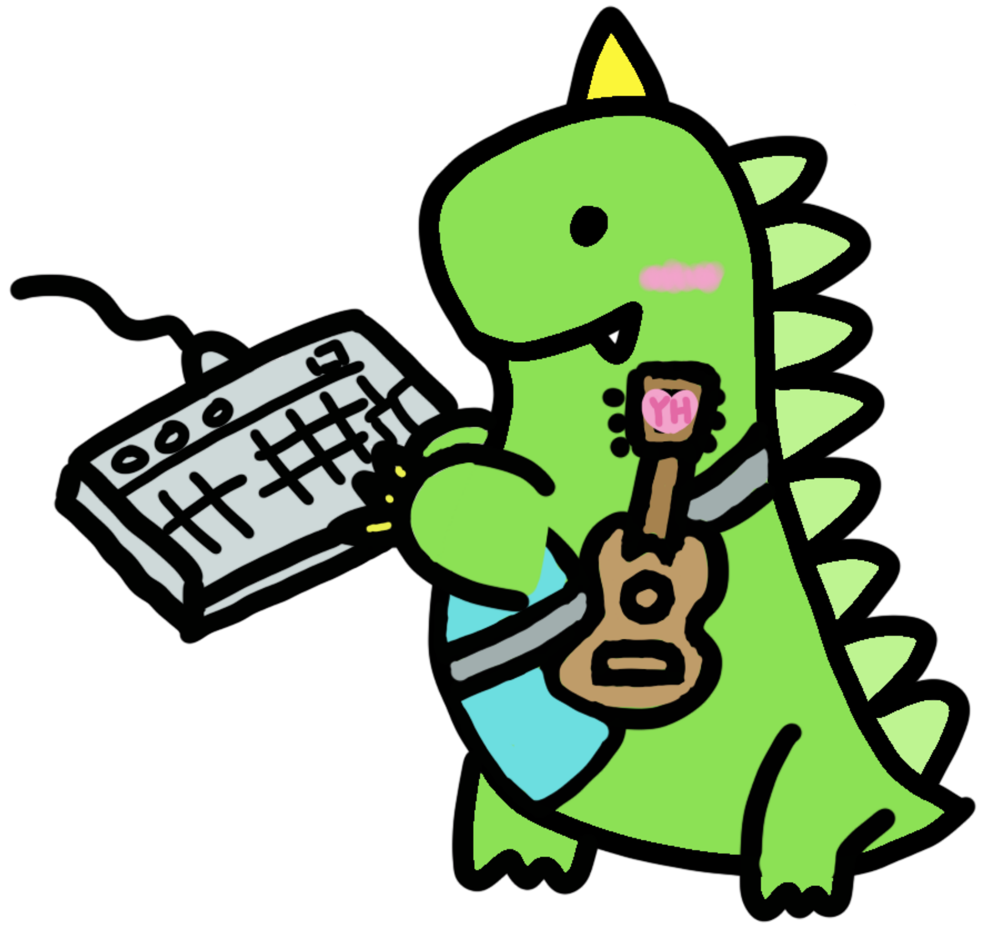
Newton Polytope-Based Strategy for Finding Roots of Multivariate Polynomials

Yansong Feng

Joint work with Abderrahmane Nitaj and Yanbin Pan



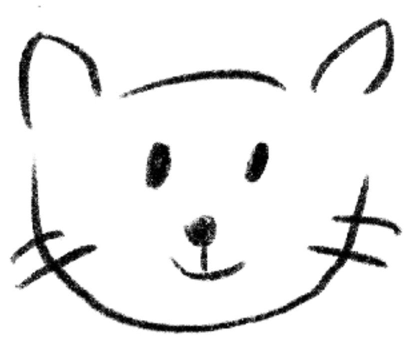
- Background
- Lattice-based Cryptanalysis: Coppersmith’s method
- Compute $\dim(\mathscr{L})$ & $\det(\mathscr{L})$
- Applications on Imogeny

Background

RSA Cryptosystem

$$ed \equiv 1 \mod \phi(N) \qquad \phi(N) = (p-1)(q-1)$$

Alice



Public Key: (N, e)

Bob

Secret Key: $(\phi(N)$, SMALL $d)$

Bob

Evil Bob wants to get the SECRET KEY!!!

To be more precise…

$$ed \equiv 1 \mod \phi(N)$$

$$\Downarrow$$

$$f(x_1, x_2) = x_1x_2 + (N+1)x_1 + 1 \equiv 0 \mod e$$ with the root $\left(\dfrac{ed-1}{\phi(N)}, -p-q\right)$

When $d < N^{0.25}$, it can be solved by Continued Fractions [Wie90] or Lattice [Cop96].

