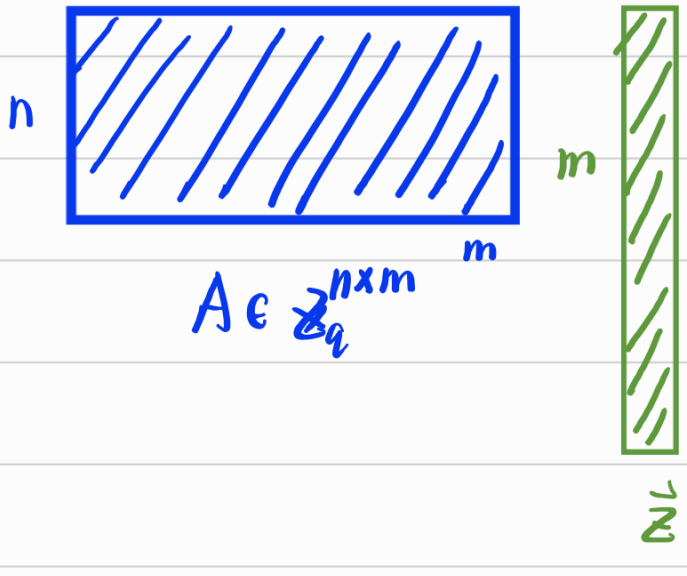
5. Learning with Errors

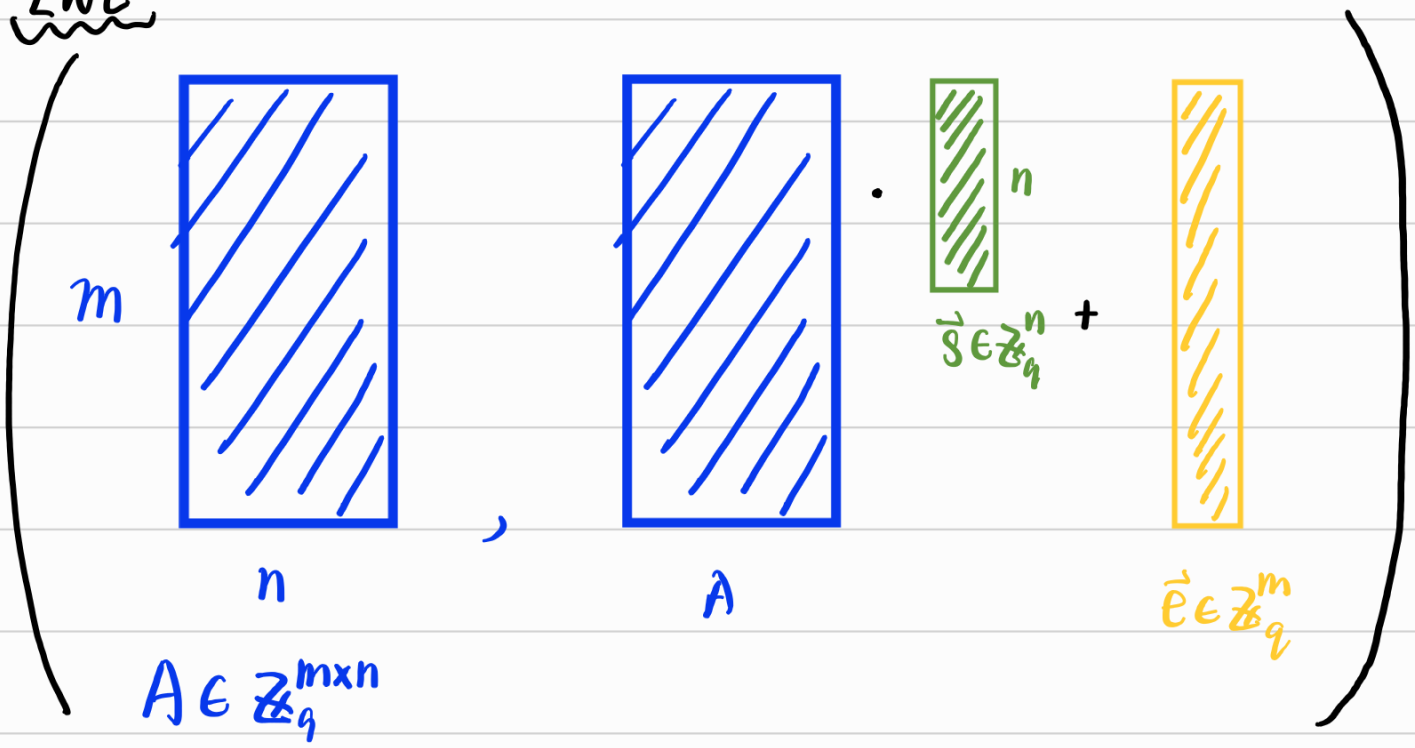
5.1. Definitions

SIS



$= \vec{0} \mod q$

LWE



→ find

Def 22 LWE distribution

$n, q > 0$ int

χ a distr over $\mathbb{Z}$

For a fixed secret $\vec{s} \in \mathbb{Z}_q^n$, the LWE distr $A_{\vec{s},\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is obtained by:

choosing $\vec{a} \leftarrow U(\mathbb{Z}_q^n)$, $e \leftarrow \chi$

outputting $(\vec{a}, b = \langle \vec{a}, \vec{s} \rangle + e \bmod q)$

$\vec{s}$: the secret

e : the noise / error of distr

LWE 2 variants : { search prob : find $\vec{s}$ (or $\vec{e}$)
decision : distinguish $A_{\vec{s},\chi}$ & U

Def 23 Search LWE

$m > 0$ int.

given m indep samples $(\vec{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from $A_{\vec{s},\chi}$ for a uniformly random $\vec{s} \in \mathbb{Z}_q^n$.

The problem search-LWE$_{n,q,\chi,m}$ asks to find $\vec{s}$.

- m's $(\vec{a}_i, b_i) \rightarrow (A \in \mathbb{Z}_q^{m \times n}, A\vec{s} + \vec{e} \bmod q)$

- Without e, easy. linear algebra.
  → e is the key point

Def 24. Decision LWE

$m > 0$ int

given m indep samples $(\vec{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$

