots, p_k, p_{\mathcal{F}}$

Output: Optimal parameters (m,t) minimizing $\dim(m,t)$ subject to the bound, or $\perp$ if no solution exists

Define the satisfaction function

$$f(m,t) = \log M \cdot (m \dim(m,t) - p_{\mathcal{F}}(m,t)) - \sum_{i=1}^{k} p_i(m,t) \log X_i$$

;

Initialize $m^\star \leftarrow -1$, $t^\star \leftarrow -1$, $\dim_{\min} \leftarrow +\infty$;

for $i = 1$ **to** $m_{\max}$ **do**

  if $\exists j \in \mathbb{N}$ *such that* $f(i,j) \geq 0$ **then**

    Compute the minimal $j \in \mathbb{N}$ satisfying $f(i,j) \geq 0$;

    if $\dim(i,j) \leq \dim_{\min}$ **then**

      Update $m^\star \leftarrow i$, $t^\star \leftarrow j$, $\dim_{\min} \leftarrow \dim(i,j)$;

    end

  end

end

if $\dim_{\min} < +\infty$ **then**

  return $(m^\star, t^\star, \dim_{\min})$;

end

return $\perp$;

While exhaustive search guarantees the minimal lattice dimension, it may be costly when $m_{\max}$ is large. We therefore propose a faster estimator based on binary search over m in Algorithm 2 in Appendix A.

The precise estimator guarantees the minimal lattice dimension, while the quick estimator efficiently identifies the smallest feasible multiplier m together with the corresponding minimal t. In practice, the latter significantly reduces the search space and provides near-optimal parameters for lattice-based small-root attacks.

5.2 Experimental Results for the Dimension Estimator

All experiments were conducted on an Intel Xeon Platinum 8480+ CPU using SageMath 10.3. We used flatter [30] for lattice reduction. Due to space limitations, we report results for the first two applications in Section 4.6, namely Theorem 2 and Theorem 4 of [34], as well as the classical small private-exponent attack [8, 19].

For each instance, we report the modulus size M, the root bound X, the selected parameters (m, t), the resulting lattice dimension $\dim = |\mathcal{M}|$, and two timing measurements: *Time 1* denotes the running time of DimOracle (i.e., parameter estimation), and *Time 2* denotes the time for lattice construction and reduction. In all cases, the correct solution was successfully recovered.

Experimental Results.

Setting	$\log_2 M$	$\log_2 X$	(m,t)	dim	Time 1 (s)	Time 2 (s)
[34, Theorem 2]	256	58	(4,0)	55	0.12	0.99
	256	59	(6,0)	140	0.18	14.43
	256	60	(7,0)	204	0.23	47.47
	512	118	(5,0)	91	0.16	6.37
	512	120	(7,0)	204	0.27	78.98
	1024	236	(5,0)	91	0.21	10.01
	1024	240	(7,0)	204	0.31	129.56
[34, Theorem 4]	256	45	(3,0)	50	0.09	0.78
	256	46	(5,0)	196	0.19	41.28
	512	92	(4,0)	105	0.14	9.85
	512	94	(5,0)	196	0.24	69.75
	1024	184	(4,0)	105	0.22	15.84
	1024	188	(5,0)	196	0.29	105.20
[8, 19]	1024	283	(7,3)	46	0.12	0.65
	1024	285	(9,3)	67	0.08	7.84
	1024	287	(10,4)	85	0.15	8.65
	1024	289	(13,5)	136	0.22	21.92

These results illustrate the trade-off between the root bound X, the multiplier m, and the resulting lattice dimension. As X increases, the estimator selects larger m (and possibly larger t), which in turn increases the lattice dimension and the cost of lattice reduction. In all tested instances, the estimator reliably predicts feasible parameters and produces lattices that recover the hidden roots.

6 Conclusion

We revisited Unravelled Linearization in the context of Coppersmith's method and addressed two central challenges: deriving asymptotic bounds rigorously and selecting appropriate lattice dimensions in practice.

