LECTURE - 15

Today

* Random Oracles (just a little bit)
* Encryption

RANDOM ORACLE : Truly random function

$$\{0,1\}^n \longrightarrow \{0,1\}^\infty$$

on any input x, $RO(x)$ is uniform random.

A hash function (SHA256) is assumed in practice to "behave like" a random oracle

COMMITMENTS in the random oracle model :

$$Com(b ; r) = RO(b||r)$$

$$Decom(str, b, r) = \text{ACCEPT iff } RO(b||r) = str.$$

ENCRYPTION (SECRET-KEY / SYMMETRIC)

How to encrypt a classical bit?

$(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ for message space $\{0,1\}^p$

$\mathsf{KeyGen}(1^\lambda; r) \longrightarrow sk$

$\mathsf{Enc}(sk, m; \cancel{r}) \longrightarrow ct$

$\mathsf{Dec}(ct, sk) \longrightarrow m \in \{0,1\}^p$ or $\perp$.

Security:

ct "should not reveal" the message m.

$\forall$ PPT/QPT $\mathcal{A}$,

Attempt 1: $\Pr_{m \leftarrow \{0,1\}^p}\left[\mathcal{A}(ct) \to m \text{ s.t. } \mathsf{Dec}(ct, sk) = m\right] = \mathsf{negl}$

NOT a good definition because it relies on m being uniformly sampled and $\mathcal{A}$ not having any "leakage" on m

SINGLE - MESSAGE CPA security

$\forall\ m_0, m_1 \in \{0,1\}^\rho \times \{0,1\}^\rho$, $\forall$ PPT $\mathcal{A}$

$$\left| \Pr_{sk \leftarrow KeyGen(1^\lambda)} \left[\mathcal{A}\left(ct \leftarrow Enc(sk, m_0)\right) = 1 \right] - \Pr_{sk \leftarrow KeyGen(1^\lambda)} \left[\mathcal{A}\left(ct \leftarrow Enc(sk, m_1)\right) = 1 \right] \right| = negl(\lambda)$$

EQUIVALENTLY, $\forall\ \mathcal{A}$, $\forall\ m_0, m_1$,

$$\Pr_{\substack{sk \leftarrow KeyGen(1^\lambda) \\ b \leftarrow \{0,1\}}} \left[\mathcal{A}\left(ct \leftarrow Enc(sk, m_b)\right) = m_b \right] \leq \frac{1}{2} + negl(\lambda)$$

ONE - TIME PAD.

KeyGen $\rightarrow$ $sk \xleftarrow{\$} \{0,1\}^\rho$

$Enc(sk, m)$: output $ct = sk \oplus m$

$Dec(ct, sk)$: output $ct \oplus sk = m$

$sk \oplus a$, $sk \oplus b$

MULTI - MESSAGE SECURITY:

$\forall\ n = \text{poly}(\lambda)$,

$\forall\ \vec{m_0}, \vec{m_1}$ where $\vec{m_0} = (m_0^1, m_0^2 \ldots\ldots m_0^n)$

for $n = \text{poly}(\lambda)$

$\vec{m_1} = (m_1^1, m_1^2 \ldots\ldots m_1^n)$

$\forall$ QPT $\mathcal{A}$

$$\left| \Pr_{sk \leftarrow KeyGen}\left[\mathcal{A}(ct_1, \ldots ct_n) = 1 \mid \forall i \in [n],\ ct_i = Enc(sk, m_0^i)\right] - \Pr_{sk \leftarrow KeyGen}\left[\mathcal{A}(ct_1, \ldots ct_n) = 1 \mid \forall i \in [n],\ ct_i = Enc(sk, m_1^i)\right] \right| = negl(\lambda)$$

Secret-key single-message CPA security

$\Uparrow \Downarrow$

Secret-key multi-message CPA security.

HOW DO WE BUILD SCHEMES SATISFYING MULTI-MESSAGE CPA SECURITY?

(Enc must be randomized.)

