LECTURE - 16

Last - time.

LWE assumption

DLWE n, m, q, χ

for every QPT adversary $\mathcal{A}$,

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

q^n possible s values,

$|\mathrm{Supp}(\chi)|^m$ possible e values

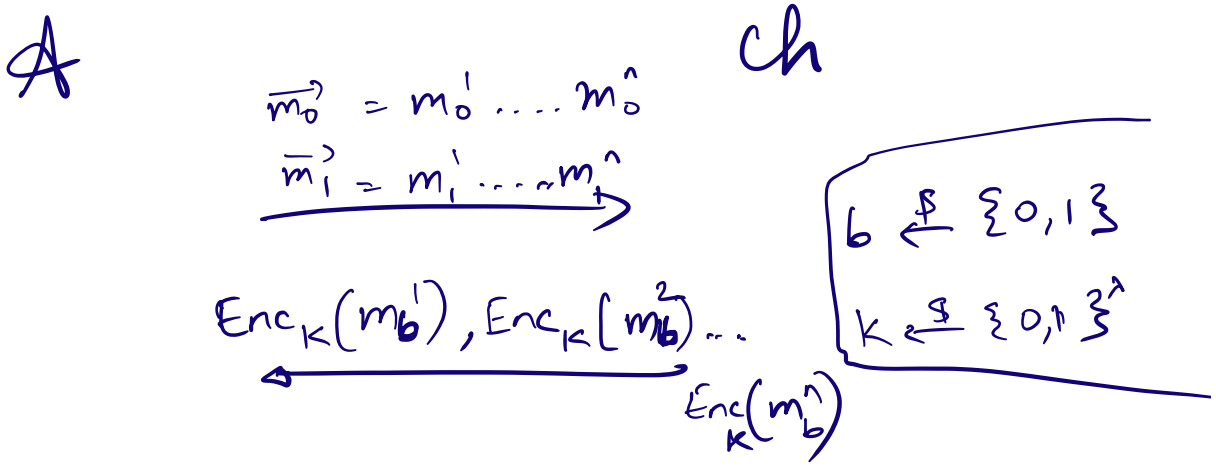
$$\left. \Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m \times n} \\ b \leftarrow \mathbb{Z}_q^{m \times 1}}} \left[\mathcal{A}(A, b) = 1 \right] \right| = \mathrm{negl}(n)$$

q^m possible b values

$$q^m >> q^n \cdot |\mathrm{supp}(\chi)|^m$$

ENCRYPTION.

Multi-message security.



We require:

$\forall$ PPT adversary A

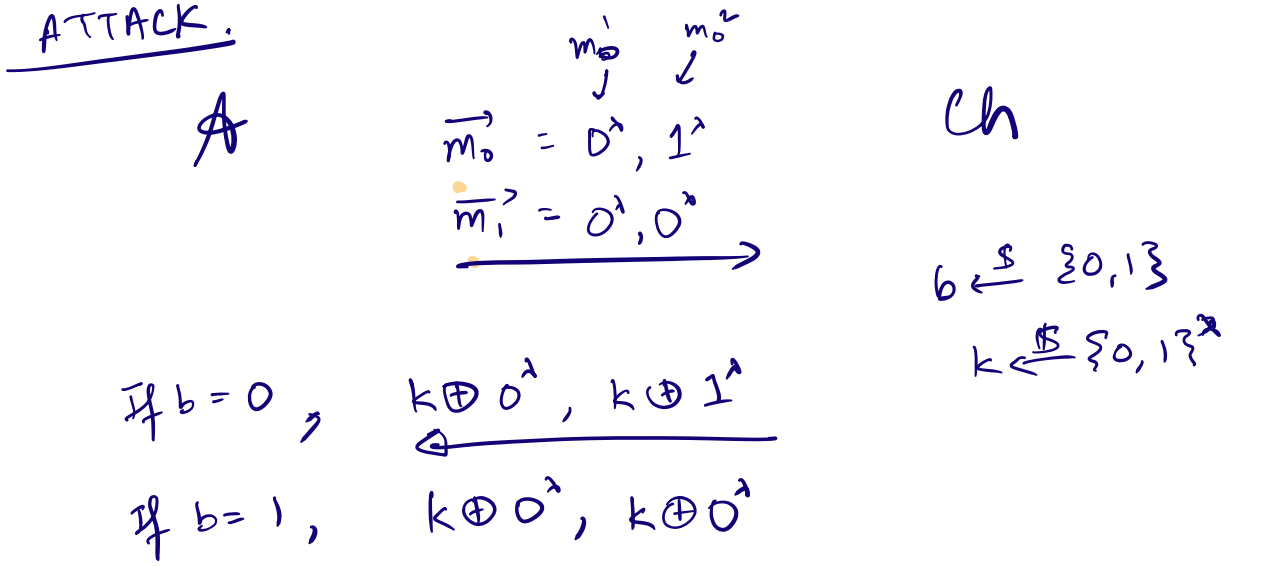
$$Pr[\tilde{b} = b] \leq \frac{1}{2} + negl(\lambda)$$