Coppersmith’s method

Coppersmith's method

Give bound X_j and $f \in \mathbb{Z}[x_1, \ldots, x_k]$ and modulus M, the goal is to find the small root $\mathbf{u} = (u_1, \ldots, u_k)$ with $u_j < X_j$, such that $f(\mathbf{u}) \equiv 0 \mod M$.

1. Construct $\{g_1, \ldots, g_n\}$ sharing common roots with f

2. Find <u>linear combinations</u> $h_1, \ldots, h_k$ whose norm less than M

$$h_j(\mathbf{u}) \equiv 0 \mod M \longrightarrow h_j(\mathbf{u}) = 0$$

Lattice Reduction

Coppersmith's method

Let $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n} \in \mathbb{R}^m$, the lattice $\mathscr{L}$ is

$$\mathscr{L} = \left\{ \mathbf{v} \in \mathbb{R}^m \mid \mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{v_i}, a_i \in \mathbb{Z} \right\}.$$

1. Use the coefficient vector of $g_j(x_1X_1, \ldots, x_kX_k)$ to construct $\mathscr{L}$

2. Find linear combinations $h_1, \ldots, h_k$ whose norm less than M

$$h_j(\mathbf{u}) \equiv 0 \mod M \longrightarrow h_j(\mathbf{u}) = 0$$

Lattice Reduction

Shorter vectors

$f(x_1, x_2) = x_1 x_2 + (N+1)x_1 + 1 \equiv 0 \mod e$ with the root $\left(\frac{ed-1}{\phi(N)}, -p-q\right)$

$X_1 = \log_e d$

$$d < e^{\frac{1}{4}} \approx N^{\frac{1}{4}}$$

$$\det(\mathscr{L})^{\frac{1}{\dim(\mathscr{L})}} < M^m \left(e^{\frac{\log_e d}{3}m^3 + \frac{1}{2}\frac{1}{6}m^3 + \frac{1}{3}m^3} < e^{\frac{1}{2}m^3}\right)$$

$\mathscr{L}$ has short vector $h_j(\mathbf{u}) \equiv 0 \mod e$ and $h_j(\mathbf{u}) = 0$

Compute $\dim(\mathscr{L})$ & $\det(\mathscr{L})$

$\mathscr{L}$ MUST satisfied $\det(\mathscr{L}) < M^{m \dim(\mathscr{L})}$.

In the Jochemsz-May Strategy, fix integer m and it holds that

$$\dim(\mathscr{L}) = |\{\lambda \,|\, \lambda \text{ is a monomial of } f^m\}|.$$

How to compute $\dim(\mathscr{L})$???

Manual calculation:

RSA Prime Leakage Attack: [Cop96,Cop97,BDF98,HM07,MNS22,FNP24…]

$f = x + 1$, the monomials of $f^m = \sum_{i=0}^{m} \binom{m}{i} x^i$ is $\{1, x, x^2, \ldots, x^m\}$

Manual calculation:

$f = x + 1$, the monomials of $f^m = \sum_{i=0}^{m} \binom{m}{i} x^i$ is $\{1, x, x^2, \ldots, x^m\}$

Small Private Key Attack: [BD99,EJMdW05,SM09,HM10,PHH+15,LZQ+23…]

$f = x_1x_2 + (N+1)x_1 + 1$, the number of monomials of f^m is

$$\sum_{i_1=0}^{m} \sum_{i_2=0}^{m-i_1} 1 = \frac{1}{2}m^2 + \frac{3}{2}m + 1 = \frac{1}{2}m^2 + o(m^2)\,.$$

Manual calculation:

$f = x + 1$, the monomials of $f^m = \sum_{i=0}^{m} \binom{m}{i} x^i$ is $\{1, x, x^2, \ldots, x^m\}$

$f = x_1(N + 1 + x_2) + 1$, the number of monomials of f^m is

$$\sum_{i_1=0}^{m} \sum_{i_2=0}^{m-i_1} 1 = \frac{1}{2}m^2 + \frac{3}{2}m + 1 = \frac{1}{2}m^2 + o(m^2)\,.$$

But how about $f = x_1^2 + a_1 x_1 x_2^2 + a_2 x_1 x_2 + a_3 x_1 + a_4 x_2^2 + a_5 x_2 + a_6$? 😈

Now time to you: HOW COULD YOU COMPUTE f^m?

