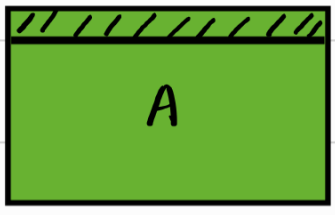
Part 3. Structured lattice Problem

previous : non-practical

reason : pk size, computations, etc.

e.g. hash fcn f_A

reading $A \in \mathbb{Z}_q^{n \times m}$ takes $nm \log_2 q > n^2$



n

m

$\log_2 q$: each # fits in $\log_2 q$ bits

- reduce size & speed-up computations : add structures

  ⇒ module variants of SIS & LWE

  + 2^n cyclotomic rings

§7. Mathematical Setting

7.1. Ring of polynomials

$\mathbb{Z}[x]$. $n = 2^k$ for $k \in \mathbb{N}$

quotient ring $R := \mathbb{Z}[x] / (x^n + 1)$

⇒ elements : mod $x^n + 1$

$x^n \equiv -1 \pmod{x^n + 1}$

A poly $f(x) = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1}$

coeffs $\tau(f) := (f_0, \cdots, f_{n-1})^T$

$\Rightarrow$ isomorphism $\tau: R \simeq \mathbb{Z}$ coefficient embedding.

Exp34 $n=4$. $f'(x) = -x^5 + x^4 + x^3 - 3x^2 + x + 2 \in \mathbb{Z}[x]$

In $\mathbb{Z}[x]/(x^4+1)$: $x^4 \equiv -1$

$f'(x) \equiv -x(-1) + (-1) + x^3 - 3x^2 + x + 2$

$\equiv x^3 - 3x^2 + 2x + 1 \pmod{x^4+1}$

let $g(x) = -2x^3 + 5$ in $\mathbb{Z}[x]/(x^4+1)$

$f(x) + g(x) = -x^3 - 3x^2 + 2x + 6$ still $\in \mathbb{Z}[x]/(x^4+1)$

For mult:

$f(x) \cdot g(x) = -2x^6 + 6x^5 - 4x^4 + 3x^3 - 15x^2 + 10x + 1$

$\equiv -2x^2(-1) + 6x(-1) - 4 \cdots$

$\equiv 3x^3 - 13x^2 + 4x + 5$

$f(x)g(x) \in R$: matrix-vector product $\mathrm{Rot}(f) \cdot \tau(g)$

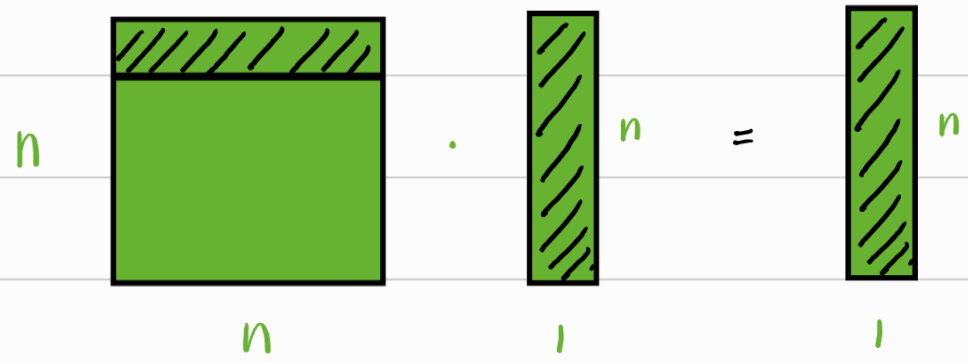
$\tau(g) := (g_0, \cdots, g_{n-1})^T \in \mathbb{Z}^n$

$$\mathrm{Rot}(f) = \begin{bmatrix} f_0 & -f_{n-1} & -f_{n-2} & -f_{n-3} & \cdots & -f_1 \\ f_1 & f_0 & -f_{n-1} & -f_{n-2} & & -f_2 \\ f_2 & f_1 & f_0 & -f_{n-1} & & -f_3 \\ f_3 & f_2 & f_1 & f_0 & \cdots & -f_4 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ f_{n-1} & f_{n-2} & f_{n-3} & f_{n-4} & & f_0 \end{bmatrix} \in \mathbb{Z}^{n \times n}$$

often called "negative cyclic" $\rightarrow$ NTT,

$f_i \rightarrow -f_i$ bc $x^n \equiv -1$

$\Rightarrow Rot(f) \cdot \tau(g)$



$= [f_0 g_0 - f_{n-1} g_1 - \cdots - f_1 g_{n-1},\ f_1 g_0 \cdots - f_2 g_{n-1},\ \cdots] \in \mathbb{Z}^n$

