LECTURE 12

IDENTITY - BASED ENCRYPTION.

$KeyGen(1^\lambda) \rightarrow MPK, MSK$

$Enc(MPK, id, m; r) \rightarrow ct$

$SKGen(MSK, id) \rightarrow SK_{id}$

$Dec(SK_{id}, ct, id) \rightarrow m \text{ or } \perp$

TODAY

* IBE without random oracles
* Attribute-Based ABE (without random oracles)
* Predicate-Encryption PE
* Functional-Encryption FE (strongest) $\equiv$ iO (indistinguishability obfuscation)

Trapdoor Extension

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

Given T_A s.t. $AT_A = 0$

one can generate a trapdoor T

s.t. $[A \| B]\, T = 0$ (for arbitrary B)

$$T = \left[\begin{array}{c|c} (T_A)_{m \times m} & Y_{m \times k} \\ \hline 0_{k \times m} & I_{k \times k} \end{array}\right]$$

Y is a "short" matrix s.t.

$$AY = -B.$$

How do you find Y?

Use T_A to find "short" solution Y s.t. $AY = -B$.

Can similarly find trapdoors for $[B \| A]$

Another IBE (without random oracle)

Cash - Hofheinz - Kiltz - Peikert

KeyGen $\rightarrow$ MPK , MSK $\hookrightarrow T_{A_{10}}$, $T_{A_{11}}$

$$\begin{bmatrix} A_{10} & A_{20} & \cdots & A_{\ell 0} \\ A_{11} & A_{21} & & A_{\ell 1} \end{bmatrix}, \quad V \in \mathbb{Z}_q^n$$

where ℓ is the length of id.

(Intuition: when we encrypt, id will help us pick $A_{1\,id_1}, A_{2\,id_2}, \ldots$ where id_j is j^{th} bit of id)

SKGen (MSK, id) $\rightarrow$ sk_{id}

Set $A_{id} = \begin{bmatrix} A_{1\,id_1} & A_{2\,id_2} & \cdots & A_{\ell\,id_\ell} \end{bmatrix}_{n \times \ell m}$

Output "short" e s.t. $A_{id}\, e = V$ and e is "nicely distributed" 3.

Enc $\left(\text{MPK} = \begin{bmatrix} A_{10} & \cdots & A_{R0} \\ A_{11} & & A_{R1} \end{bmatrix}, \text{id}, \mu\right) \rightarrow$

Compute dual-Regev PK $= (A_{id}, v)$

where $A_{id} = [A_{1id_1} \| \cdots \| A_{\ell id_\ell}]$

Encrypt μ to PK (via Dual-Regev)

Dec (sk_{id}, c) → dual-Regev ct computed w.r.t. $pk = (A_{id}, v)$

$\downarrow$

e s.t. $A_{id} \cdot e = v$

NOTE: e = dual-Regev sk corresp. to $pk = (A_{id}, v)$

Dual-Regev decryption gives you m!

