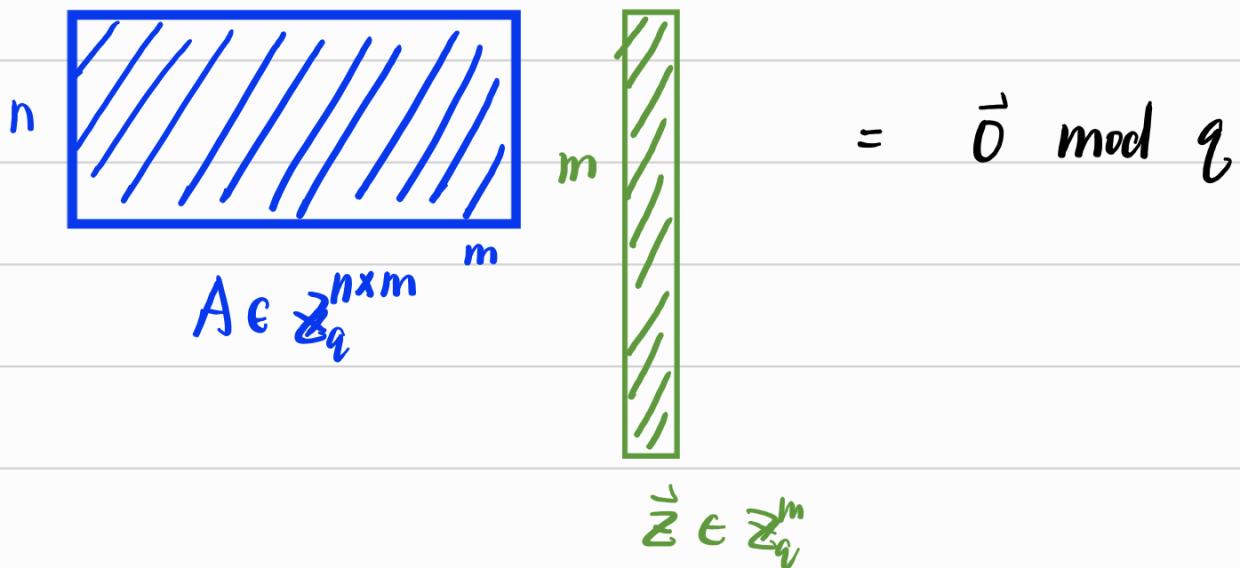


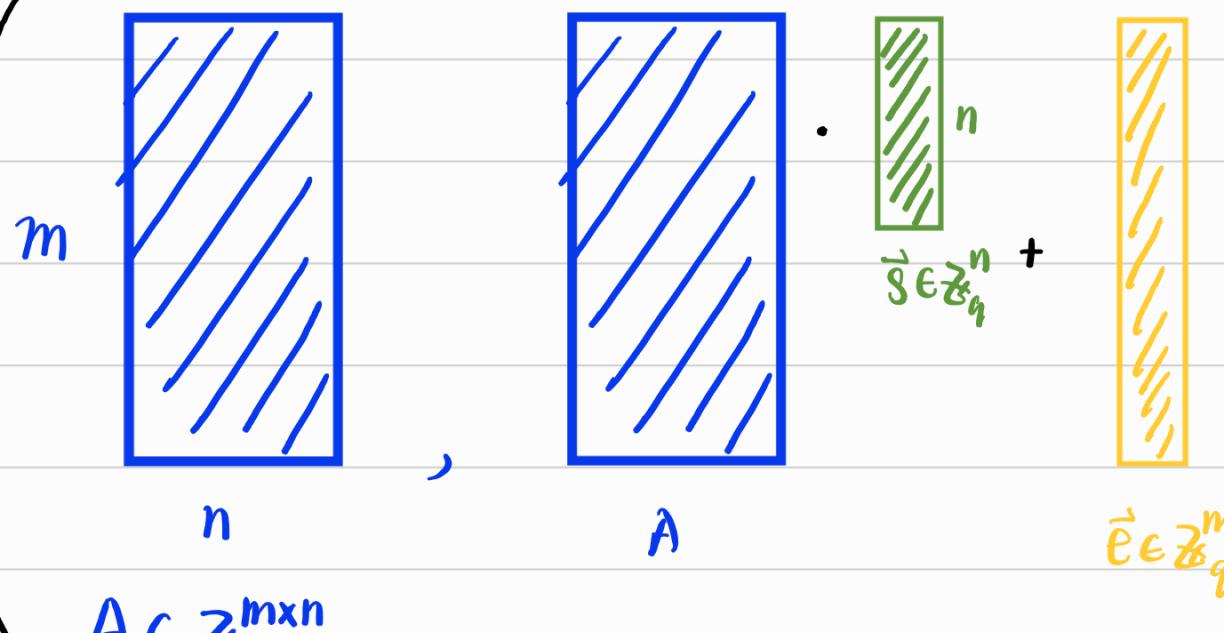
## 5. Learning with Errors

### 5.1. Definitions

SIS

$$\begin{array}{c} \text{A} \in \mathbb{Z}_q^{n \times m} \\ \vec{s} \in \mathbb{Z}_q^n \\ \vec{z} \in \mathbb{Z}_q^m \end{array} = \vec{0} \pmod{q}$$


LWE

$$\begin{array}{c} \text{A} \in \mathbb{Z}_q^{m \times n} \\ \vec{s} \in \mathbb{Z}_q^n \\ \vec{e} \in \mathbb{Z}_q^m \end{array}, \quad \vec{z} = \text{A} \cdot \vec{s} + \vec{e}$$


$$\text{A} \in \mathbb{Z}_q^{m \times n}$$

→ find

$$\begin{array}{c} \vec{s} \in \mathbb{Z}_q^n \\ \vec{z} \in \mathbb{Z}_q^m \end{array}$$

## Def 22 LWE distribution

$n, q > 0$  int

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

$\vec{s}$ : 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  $\text{Search-LWE}_{n, q, \chi, m}$  asks to find  $\vec{s}$ .

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

• Without  $e$ , easy. linear algebra.

→  $e$  is the key point

## Def 24. Decision LWE

$m > 0$  int

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

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

dec-LWE <sub>$n, q, x, m$</sub>  asks to distinguish both cases with  
non-negligible advantage.

## Parameters

$B$ : bound of  $e$  from  $X$ .

LWE harder  $\leftarrow B/q$  or dim  $n$  increases

$m$  usually no large impact

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

{ SIS : multiple sols

LWE: usually unique.

→ LWE is injective

## Noise distribution $\vec{e}$

$X \rightarrow$  hardness of the prob

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

2)  $X \sim \text{Bernoulli}(p)$  with small p of = 1  
