LECTURE - 5

ENCRYPTION SCHEMES

$(\text{KeyGen}, \text{Enc}, \text{Dec})$

$\text{KeyGen}(1^k; r_g) \rightarrow (ek, dk)$

$\text{Enc}(ek, m; r_{enc}) \rightarrow c$

$\text{Dec}(dk, c) \rightarrow m$

CORRECTNESS

$$\Pr_{(ek, dk) \xleftarrow{\$} \text{KeyGen}(1^k)} [\text{Dec}(dk, \text{Enc}(ek, m)) = m]$$

$= 1$ [perfect ~~correction~~ correctness]

or $\geq 1 - \text{negl}(k)$ [statistical correctness]

SEMANTIC OR CPA SECURITY.

DETERMINISTIC ENCRYPTION $\Rightarrow$ $m \xrightarrow{\text{unique}} ct$

Private-Key Encryption $= \{KG, Enc, Dec\}$

$Game(1^k)$:

$\mathcal{A}$ $\qquad$ Ch

$ek = dk = pvt\ key \leftarrow KG(1^k)$

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

$\xrightarrow{m_0, m_1}$

$\xleftarrow{ct = Enc_{pvt\ key}(m_b)}$

$\xrightarrow{m_0', m_1'}$

$\xleftarrow{ct' = Enc_{pvt}(m_b')}$

$\vdots$

$\xrightarrow{b'}$

$\forall$ nu PPT $\mathcal{A}$,

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

Public-Key Encryption.

