PUBLIC-KEY ENCRYPTION FOR CLASSICAL MSGS.

Syntax

(KeyGen, Enc, Dec)

$\text{KeyGen}(1^\lambda) \to (pk, sk)$

$\text{Enc}(\underset{(k)}{pk}, m; r) \to ct$

$\text{Dec}(\underset{(k)}{sk}, ct) \to m$

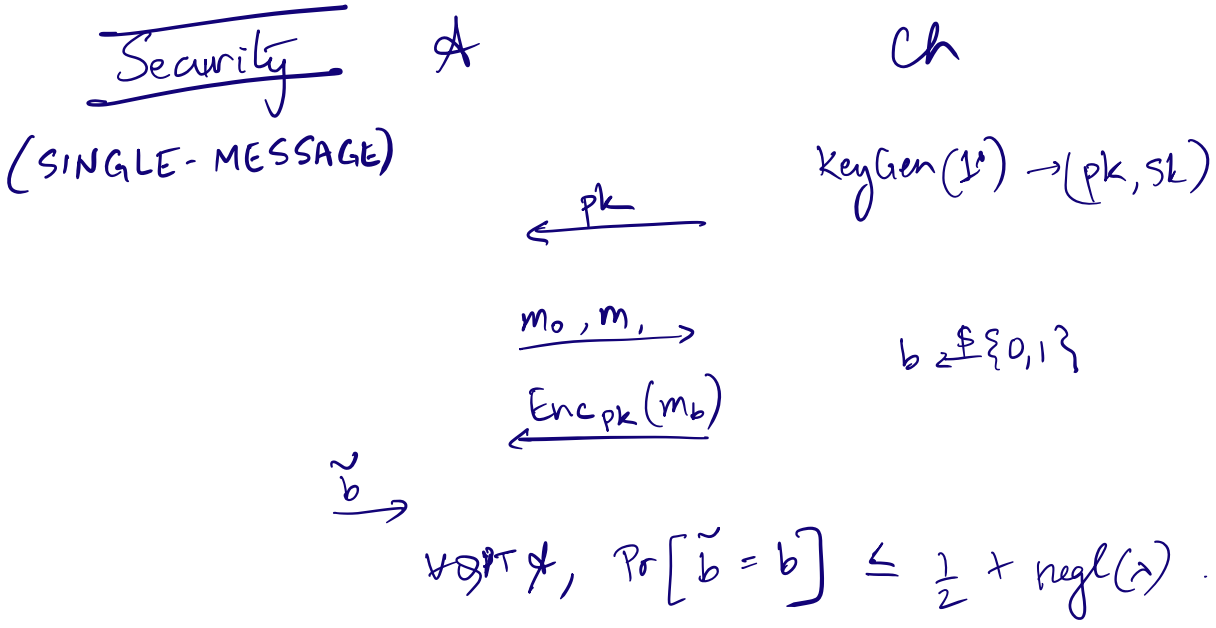
Correctness.

$\forall\, m, (pk, sk) \in \text{Supp}(\text{KeyGen})$

$\Pr_r\left[\text{Dec}(sk, \text{Enc}(pk, m; r)) = m\right] = 1 - \text{negl}(\lambda)$