LEARNING WITH ERRORS

$$14s_1 + 15s_2 + 5s_3 + 2s_4 \overset{\approx}{+ e_1} = 8 \bmod 17$$

$$13s_1 + 14s_2 + 14s_3 + 6s_4 \overset{\approx}{+ e_2} = 16 \bmod 17$$

$$6s_1 + 10s_2 + 13s_3 + 15s_4 \overset{\approx}{+ e_3} = 3 \bmod 17$$

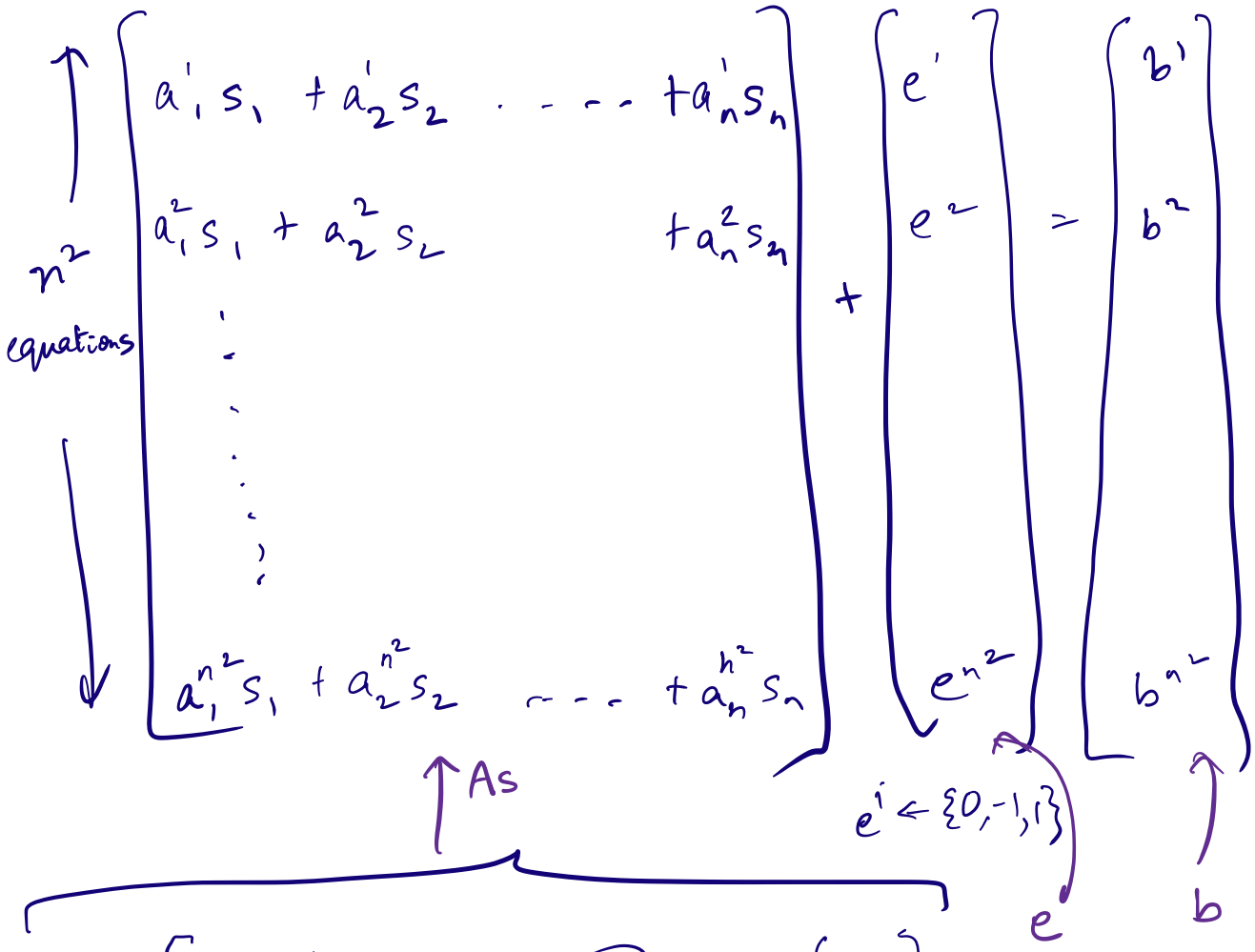
$$6s_1 + 7s_2 + 16s_3 + 2s_4 \overset{\approx}{+ e_4} = 3 \bmod 17$$

given e_i's $\in \{-1, 0, 1\}$.

Gaussian elimination solves sequences of n equations in time poly(n).

n equations in n variables "s" but with unknown small errors.

n^2 equations in n variables but with unknown small errors.



$$A = \begin{bmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ \vdots & & & \vdots \\ a_1^{n^2} & \cdots & & a_n^{n^2} \end{bmatrix} \qquad s = \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}$$

LWE Given A, $As + e$, find s.

"Informal".

Search-LWE assumption

First sample a "large" random prime $q \sim O(2^n)$

then sample $\vec{s} = \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}$ where each $s_i \xleftarrow{\$} \mathbb{Z}_q$.

then sample $\vec{A} = \begin{bmatrix} a & & \\ & \ddots & \\ & & \end{bmatrix} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$

$n^2 \times n$

m

then sample $\vec{e} = \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} \xleftarrow{\$} \{0,1,-1\}^n$.

then output $A, As+e$.

$\forall$ QPT adversary $\mathcal{A}$,

$$\Pr_{A \xleftarrow{\$} \mathbb{Z}_q^{m \times n},\ s \xleftarrow{\$} \mathbb{Z}_q^{n \times 1},\ e \xleftarrow{\$} \{0,1,-1\}^n,\ b = As+e} \left[\mathcal{A}(A,b) \to s' \text{ s.t. } \exists e' \underset{\in\{0,1,-1\}}{\text{ s.t. }} b = As'+e' \right] = \text{negl}(n)$$

Decisional LWE.

$\forall$ QPT adversary $\mathcal{A}$,

$$\left| \Pr_{A \leftarrow \mathbb{Z}_q^{m \times n},\ s \leftarrow \mathbb{Z}_q^{n \times 1},\ e \xleftarrow{\$} \{0,1,-1\},\ b \leftarrow As+e} \left[\mathcal{A}(A,b) = 1 \right] - \right.$$

($q^n \cdot 3^n$ possible)

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

(q^m possible)

$q^n \cdot 3^n \ll q^m$.