that are either drawn from $\begin{cases} A_{\vec{s},\chi}, \vec{s} \\ \text{or} \quad U(\mathbb{Z}_q^n \times \mathbb{Z}_q) \end{cases}$

$\text{dec-LWE}_{n,q,\chi,m}$ asks to distinguish both cases with non-negligible advantage.

Parameters

B: bound of e from χ.

LWE harder ← B/q or dim n increases

m usually no large impact

(AGII: when $m \geq n^{2B+1}$. solve in time n^{2B})

$\begin{cases} \text{SIS}: \text{multiple sols} \\ \text{LWE}: \text{usually unique.} \end{cases}$

→ LWE is injective

Noise distribution $\vec{e}$

$\chi \longrightarrow$ hardness of the prob

if 1) $\chi \sim U(\mathbb{Z}_q)$ vacuously hard.

2) $\chi \sim$ Bernoulli(p) with small p of $= 1$

$\rightarrow$ easy to solve

「 $\vec{e}$ is a very sparse binary poly

e.g. $\vec{e} = [0\,0\,0\,0\,1\,0\,0\,0\,0\,\cdots\,0\,0\,0\,1\,0\,0\,0\,\cdots\,0]_m \in \mathbb{Z}_q^m$

$\Rightarrow$ lots of $\vec{a}_i \vec{s} + 0$ without noise

$\Rightarrow$ enough to solve. 」

- typical choice of χ :
  - a) small norm
  - b) enough entropy

$\Rightarrow$ often: discrete Gaussian distribution $D_{\mathbb{Z},\sigma}$

[More on §3.2]

- Practice. usually

$\chi \sim$ uniform over $\{-\beta, \cdots, \beta\}$ for small β such as 3

or $\sim$ binomial $\{-\beta, \cdots, \beta\}$, $\beta = 3$ for exp.