Side ~~NOTE~~

Trivial IBE: $[pk_1, pk_2 \cdots pk_{id} \cdots pk_N] \equiv$ MPK

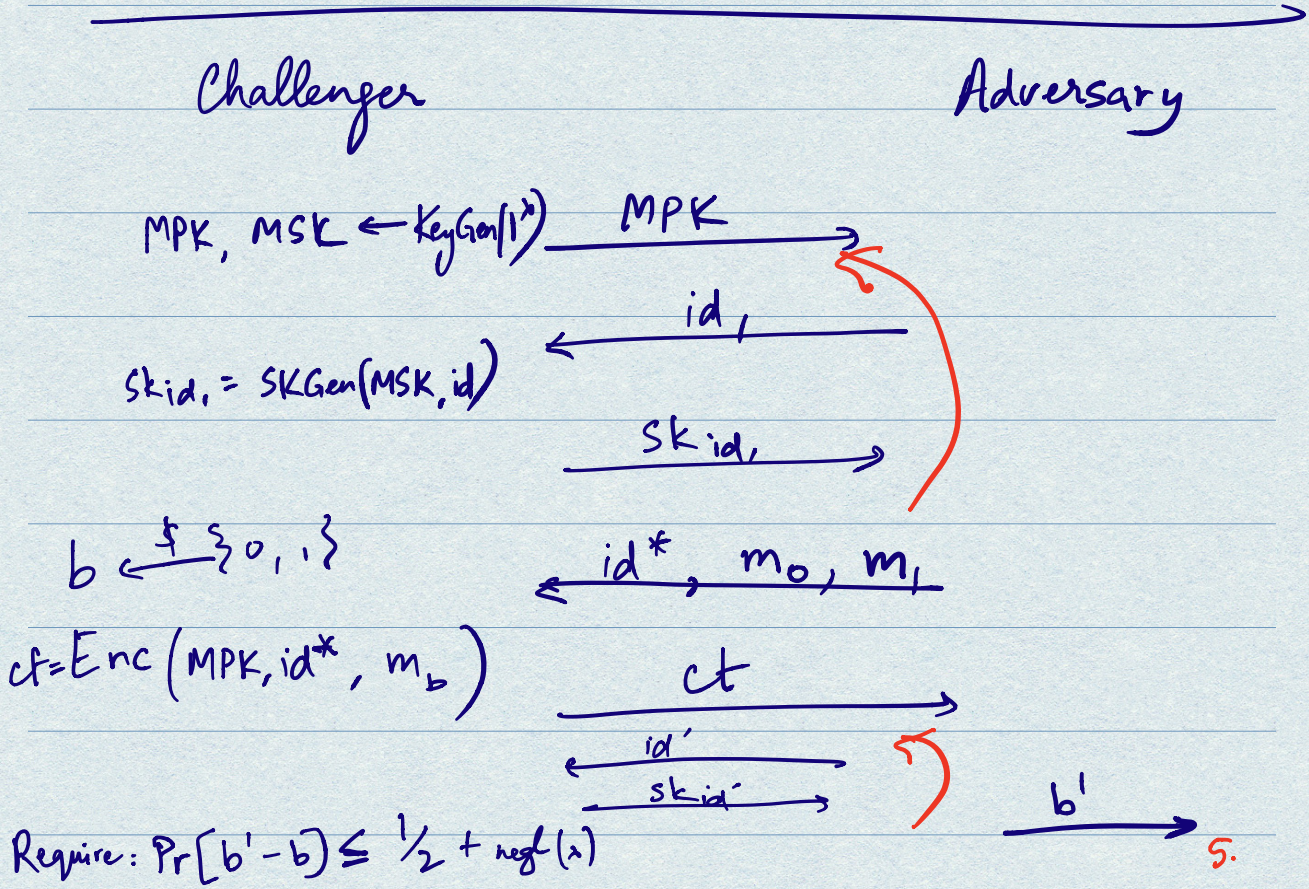
$[sk_1, sk_2 \cdots \cdots sk_N] \equiv$ MSK