In Vadim's tutorial, this is explained in more details

$f \cdot g \bmod h = f \cdot (\sum_{i=0}^{n-1} g_i x^i) \bmod h$

$= \sum_{i=0}^{n-1} (f x^i \bmod h) g_i$

$i = 0 \quad (f \bmod h) g_0 = g_0 (f_0, f_1, \cdots, f_{n-1})$

$i = 1 \quad (fx \bmod h) g_1 = g_1 (-f_{n-1}, f_0, \cdots, f_{n-2})$

$\vdots$

$i = n-1 \quad (f x^{n-1} \bmod h) g_{n-1} = g_{n-1} (-f_1, -f_2, \cdots, f_0)$

thus for

degree $= 0$: $[f_0, -f_{n-1}, \cdots, -f_1] \begin{bmatrix} g_0 \\ \vdots \\ g_{n-1} \end{bmatrix}$

other degree similar.

$Rot(f) = \begin{bmatrix} v_{f \bmod h} & v_{fx \bmod h} & \cdots & v_{f x^{n-1} \bmod h} \end{bmatrix} \in \mathbb{Z}^{n \times n}$

$Rot(f) \cdot \tau(g) = [\cdots] \quad [\vdots] \quad \in \mathbb{Z}^n$

vectors over R

$\vec{f} = (f_j)_{j \in [d]}$, $\vec{g} = (g_j)_{j \in [d]}$ $\in R^d$, $d \in \mathbb{N}$

where f_j, g_j are poly.

inner product $\langle \vec{f}, \vec{g} \rangle$

$= f_1 g_1 + \cdots + f_d g_d \pmod h \in R$

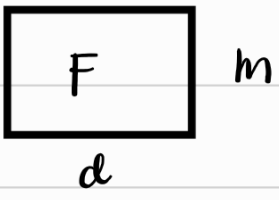
the coefficients of the result poly in $\mathbb{Z}^n$ is

$= Rot(f_1)\, \tau(g_1) + \cdots + Rot(f_d) \cdot \tau(g_d)$

$= [Rot(f_1) | \cdots | Rot(f_d)]_{n \times nd} \cdot \begin{bmatrix} \tau(g_1) \\ \vdots \\ \tau(g_d) \end{bmatrix}_{nd \times 1} \in \mathbb{Z}^n$

matrix over R

$F = (f_{kj})_{\substack{k \in [m] \\ j \in [d]}} \in R^{m \times d}$



$\vec{g} = (g_j)_{j \in [d]}$

matrix-vector product $F \cdot \vec{g}$

$$F \cdot \vec{g} = \begin{pmatrix} f_{11} & \cdots & f_{1d} \\ \vdots & & \\ f_{m1} & & f_{md} \end{pmatrix} \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_d \end{pmatrix}$$

(See next page)

$$= \begin{pmatrix} \sum_{i=1}^{d} f_{1i} g_i \\ \vdots \\ \sum_{i=1}^{d} f_{mi} g_i \end{pmatrix} \in R^m$$

The integer coefficient of this result poly vector is

$$= \underbrace{\begin{pmatrix} Rot(f_{11}) & \cdots & Rot(f_{1d}) \\ & \vdots & \\ Rot(f_{m1}) & \cdots & Rot(f_{md}) \end{pmatrix}_{mn \times dn}} \cdot \underbrace{\begin{pmatrix} \tau(g_1) \\ \vdots \\ \tau(g_d) \end{pmatrix}_{dn \times 1}}$$

$$\in \mathbb{Z}^{nm}$$

- Now. we can replace $A \in_r \mathbb{Z}_q^{m \times n}$ by some matrix in R by using above property.

Geometry

$\tau \longrightarrow$ a geometry on R

length / distance : $\|f\| := \|\tau(f)\|$

↳ standard l_2-norm.

