LECTURE - 11

IDENTITY - BASED ENCRYPTION

* $\text{KeyGen}(1^\lambda) \longrightarrow \text{MPK}, \text{MSK}$
* $\text{Encrypt}(\text{MPK}, \text{id}, \mu; r) \longrightarrow \text{ct}$
* $\text{SKGen}(\text{MSK}, \text{id}; r_G) \longrightarrow \text{SK id}$
* $\text{Decrypt}(\text{sk}_{\text{id}}, \text{id}, \text{ct}) \longrightarrow \mu \text{ or } \perp$

Correctness: $\forall$ id, whp over MPK, MSK, r, r_G

$\text{Decrypt}(\text{sk}_{\text{id}}, \text{id}, \text{Encrypt}(\text{MPK}, \text{id}, \mu; r)) = \mu$

as long as $\text{sk}_{\text{id}} \leftarrow \text{SKGen}(\text{MSK}, \text{id}; r_G)$

Security:

Challenger: $\text{KeyGen}(1^\lambda) \rightarrow \text{mpk}, \text{msk}$

Adv. = A

mpk →

← id_1 $\quad v_1 = H(\text{id}_1)$

$\text{sk}_{\text{id}_1} = e_1$ →

← id_2 $\quad v_2 = H(\text{id}_2)$

$\text{sk}_{\text{id}_2} = e_2$ →

⋮

← id^*, m_0, m_1

$\text{Enc}(\text{mpk}, \text{id}^*, m_b)$ →

← id_{n+1}

~~$\text{sk}_{\text{id}_{n+1}}$~~ →

⋮

b' →

"FULL" security

"SELECTIVE" security: id^* is known to challenger before sending mpk.

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

$$\Pr\left[\text{id}^* \notin \{\text{id}_1, \ldots, \text{id}_{n_1}, \text{id}_{n_1+1}, \ldots, \text{id}_{n_2}\} \wedge (b' = b)\right] = \frac{1}{2} + \text{negl}(\lambda)$$

* KeyGen $\longrightarrow$ MPK A , MSK T_A

* $Enc(MPK, id, \mu)$ $\longrightarrow$ Set (A, v) as a "public key" for Dual-Regev
  A $H(id)=v$
  Dual-Regev Encrypt μ w.r.t. (A, v)

* $SKGen(MSK, id)$ $\longrightarrow$ $sk_{id} = e$.
  T_A $H(id)=v$ find e s.t. $Ae = v$
  "nicely distributed"

* $Dec(sk_{id}, id, ct)$ $\longrightarrow$ μ or $\perp$.
  e Dual-Regev ct. Dual-Regev decryption

Recall: Dual-Regev

$pk = (A, v)$ (s.t. $v = Ae$)