→ easy to solve

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

e.g.  $\vec{e} = [000010000 \dots 0001000 \dots]_m \in \mathbb{Z}_q^m$

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

⇒ enough to solve. ↴

• typical choice of  $X$ :

a) small norm

b) enough entropy

⇒ often: discrete Gaussian distribution  $D_{\mathbb{Z}, 6}$

• Practice. Usually [More on 3.2 ]

$X \sim$  uniform over  $\{-\beta, \dots, \beta\}$  for small  $\beta$  such as 3

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

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

## Secret distribution $\vec{s}$

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

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

- choice of distributions  $\rightarrow$  efficiency, PHE

## Hidden Lattices Problem

$\top$  Review SIS : an instance of  $SVP_q$  in random lattice  
 $L_q^\perp(A) = \{\vec{y} \in \mathbb{Z}^m : A\vec{y} = \vec{0} \pmod{q}\}$

Now LWE : an instance of BDD in random lattice  
 $L_q(A) = \{\vec{y} \in \mathbb{Z}^m : \vec{y} = A\vec{s} \pmod{q} \text{ for some } \vec{s} \in \mathbb{Z}^n\}$

$\top$  Review : BDD

$L(B)$ , n-dim.  $\delta$

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

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

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

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

## (Re-)randomization

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

How?  $A\vec{s}, x \rightarrow A\vec{s} + \vec{t}, x$

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  $\vec{e}'$

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

- re-random will increase the noise.