- can extend to component-wise to vectors
- sample over $R \Leftrightarrow$ sample coe in poly independently in $\mathbb{Z}$.

e.g. sample each $c_i \in_r \mathbb{Z}$ or $\vec{c} \in_r \mathbb{Z}^n$.

choice of n

n: degree of cyclotomic poly x^n+1

$n = 2^k$ then x^n+1 is irreducible

→ guarantee R is an integral domain

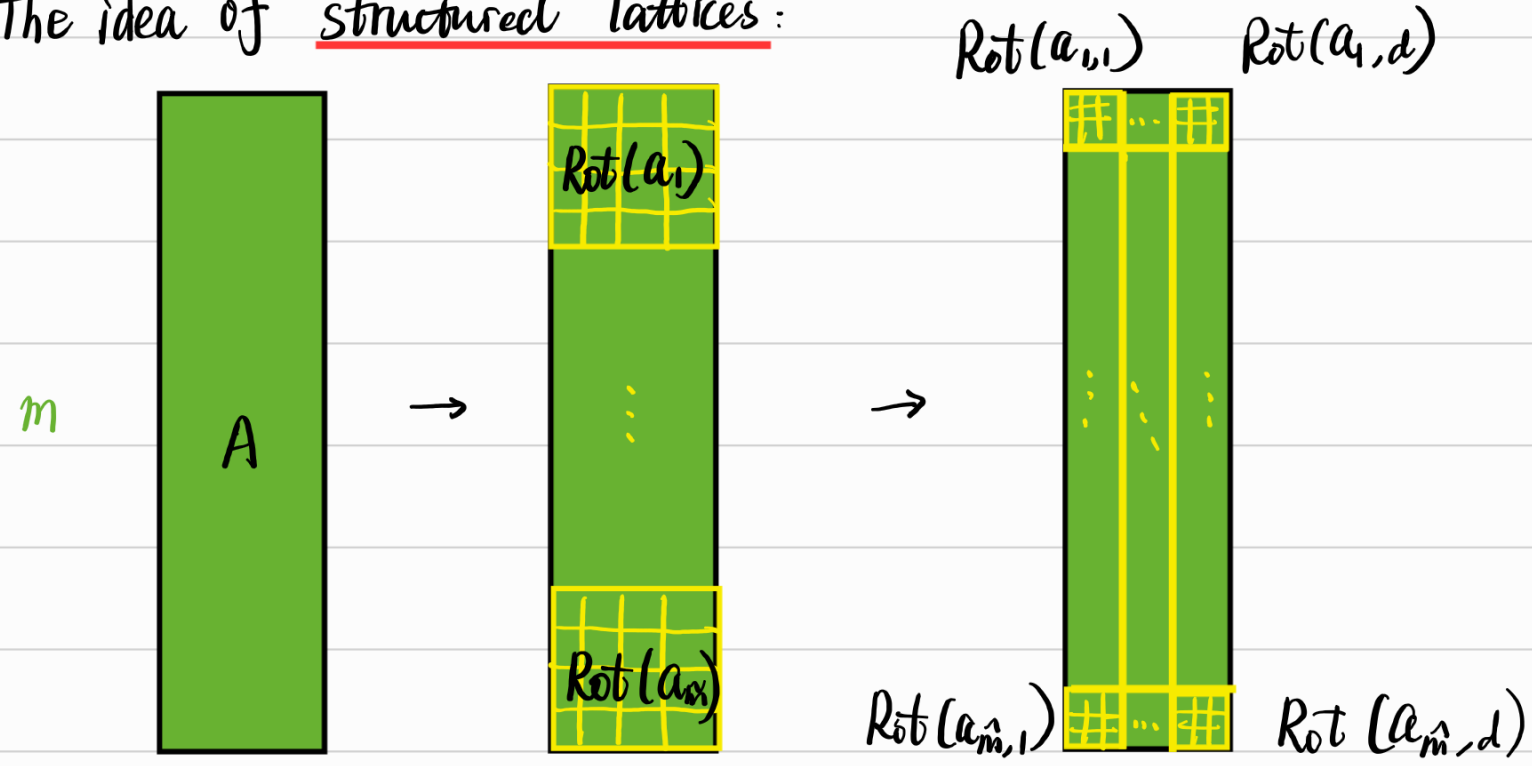
→ prevent attacks

also $2n$-th cyclotomic poly → int cyclotomic field.

→ good algebraic structure !

7.2 Module lattices

The idea of structured lattices:



Ideal Lattices

Ideal $\mathcal{I} \subseteq R$ is an additive subgroup of ring R that is $r \in R$, $x \in \mathcal{I}$, $rx \in \mathcal{I}$, $xr \in \mathcal{I}$.