On the theoretical side, we showed that in the Unravelled Linearization setting the lattice dimension and determinant exponent are not always polynomial in the scaling parameter. As a result, interpolation-based approaches used in prior work may yield incorrect asymptotic bounds or incur unnecessary computational cost. We provided a geometric interpretation of Unravelled Linearization and a rigorous asymptotic analysis based on Ehrhart theory (Section 4). As applications, we improved the best-known asymptotic bounds in five settings: LCGs (both consecutive and non-consecutive outputs), the quadratic generator, the subset-sum PRG, and the LIPH isogeny setting. We also clarified why the small private-exponent bound in [29] is close to, but strictly smaller than, $1 - \sqrt{2}/2$.

On the practical side, we introduced DimOracle, a dimension estimator for Coppersmith's method (Section 5). By adapting Ehrhart theory, we developed algorithms to compute the leading coefficients of relevant Ehrhart (quasi-)polynomials efficiently. Our experiments demonstrate both the efficiency and the correctness of the estimator.

A natural direction for future work is to extend DimOracle to more general polynomial systems and to further automate parameter selection in Coppersmith's method.

Acknowledgement

We thank Qiyuan Chen and Hengyi Luo for discussion about the Ehrhart Theory and also the computation of the determinate. AI tools were used as typing assistants for grammar and basic editing.

References

1. Aardal, M.A., Aranha, D.F., Feng, Y., Gao, Y., Pan, Y.: Better bounds for finding fixed-degree isogenies via coppersmith's method. Cryptology ePrint Archive, Paper 2025/1812 (2025), https://eprint.iacr.org/2025/1812
2. Ajtai, M.: The shortest vector problem in L_2 is NP-hard for randomized reductions. In: Proceedings of the thirtieth annual ACM symposium on Theory of computing. pp. 10–19 (1998)
3. Baldoni, V., Berline, N., De Loera, J.A., Köppe, M., Vergne, M.: Computation of the highest coefficients of weighted ehrhart quasi-polynomials of rational polyhedra. Foundations of Computational Mathematics 12(4), 435–469 (2012)
4. Barvinok, A.I.: Computing the ehrhart polynomial of a convex lattice polytope. Discrete & Computational Geometry 12(1), 35–48 (1994)
5. Bauer, A., Vergnaud, D., Zapalowicz, J.C.: Inferring sequences produced by nonlinear pseudorandom number generators using coppersmith's methods. In: International Workshop on Public Key Cryptography. pp. 609–626. Springer (2012)

6. Beck, M., Robins, S.: Computing the continuous discretely (2020)
7. Benčina, B., Kutas, P., Merz, S.P., Petit, C., Stopar, M., Weitkämper, C.: Improved algorithms for finding fixed-degree isogenies between supersingular elliptic curves. In: Annual International Cryptology Conference. pp. 183–217. Springer (2024)
8. Boneh, D., Durfee, G.: Cryptanalysis of rsa with private key d less than n/sup 0.292. IEEE transactions on Information Theory 46(4), 1339–1349 (2000)
9. Bouillaguet, C., Martinez, F., Vergnaud, D.: Cryptanalysis of a generalized subset-sum pseudorandom generator. In: 48th International Symposium on Mathematical Foundations of Computer Science (MFCS 2023). pp. 23–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik (2023)
10. Brion, M., Vergne, M.: Lattice points in simple polytopes. Journal of the American Mathematical Society pp. 371–392 (1997)
11. Coppersmith, D.: Finding a small root of a univariate modular equation. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 155–165. Springer (1996)
12. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of cryptology 10(4), 233–260 (1997)
13. Das, S., Invernizzi, R., Kutas, P., Meers, J.: Leveled isogeny problems with hints. Cryptology ePrint Archive (2025)
14. Ehrhart, E.: Sur les polyèdres rationnels homothétiques à n dimensions. CR Acad. Sci. Paris 254, 616 (1962)
15. Feng, Y., Luo, H., Chen, Q., Nitaj, A., Pan, Y.: Computing asymptotic bounds for small roots in coppersmith's method via sumset theory. Cryptology ePrint Archive, Paper 2024/1330 (2024), `https://eprint.iacr.org/2024/1330`
16. Feng, Y., Luo, H., Chen, Q., Nitaj, A., Pan, Y.: Computing asymptotic bounds for small roots in coppersmith's method via sumset theory. In: Annual International Cryptology Conference. pp. 3–32. Springer (2025)
17. Feng, Y., Nitaj, A., Pan, Y.: Partial prime factor exposure attacks on some RSA variants. Theoretical Computer Science 999, 114549 (2024)
18. Herrmann, M., May, A.: Attacking power generators using unravelled linearization: When do we output too much? In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 487–504. Springer (2009)
19. Herrmann, M., May, A.: Maximizing small root bounds by linearization and applications to small secret exponent rsa. In: Public Key Cryptography–PKC 2010: 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings 13. pp. 53–69. Springer (2010)
20. Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: IMA International Conference on Cryptography and Coding. pp. 131–142. Springer (1997)
21. Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: Advances in Cryptology–ASIACRYPT 2006: 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006. Proceedings 12. pp. 267–282. Springer (2006)
22. Kunihiro, N.: On optimal bounds of small inverse problems and approximate gcd problems with higher degree. In: International Conference on Information Security. pp. 55–69. Springer (2012)
23. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische annalen 261, 515–534 (1982)
24. May, A.: New RSA vulnerabilities using lattice reduction methods. Ph.D. thesis, Citeseer (2003)