↑ Note: this happens A LOT in FHE ]

Search-to-decision

Lemma 25

Search-LWE & dec-LWE are computationally equivalent.

Reg 05: prime moduli

Prob 1a: any moduli

Hermite Normal Form

Lemma 26.

HNF-LWE & LWE are computationally eq

Learning Parity with Noise (LPN)

[Regev 05, 09]

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

- behaves differently

1) LWE: a geometric problem  $\rightarrow$  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:  $e \approx x$  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  $L\lceil_p : \mathbb{Z}_q \rightarrow \mathbb{Z}_p$

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

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

$$\left[ \frac{q}{p} \cdot \lfloor x \rceil_p \right]_q = x + e, |e| \leq \frac{q}{p}$$

↑ Proof.

$$\begin{aligned} & \left[ \frac{q}{p} \cdot \left( \lfloor \frac{p}{q} \cdot x \rceil \bmod p \right) \right]_q \\ &= \left[ \frac{q}{p} \cdot \left( \frac{p}{q} \cdot x + e_1 \right) \right] \bmod q \end{aligned}$$

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

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

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

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

which is a bit weird.

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

- LWR:  $(\vec{a}, b = L<\vec{a}, \vec{s}>)_p \in \mathbb{Z}_q^n \times \mathbb{Z}_p$
- 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  $p_{s, \vec{c}}$  & Gaussian Distr  
 $D_{s, \vec{c}}$  of width  $s$  & center  $\vec{c}$  as:

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

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

- 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

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

### Lemma 27.

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

$$\Pr_{\vec{x} \sim D_s} [\|\vec{x}\| \geq \sqrt{n}s] \leq 2^{-n}$$

T Single element

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

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

## 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 continuous one.

Exp

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

but

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

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

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

As  $P_{1/S}$  is continuous & strictly  $\downarrow$  of  $s$

$\rightarrow$  so is  $\eta_\varepsilon$

Lemma 28 (bound the smoothing param)

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

$$\frac{\sqrt{n}}{\sqrt{n} \lambda_1(\Lambda^\vee)} \leq \eta_\varepsilon(\Lambda) \leq \frac{\sqrt{n}}{\lambda_1(\Lambda^\vee)}$$

Exp

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

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

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

Lemma 30.

$\mathcal{L}$ . n-dim. For  $t \in (0, 1)$ .  $s \geq \eta_\varepsilon(\Lambda)$ .  $\vec{c} \in \mathbb{R}^n$ .

We have :

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

This note write it another way:

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

$$p_{s, \vec{c}}(\Lambda) = p_s(\Lambda + \vec{c})$$

### Lemma 31 (useful property)

$\Lambda$ . n-dim.  $\mathcal{E} \geq 0$ .  $s \geq \eta_{\mathcal{E}}(\Lambda)$

Then the distribution of the coset  $\vec{e} + \Lambda$ , where  $\vec{e} \in D_{s, \vec{c}}$ , is within **statistical distance**  $\varepsilon/2$  of the uniform distribution over cosets of  $\Lambda$ :

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

### Lemma 32

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

For  $t \in (0, \frac{1}{2})$ ,  $s \geq \eta_{\mathcal{E}}(\Lambda')$ ,  $t \in \mathbb{R}$ ,

the distribution of  $(D_{\Lambda, s, \vec{c}} \bmod \Lambda')$  is within  $\varepsilon/2$  of uniform distribution over  $(\Lambda \bmod \Lambda')$

- if  $s+t > \eta_{\mathcal{E}}(\Lambda)$ , the sum of ddist on the **same lattice** will also be a ddist:

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

### 5.3. Hardness

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

### Thm 33

For  $t^m = \text{poly}(n)$ .  $t$  modulus  $q \leq 2^{\text{poly}(n)}$

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

Solving (search/decision)  $LWE_{n,q,x,m}$  with  $n-n$  Pr is  
ALAH A solving quantumly the problem  $\text{GapSVP}_r$  &  
 $\text{SIVP}_r$  on arbitrary  $n$ -dim lattices with overwhelming  
Pr, for some  $\gamma = \tilde{\Theta}(n/\alpha)$