$\mathcal{A}$ $\qquad$ Ch

$(ek, dk) \leftarrow KG(1^k)$

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

$\xleftarrow{ek}$

$\xrightarrow{m_0, m_1}$

$\xleftarrow{ct = Enc_{ek}(m_b)}$

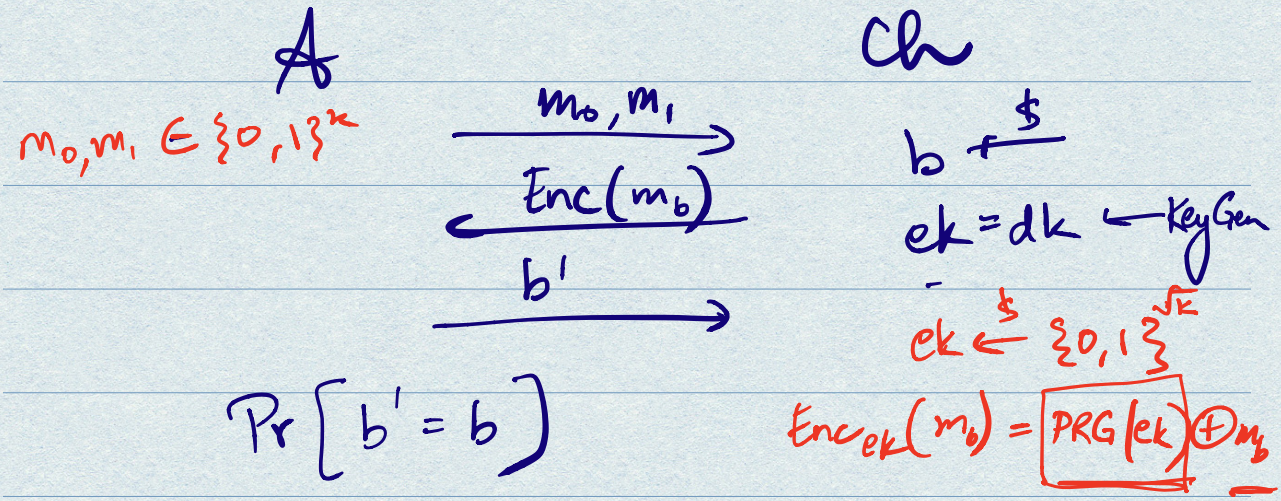
$\xrightarrow{b'}$

$\forall$ nu PPT $\mathcal{A}$,

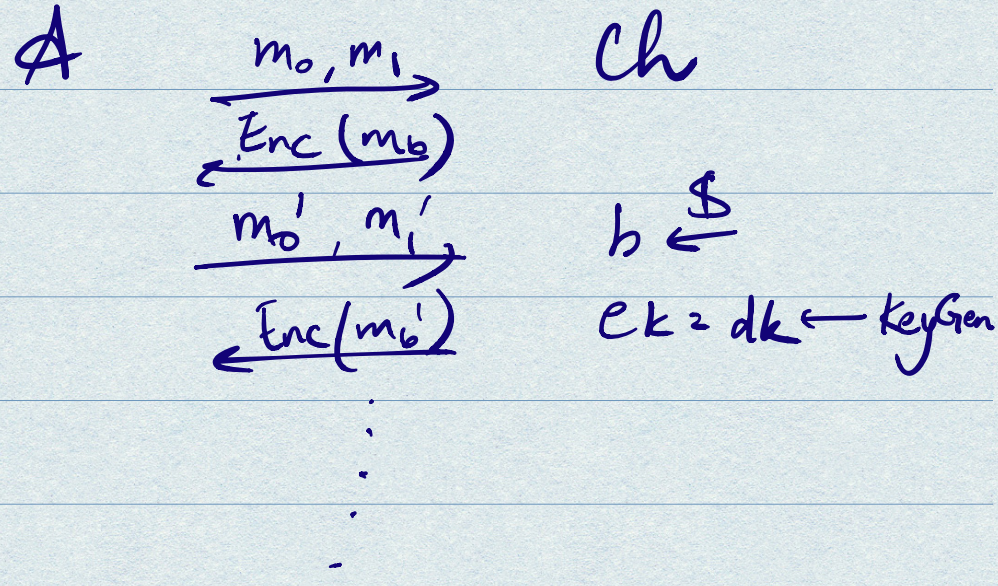
$Pr[b' = b] \leq \frac{1}{2} + negl(k)$

PRIVATE - KEY ENCRYPTION.

"single - message" security:



"multi - message" security:



Simple Pvt key Encryption from a PRF:

$ek = dk = \text{PRF key } K$

$\text{Enc}_K(m)$: Sample x at random.

Output $\left(x, \text{PRF}(K, x) \oplus m\right)$

$\text{Dec}(ct)$: Parse $ct = (x, c)$

Output $\text{PRF}(k, x) \oplus c = m$.

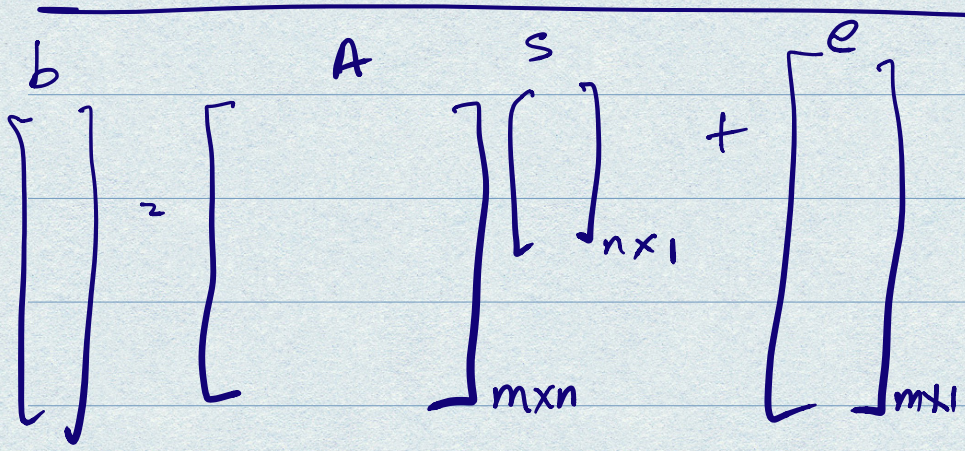
SIS, LWE

↳ OWF $\Rightarrow$ PRG $\Rightarrow$ PRF $\Rightarrow$

[multi-message secure private-key encryption]

PRIVATE-KEY ENCRYPTION

DIRECTLY FROM LWE.



$$\{(A, b) \approx_c (A, \text{uniform})\}_{A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}}$$

$b \in \mathbb{Z}_q^{m \times 1}$ $\quad$ $b \in \mathbb{Z}_q^{m \times 1}$ $\quad$ $\mathbb{Z}_q^{m \times n}$