One-time pad. $Enc(k, m) = k \oplus m$.

This is not multi-message secure.

Why?

ATTACK.



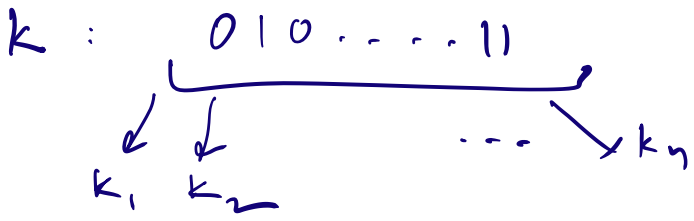
If $\mathcal{A}$ obtains $(k, k \oplus 1^\lambda)$, it outputs $\tilde{b} = 0$

(k, k) it outputs $\tilde{b} = 1$.

$$Pr[b = \tilde{b}] = 1.$$

Single k of size λ,

that can be used to derive "pseudorandom" one-time keys, as a deterministic function of k, one for every message.



$k_1 \oplus m_b^1$

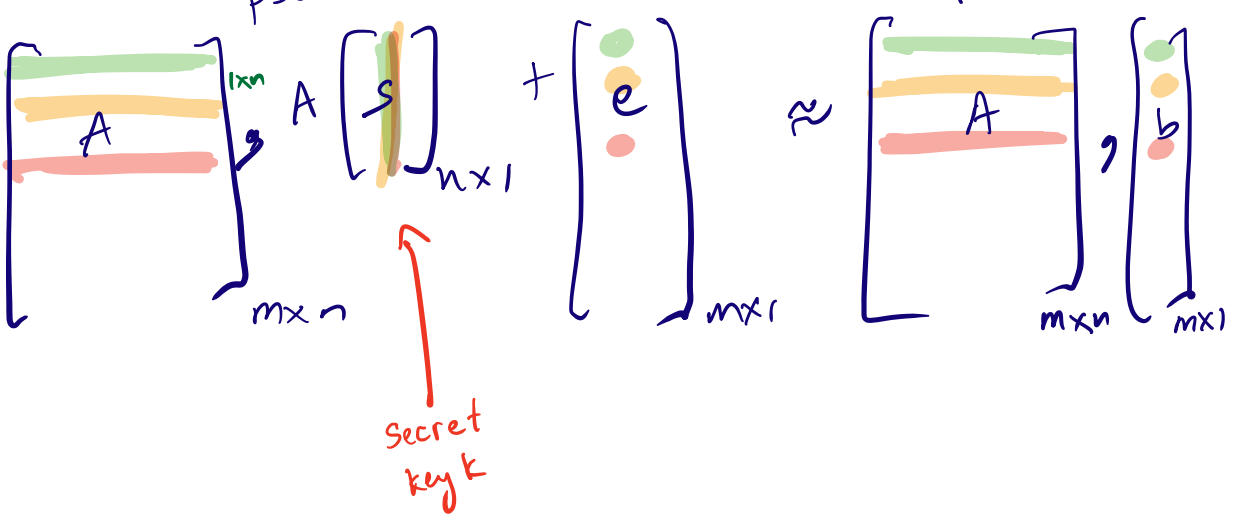
$k_2 \oplus m_b^2$

.
.
.