Security

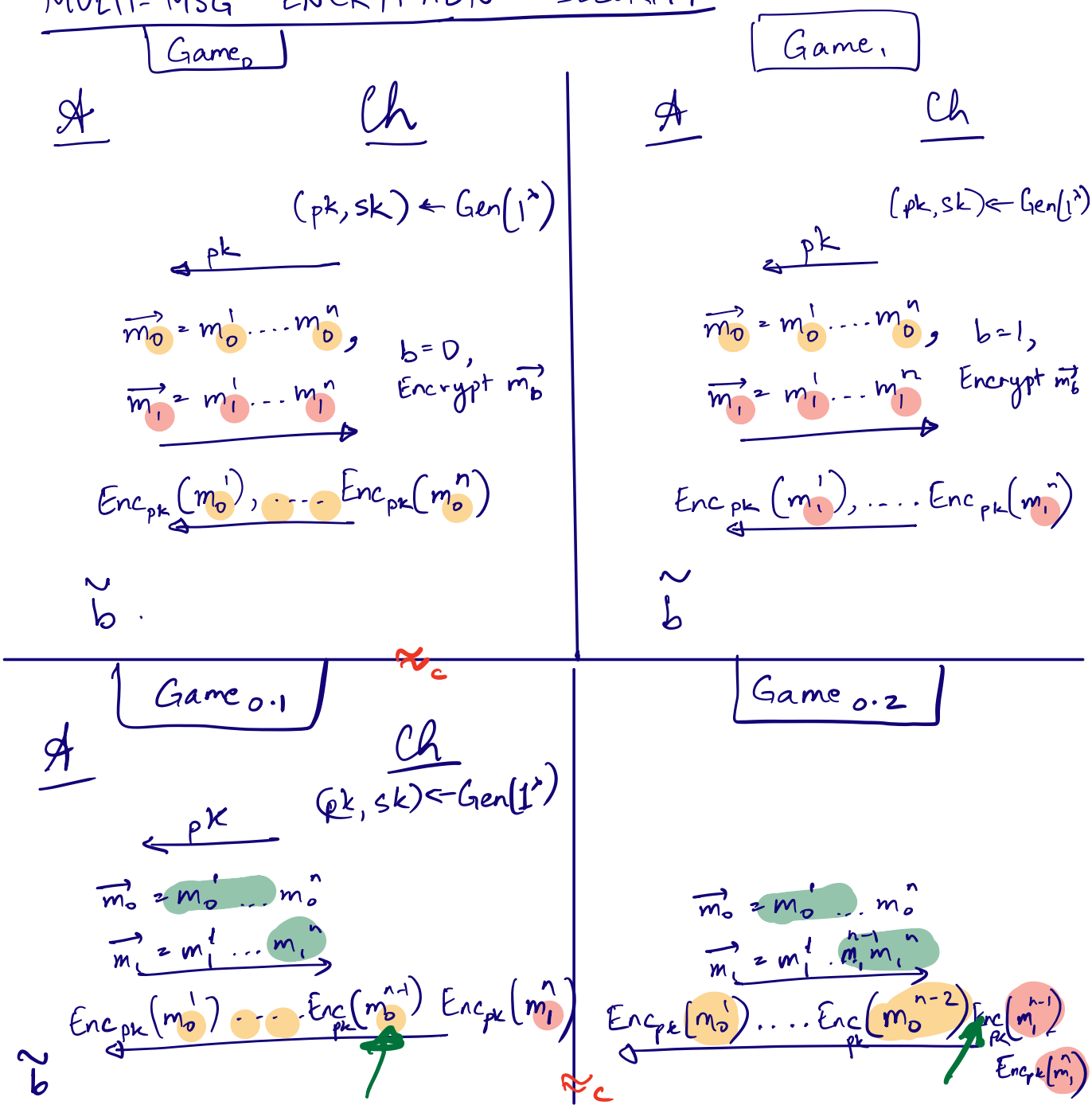
(SINGLE-MESSAGE)



PUBLIC-KEY ENCRYPTION

1) Single-message ⇒ Multi-message security

MULTI-MSG ENCRYPTION: SECURITY



Reduction $\mathcal{R}^{\mathcal{A}}$

Obtains $pk,\ ct \leftarrow Enc(m_b^n)$

Generates $Enc_{pk}(m_0^1) \overset{ct_1}{=} \ldots Enc_{pk}(m_0^{n-1}) \overset{ct_{n-1}}{=}$

Runs $\mathcal{A}[pk](ct_1, ct_2 \ldots ct_{n-1}, ct)] \rightarrow \tilde{b}$

If $Pr[\tilde{b}=1 \mid \text{Game}_0^{b=0}] - Pr[\tilde{b}=1 \mid \text{Game}_{0.1}^{b=1}] > \varepsilon$

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

$$\left| Pr[\tilde{b}=1 \mid Game_0] - Pr[\tilde{b}=1 \mid Game_1] \right| \leq negl(\lambda)$$

$\Updownarrow$ EQUIVALENT DEFNS.

$$\Pr_{b \leftarrow \{0,1\}}[\tilde{b} = b] \leq \frac{1}{2} + negl(\lambda).$$

Employ $Game_b$ strategy

PKE for classical messages from LWE.