$\text{KeyGen}(1^n) \longrightarrow s \in \mathbb{Z}_q^{n \times 1}, e \leftarrow \chi^m$

$\text{Enc}(\underset{=s}{sk}, m; r) \longrightarrow A \in \mathbb{Z}_q^{m \times n}$ $\quad$ $r \in \{0,1\}$

$b = As + e$

$\left(A, b' = b + \begin{bmatrix} m \\ \vdots \\ 0 \end{bmatrix}\right)$

$$\text{Enc}(m_0) = A_0, A_0 s + \begin{bmatrix} m_0 \\ \vdots \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

$$\text{Enc}(m_1) = A_1, A_1 s + \begin{bmatrix} m_1 \\ \vdots \\ 0 \\ \vdots \end{bmatrix}$$

$$\text{Enc}(m_0) - \text{Enc}(m_1) = (A_0 - A_1), (A_0 - A_1)\underline{s} + \begin{bmatrix} 0 \text{ or } 1 \\ m_0 - m_1 \\ \vdots \\ 0 \end{bmatrix}$$

$\underline{s}$

✗ THIS IS BAD.

INSTEAD,

$$\text{KeyGen}(1^n) \to \underline{s} \in \mathbb{Z}_q^{n \times 1}.$$

$\text{Enc}(sk, m; r)$: Sample $A_{m \times n}$

$sk = \underline{s}$

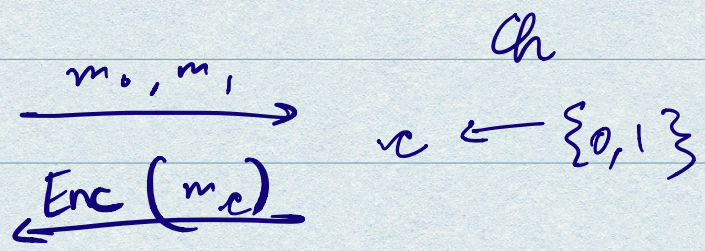
Sample $e_{m \times 1}$

As long as each $|e_i| < \frac{q}{4} \bmod q$.

$$\left(A, As + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix} + \begin{bmatrix} m \cdot \lfloor \frac{q}{2} \rfloor \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right)$$

As

SINGLE-MESSAGE SECURITY.



$$Enc(m_c) = A, As+e+\begin{bmatrix} m_c\lfloor \frac{q}{2} \rfloor \\ \uparrow 0 \\ \downarrow \end{bmatrix}$$

$$\approx_c A, b+\begin{bmatrix} m_c\lfloor \frac{q}{2} \rfloor \\ \uparrow 0 \\ \downarrow \end{bmatrix}_{m\times 1}$$

where $b \xleftarrow{\$} \mathbb{Z}_q^{m\times 1}$

(By $LWE_{m,n,q,\chi}$)

$$= A, b+\begin{bmatrix} m_{1-c}\lfloor \frac{q}{2} \rfloor \\ \uparrow 0 \\ \downarrow \end{bmatrix}$$

$$\approx_c A, As+e+\begin{bmatrix} m_{1-c}\lfloor \frac{q}{2} \rfloor \\ \uparrow 0 \\ \downarrow \end{bmatrix}$$ (By LWE)

$$= Enc(m_{1-c})$$

If $\mathcal{D}_1 \approx_c \mathcal{D}_2$, and $\mathcal{D}_2 \approx_c \mathcal{D}_3$ then $\mathcal{D}_1 \approx_c \mathcal{D}_3$

OPTIMIZED CONSTRUCTION.

OF PVT - KEY ENCRYPTION

$\text{KeyGen}(1^n) \rightarrow \vec{s} \xleftarrow{\$} \mathbb{Z}_q^{n \times 1}$

$\text{Enc}(s, m; r)$: Sample $\vec{a} \xleftarrow{\$} \mathbb{Z}_q^{1 \times n}$

Sample $e \xleftarrow{\$} \chi$.