(e.g. kyber, Saber use centred bino distr)

Secret distribution $\vec{s}$

Standard: $U(\mathbb{Z}_q^n)$

other ok: Gaussian, $U(\mathbb{Z}_q^n)$ + small q.

- choice of distributions → efficiency, FHE

Hidden Lattices Problem

Review SIS: an instance of SVP_γ in random lattice

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

Now LWE: an instance of BDD in random lattice

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

Review: BDD

$\Lambda(B)$. n-dim. δ

point $\vec{t} \in \mathbb{R}^n = \vec{x} + \vec{e}$, $\vec{x} \in \Lambda(B)$, $\|\vec{e}\| \le \delta$

prob: find $\vec{x}$ (or $\vec{e}$)

For LWE, $\vec{b} = A\vec{s} + \vec{e} \equiv \vec{t}$

↳ the distance between $(\vec{t}, A\vec{s})$ given by χ^m.

(Re-) randomization

A fixed secret $\vec{s}$ (wc) → random secret $\vec{s}'$ (ac)

How? $A_{\vec{s},\chi} \to A_{\vec{s}+\vec{t},\chi}$

Given $(A, \vec{b})$, compute $(A, \vec{b} + A\vec{t}) = (A, A(\vec{s}+\vec{t}) + \vec{e})$

Also, can add randomness to $\vec{e}$ by $\vec{e}'$

→ $(A, A(\vec{s}+\vec{t}) + \vec{e} + \vec{e}')$

• rerand will increase the noise.

[Note: this happens A LOT in FHE]

Search-to-decision

Lemma 25

search-LWE & dec-LWE are computationally equivalent.

Reg05: prime moduli

Pes1ba: any moduli

Hermite Normal Form

Lemma 26.

HNF-LWE & LWE are computationally eq

Learning Parity with Noise (LPN)

[Regev 05, 09]

$q = 2$. $x \sim Ber(p)$ over $\{0,1\}$ → LWE ≡ LPN

• behaves differently

1) LWE: a geometric problem → lattice

e has small Euclidean norm. / small ℓ_p-norm

2) LPN: decoding prob distance between code words is measuring by Hamming distance.

★ A good research direction to understand LWE & LPN.

Learning with Rounding (LWR)

deterministic variant of LWE

- Advantage: $e \sim x$ no more.
- core: round element from $\mathbb{Z}_q$ to $\mathbb{Z}_p$

  where $p \leq q$

  ↳ so, from a large range to a smaller range.
- modular rounding function $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$

$$\lfloor x \rceil_p = \left\lfloor \frac{p}{q} \cdot x \right\rceil \bmod p$$

- component-wise / coefficient-wise ✓
- map back: $\mathbb{Z}_p \to \mathbb{Z}_q$

$$\left\lfloor \frac{q}{p} \cdot \lfloor x \rceil_p \right\rceil_q = x + e, \quad |e| \leq \frac{q}{p}$$

Proof.

$$\left\lfloor \frac{q}{p} \cdot \left(\left\lfloor \frac{p}{q} \cdot x \right\rceil \bmod p \right) \right\rceil \bmod q$$

$$= \left\lfloor \frac{q}{p} \cdot \left(\frac{p}{q} \cdot x + e_1 \right) \right\rceil \bmod q$$

$$= \frac{q}{p} \cdot \left(\frac{p}{q} x + e_1\right) + e_2$$

$$= x + \boxed{\frac{q}{p} e_1 + e_2}$$

$|e_1| \le 0.5 \rightarrow \left|\frac{q}{p} e_1\right| \le \left|\frac{1}{2} \cdot \frac{q}{p}\right|$

So, $|e_2|$ should be $\le \left|\frac{q}{2p}\right|$ to let $|e| \le \left|\frac{q}{p}\right|$.

which is a bit weird.

