8. Module Variants

8.1. Module SIS

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

$\mathcal{R}_q = \mathcal{R}/q\mathcal{R} = \mathbb{Z}_q[x]/(x^n+1)$

Def 35 Module-SIS

m. d. $q > 0$ $\mathbb{Z}$

$\beta > 0$ $\mathbb{R}$

Given m indep $\vec{a}_j$ sampled uniformly at random over $\mathcal{R}_q^d$, forming columns of $A \in \mathcal{R}_q^{d \times m}$

e.g.

$$A = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1d} & \cdots & a_{md} \end{pmatrix}_{d \times m}$$

$$(\vec{a}_1, \cdots, \vec{a}_m)$$

the problem M-SIS$_{d,q,\beta,m}$ asks to find a $\vec{z} \setminus \{\vec{0}\} \in \mathcal{R}^m$ of norm $0 < \|\vec{z}\| < \beta$ st.

$$A\vec{z} = \sum_{i=1}^{m} z_i \vec{a}_i = \vec{0} \mod q$$

- $n=1 \rightarrow \mathcal{R} = \mathbb{Z} \rightarrow$ plain SIS.
- $d=1 \rightarrow$ R-SIS

$$A = (a_1 \cdots a_m)_{1 \times m} = \vec{a}^T$$

$$A\vec{z} = \langle \vec{a}, \vec{z} \rangle$$

- R-SIS: PROB & LMOB, before M-LWE.
- Also, inhomo version & HNF ver for M-SIS.

Efficiency

$Rot(A) \in \mathbb{Z}_q^{nd \times nm}$

$$= \begin{pmatrix} Rot(a_{11})_{n\times n} & \cdots & Rot(a_{m1})_{n\times n} \\ \vdots & \ddots & \vdots \\ Rot(a_{1d})_{n\times n} & \cdots & Rot(a_{md})_{n\times n} \end{pmatrix}$$

→ $n\log_2 q$ bits to store!

rows: nd

columns: nm

} $\mathbb{Z}_q^{nd \times nm}$

- plain SIS: $(nd)(nm)\log_2 q$ bits to store
- M-SIS: $(ndm)\log_2 q$
- Also: FFT/NTT technique.

→ compute $z_i a_{ij}$ (poly × poly) in $O(n\log n)$

⇒ $A\vec{z}$ → compute in $O(dmn\log_2 n)$

Hidden structured Lattice

M-SIS (problem) defs an instance of Mod-SVP$_\gamma$ (problem) in random module lattice: (→ lattice)

$$\Lambda_q^\perp(A) = \{\vec{y} \in \mathcal{R}^m : A\vec{y} = \vec{0} \bmod q\}$$

γ depends on norm β.

L why not R_q^m? (Similar Q for MLWE)

Hardness

wc to ac for suitable params

Thm 36 (see Thm 20 for plain SIS)

$\forall m = poly(n)$, $d \in \mathbb{N}$, $\forall \beta > 0$, $\forall q \geq \beta \cdot poly(nd)$

Solving $M\text{-}SIS_{d,q,\beta,m}$ with n-ng proba is ALAHA solving $Mod\text{-}SIVP_\gamma$ on arbitary nd-dim module lattices w/ overwhelming proba, for some $\gamma = \beta \cdot poly(nd)$

e.g. [LS15] requires $q \geq \beta \cdot \sqrt{nd} \cdot \omega(\log nd)$

$\gamma \geq \beta \cdot \sqrt{nd} \cdot \omega(\sqrt{\log(nd)})$

8.2. Module LWE

[BGV12], [LS15]

Def 37 M-LWE

d. q. >0 ints. χ distr over $\mathcal{R}$. fixed secret $\vec{s} \in \mathcal{R}_q^d$

M-LWE distr $A_{\vec{s},\chi} \xleftarrow{r} \mathcal{R}_q^d \times \mathcal{R}_q$:

$\vec{a} \leftarrow U(\mathcal{R}_q^d)$, $e \leftarrow \chi$

out: $(\vec{a}, b = \langle \vec{s}, \vec{a} \rangle + e \mod q)$

Def 38 Search M-LWE

$m > 0$. Given m indep $(\vec{a}_i, b_i) \in \mathcal{R}_q^d \times \mathcal{R}_q$ from $A_{\vec{s},\chi}$ and $\vec{s} \xleftarrow{r} U(\mathcal{R}_q^d)$.