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

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

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

other distr for  $\vec{s}$  &  $\vec{e}$ : Various results

↳ e.g.  $\vec{s} \sim U(\mathbb{B}^n)$ ,  $\beta$  small

$\vec{e} \sim \uparrow$  (bound on  $m$  for this one,

$m$  can't be too large. or 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 interesting 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: Regen's PKE

### 5.4.1. Original description.

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

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

to encrypt a single bit:

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

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

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

return:  $sk = \vec{s}$

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

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

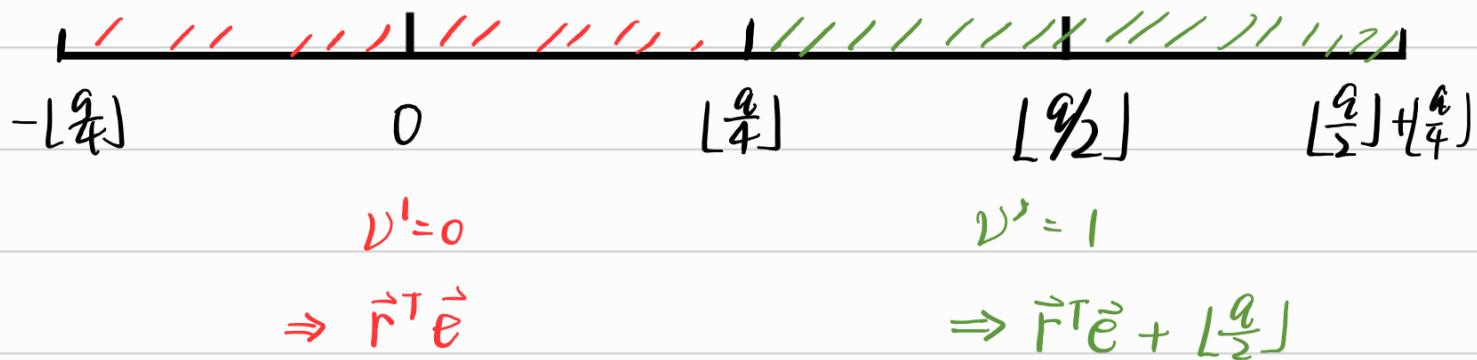
$$\vec{r} \leftarrow U(\{0,1\}^m)$$

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

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

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

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



Correctness

$$\begin{aligned} V - \vec{u}^T \vec{s} &= \vec{r}^T \vec{b} + \lfloor \frac{q}{2} \rfloor \cdot V - \vec{r}^T A \vec{s} \\ &= \vec{r}^T (A \vec{s} + \vec{e}) + \lfloor \frac{q}{2} \rfloor \cdot V - \vec{r}^T A \vec{s} \\ &= \vec{r}^T \vec{e} + \lfloor \frac{q}{2} \rfloor V \end{aligned}$$

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

$$\Rightarrow \|\vec{e}\| \leq \frac{q}{4\sqrt{m}}$$
 (I can't remember which one is

correct,  $\frac{q}{4}$  or  $\frac{q}{8}$ . My derivation is  $\frac{q}{4}$ , maybe check later in Vadim's tutorial)

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

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

## Security

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

IND-CPA : Game-based model

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

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

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

- 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),  $m \geq 3(h+1) \log_2 q \vee$

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

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

$\Rightarrow G1 \& G2 \text{ IND.}$

**Now :** in G2, ct contains no info on msg  
so the adv can only guess.

## Dual Regen

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

- The role of LHL & LW $\bar{E}$  switched
- LHL for pk  $\rightarrow$  uniform  
LW $\bar{E}$  for IND-CPA.

(TBC)

### 3.4.2. A better template

- prev: LHL + comp asp

- only CP asp?

→ OK. but  $\vec{s}$  to be short.