Output $\vec{a}, \langle \vec{a} . \vec{s} \rangle + e + m\left\lfloor \frac{q}{2} \right\rfloor$

$\text{Dec}(s, c)$: Parse $c = \vec{a}, b'$

Compute $\mu = b' - \langle \vec{a} . \vec{s} \rangle$

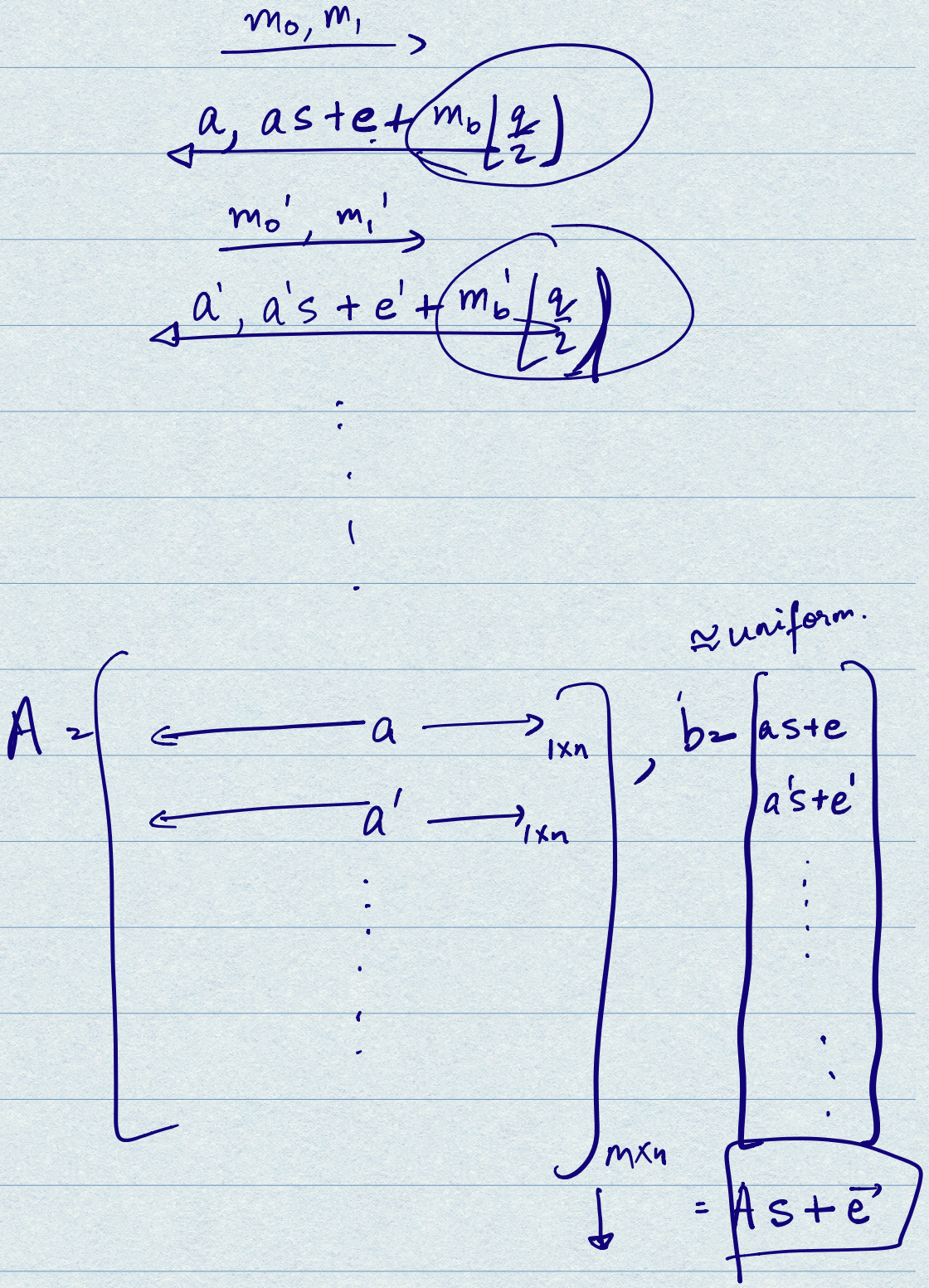
$= e + m\left\lfloor \frac{q}{2} \right\rfloor$