25. May, A., Nowakowski, J., Sarkar, S.: Partial key exposure attack on short secret exponent CRT-RSA. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 99–129. Springer (2021)
26. May, A., Nowakowski, J., Sarkar, S.: Approximate divisor multiples–factoring with only a third of the secret CRT-exponents. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 147–167. Springer (2022)
27. May, A., Ritzenhofen, M.: Implicit factoring: On polynomial time factoring given only an implicit hint. In: International Workshop on Public Key Cryptography. pp. 1–14. Springer (2009)
28. Meers, J., Nowakowski, J.: Solving the Hidden Number Problem for CSIDH and CSURF via Automated Coppersmith. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 39–71. Springer (2023)
29. Ryan, K.: Solving multivariate coppersmith problems with known moduli. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 355–384. Springer (2025)
30. Ryan, K., Heninger, N.: Fast practical lattice reduction through iterated compression. In: Annual International Cryptology Conference. pp. 3–36. Springer (2023)
31. Sarkar, S.: Enhanced bound for the commutative isogeny hidden number problem in csurf. In: International Conference on Cryptology in India. pp. 201–211. Springer (2024)
32. Stanley, R.P.: Hilbert functions of graded algebras. Advances in Mathematics 28(1), 57–83 (1978)
33. Stanley, R.P.: Enumerative combinatorics volume 1 second edition. Cambridge studies in advanced mathematics (2011)
34. Zhang, R., Bi, J., Li, L., Peng, H.: Cryptanalysis on two kinds of number theoretic pseudo-random generators using coppersmith method. IET Information Security 2025(1), 5569393 (2025)

A Quick Dimension Estimator

B Proof of Lemma 16

Proof. For $\lambda = u^{i_0} \prod_{j \neq j_0} x_j^{i_j} \in \mathcal{M}_{\text{init}}$, by definition of $\phi_{\text{LM}(f)}$ we have

$$\phi_{\text{LM}(f)}(\lambda) = \max\{r \geq 0 : \ i_0 \geq r\alpha_0, \ i_j \geq r\alpha_j \ \forall j \neq j_0\}.$$

Equivalently,

$$\phi_{\text{LM}(f)}(\lambda) = \sum_{r=1}^{\infty} \mathbf{1}_{\{\, i_0 \geq r\alpha_0, \ i_j \geq r\alpha_j \ \forall j \neq j_0 \,\}}.$$

Summing over all $\lambda \in \mathcal{M}_{\text{init}}$ gives

$$\sum_{\lambda \in \mathcal{M}_{\text{init}}} \phi_{\text{LM}(f)}(\lambda) = \sum_{r=1}^{\infty} \#\Big\{(i_0, (i_j)_{j \neq j_0}) \in \mathbb{Z}_{\geq 0}^{k+1} : \sum_j i_j \leq m, \ i_0 \geq r\alpha_0, \ i_j \geq r\alpha_j \ (j \neq j_0)\Big\}.$$