(closed under mult by any ring element at both sides)

- using τ we can embed the ideal into $\mathbb{Z}^n$

subgroup → $\tau(\mathcal{I})$ is a lattice in $\mathbb{Z}^n$

additional ideal → $\tau(\mathcal{I})$ is a ideal lattice

e.g. x^i, $i \in [n-1]$ → always $\in R$

$y \in \mathcal{I}$, then $\|x^i y\| = \|y\|$

Note: mult monomial only shift coefts but not norm.

- Thus, $y \in \mathcal{I}$ → $y, yx, \dots, yx^{n-1} \in \mathcal{I}$

→ n L-indep vectors

$(\tau(y), \tau(yx), \dots \tau(yx^{n-1}))$

What if the switched coeff are the same? Collision?

- If we found one SV, then n L-indep SV

→ $\lambda_1(\tau(\mathcal{I})) = \dots = \lambda_n(\tau(\mathcal{I}))$

- Recall: for any lattice, $\exists$ reduction $\text{SIVP}_\gamma \to \text{SVP}_{\gamma\sqrt{n}}$
- In ideal lattice & $n = 2^k$, the reduction is improved by a factor $\sqrt{n}$

See 2.4 at the end.

Steib: $SIVP_\gamma \to SVP_{\gamma\sqrt{n}}$

Bang3: $GapSVP_\gamma \to SIVP_{n\gamma}$

Module lattice

Recall: module

ring R. mult iden 1.

left R-module ${}_R M$ consist of:

1) an abelian group $(M, +)$

2) an operation $\cdot : R \times M \to M$ st. for all $r, s \in R$, $x, y \in M$:

   a) $r \cdot (x+y) = r \cdot x + r \cdot y$

   b) $(r+s)x = r \cdot x + s \cdot x$

   c) $(rs) \cdot x = r \cdot (s \cdot x)$

   d) $1 \cdot x = x$

"$\cdot$" : scalar multiplication

Right R-mod M_R : $M \times R \to M$

· If R is commutative then L & R, R-mod. ⌟

(See next page)

interested : modules over $\mathcal{R}$

$\mathcal{M} \subseteq \mathcal{R}^d$, "." elements over $\mathcal{R}$

(In fact: K^d, K is the cyclotomic field to $\mathcal{R}$)

- ideals are modules for $d=1$
- $\tau(\mathcal{M}) \subset (\mathbb{Z}^n)^d = \mathbb{Z}^{nd}$

e.g. $\vec{a} = [a_1, \cdots, a_d] \in \mathcal{M}$, where $a_i = f_0^i + f_1^i x + \cdots + f_{n-1}^i x^{n-1}$

$\tau(a_i) = [f_0^i, \cdots, f_{n-1}^i] \in \mathbb{Z}^n$

$\tau(\vec{a}) = [f_0^1, \cdots, f_{n-1}^1, \cdots, f_{n-1}^d] \in \mathbb{Z}^{nd}$

- Similar to $\mathbb{I}$,

$\forall \vec{y} \in \mathcal{M}$. x^j for some $j \in [n-1]$

$x^j \vec{y}$ only shift. won't change norm.

- But $x^j \vec{y}$ only gives n L-ind vectors. not $n \cdot d$

Since $SIVP_\gamma \rightarrow SVP_{\gamma\sqrt{n}}$,

an oracle for Mod-SVP isn't enough to solve Mod-SIVP

Carnonical Embedding

In shoup's <Design of Hlib>, the maths perspective of this explains pretty well. I'll later use that to refresh this part.

Hardness of Ideal Lattice Problems

Structureed lattices: how hard?

module structure: not yet

ideal structure: yes Id-SVP

- wc to ac

[Gen09, Boe+20]: random lattices → ideal lattices.

- weakness of Id-SVP: param choices

e.g.

[Cra+16]: solve Id-SVP in quantum poly time.
for principle ideals of cyclotomic fields
↳ ideals generated by a single ring element.
& Gen from Gaussian.

[CDW21]: $\mathrm{Id\text{-}SVP}_\gamma$, $\gamma \approx 2^{\sqrt{d}}$, quantum

[Pan+21]: For some prime ideals + symmtric, Id-SVP in classical poly time.

[BGP22]: ↳ any ideals (prime factors are not ramified) over any # field.

[PHS19, BR20, Ber+21]: Id-SVP for all ideals of all # fields in exp time & w/ preprocessing.
(no better than lattice red alg)