$search\text{-}MLWE_{d,q,\chi,m}$ asks to find $\vec{s}$

· usually write $A \in R_q^{m \times d}$ whose rows are given by $\vec{a}_i$.

$$A = \begin{pmatrix} \vec{a}_1 \to \\ \vec{a}_2 \to \\ \vdots \\ \vec{a}_m \to \end{pmatrix}$$

Def 39 decision MLWE

$m > 0$. Given m indep $(\vec{a}_i, b_i)$

$$\begin{cases} \text{either from} & A\vec{s}, \vec{x} \\ \text{or from} & U(R_q^d \times R_q) \end{cases}$$

★ different from M-SIS : $A \in R_q^{d \times m}$

dec-MLWE$_{d,q,\chi,m}$ asks to distinguish both cases w/ n-n prob.

· variants ✓ HNF form ✓ MLWR ✓

Hidden Structured Lattice

M-LWE → BDD (to module lattices) in

$$\Lambda_q(A) = \{\vec{y} \in R^m : \vec{y} = A\vec{s} \bmod q \text{ for some } \vec{s} \in R^d\}$$

$\vec{b}$: target point. $\vec{e} \leftarrow \chi^m$: distance.

Hardness

wc to ac

Thm 40 [LSIS] Thm 4.7.

For $\forall m = \text{poly}(n)$. modulus $q \le 2^{\text{poly}(n)}$. DGD χ of size $\alpha q \ge 2\sqrt{d} \cdot \omega(\sqrt{\log n})$ $(0 < \alpha < 1)$

solving (Search/decison) M-LWE$_{d,q,\chi,m}$ w/ nn

is ALAHA solving quantumly the problem Mod-GapSVP$_\gamma$ & Mod-SIVP$_\gamma$ on arbitrary nd dim module lattices with ow proba.

for some $\gamma = \tilde{O}(n\sqrt{d}/\alpha)$

- Later works:

[Bout20]: dequantized this red. (only work for Mod-GapSVP$_\gamma$ + large enough rank d)

[Bout22b]: χ unif $\{-\beta, \cdots, \beta\}^n$

[LWW20] [Bout22a]: entropic hardness.

[LS15]: M-LWE $\xrightarrow{\text{rd}}$ Mod-SIVP$_\gamma$ for 2^n cyclotomics

[WW19]: ↳ for all cyclotomics

other ring structures

$\mathbb{Z}[x]/f(x)$. not all $f(x)$ suitable (performance / security). see [Pei16].

8.3. Ring-LWE & R-SIS

- Recall

SIVP$_\gamma$ → SIS for $\beta = \gamma \cdot \lambda_n(\Lambda)$

BDD → SIVP$_\gamma$ → LWE for some params

- module variants: difference bet M-SIS & M-LWE

①

For consistency of notion, let $A \in R_q^{m \times d}$

M-SIS: $\Lambda_q^{\perp}(A^T)$

$A^T \in R_q^{d \times m} \rightarrow \vec{y} \in R_q^m : A\vec{y} = \vec{0} \bmod q$

M-LWE: $\Lambda_q(A)$

$A \in R_q^{m \times d} \rightarrow \vec{y} \in R_q^m :$

$\vec{y} = A\vec{s} \bmod q$ for some $\vec{s} \in R^d$

② $d=1$ → ring SIS/LWE

must: rank $m > 1$

if $m=1$

R-SIS: $ay = 0 \bmod q$, $a, y \in R_q$

no solution

decision R-LWE: vacuously hard

- wc to ae for rank 1

Id-SIVP $\not\equiv$ R-LWE / SIS

attacks vs. Id-SIVP $\not\equiv$ vs. R-LWE

less for M-LWE

8.4. "Subtle" over Number Fields

e.g. LHL.

In $\mathbb{Z}_q$: prime q → $\mathbb{Z}_q$ a field → non-0 ele is a unit

In R_q: prime q → may not be a field.

→ not every $\mathbb{Q}$ ele is a unit.

Sol 1: [LNW20] restricts to NF & modulus that R_q is a $\mathbb{F}$

↳ very strong

↳ may no q exists

eg. m-th CNF requires at least $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic.

2^n cyclotomics not the case

Sol 2: [Mic07] [Bou21] prove LHL from scratch

Sol 3: DGD & Smoothing params of R [RSW18]

8.5 Fiat-Shamir w/ Abort Signatures

① FS sig: ≈ lattice ver Schnorr sig.