Recall: LWE assumption.

$$(A, As+e) \approx (A, b)$$

↑ pseudorandom ↑ uniform.



$\text{Enc}(k, \mu)$: (μ → bit)

$k = s$ (LWE secret)

Sample $a \leftarrow \mathbb{Z}_q^{l \times n}$, $e \leftarrow \chi$

Output $ct = \left(a, (as + e + \mu \lfloor \frac{q}{2} \rfloor) \bmod q\right)$

How do we decrypt?

$\text{Dec}(k, ct)$ where $ct = (a, c')$, $k = s$

how should we recover μ,
given that $c' = (as + e + \mu) \bmod q$?

If no error, then $\mu = (c' - a \cdot s)$

~~When there is error, $\mu + e = (c' - a \cdot s)$~~

~~expand. small~~

Decrypt (k , ct)
$= s$

where $ct = (a, c')$.

Compute $(c' - a.s) = \mu \lfloor \frac{q}{2} \rfloor + e$

$= e$ (i.e. low norm, when $\mu = 0$).

$= \lfloor \frac{q}{2} \rfloor + e$ (i.e. high norm, when $\mu = 1$).

Multi-message security.

$\mathcal{A}$ $\qquad \vec{\mu_0} = \mu_0^1 \ldots \mu_0^m$ $\qquad$ Ch.

$\vec{\mu_1} = \mu_1^1 \ldots \mu_1^m$ $\longrightarrow$

$b \xleftarrow{\$} \{0,1\}$.

$\text{Enc}_s(\mu_b^1) \ldots \text{Enc}_s(\mu_b^m)$ $\longleftarrow$

$$Enc_s(\mu) = a,\ a\,s + e + \mu\left\lfloor \frac{q}{2} \right\rfloor$$

$$a_1,\ a_1 s + e_1 + \mu_b^1 \left\lfloor \frac{q}{2} \right\rfloor,\ \ldots\ldots a_m,\ a_m s + e_m + \mu_b^m \left\lfloor \frac{q}{2} \right\rfloor$$

$\mathcal{A}$ outputs $\tilde{b}$.

$\forall$ PPT $\mathcal{A}$, $Pr\left[\tilde{b} = b\right] \leq \frac{1}{2} + negl(n)$

equivalently

$$\left| Pr\left[\tilde{b} = 1 \mid b = 1\right] - Pr\left[\tilde{b} = 1 \mid b = 0\right] \right| = negl(n)$$

$$a_1,\ a_1 s + e_1 + \mu_b^1 \left\lfloor \frac{q}{2} \right\rfloor,\ \ldots\ldots a_m,\ a_m s + e_m + \mu_b^m \left\lfloor \frac{q}{2} \right\rfloor$$

$$\begin{pmatrix} \longleftarrow & A & \longrightarrow \\ \longleftarrow & a_1 & \longrightarrow \\ \longleftarrow & a_2 & \longrightarrow \\ & \vdots & \end{pmatrix} A \begin{bmatrix} s \end{bmatrix}_{n \times 1} + \begin{pmatrix} e_1 \\ \vdots \end{pmatrix} + \begin{pmatrix} \mu_b^1 \left\lfloor \frac{q}{2} \right\rfloor \\ \mu_b^2 \left\lfloor \frac{q}{2} \right\rfloor \\ \vdots \\ \mu_b^m \left\lfloor \frac{q}{2} \right\rfloor \end{pmatrix}$$

