DECISIONAL LWE ASSUMPTION

$A = a_{11} s_1$

$$14 s_1 + 5 s_2 + 10 s_3 + 2 s_4 + e_1 = 8 \pmod{17}$$

$$13 s_1 + 14 s_2 + 14 s_3 + 6 s_4 + e_2 = 0 \pmod{17}$$

$$6 s_1 + 10 s_2 + 13 s_3 + 15 s_4 + e_3 = 2 \pmod{17}$$

$$6 s_1 + 7 s_2 + 16 s_3 + 5 s_4 + e_4 = 3 \pmod{17}$$

$$8 s_1 + 5 s_2 + 12 s_3 + s_4 + e_5 = 2 \pmod{17}$$

4 columns

6 rows

$$A = \begin{bmatrix} 14 & 5 & 10 & 2 \\ 13 & 14 & 14 & 6 \\ 6 & 10 & 13 & 15 \\ 6 & 7 & 16 & 5 \\ 8 & 5 & 12 & 1 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{bmatrix} = \begin{bmatrix} 8 \\ 0 \\ 2 \\ 3 \\ 2 \end{bmatrix}$$

$\vec{s}$ $\vec{e}$ $\vec{b}$

LWE assumption :

q : "large" prime

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

$s \leftarrow \mathbb{Z}_q^{n \times 1}$

$e \leftarrow \{0,1,-1\}^{m \times 1}$

$\vec{b} = A\vec{s} + \vec{e}$

Output $(A, \vec{b})$.

$\boxed{\text{Search}}$: No PPT Adv can, given $(A, \vec{b})$ output any $\vec{s}$ s.t. $A\vec{s} \approx b$.

[$A\vec{s} \approx b$ means $A\vec{s} - \vec{b}$ has all entries in $\{0,1,-1\}$]

Note

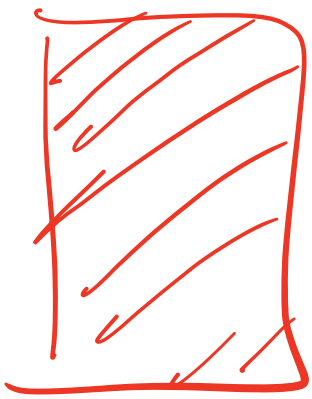
$\boxed{\text{Decision}}$: $(A, \vec{b}) \to q^n$ possib.

$\approx (A, \vec{u}) \to q^m$ possib.

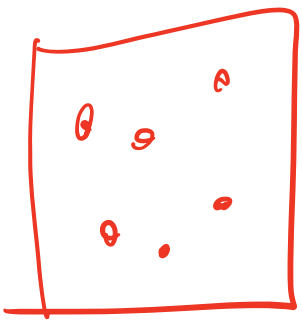
$m >> n.$

$\Downarrow$

$(A, \vec{u})$



$(A, \vec{b})$



Build private-key encryption from LWE with reusable keys.

<u>Hint 1:</u>

$$(A, As+e)$$

$$\approx$$

$$(A, u)$$

$\longrightarrow$ uniform.

<u>Hint 2</u>: $\forall i$

$$(\vec{a}_i, \vec{a}_i \cdot s + e_i)$$

$$\approx$$

$$(\vec{a}_i, \text{uniform}).$$

Private Key Encryption.

Gen $\longrightarrow$ $k = \vec{s} \longleftarrow \mathbb{Z}_q^n$

$\boxed{\text{Enc}(m\,;\,r)}$

* Use r to sample a row of A.

  Call it $\vec{a} = (a_1, \ldots, a_n)$

* Compute $\vec{a} \cdot \vec{s}$

  $= a_1 s_1 + a_2 s_2 \ldots a_n s_n$

* Sample $e \longleftarrow \{0, 1, -1\}$

* Output $\vec{a}, \left(\vec{a} \cdot \vec{s} + e + \overset{\mathbb{Z}_m}{m} \left\lfloor \frac{q}{2} \right\rfloor\right) \bmod q$

Dec(s, ct)

$ct = \vec{a}, b \quad = (\vec{a}s + e + m) \bmod q$

Compute $\vec{a} \cdot \vec{s}$

$$b - \vec{a} \cdot \vec{s} = \left(e + m\left\lfloor \frac{q}{2} \right\rfloor\right)$$

$3m \rightarrow$

$3m-1 \rightarrow$

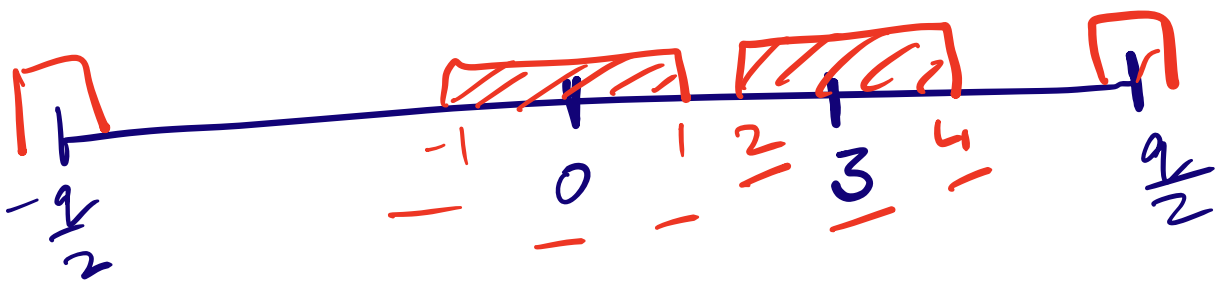
$3m+1 \rightarrow$

find m.

$= e \in \{0, 1, -1\}$ when $m = 0$

$= e + \left\lfloor \frac{q}{2} \right\rfloor$ when $m = 1$

$\in \left\{ \left\lfloor \frac{q}{2} \right\rfloor - 1, \left\lfloor \frac{q}{2} \right\rfloor, \left\lfloor \frac{q}{2} \right\rfloor + 1 \right\}$



LWE RLWE

SECURITY

$\forall m_0, m_1$

$$\mathrm{enc}(m_0) \approx \mathrm{enc}(m_1)$$

$$\vec{a}, \vec{a}\vec{s} + e + m_0 \cdot 3 \approx_c \vec{a}, u + m_0 \cdot 3$$

(by LWE)

$$\vec{a}, u + m_0 \cdot 3 = \vec{a}, u + m_1 \cdot 3$$

(one time pad)

$$\vec{a}, u + m_1 \cdot 3 \approx \vec{a}, \vec{a}\vec{s} + e + m_1 \cdot 3$$

(LWE)