$\boxed{(A, As+e) \approx (A, unif)}$

KeyGen $(1^\lambda) \rightarrow pk, sk$

$pk = (A, As+e)$ $\quad sk = s$

$$\left[\begin{array}{c} A \end{array}\right]_{m \times n}, \left[\begin{array}{c} b \\ = As+e \end{array}\right]_{m \times 1}$$

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

$Enc(pk, \mu; r) \rightarrow ct$

$r \leftarrow \{0,1\}^m$. $\quad [\ r\ ]_{1 \times m} \left[\begin{array}{c} A \end{array}\right]_{m \times n}, \underset{1 \times m}{r}\ \underset{m \times 1}{b}$

$= [\ r\ \ A\ ]_{1 \times n}, rb + \mu \lfloor \frac{q}{2} \rfloor$

$= [\ r\ \ A \| b\ ]_{1 \times (n+1)} + [0 \ldots\ldots 0\ \mu \lfloor \frac{q}{2} \rfloor]$

$Dec(sk, ct) \rightarrow \mu$

$sk = s$ $\quad ct = (c_1, c_2)$

$c_1 = rA$ $\quad c_2 = rb + \mu \lfloor \frac{q}{2} \rfloor$

$\boxed{c_2 - c_1 s}$

$= rb + \mu \lfloor \frac{q}{2} \rfloor - rA.s$

$= r(As+e) + \mu \lfloor \frac{q}{2} \rfloor - rAs$

$= re + \mu \left\lfloor \frac{q}{2} \right\rfloor .$

If $|r \cdot e| \leq \frac{q}{10}$, then to decrypt, we would output $\mu = 0$ when $-\frac{q}{10} \leq \boxed{c_2 - c_1 s} \leq \frac{q}{10}$

and $\mu = 1$ when $\frac{q}{2} - \frac{q}{10} \leq c_2 - c_1 s \leq \frac{q}{2} + \frac{q}{10}$

If every coordinate in $e^{m \times 1}$ has absolute value at most β, then $|re| \leq m\beta$.

So, setting $\beta \leq \frac{q}{10m}$, we have that $|r \cdot e| \leq m\beta \leq \frac{mq}{10m} \leq \frac{q}{10}$.

Security: $pk = \begin{bmatrix} A \end{bmatrix} \begin{bmatrix} b \\ = As+e \end{bmatrix}$

$\approx_c$ (by LWE)

$$\begin{bmatrix} A \end{bmatrix} \begin{bmatrix} unif \end{bmatrix} = \begin{bmatrix} c \end{bmatrix}_{m \times (n+1)}$$

$= unif_{m \times (n+1)}$

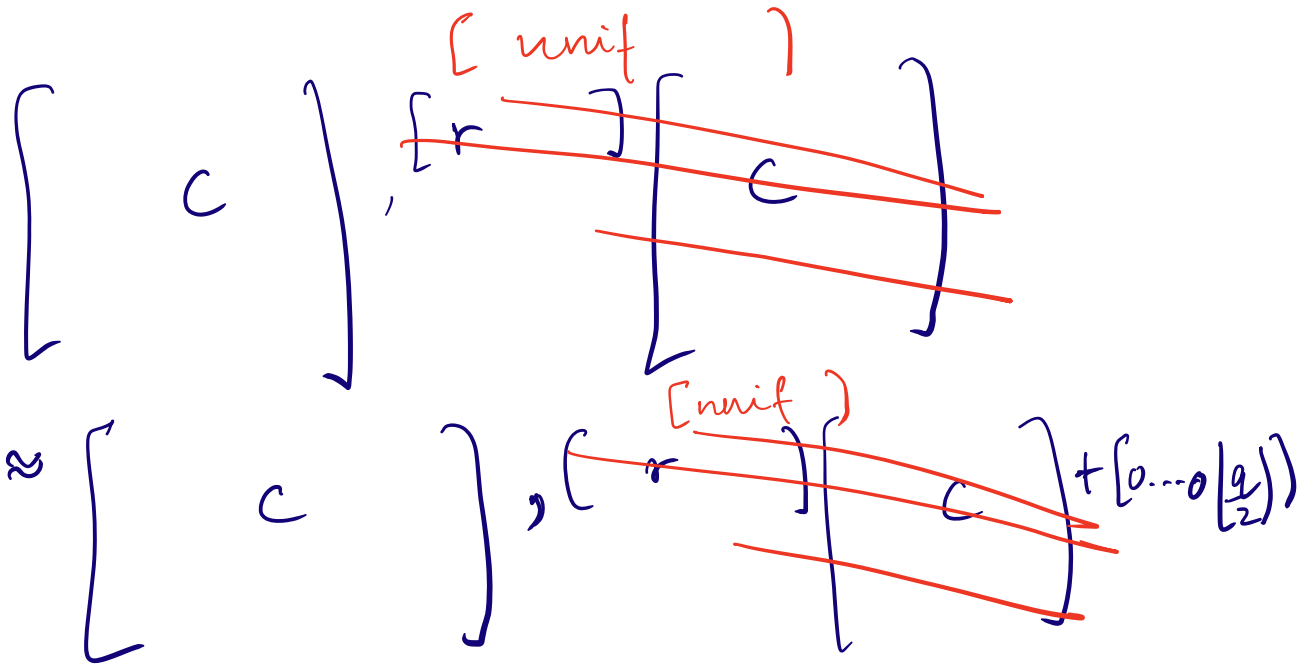
$$ct = [r] \begin{bmatrix} A \end{bmatrix}, rb + \mu \lfloor \frac{q}{2} \rfloor$$