(I actually remember this conclusion from somewhere else. maybe back to this later)

- LWR: $(\vec{a}, b = \lfloor \langle \vec{a}, \vec{s} \rangle \rceil_p) \in \mathbb{Z}_q^n \times \mathbb{Z}_p$
- hardness on LWE

5.2. Discrete Gaussian Distribution

use: wc hardness LWE

lattice trapdoor functions

(spherical) Gaussian function

$s > 0$. $\vec{c} \in \mathbb{R}^n$. $\vec{x} \in \mathbb{R}^n$

spherical Gaussian function $\rho_{s,\vec{c}}$ & Gaussian Distr $D_{s,\vec{c}}$ of width s & center $\vec{c}$ as:

$$\rho_{s,\vec{c}}(\vec{x}) = e^{(-\pi \|\vec{x}-\vec{c}\|^2 / s^2)}$$

$$D_{s,\vec{c}}(\vec{x}) = \rho_{s,\vec{c}}(\vec{x}) \;/\; s^n$$

- if it's original-centered, $\vec{c} = \vec{0}$

2 important properties:

1) Tail bound

An element sampled from Gaussian distr has (with high pr) small norm.

2) Sum

The sum of 2 Gaussian is still a Gaussian

i.e. $D_s + D_t = D_{\sqrt{s^2+t^2}}$

Lemma 2]

$s > 0$. $\vec{x} \in \mathbb{R}^n$. then:

$$Pr_{\vec{x} \hookleftarrow D_s}\left[\|\vec{x}\| \geq \sqrt{n}\, s\right] \leq 2^{-n}$$

T Single element

$$Pr(x_i \geq s) \leq \frac{1}{2}$$

$$\Rightarrow Pr(\|\vec{x}\| \geq \sqrt{n}\, s) \leq 2^{-n} \quad \rfloor$$

Discrete Gaussian

$\Lambda \in \mathbb{R}^n$. $s > 0$. $\vec{c} \in \mathbb{R}^n$.

def dGd $D_{\Lambda,s,\vec{c}}$ by $D_{s,\vec{c}}$ with $\vec{x} \in \Lambda$

$$D_{\Lambda,s,\vec{c}}(\vec{x}) = \frac{D_{s,\vec{c}}(\vec{x})}{\sum_{\vec{y}\in\Lambda} D_{s,\vec{c}}(\vec{y})}$$

Smoothing Parameter

- dGd doesn't behave like countinous one.

Exp

$$D_{s,\vec{c}}(\vec{x}) = D_{s,\vec{0}}(\vec{x}-\vec{c})$$

but

$$D_{\Lambda,s,\vec{c}}(\vec{x}) = D_{\Lambda+\vec{c},\vec{s},\vec{0}}(\vec{x}-\vec{c})$$
$$\neq D_{\Lambda,\vec{s},\vec{0}}(\vec{x}-\vec{c})$$

- Sum of dGd will in general not be dGd any more.
- smoothing param → makes dGd like countinous.
- ↳ $\eta_\varepsilon(\Lambda)$: the smallest $s > 0$ st.

$$\rho_{1/s}(\Lambda^\vee \setminus \{\vec{0}\}) \leq \varepsilon$$

As $\rho_{1/s}$ is continous & strictly ↓ of s

→ so is η_ε

Lemma 28 (bound the smoothing param)

Λ. n-dim. $\varepsilon = e^{-n}$. it holds

$$\frac{\sqrt{n}}{\sqrt{\pi}\,\lambda_1(\Lambda^\vee)} \le \eta_\varepsilon(\Lambda) \le \frac{\sqrt{n}}{\lambda_1(\Lambda^\vee)}$$

Exp

For $\Lambda = \mathbb{Z}^n$. $\lambda_1(\Lambda^\vee) = 1$ thus

$$\sqrt{\frac{n}{\pi}} \le \eta_\varepsilon(\mathbb{Z}^n) \le \sqrt{n}$$

for $\varepsilon = e^{-n}$.

Lemma 30.

Λ. n-dim. For $\forall\, \varepsilon \in (0,1)$. $s \ge \eta_\varepsilon(\Lambda)$. $\vec{c} \in \mathbb{R}^n$.