Below: [GLP12] → Dilithium

② GPV approach: hash-then-sign

Setting

$R_q = \mathbb{Z}_q[x]/(x^n+1)$. $n = 2^k$. q prime. st. $q = 1 \bmod 2n$

(good for NTT).

For $k, \ell \in \mathbb{N}$, let $A \leftarrow U(R_q^{k \times \ell})$ pub shared.

ℓ: # of cols, k: # of rows → Const for diff sec level

let $H_c: \{0,1\}^* \to C$

$$C = \{c \in R : \|c\|_1 = d, \ \|c\|_\infty = 1\}$$

be a RO with d st. $|C| > 2^{2\lambda}$, λ = sec level

Let $s, \beta \in \mathbb{Z}$, msg space $\mathcal{M} = \{0,1\}^*$

We rely on key set $S_\beta = \{ a \in \mathcal{R} : \|a\|_\infty \leq \beta \}$

Let D a distr over $\mathcal{R}^{l+k}$ providing vectors with norm $\leq B$ → a rejection proba Pr_{rej}

Sig Sheme : $\Pi = (KGen, Sig, Vf)$

KeyGen(1^λ)

Sample $\vec{s} \leftarrow U(S_\beta^{l+k})$

set $sk = \vec{s}$

$A \in R_q^{k \times l}$

$vk = \vec{t} = [A \mid I_k] \cdot \vec{s} \in R_q^k$

return (sk, vk)

Sig(sk, m)

set $\vec{z} = \perp$

while $\vec{z} = \perp$ do:

samply $\vec{y} \leftarrow D$

set $\vec{u} = [A \mid I_k] \cdot \vec{y} \in R_q^k$

compute $c = H_c(\vec{u}, m) \in C$

set $\vec{z} = \vec{s} \cdot c + \vec{y}$

with proba $1 - Pr_{rej}$ set $\vec{z} = \perp$ } rejection sampling : to make $D_{\vec{z}} \neq D_{\vec{s}}$

↓

$\|\vec{z}\|_2 > B \Rightarrow$ reject

return $\sigma = (\vec{u}, \vec{z})$

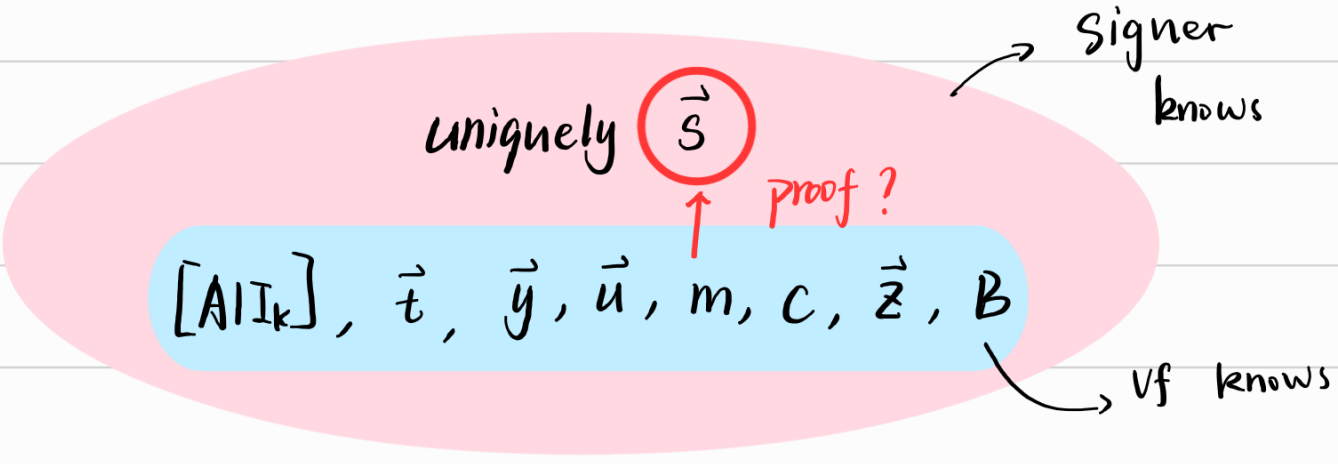
Vf (vk, σ, m)

re-construct $c = H_c(\vec{u}, m)$

if $\|\vec{z}\|_2 < B$ & $[A|I_k] \cdot \vec{z} = \vec{t} \cdot c + \vec{u}$

return 1

else return 0



$$[A|I_k]\vec{z} = [A|I_k](\vec{s} \cdot c + \vec{y})$$
$$= [A|I_k]\vec{s} \cdot c + [A|I_k]\vec{y}$$
$$= \vec{t} \cdot c + \vec{u}$$

- params β, d, B & Pr_{rej}
  → correct, secure, efficient.