Heuristic Method: Meers & Nowakowski, Asiacrypt'23

Heuristic: $\dim(\mathscr{L})$ equals a polynomial in m with degree k

$\Big\downarrow$ **Interpolation** at $m = 0, 1, \ldots, k$.

Compute $\dim(\mathscr{L})$

Manual calculation vs. Heuristic Interpolation:

$f = x_1 x_2 + (N+1)x_1 + 1$, the number of monomials of f^m is

$$\sum_{i_1=0}^{m} \sum_{i_2=0}^{m-i_1} 1 = \frac{1}{2}m^2 + \frac{3}{2}m + 1 = \frac{1}{2}m^2 + o(m^2)\,.$$

---

m	0	1	2
dim(L)	1	3	6

$$\dim(\mathscr{L}) = \frac{1}{2}m^2 + \frac{3}{2}m + 1 = \frac{1}{2}m^2 + o(m^2)\,.$$

It seems reasonable but is this Heuristic really CORRECT?

Counterexample

Consider $f = x^5 + x + 1$, is the number of monomials in f^m always a polynomial in m with degree 1???

m	0	1	2	3	4	5
dim(L)	1	3	6	10	15	20

- Interpolation at $m = 0,1 -> \dim(\mathscr{L}) = 2m + 1$
- Interpolation at $m = 1,2 -> \dim(\mathscr{L}) = 3m$
- Interpolation at $m = 2,3 -> \dim(\mathscr{L}) = 4m - 2$
- Interpolation at $m = 3,4 -> \dim(\mathscr{L}) = 5m - 5$
- Interpolation at $m = 4,5 -> \dim(\mathscr{L}) = 5m - 5$

No!!!

Fixed *Heuristic***:**

$\dim(\mathscr{L})$ equals a polynomial in m with degree k, for large enough m.

Is this correct now?

Fixed *Heuristic***:**

$\dim(\mathscr{L})$ equals a polynomial in m with degree k, for large enough m.

Is this correct now? Yes!

Theorem [FNP24]: $\dim(\mathscr{L})$ equals a polynomial in m with degree k, for large enough m.

"*Proof*" : $\dim(\mathscr{L})(m)$ is the dimension of some graded modular. Hence using Hilbert theorem, the Hilbert function becomes polynomial when m is large enough, which is called Hilbert polynomial.

Fixed *Heuristic*:

$\dim(\mathscr{L})$ **equals a polynomial in m with degree k, for large enough m.**

Is this correct now? Yes! For a 4-variable f, we sometimes need $m > 2^{300}$!

Proof : $\dim(\mathscr{L})(m)$ is the dimension of some graded modular. Hence using Hilbert theorem, the Hilbert function becomes polynomial when m is large enough, which is called Hilbert polynomial.

???

So I should to compute f^m for $m > 2^{300}$?! Impossible!!!

Newton polytope

As we just need the leading term/coefficient…

For $f = x_1x_2 + (N+1)x_1 + 1$, $\dim(\mathscr{L}) = \frac{1}{2}m^2 + o(m^2)$.

Newton polytope

As we just need the leading term/coefficient…

For $f = x_1(N + 1 + x_2) + 1$, $\dim(\mathscr{L}) = \sum_{i_1=0}^{m} \sum_{i_2=0}^{m-i_1} 1 = \frac{1}{2}m^2 + o(m^2)$.

Define $A(f) = \{(i_1, \ldots, i_k) \,|\, x_1^{i_1} \cdot \ldots \cdot x_k^{i_k}$ is a monomial of $f\}$. Eg. $x_1x_2 \mapsto (1{,}1)$

Theorem: $\dim(\mathscr{L}) = V(A(f))m^k + o(m^k)$.

