3.4.2. A better template

- prev: LHL + comp asp
- only cp asp?

→ ok. but $\vec{s}$ to be short.

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

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

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

return: $sk = \vec{s}$

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

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

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

$f' \leftarrow \chi$

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

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

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

~ 0 then $\nu' = 0$

$\sim \lfloor q/2 \rfloor$ then $\nu' = 1$

Correctness

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

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

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

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

Assume elements from χ has bound on norm

$\|\chi\| \leq B$

$2nB^2 + B < q/4$

Again, I have to check another note

I may remember / understand

something wrong

$\Rightarrow |\vec{r}^T \vec{e} - \vec{f}^T \vec{s} + f'| \leq \|\vec{r}\| \cdot \|\vec{e}\| + \|\vec{f}\| \cdot \|\vec{s}\|$

$+ |f'| \leq (\sqrt{m} B)^2 + (\sqrt{m} B)^2 + B \leq q/4$

More msg bits

msg m has $k = poly(n)$ bits

replace $\vec{r}$ & $\vec{f}$ by $R, F \leftarrow \chi^{n \times k}$

$\Rightarrow \begin{cases} U = A^T R + F, & U^T = R^T A + F^T \\ \vec{v} = R^T \vec{b} + \vec{f}' + \lfloor q/2 \rfloor \cdot m \end{cases}$

Security

HNF - LWE.

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

G2:

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

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

thus previous res applies → G2 IND.

Improvements

- use a more compact random seed
  - a PRF

→ $A = PRF(seed_A)$

- efficient: saves storage

(bc: send $seed_A$ rather than full A)

- More important: PKE → KEM

e.g. Frodo.

b. Connection between SIS & LWE

Decision LWE to Search SIS

- use: dual attacks [APS15]

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

Forward A to an SIS-oracle

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

$\|\vec{z}\| < \beta$, st. $\vec{z}^T A = \vec{0} \bmod q$

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 uniform, so will $\vec{z}^T \vec{b}$ be. thus not short.

Duality between Knapsack & LWE

search / decision Ks $\xleftarrow{\text{reduce}}$ search / decision LWE

- "syndrome decoding".
- $A \leftarrow U(\mathbb{Z}_q^{m \times n})$ for sufficiently large m

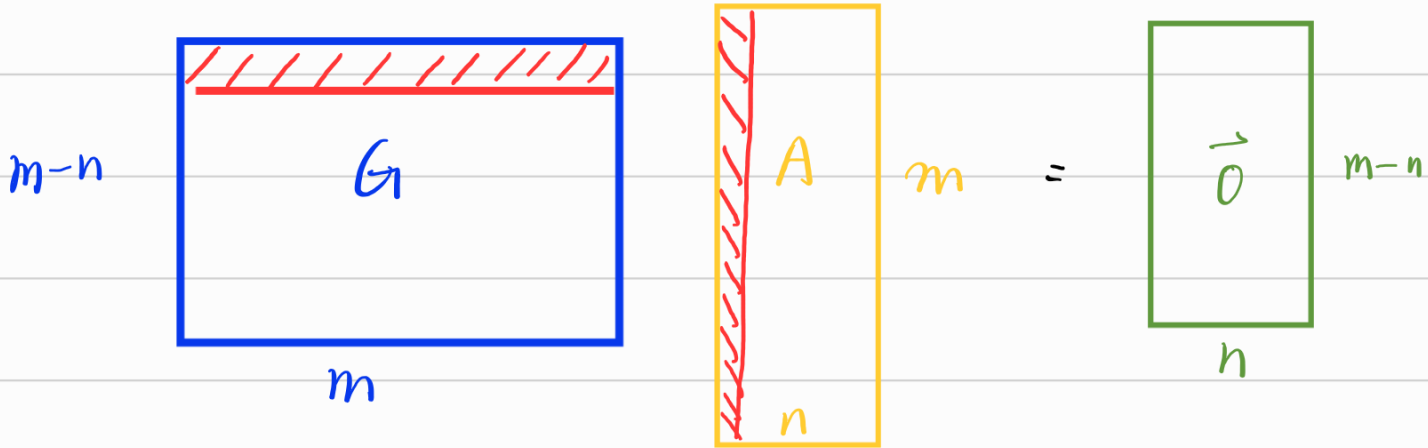
  ↳ $m \geq n + \omega(\log n)$

→ A highly possible be a non-singular matrix.

(invertible)

The rows of A generate $\mathbb{Z}_q^n$ 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 generates $\mathbb{Z}_q^{m-n}$

- radomize G 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 $\vec{b}$ uni → $\vec{t}$ uni

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

⇒ The noise distr in LWE → the secret distr in ks.

(other direction similar)

Quantumly SIS to LWE

Ste+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 futher look at the paper

open prob: classical reductions.