Distr D

① DGD over R

② U over set of small norms

$> Pr_{rej}$ ✓ B ✓

e.g. For $D = D_s^{k+l}$, dGd of width s

B: from tail bound

Recall

Lemma 2]: Let $s>0$. $\vec{x} \in \mathbb{R}^n$.

then $Pr_{\vec{x} \leftarrow D_s}[\|\vec{x}\| > \sqrt{n}\, s] \le 2^{-n}$ ⌟

Pr_{rej}: $\min\left(1, D_s^{k+l}(\vec{z}) / M \cdot D_{\vec{c}\vec{s},s}^{k+l}(\vec{z})\right)$

where M is a const depending on β. ($\|\vec{s}\| < \beta$)

and d ($\|c\|_1 = d$)

Lattice Peculiarities

$\vec{s}, c, \vec{y}$ are all Short norm → $\vec{z}$ easy to leak info on $\vec{s}$ → thus, rejection sampling

- Save size → send c rather than $\vec{u}$

  Verify $H_c([A|I_k]\vec{z} - \vec{t}\cdot c, m) \stackrel{?}{=} c$

  ($[A|I_k]\vec{z} - \vec{t}\cdot c = \vec{u}$)

- reduce $k \to 1$ ($\to R_q^k$; c is a poly w/ 3 coefts)

  total bit length from $nk\log_2 q$ to $n\log_2 3$

Security.

- A high level proof of $\Pi = (KGen, Sig, Vf)$

Step 1

- Modify signing alg → doesn't depend on $\vec{s}$

origin: $\vec{z} = \vec{s} \cdot c + \vec{y}$ Now: $\vec{z} \leftarrow D$

$c = H_c(\vec{u}, m)$ $c \leftarrow U(C)$

only compute: $\vec{u} = [A|I_k]\vec{z} - \vec{t} \cdot c$

then: $H_c(\vec{u}, m)$

Δ With very small proba H_c has been queried on $(\vec{u}, m)$ before.

Step2

- Mod KeyGen → $\vec{s}$ from $S_{\beta'}^{l+k}$ with $\beta' > \beta$.

β': high proba of existing multiple sols for a given $\vec{t}$

Assuming hardness of M-LWE → both computationally close

If $(\vec{z}_1, c_1)$ & $(\vec{z}_2, c_2)$ for same msg & same $\vec{u}$

$\Rightarrow [A|I_k](\vec{z}_1 - c_1\vec{s} - \vec{z}_2 + c_2\vec{s}) = \vec{0}$

$\Rightarrow$ Solves M-SIS.

9. NTRU

9.1 NTRU Problem

[HPS98] : intro **NTRU**

↳ Number Theory Research Unit

- a problem over random q-ary module lattice → presumably qt resist
- reduction: see "On the hardness ..." by Alice & Damien in Asiacrypt 2021.

For NTRU, $\mathcal{R} = \mathbb{Z}[x]/(x^n-1)$, n is any prime.

denote $\mathcal{R}_q^\times$ the elements of $\mathcal{R}_q$ that are **invertible**

(i.e. for $f \in \mathcal{R}_q^\times$, $\exists f_q^{-1}$ st. $f \cdot f_q^{-1} = 1 \mod (x^n-1, q)$

Def 41 NTRU distribution

$q > 0$ int. χ distr over $\mathcal{R}_q$

fixed $f \in \mathcal{R}_q^\times$. NTRU distr $N_{f,\chi}$ over $\mathcal{R}_q$ is by

sample $g \leftarrow \chi$

output $h = g/f \in \mathcal{R}_q$

- f, g : small coeffs.

  but not f^{-1}, h

Def 42 Search NTRU

$\beta > 0 \in \mathbb{R}$. Given $h \in R_q$ from $N_{f,x}$.

find: $(z_1, z_2) \in \mathcal{R}^2$ st. $\begin{cases} z_1 + h z_2 = 0 \mod q \\ 0 < \|(z_1, z_2)\| \leq \beta \end{cases}$

- $\|(z_1, z_2)\|$: the norm of vector $[\tau(z_1) \mid \tau(z_2)]$
- quite like R-LWE in HNF

△ why not R-SIS? $A\vec{z} \equiv 0 \mod q \rightarrow A\vec{s} + \vec{e} \equiv 0 \mod q$

- Decision prob:

[LTV12]: "Decision Small Poly Ratio" (DSPR)

[Stel4]: "NTRU Decisional key Cracking"

Def 43 Decision NTRU

Given $h \in R_q$. decision-$NTRU_{q,x}$

distinguish: ① $h \leftarrow N_{f,x}$ for some random $f \in R_q^\times$

② $h \leftarrow U(R_q)$

Module variant.