Newton polytope

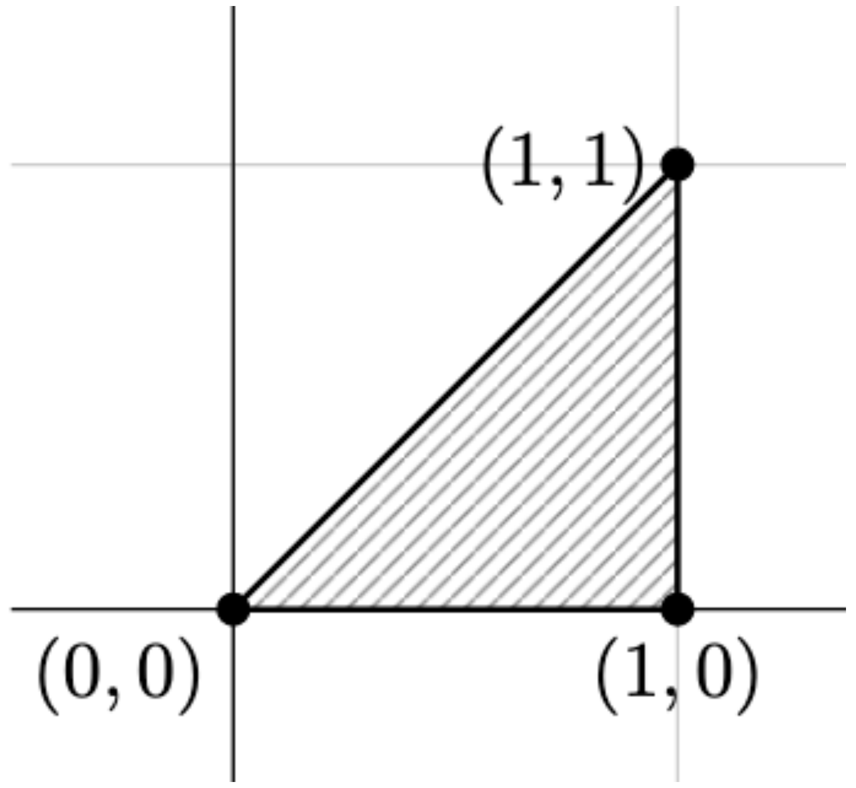
~~Manual calculation~~ 🤮

As we just need the leading term/coefficient…

For $f = x_1x_2 + (N+1)x_1 + 1$, $\dim(\mathscr{L}) = \sum_{i_1=0}^{m} \sum_{i_2=0}^{m-i_1} 1 = \frac{1}{2}m^2 + o(m^2)$.

Define $A(f) = \{(i_1, \ldots, i_k) \mid x_1^{i_1} \cdot \ldots \cdot x_k^{i_k}$ is a monomial of $f\}$.

Theorem: $\dim(\mathscr{L}) = V(A(f))m^k + o(m^k)$.



$$V(A(f)) = \frac{1}{2}.$$

Explicit formulas for $\dim(\mathscr{L})$ & $\det(\mathscr{L})$

Now $\det(\mathscr{L}) < M^{\dim(\mathscr{L})}$ can be written as

$$X_1^{\int_{N(f)} x_1\, dV} \cdot \ldots \cdot X_k^{\int_{N(f)} x_k\, dV} M^{\frac{k}{k+1}\int_{N(f)} 1\, dV} < M^{\int_{N(f)} 1\, dV},$$

where $N(\cdot)$ means the convex hull.

Good! What's the use?

Applications

Commutative Isogeny Hidden Number Problem

Definition (CI-HNP for CSURF):

Solve the following equations:

$$f_1(x_1, x_2, x_3) := x_1^2 + a_1x_1x_2^2 + a_2x_1x_2 + a_3x_1 + a_4x_2^2 + a_5x_2 + a_6,$$
$$f_2(x_1, x_2, x_3) := x_3^2 + b_1x_1^2x_3 + b_2x_1x_3 + b_3x_3 + b_4x_1^2 + b_5x_1 + b_6,$$

Manual calculation 🤮 Newton polytope 😄

$\dim(\mathscr{L}) = \dfrac{8}{3}m^3 + o(m^3)$ and $\det(\mathscr{L}) = X^{(2+\frac{5}{3}+\frac{3}{2})m^4+o(m^4)}M^{\frac{4}{3}m^4+o(m^4)}$.

Commutative Isogeny Hidden Number Problem

Definition (CI-HNP for CSURF):

Solve the following equations:

$$
\begin{aligned}
f_1(x_1, x_2, x_3) &:= x_1^2 + a_1 x_1 x_2^2 + a_2 x_1 x_2 + a_3 x_1 + a_4 x_2^2 + a_5 x_2 + a_6, \\
f_2(x_1, x_2, x_3) &:= x_3^2 + b_1 x_1^2 x_3 + b_2 x_1 x_3 + b_3 x_3 + b_4 x_1^2 + b_5 x_1 + b_6,
\end{aligned}
$$

Manual calculation 🤮 Newton polytope 😄

Improve the required MSBs in [MN23, Asiacrypt'23] and the concurrent work by Keegan Ryan (2024/1577).

Both [MN23] and [Rya24] require heuristic, but the Newton polytope approach doesn't!

Thanks for listening!

www.fffmath.com

Paper (2024/1330)