- Simplicity:  $m=n$ , then  $A \in \mathbb{Z}^{n \times n}$  is quadratic

Key Gen:  $A \leftarrow U(\mathbb{Z}_q^{n \times n})$

$\vec{s}, \vec{e} \leftarrow x^n$

return:  $sk = \vec{s}$

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

Enc: For  $v \in \{0,1\}$ .

$\vec{r}, \vec{f} \leftarrow x^n$

$f' \leftarrow x$

$$\vec{u} = A^T \vec{r} + \vec{f} \rightarrow \vec{u}^T = \vec{r}^T A + \vec{f}^T$$

$$v = \vec{r}^T \vec{b} + f' + \lfloor q/2 \rfloor \cdot v$$

Dec: CP  $v - \vec{u}^T \vec{s}$

$\approx 0$  then  $v = 0$

$\approx \lfloor q/2 \rfloor$  then  $v = 1$

### Correctness

$$v - \vec{u}^T \vec{s} = \vec{r}^T \vec{b} + f' + \lfloor q/2 \rfloor \cdot v - (\vec{r}^T A + \vec{f}^T) \vec{s}$$

$$= \vec{r}^T \vec{e}^T + f' - \vec{f}^T \vec{s} + \lfloor q/2 \rfloor v$$

$$v=0 \rightarrow \vec{r}^T \vec{e}^T + f' - \vec{f}^T \vec{s}$$

$$U=1 \rightarrow \vec{r}^T \vec{e}^T + f' - \vec{f}^T \vec{s} + \lfloor \varepsilon/2 \rfloor$$

Assume elements from  $x$  has bound on norm

$$\|x\| \leq B$$

$$2nB^2 + B < \frac{\varepsilon}{4}$$

Again, I have to check another note

I may remember / understand

Something wrong

$$\begin{aligned} \Rightarrow |\vec{r}^T \vec{e} - \vec{f}^T \vec{s} + f'| &\leq \|\vec{r}\| \cdot \|\vec{e}\| + \|\vec{f}\| \cdot \|\vec{s}\| \\ + |f'| &\leq (\sqrt{n}B)^2 + (\sqrt{n}B)^2 + B \leq \frac{\varepsilon}{4} \end{aligned}$$

More msg bits

msg  $m$  has  $K = \text{poly}(n)$  bits

replace  $\vec{r}$  &  $\vec{f}$  by  $R, F \in \mathcal{X}^{n \times k}$

$$\Rightarrow U = A^T R + F, \quad U^T = R^T A + F^T$$

$$\vec{v} = R^T \vec{b} + \vec{f}' + \lfloor \varepsilon/2 \rfloor \cdot m$$

Security

HNF - LWE.

G0, G1: uniform  $\vec{b} \rightarrow A \vec{s} + \vec{e}$  &  $\vec{b}$  IND.

G2:

$(\vec{r}^T A + f^T, \vec{r}^T \vec{b} + f')$  defns another LWE with

secrets  $\vec{r}$ , pk  $(A, \vec{b})^T$ , noise  $(\vec{f}, f')$

thus previous res applies  $\rightarrow$  G2 IND.

## Improvements

- Use  $\vec{A}$  more compact random seed  
| a PRF

$$\rightarrow A = \text{PRF}(\text{seed}_A)$$

- efficient: saves storage

(bc: send  $\text{seed}_A$  rather than full  $A$ )

- More important: PKE  $\rightarrow$  KEM

e.g. Frodo.

## b. Connection between SIS & LWE

### Decision LWE to Search SIS

- Use: dual attacks [APS15]

Given LWE instance  $(A, \vec{b}) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n$

Forward  $A$  to an SIS-oracle

↳ output a short non-0  $\vec{z} \in \mathbb{Z}^n$ ,

$$\|\vec{z}\| < \beta, \text{ s.t. } \vec{z}^T A = \vec{0} \pmod{q}$$

Now one can compute  $\vec{z}^T \vec{b}$

If  $(A, \vec{b})$  is indeed a LWE instance, then:

$$\vec{z}^T \vec{b} = \vec{z}^T (A \vec{s} + \vec{e})$$

$$= \vec{z}^T \vec{e}$$

and  $|\vec{z}^T \vec{e}| \leq \underbrace{\|\vec{z}\| \cdot \|\vec{e}\|}$

↳ both short

Thus, if  $\vec{z}^T \vec{b}$  short, guess LWE.