We have:

$$\Pr_{\vec{x} \leftarrow D_{\Lambda,s,\vec{c}}}\left[\, \|\vec{x}-\vec{c}\| > s\sqrt{n} \,\right] \le \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n} \quad \text{(MR07)}$$

This note write it another way:

$$\rho_{s,\vec{c}}(\Lambda) \in \left[\frac{1+\varepsilon}{1-\varepsilon}, 1\right] \cdot \rho_s(\Lambda)$$

$\rho_{s,\vec{c}}(\Lambda) = \rho_s(\Lambda+\vec{c})$

Lemma 31 (useful property)

Λ. n-dim. $\varepsilon > 0$. $s > \eta_\varepsilon(\Lambda)$

Then the distribution of the coset $\vec{e} + \Lambda$, where $\vec{e} \leftarrow D_{s,\vec{0}}$, is within statistical distance $\varepsilon/2$ of the unif distr over coset of Λ:

$$\Delta(D_{s,\vec{c}} \bmod \mathcal{P}(B),\ U(\mathcal{P}(B))) \leq \varepsilon/2$$

Lemma 32

Λ, Λ' n-dim. $\Lambda' \subseteq \Lambda$

For $\forall\, \varepsilon \in (0, \frac{1}{2})$, $s \geq \eta_\varepsilon(\Lambda')$, $\forall\, uc \in \mathbb{R}^n$, the distribution of $(D_{\Lambda,s,\vec{c}} \bmod \Lambda')$ is within sd 2ε of uni distr over $(\Lambda \bmod \Lambda')$

- if $s,t > \eta_\varepsilon(\Lambda)$, the sum of dGd on the same lattice will also be a dGd:

$$D_{\Lambda,s} + D_{\Lambda,t} = D_{\Lambda,\sqrt{s^2+t^2}}$$

5.3. Hardness

- Recall: LWE defines an instance of BDD on random q-ary lattice

Thm 33

For $\forall m = poly(n)$, $\forall$ modulus $q \leq 2^{poly(n)}$

$\forall$ dGd χ of size $\alpha q \geq 2\sqrt{n}$, $\alpha \in (0,1)$

Solving (search / decision) $LWE_{n,q,\chi,m}$ with n-n Pr is ALAHA solving quantumly the problem $GapSVP_\gamma$ & $SIVP_\gamma$ on arbitrary n-dim lattices with overwhelming Pr, for some $\gamma = \tilde{O}(n/\alpha)$

- $\gamma \downarrow$ as $\alpha \uparrow$

▪ a bit confused about "quantumly". even with the explanation.

- Later: dequantiseed for GapSVP
- Thm 33 is only for: uniform $\vec{s}$ & dGd $\vec{e}$

  other distr for $\vec{s}$ & $\vec{e}$: various results
  - ↳ e.g. $\vec{s} \sim U([\beta]^n)$, β small

    $\vec{e} \sim \nearrow$ (bound on m for this one, m can't be too large. ow poly time attack)
  - ↳ as hard as the standard LWE

- BD20: entropic hardness

  LWE hard to solve for all $\vec{s}/\vec{e} \sim$ distr has enough min-entropy ▪ This might be interested to think deeper?

- In practice

Kyber : CBD

Frodo : approximations of rounded Gaussian distr

LAC : distr over ternary vectors with fixed Hamming weight.

- No hardness reductions exist

but is argued by the fact that no lattice-attack exploits the concrete structure of the distr, only the size of the resulting coefficients.