Algorithm 2: Quick Dimension Estimator

Input: Bounds X, modulus M, maximum multiplier $m_{\max}$, symbolic expressions $\dim(m,t)$, $p_1,\ldots,p_k,p_{\mathcal{F}}$

Output: Smallest feasible m and corresponding minimal t satisfying the bound, together with $\dim(m,t)$, or $\perp$ if no solution exists

Define

$$f(m,t) = \log M \cdot (m\dim(m,t) - p_{\mathcal{F}}(m,t)) - \sum_{i=1}^{k} p_i(m,t)\log X_i$$

;

if $\nexists j \in \mathbb{N}$ *such that* $f(m_{\max}, j) \geq 0$ **then**
  return $\perp$;
end
$l \leftarrow 1$, $r \leftarrow m_{\max}$;
while $l < r$ **do**
  $m \leftarrow \lfloor (l+r)/2 \rfloor$;
  if $\exists j \in \mathbb{N}$ *such that* $f(m,j) \geq 0$ **then**
    $r \leftarrow m$;
  end
  else
    $l \leftarrow m+1$;
  end
end
$m^\star \leftarrow l$;
Compute the minimal $t^\star \in \mathbb{N}$ such that $f(m^\star, t^\star) \geq 0$;
return $(m^\star, t^\star, \dim(m^\star, t^\star))$;

If we also include the case $r = 0$, then each exponent vector $(i_0, (i_j)_{j\neq j_0})$ with $\sum_j i_j \le m$ contributes exactly one additional term. Hence

$$\#\Big\{(i_0,(i_j)_{j\neq j_0},r)\in\mathbb{Z}_{\ge 0}^{k+2} : \sum_j i_j \le m,\ i_0 \ge r\alpha_0,\ i_j \ge r\alpha_j\ (j\neq j_0)\Big\} = E_{N_{f_{\mathrm{ul}}}}(m) + \sum_{\lambda\in\mathcal{M}_{\mathrm{init}}} \phi_{\mathrm{LM}(f)}(\lambda).$$

Introduce the scaled variables

$$x_0 = \frac{i_0}{m}, \qquad x_j = \frac{i_j}{m}\ (j\neq j_0), \qquad y = \frac{r}{m}.$$

Dividing the inequalities by m, we obtain

$$y \ge 0, \qquad x_0 \ge \alpha_0 y, \qquad x_j \ge \alpha_j y\ (j\neq j_0), \qquad x_0 + \sum_{j\neq j_0} x_j \le 1,$$

together with the condition $x_{j_0} = 0$. These linear inequalities define a rational polytope in $\mathbb{R}^{k+2}$, which we denote by N^*. By construction,

$$\#(mN^*\cap\mathbb{Z}^{k+2}) = E_{N_{f_{\mathrm{ul}}}}(m) + \sum_{\lambda\in\mathcal{M}_{\mathrm{init}}} \phi_{\mathrm{LM}(f)}(\lambda),$$

and therefore

$$\sum_{\lambda\in\mathcal{M}_{\mathrm{init}}} \phi_{\mathrm{LM}(f)}(\lambda) = E_{N^*}(m) - E_{N_{f_{\mathrm{ul}}}}(m).$$

It remains to verify that this polytope coincides with the convex hull described in the statement. If $y = 0$, the inequalities reduce to $x_0,\dots,x_k \ge 0$ and $x_0 + \sum_{j\neq j_0} x_j \le 1$ with $x_{j_0} = 0$, whose vertices are $\mathbf{0}^{(k+2)}$ and $\mathbf{e}_i^{(k+2)}$ for $i \neq j_0$. On the other hand, imposing $x_0 = \alpha_0 y$ and $x_j = \alpha_j y$ $(j \neq j_0)$ together with $x_0 + \sum_{j\neq j_0} x_j = 1$ gives $\deg(f)\, y = 1$, hence the additional vertex

$$\left(0, \frac{\alpha_1}{\deg(f)}, \dots, \frac{\alpha_k}{\deg(f)}, \frac{1}{\deg(f)}\right),$$

where the j_0-th coordinate is 0. This matches exactly the convex-hull description in the lemma, and completes the proof. □