$\left[\longleftarrow a_m \longrightarrow \right]_{m \times n}$ $\left[e_m \right]_{m \times 1}$ $\left[\quad \right]_{m \times 1}$

$A \leftarrow \mathbb{Z}_q^{m \times n}$,
$s \leftarrow \mathbb{Z}_q^{n \times 1}$, $e \leftarrow \chi^m$ $\approx$ by LWE.

$$\begin{bmatrix} & A & \\ & & \end{bmatrix} \approx \begin{bmatrix} b \end{bmatrix}_{m \times 1} + \begin{bmatrix} \mu_b^1 \lfloor \frac{q}{2} \rfloor \\ \vdots \\ \mu_b^m \lfloor \frac{q}{2} \rfloor \end{bmatrix}_{m \times 1}$$

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

$=$

$$\begin{bmatrix} & A & \\ & & \end{bmatrix}, \begin{bmatrix} b \end{bmatrix}_{m \times 1}$$

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

Quantum One-Time Pad

Goal: Given an arbitrary quantum (mixed) state ρ, and a classical key k sampled uniformly, develop an alg $\text{Enc}(k, \rho) \to \frac{I}{2}$.

$$\rho = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

Modify ρ by applying unitaries derived from k, so that averaged over all keys, the resulting density matrix is $\frac{I}{2}$.

Key: $(a, b) \xleftarrow{\$} \{0,1\}$.

$$\text{Enc}\left((a,b),\rho\right) \longrightarrow X^a Z^b \rho \left(X^a Z^b\right)^\dagger$$

X and Z are Pauli gates

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\text{Enc}\left((00),\rho\right) \longrightarrow \rho$$

$$\text{Enc}\left((01),\rho\right) \longrightarrow Z\rho Z^\dagger$$

$$\text{Enc}\left((10),\rho\right) \longrightarrow X\rho X^\dagger$$

$$\text{Enc}\left((11),\rho\right) \longrightarrow XZ\,\rho\,(XZ)^\dagger$$

$$\text{Dec}\left((a,b),\sigma\right) \longrightarrow \left(X^a Z^b\right)^\dagger \sigma \left(X^a Z^b\right)$$

We want to prove:

$$\frac{1}{4} \sum_{a,b \in \{0,1\}} \left(X^a Z^b\right) \rho \left(X^a Z^b\right)^\dagger = \frac{\mathbb{I}}{2}$$

Proof. $\rho = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, $\alpha + \delta = 1$

$$\frac{1}{4} \sum_{a,b \in \{0,1\}} (X^a Z^b) \rho (X^a Z^b)^\dagger$$

$$= \frac{1}{4} \left(\rho + Z\rho Z^\dagger + X\rho X^\dagger + (XZ)\rho(XZ)^\dagger \right)$$

$$= \frac{1}{4} \left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} + \begin{bmatrix} \alpha & -\beta \\ -\gamma & \delta \end{bmatrix} + \begin{bmatrix} \delta & \gamma \\ \beta & \alpha \end{bmatrix} + \begin{bmatrix} \delta & -\gamma \\ -\beta & \alpha \end{bmatrix} \right)$$

$$= \frac{1}{4} \begin{bmatrix} 2(\alpha+\delta) & 0 \\ 0 & 2(\alpha+\delta) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{\mathbb{I}}{2}.$$

$$Z\rho Z^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha & \beta \\ -\gamma & -\delta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha & -\beta \\ -\gamma & \delta \end{bmatrix}$$

$$X\rho X^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} \gamma & \delta \\ \alpha & \beta \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} \delta & \gamma \\ \beta & \alpha \end{bmatrix}$$

$$\frac{1}{4} \sum_{a,b \in \{0,1\}} X^a Z^b \rho_1 (X^a Z^b)^\dagger \otimes X^a Z^b \rho_2 (X^a Z^b)^\dagger$$

$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ or } \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

$X\rho X^\dagger$ or ρ.