If $-\frac{q}{4} < \mu < \frac{q}{4}$, output $m = 0$

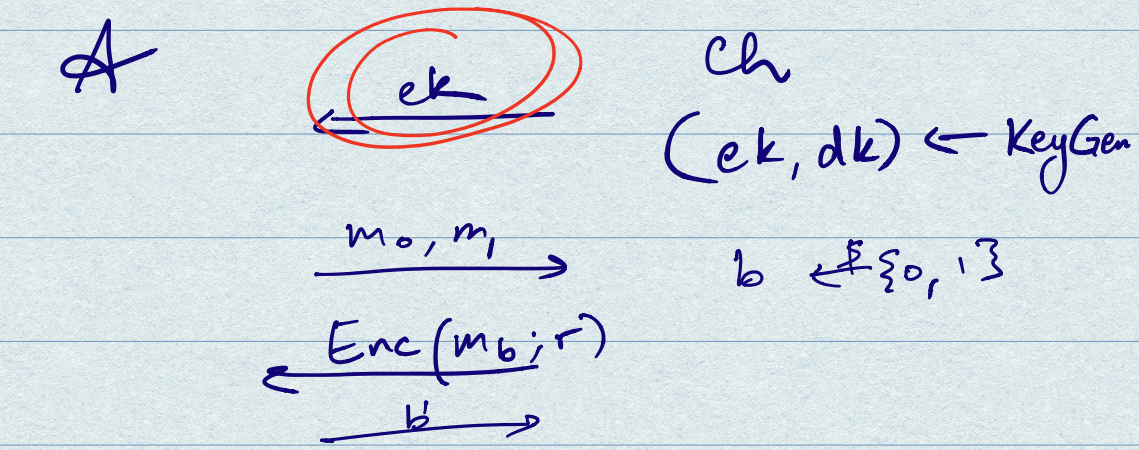
else $m = 1$.

Correctness holds as long as

$|e| < \frac{q}{4} \pmod q$


m_0, m_1
$a,\ as+e+m_b\lfloor\frac{q}{2}\rfloor$
m_0', m_1'
$a',\ a's+e'+m_b'\lfloor\frac{q}{2}\rfloor$
$\approx$ uniform.
$A =$
a
$1\times n$
a'
$1\times n$
$m\times n$
$b =$
$as+e$
$a's+e'$
$= As+\vec{e}$

PUBLIC - KEY ENCRYPTION.



H.W. Prove that in the case of public-key encryption, single-message security $\Rightarrow$ multi-message security.

Public-Key Encryption from LWE:

[Regev] encryption.

Sample $A_{m \times n}, s_{n \times 1}, e \leftarrow \chi^m$.

$\text{KeyGen}(1^\lambda)$: $ek = (A, \underbrace{As + e}_{b}) = (A, b)$

$dk = s$

NOTE: ek is public! So $b \oplus m$ does not hide m!

$\text{Enc}(ek, \mu; r)$: $\mu \hookrightarrow \{0,1\}$

(A, b)

$A = \begin{bmatrix} & \\ & \end{bmatrix}_{m \times n}$ $b = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \end{bmatrix}_{m \times 1}$

Sample $r = [0\,1\,0 \ldots \ldots]_{1 \times m} \leftarrow \{0,1\}^m$

Compute $\underline{rA}$, $\underline{rb + \mu \lfloor \frac{q}{2} \rfloor}$

$[0\,1 \ldots \ldots]_{1 \times m} \begin{bmatrix} & \\ & \end{bmatrix}_{m \times n} = [\quad]_{1 \times n}$ rA

Dec (s, ct)

Parse $ct = c, c'$

$c \to r_A$, $c' \to r_b + \mu\lfloor \frac{q}{2} \rfloor$

Compute $c \cdot s = r_A s$.

" $c' - c \cdot s$

$= r_b - r_A s + \mu\lfloor \frac{q}{2} \rfloor$

$\downarrow$

Aste

$= \cancel{r_A s} + e - \cancel{r_A s} + \mu\lfloor \frac{q}{2} \rfloor$

$\ll \lfloor \frac{q}{2} \rfloor$

MODULUS - TO - NOISE RATIO

"q" "e"

MODULUS / NOISE is relatively "small"

LWE is more secure

MODULUS / NOISE is relatively "large"

LWE is less secure.