5.4 Interlude: Regev's PKE

5.4.1. Original description.

m, n, q : >0 int. χ distr. over $\mathbb{Z}$.

assume $\vec{s} \sim U(\mathbb{Z}_q^n)$. msg space $\in \{0,1\}$

to encrypt a single bit:

KeyGen: $\vec{s} \leftarrow U(\mathbb{Z}_q^n)$

$A \leftarrow U(\mathbb{Z}_q^{m \times n})$

$\vec{e} \leftarrow \chi^m$

return: $sk = \vec{s}$

$pk = (A, \vec{b}) = (A, A\vec{s} + \vec{e})$

Enc : msg $\nu \in \{0,1\}$

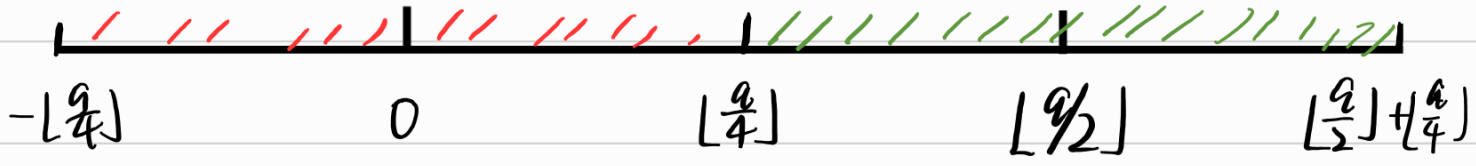
$\vec{r} \leftarrow U(\{0,1\}^m)$

$\vec{u} = A^T \vec{r}$ ($\vec{u}^T = \vec{r}^T A$)

$v = \vec{r}^T \vec{b} + \lfloor q/2 \rfloor \cdot \nu$

return : $(\vec{u}, v)$

Dec : compute $v - \vec{u}^T \vec{s}$ falls in :



$\nu' = 0$ $\Rightarrow \vec{r}^T \vec{e}$

$\nu' = 1$ $\Rightarrow \vec{r}^T \vec{e} + \lfloor \frac{q}{2} \rfloor$

Correctness

$$v - \vec{u}^T \vec{s} = \vec{r}^T \vec{b} + \lfloor q/2 \rfloor \cdot \nu - \vec{r}^T A \vec{s}$$
$$= \vec{r}^T (A\vec{s} + \vec{e}) + \lfloor q/2 \rfloor \cdot \nu - \vec{r}^T A \vec{s}$$
$$= \vec{r}^T \vec{e} + \lfloor q/2 \rfloor \nu$$

$\Rightarrow |\vec{r}^T \vec{e}| \leq \lfloor \frac{q}{4} \rfloor$

$\Rightarrow \|\vec{e}\| \in q/4\sqrt{m}$ (I can't remember which one is correct, $q/4$ or $q/8$. My derivation is $q/4$, maybe check later in Vadim's tutorial)

Thus, when x^m provides short noise elements of Eu norm $\leq q/4\sqrt{m}$ we have

$\begin{cases} v'=0 \rightarrow & v - \vec{u}^T\vec{s} \text{ closer to } 0 \\ v'=1 \rightarrow & \lfloor q/2 \rfloor \end{cases}$

Security

require: $m \geq 3(n+1)\log_2 q$

IND-CPA: game-based model

Game 0: IND-CPA game uses the above scheme.

Game 1: $\vec{b}$ isn't sampled honestly

instead: $U(\mathbb{Z}_q^m)$

- Assuming hardness of dec-LWE, G0 & G1 are computationally indistinguishable.

Game 2: $(\vec{u}, v)$ is replaced by a rd $(\vec{u}, v)$

Sampled over $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

- $(\vec{r}^T A, \vec{r}^T\vec{b}) = \vec{r}^T A'$, $A' = (A | \vec{b})$

As both $A, \vec{b}$ are random, so is A'.

Using Lemma 21 - LHL (in P2 SIS), $m \geq 3(n+1)\log_2 q$ ✓

$\Rightarrow \Delta((A'^T, A'^T\vec{r}), (A'^T, \vec{w})) \leq \varepsilon$

where $\vec{w} \leftarrow U[(\mathbb{Z}_q^n | \mathbb{Z}_q)]$

$\Rightarrow$ G1 & G2 IND.

Now: in G2, ct contains no info on msg

so the adv can only guess.

Dual Regev

GPV08 : possible to def a dual version of Regev encryption scheme.

- The role of LHL & LWE switched
- LHL for pk → uniform
  LWE for IND-CPA.

(TBC)