[Chu+20]

old: sample ring elem g, f

new: matrices G, F

F invertible over R_q

→ output : $H = G \cdot F_q^{-1}$

Hidden Structured Lattice

search-NTRU (→ prob) defs an inst of SVP (→ prob) (mod lattice of (restriction) rank 2) in rd lattice (→ Λ)

$$\Lambda_q^{\perp}(h) = \{(z_1, z_2) \in \mathcal{R}^2 : h \cdot z_1 + z_2 = 0 \mod q\}$$

→ unique SVP

Multiple Samples

input : $h_1, \dots, h_t$

hidden lattice :

$$\Lambda_q^{\perp}(h_1, \dots, h_t) = \{(z_0, \dots, z_t) \in \mathcal{R}^{t+1} : h_j \cdot z_0 + z_j = 0 \mod q, \ \forall j \in [t]\}$$

- mult samples + same f + proper params → secure (for now)
- Small loss in concrete security. bc the gap in unique SVP gets slightly larger.

Hardness

- For $f, g \leftarrow dGd$ with $\sigma > \sqrt{q}$ (→ how large? depends on splitting degree.)

→ decision NTRU : vacuously hard [SS11]
(bc $N_{f,x}$ gets stat close to U)

- [DW21]

For overstretched params, NTRU solvable in poly time
↳ $q = \text{subexp}(n)$

but for crypto : smaller q. → no efficient attacks

- [PS 21]

variant of search NTRU → SVP over Id lattices

- Still open.

① Search to decision ?

② wc to ac reduction to decision NTRU?

NTRU to Ring-LWE

[Pei16a] : decision NTRU → search R-LWE

Given indep $h_i \in R_q$. fixed s. e_i

Input : (h_i, b_i) → Search RLWE Oracle → $\begin{cases} s \to \text{"NTRU"} \\ \text{else} \to \text{"Uniform"} \end{cases}$

$b_i = h_i \cdot s + e_i$

- if $h_i \leftarrow U(R_q)$, so will be (h_i, b_i) for RLWE → correct
- if $h_i \leftarrow g_i/f$, then $b_i = (g_i \cdot s)/f + e_i$

→ info of s is hidden (theoretically), if χ_e of RLWE is sufficiently larger than Secrete distr in NTRU

- possible hardness: Id-SVP or Mod SVP ($\geq$ rank 2)

  open problem: NTRU hardness

9.2. NTRU Encrypt

$n, p, q > 0$ ints. st. p, q prime & co-prime w eo

$L_f, L_g, L_\phi, L_m \subseteq \mathbb{Z}[x]/(x^n - 1)$

↳ commonly: coeffs in $\{-1, 0, 1\}$

& fixed Hamming weight.

elem in L_f: inv (mod p) & (mod q)

→ $\exists$ polys F_p, F_q, st. $f \cdot F_q = 1 \in R_q$

$f \cdot F_p = 1 \in R_p$

KeyGen

Sample $f \leftarrow U(L_f)$, $g \leftarrow U(L_g)$

compute F_p, F_q st. $f \cdot F_q = 1 \in R_q$

$f \cdot F_p = 1 \in R_p$

return $sk = (f, F_p)$

$pk = h = F_q \cdot g \in R_q$

Enc

msg $m \in L_m$

Sample $\phi \leftarrow U(L_\phi)$

return $c = p\phi h + m \in R_q$

Dec

return $m' = F_p \cdot (f \cdot c \bmod q) \bmod p$

correctness

$$f \cdot c \bmod q = f \cdot p\phi h + f \cdot m \bmod q$$
$$= p\phi g + fm \bmod q$$

→ coeffs all small. Can remove mod q

Actually, p is not small. don't know if this affects

$$F_p \cdot (f \cdot c \bmod q) \bmod p = F_p \cdot (p\phi g + fm) \bmod p$$
$$= F_p fm \bmod p$$
$$= m \bmod p$$

Security

No security reduction for NTRU Encrypt.

Analyse the sec by attacks

e.g. recover secret key → search NTRU → rank-2 SVP.