If  $\vec{b}$  is univ. rd. so will  $\vec{z}^T \vec{b}$  be. thus not short.

## Duality between Knapsack & LWE

Search / decision  $K_S \xleftarrow{\text{reduce}} \text{search/decision LWE}$

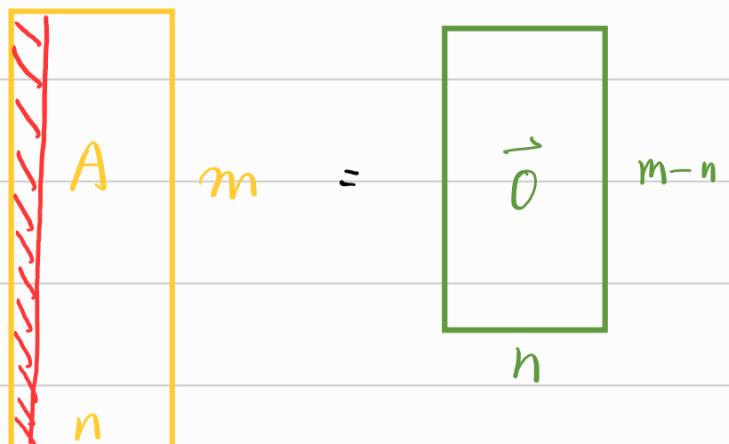
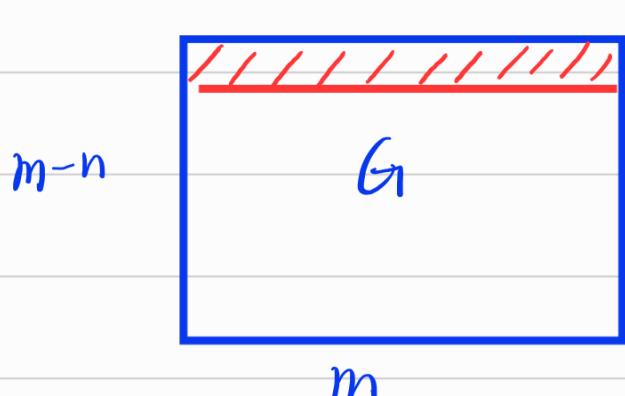
• "syndrome decoding".

•  $A \leftarrow U(\mathbb{Z}_q^{m \times n})$  for sufficiently large  $m$   
↳  $m \geq n + w(\log n)$

→  $A$  highly possible be a non-singular matrix.

(invertible)

The rows of  $A$  generate  $\mathbb{Z}_q^n$  M a bit confused w/ this sentence.  
 $G \in \mathbb{Z}_q^{(m-n) \times m}$  st.  $GA = \vec{0} \in \mathbb{Z}_q^{(m-n) \times n}$



- the column of  $G_1$  generates  $\mathbb{Z}_q^{m-n}$
- randomize  $G_1$  by  $UG$ , where  $U$  is a unimodular matrix  
( same lattice )

•  $(A, \vec{b})$  LWE

• transform this to  $(G, \vec{t})$  where  $\vec{t} = G\vec{b}$

If  $\vec{b} \sim_{uni} \rightarrow \vec{t} \sim_{uni}$

If  $\vec{b} = A\vec{s} + \vec{e} \rightarrow \vec{t} = G\vec{e}$

⇒ The noise distr in LWE → the secret distr in KS.  
( other direction similar )

### Quantumly SIS to LWE

Step 09: duality connection between  $q$ -ary lattice  $\Lambda_q(A)$

and  $\Lambda_q^\perp(A)$  to show a quantum reduction from SIS  
to search-LWE ■ need a further look at the paper

open prob: classical reductions.