LECTURE 25

* First sample prime q. (n bits long)

* Sample $\vec{s} = (s_1 \ldots\ldots s_n)$ where each $s_i \xleftarrow{\$} \mathbb{Z}_q$.

  $n \longrightarrow$ # variables

* Set $m = n^2$.

  $m \longrightarrow$ # equations

  (m can be ANY polynomial in n)

* For every $i \in [m]$,

  sample $\vec{a_i} = (a_{i1}, a_{i2} \ldots\ldots a_{in})$ where each $a_{ij} \xleftarrow{\$} \mathbb{Z}_q$

  sample $e_i \leftarrow \chi$. [Discrete Gaussian s.t. w.h.p. $e_i \in [-\frac{q}{4}, \frac{q}{4}]$]

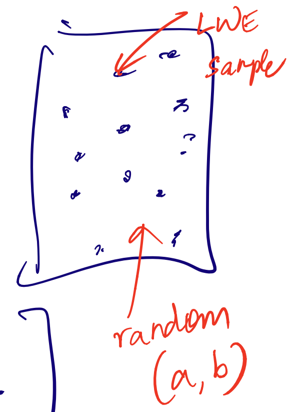
  Compute $b_i = \langle \vec{a_i}, s \rangle + e_i \pmod{\mathbb{Z}_q}$

  $$(a_{i1} s_1 + a_{i2} s_2 + \ldots\ldots a_{in} s_n) + e_i$$

* Output $(\vec{a}_1 \ldots\ldots \vec{a}_m), (b_1 \ldots\ldots b_m)$

Decision LWE assumption

$\forall$ PPT Adv. $\mathcal{A}$,



$$\Big| \Pr_{\substack{\vec{a},\,\vec{s},\,\vec{e} \text{ as above} \\ b = \vec{a}\vec{s} + e}} \left[\mathcal{A}(\vec{a}_1, \ldots, \vec{a}_m, b_1, \ldots, b_m) = 1 \right]$$

$$- \Pr_{\substack{\vec{a} \text{ as above} \\ \forall i \in [m]\ b_i \xleftarrow{\$} \mathbb{Z}_q}} \left[\mathcal{A}(\vec{a}_1, \ldots, \vec{a}_m, b_1, \ldots, b_m) = 1 \right] \Big| = \text{negl}(n)$$

$$\vec{s} = \underbrace{(s_1, \ldots, s_n)}_{q^n}$$

$$\left(\left\lfloor \frac{q}{4} \right\rfloor\right)^m \times q^n$$

Fix $\vec{a}_1 \ldots \vec{a}_m$. How many possible $(b_1 \ldots b_m) \rightarrow q^n$

How many possible $\vec{b}$ when $\vec{b}$ is chosen at random $\rightarrow$ q^m

Symmetric Encryption

KeyGen(r) : $\vec{s} = (s_1 \dots s_n)$

use r' to sample $\underline{a}$ and $\underline{e}$

Enc$(s, m; r')$: $\left(a, \left(\langle a, s\rangle + e\right) + m\lfloor \frac{q}{2} \rfloor\right)$

where $m \in \{0, 1\}$

Dec(s, ct) : Parse $ct = (a, b)$

Output 0 if $b - \langle a, s\rangle \bmod q \in \left[-\frac{q}{4}, \frac{q}{4}\right]$

1 if $b - \langle a, s\rangle \bmod q \in \left[\frac{q}{4}, \frac{3q}{4}\right]$

Single message CPA/semantic security

$$\underset{\substack{s \leftarrow \\ r \leftarrow}}{\text{Enc}(s, 0; r)} \approx_c \underset{\substack{s \leftarrow \\ r \leftarrow}}{\text{Enc}(s, 1; r)}$$

$$\mathrm{Enc}(s, 0; r) = (a, \langle a, s\rangle + e)_{a \leftarrow \mathbb{Z}_q^n, e \leftarrow \chi}$$

$$\mathrm{Enc}(s, 1; r) = \left(a, \langle a, s\rangle + e + \left\lfloor \frac{q}{2} \right\rfloor\right)_{a \leftarrow \mathbb{Z}_q^n, e \leftarrow \chi}$$