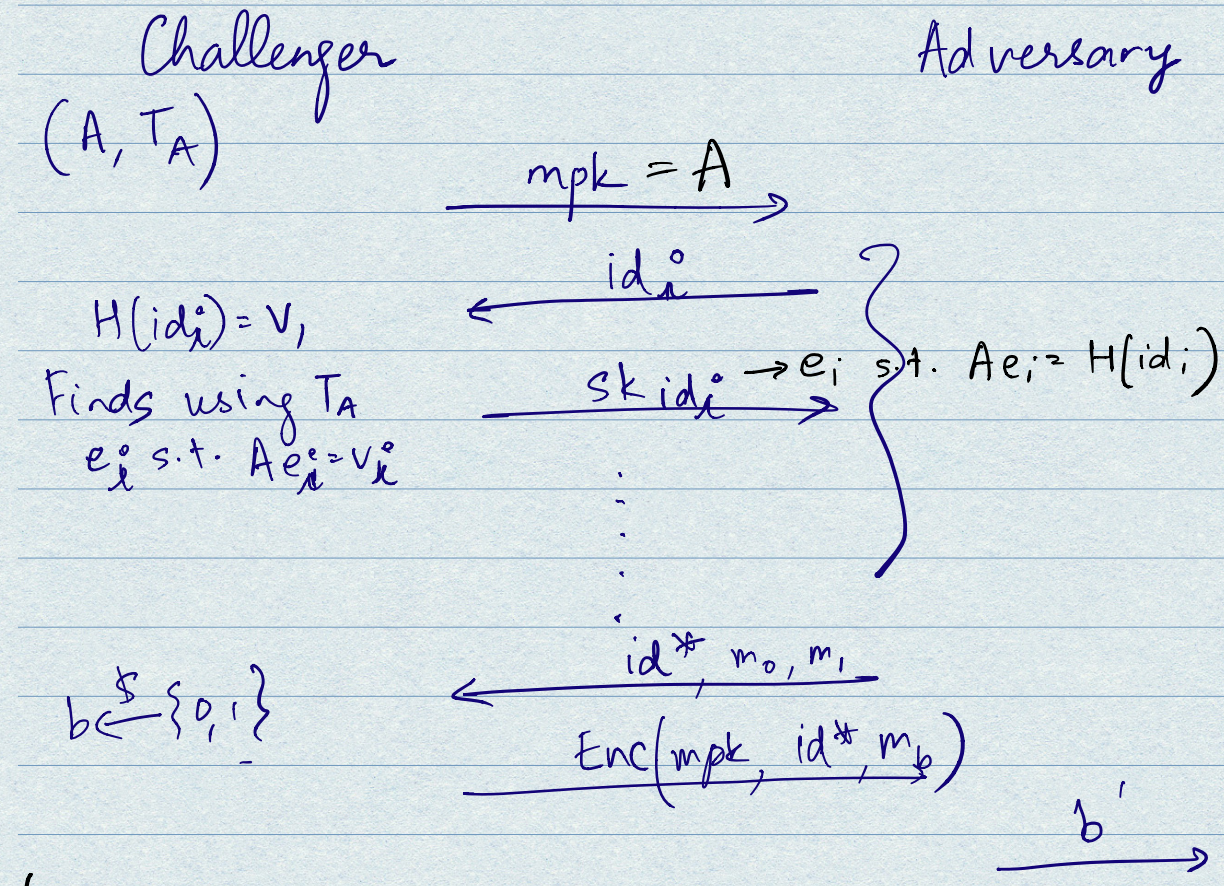
$sk = e$

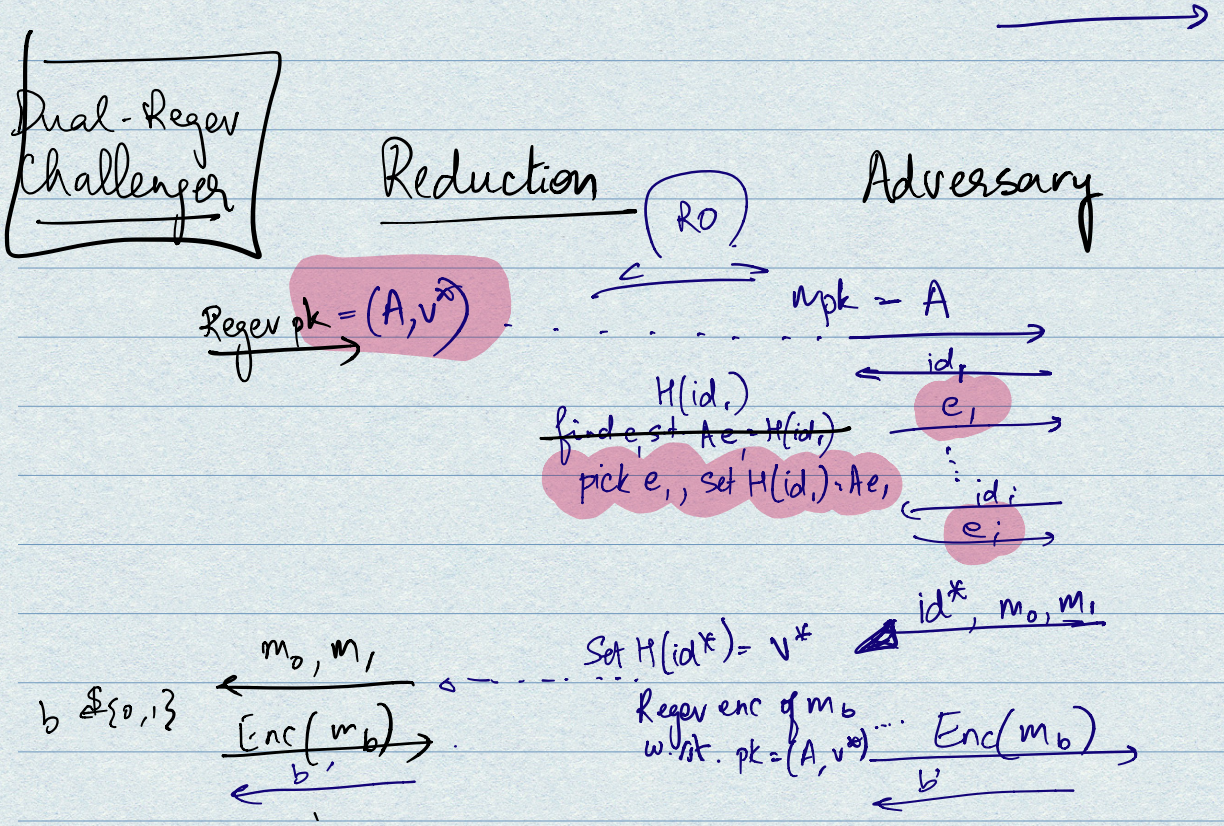
$Enc(pk, \mu; r)$: Set $A' = [A \| v]$

Sample s, $\tilde{e}$ and set $ct = s^T A' + \tilde{e}^T + [0 \ldots 0 \ \mu \lfloor \frac{q}{2} \rfloor]$

$Dec(sk, ct)$: Parse $ct = (c_1, c_2)$

Compute $c_2 - c_1 \cdot \underbrace{e}_{sk} = \left(s^T A e + \text{error} + \mu \lfloor \frac{q}{2} \rfloor\right) - \left(s^T A e + \text{error}\right)$


Challenger
Adversary
(A, T_A)
mpk = A
id_i^*
$H(id_i^*) = v_i$
Finds using T_A
e_i^* s.t. $Ae_i^* = v_i^*$
$sk_{id_i^*} \rightarrow e_i$ s.t. $Ae_i = H(id_i)$
id^*, m_0, m_1
$b \xleftarrow{\$} \{0,1\}$
$Enc(mpk, id^*, m_b)$
b'


Dual-Regev Challenger
Reduction
Adversary
RO
Regev pk = (A, v^*)
mpk = A
id_1
H(id_1)
find e_1 s.t. $Ae_1 = H(id_1)$
pick e_1, set $H(id_1) = Ae_1$
e_1
id_i
e_i
id^*, m_0, m_1
Set $H(id^*) = v^*$
m_0, m_1
$b \xleftarrow{\$} \{0,1\}$
$Enc(m_b)$
b'
Regev enc of m_b w.r.t. pk = (A, v^*)
$Enc(m_b)$
b'