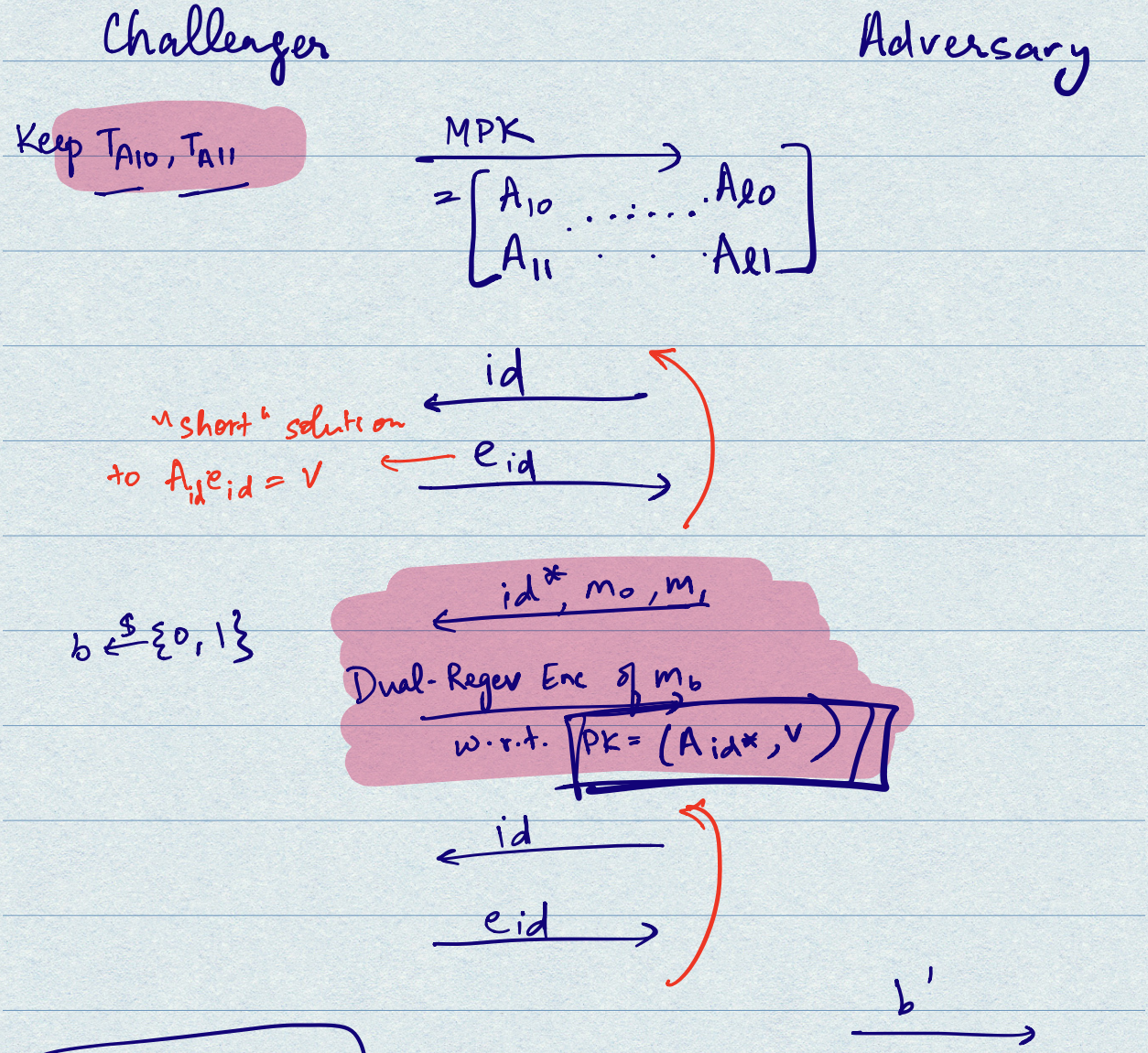
SK Gen (MSK, id) outputs sk_{id}.

Dual-regev : Sample (A, v)

As long as you can compute T_A, you can find (and distribute...) e s.t. $Ae = v$

e ← D-R secret key.





Reduction

obtains D-Reg

$pk = (A', v')$

$Enc_{pk}(m_b)$

Reduction must play this game without knowing trapdoors for A_{id^*}.

Dual-Regev Challenger

Reduction

Dual-Reg Adversary / IBE Challenger

IBE Adversary

id^*

$MPK = \left(\begin{bmatrix} A_{10} & \cdots & A_{\ell 0} \\ A_{11} & & A_{\ell 1} \end{bmatrix}, v' \right)$

s.t. $[A_{1\,id^*_1} \| A_{2\,id^*_2} \| \cdots \| A_{\ell\,id^*_\ell}] = A'$

Sample $A_{j\,(1-id^*_j)}$ at random and with trapdoors T_{A_j} FOR EVERY $j \in [\ell]$

(A', v')

MPK

$\tilde{id}$

$A_{\tilde{id}}$

Find k s.t. $A_{id,k} \cdot e = v'$

Reduction can do this because it has T_{A_j} for some j.

$\begin{bmatrix} A_{10} & \cdots & A_{\ell 0} \\ A_{11} & & A_{\ell 1} \end{bmatrix}$

e

m_0, m_1

ct

m_0, m_1

$ct = Enc_{(A', v')}(m_b)$

b'

(Orthogonal discussions on Random Oracles)