Goal : P.T. $\underset{s, r \leftarrow}{\mathrm{Enc}(s, 0; r)} \approx_c \underset{s, r \leftarrow}{\mathrm{Enc}(s, 1; r)}$

$$\boxed{(a, \langle a, s\rangle + e)}_{a \leftarrow \mathbb{Z}_q^n, e \leftarrow \chi} \qquad \left(\boxed{a, \langle a, s\rangle + e} + \left\lfloor \frac{q}{2} \right\rfloor\right)_{a \leftarrow \mathbb{Z}_q^n, e \leftarrow \chi}$$

$\approx_c$ by LWE $\qquad\qquad$ $\approx_c$ by LWE

$$\boxed{(a, b)}_{a \leftarrow \mathbb{Z}_q^n, b \leftarrow \mathbb{Z}_q} = \left(\boxed{a, b} + \left\lfloor \frac{q}{2} \right\rfloor\right)_{a \leftarrow \mathbb{Z}_q^n, b \leftarrow \mathbb{Z}_q}$$

Multi-Message Security

$\forall\ c_0, b_0, c_1, b_1, \ldots$

$\boxed{\mathrm{Enc}(s, c_0, r_1)}, \boxed{\mathrm{Enc}(s, b_0, r_2)} \ldots$

$\approx_c \mathrm{Enc}(s, c_1, r_1), \mathrm{Enc}(s, b_1, r_2) \ldots$

$\boxed{a, \langle s, a\rangle + e} + c_0 \lfloor \frac{q}{2} \rfloor$ — 1 noisy lin. eqn in s

$\boxed{\bar{a}, \langle s, \bar{a}\rangle + \bar{e}} + b_0 \lfloor \frac{q}{2} \rfloor$ — 2nd noisy lin. eqn in s

$\approx_c \boxed{a, b} + c_0 \lfloor \frac{q}{2} \rfloor$, where $b \leftarrow \mathbb{Z}_q$, $\bar{b} \leftarrow \mathbb{Z}_q$

$\boxed{\bar{a}, \bar{b}} + b_0 \lfloor \frac{q}{2} \rfloor$

$= a, b + c_1 \lfloor \frac{q}{2} \rfloor,$

$\bar{a}, \bar{b} + b_1 \lfloor \frac{q}{2} \rfloor$

$\approx_c a, \langle s, a\rangle + e + c_1 \lfloor \frac{q}{2} \rfloor$

$\bar{a}, \langle s, \bar{a}\rangle + \bar{e} + b_1 \lfloor \frac{q}{2} \rfloor$

$\downarrow$

$\mathrm{Enc}(c_1), \mathrm{Enc}(b_1).$

LWE : Matrix Representation

Let $A = \underbrace{\left.\begin{array}{c} \\ n \text{ rows} \\ \\ \end{array}\right. \begin{bmatrix} a_1 & \cdots & a_m \end{bmatrix}}_{m \text{ columns}}$ each element $\in \mathbb{Z}_q$

$E \quad [b_1 \ \cdots \ b_m]$

$\vec{S} = \begin{array}{c} n \\ \text{rows} \end{array} \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}$ each element $\in \mathbb{Z}_q$

1 column $\qquad [s_1 \ldots s_n]$

$\vec{e} = m \text{ rows} \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix}$ each element $\leftarrow \chi$

1 column

$\vec{b} = m \text{ rows} \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$ s.t.

1 column

$$\boxed{\vec{b}^T = \vec{S}^T A + e^T}$$

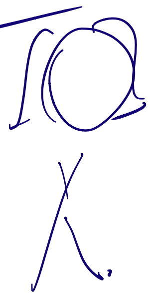
each $b_i = \langle a_i, s \rangle + e_i$

DLWE: $\forall$ PPT adversary $\mathcal{A}$,

$$\left| \Pr_{\substack{A\leftarrow \mathbb{Z}_q^{n\times m} \\ s\leftarrow \mathbb{Z}_q^{n\times 1} \\ e\leftarrow \chi^{m\times 1} \\ b = (s^TA+e^T)^T}}\left[\mathcal{A}(A,\vec{b})=1\right] - \Pr_{\substack{A\leftarrow\mathbb{Z}_q^{n\times m} \\ b\leftarrow \mathbb{Z}_q^{m\times 1}}}\left[\mathcal{A}(A,b)=1\right]\right| = \text{negl}(n)$$