New Trick: Trapdoor Extension.

Q: Given (A, T_A, T_{AG}) s.t. $A T_A = 0$, $A T_{AG} = G$.

$A_{n \times m}$ $T_{A\ m \times m}$

for some arbitrary matrix B

Can you sample a type-1 trapdoor for

$[A \| B]$?

$A \in \mathbb{Z}_q^{n \times m}$, $B \in \mathbb{Z}_q^{n \times k}$

$$[A \| B] \begin{bmatrix} T_A & Y \\ 0 & I \end{bmatrix}$$

$T_{A\ m \times m}$ $Y_{m \times k}$ $0_{k \times m}$ $I_{k \times k}$

$$= \left[\underbrace{AT_A + B0}_{=0} \,\middle\|\, \underbrace{AY + BI}_{=0} \right]$$

(by design)

Solve for Y!

Find SHORT Y s.t. $AY = -BI$

$$\begin{bmatrix} A \end{bmatrix}_{n \times m} \begin{bmatrix} | & & | \\ y_1 & \cdots & \\ | & & | \end{bmatrix}_{m \times k} = \begin{bmatrix} | & & | \\ -b_1 & \cdots & \\ | & & | \end{bmatrix}_{n \times k}$$

find e' s.t.

$G \cdot e' = b_1$

$T_{AG}\ e'$ is the SIS

To solve solution, SIS

Trapdoors for $[B \| A]$?

$$[B \| A] \begin{bmatrix} 0 & I \\ T_A & Y \end{bmatrix}$$

Solve for "short" Y s.t.

$$-B = AY$$