PUBLIC KEY ENCRYPTION

Alice



$\boxed{pk}$

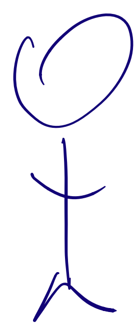
(sk, pk)

$s\leftarrow\mathbb{Z}_q^n$ (A,b) where $A\leftarrow\mathbb{Z}_q^{n\times m}$, $e\leftarrow\chi^m$, $b=(s^TA+e^T)^T$

$pk = (A,\vec{b}) \longrightarrow$

$\longleftarrow Ar,\ \boxed{br+m}$

Bob



$(m;r)$

Note: χ is set s.t. samples from $\chi \in [-q/4m, q/4m]$

$$\text{KeyGen}(\text{randomness}) \rightarrow sk = \vec{s} \leftarrow \mathbb{Z}_q^{n\times 1}$$

$$pk = \begin{bmatrix} A \\ \hline \vec{b}^T \\ \hline \end{bmatrix} \quad A \leftarrow \mathbb{Z}_q^{n\times m}, \quad \vec{b}^T = (s^T A + e^T) \text{ where } e \leftarrow \chi^{m\times 1}$$

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

Parse $pk = (A, \vec{b}^T)$

Sample vector $\vec{r} \leftarrow \{0,1\}^{m\times 1}$ $\quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$

Compute $\underset{n\times 1}{\vec{c}} = \underset{n\times m}{A} \cdot \vec{r}_{m\times 1}$

$$d = \left(\vec{b}^T_{1\times m} \cdot \vec{r}_{m\times 1} + m\left\lfloor \frac{q}{2} \right\rfloor\right) \bmod q$$

$$\text{Enc}(m, pk; r) = (\vec{c}, d).$$

$\mathrm{Dec}(ct, pk)$.

Parse $ct = (\vec{c}, d)$.

Compute $\alpha = \vec{S}^T_{1\times n} \cdot \vec{C}_{n\times 1} \left(= \vec{s}^T A \cdot \vec{r}\right)$

$\beta = (d - \alpha) = m\left\lfloor \frac{q}{2} \right\rfloor + \underbrace{\vec{b}^T \cdot \vec{r} - \vec{s}^T A \cdot \vec{r}}_{= \vec{e}^T \cdot \vec{r}}$

If $\vec{r} \in \{0,1\}^{m\times 1}$, $\to \in \chi \in \left[\frac{-q}{4m}, \frac{q}{4m}\right]$

and every entry in $\vec{e} \in \left[\frac{-q}{4m}, \frac{q}{4m}\right]$

then $\left(\vec{e}^T \cdot \vec{r}\right) \in \left[-\frac{q}{4}, \frac{q}{4}\right]$

Dec. checks if $\beta \in \left[\frac{-q}{4}, \frac{q}{4}\right]$. If so, output $m = 0$.

Else output $m = 1$.

Note: In the public-key setting

$\boxed{\text{Single-message CPA}} \equiv$ multi-message CPA.

$$\left(pk, \mathrm{Enc}(pk, 0; r)\right) \approx_c \left(pk, \mathrm{Enc}(pk, 1; r)\right)$$

$$(A, \vec{b}^T), (A\vec{r}, \vec{b}^T\vec{r})$$

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

$$\approx_c$$

$$(A, \vec{b}^T), (A\vec{r}, \vec{b}^T\vec{r})$$

$b \leftarrow \mathbb{Z}_q^m$

$$(A, \vec{b}^T), \left(A\vec{r}, \vec{b}^T\vec{r} + \lfloor \tfrac{q}{2} \rfloor\right)$$

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

$$\approx_c$$

$$(A, \vec{b}^T), \left(A\vec{r}, \vec{b}^T\vec{r} + \lfloor \tfrac{q}{2} \rfloor\right)$$

$b \leftarrow \mathbb{Z}_q^m$

(E, Er)

Leftover Hash Lemma

$\approx$ unif. random vector

$\approx_s$ random matrix

$\vec{b}^T\vec{r} + \lfloor \tfrac{q}{2} \rfloor \approx$ unif. random $+ \lfloor \tfrac{q}{2} \rfloor$