$$= [r] \begin{bmatrix} c \end{bmatrix} + [0 \ldots 0 \ \mu \lfloor \frac{q}{2} \rfloor]$$

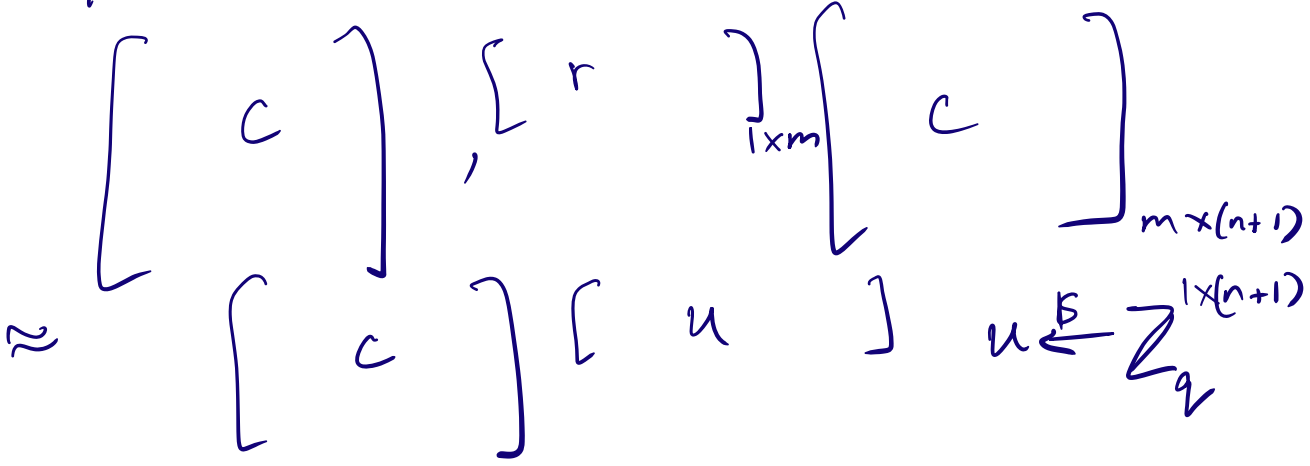
$$pk = \begin{bmatrix} c \end{bmatrix},$$

$$ct = [r] \begin{bmatrix} c \end{bmatrix} + [0 \ldots 0 \ \mu \lfloor \frac{q}{2} \rfloor]$$

Single-msg security in case of 1-bit msgs is equivalent to proving that $pk, Enc_{pk}(0) \approx pk, Enc_{pk}(1)$.



Leftover Hash Lemma ⇒



for any fixed $m \in \mathbb{Z}_q$, $(r + m) \equiv r$ for $r \xleftarrow{\$} \mathbb{Z}_q$

ENCRYPTING QUANTUM STATES

$\text{KeyGen}(1^\lambda) \longrightarrow pk_c, sk_c$

$\text{Enc}(pk, \rho) \longrightarrow a, b \xleftarrow{\$} \{0,1\}^2$

$\sigma = X^a Z^b \rho (X^a Z^b)^\dagger$

$ct = \text{Enc}_c(pk_c, (a, b))$

Output (σ, ct).

(ρ: single qubit density matrix)

$\text{Dec}(sk, ct = (\sigma, ct))$

$\text{Dec}_c(sk, ct) \rightarrow (a, b)$

$\rho = (X^a Z^b)^\dagger \sigma (X^a Z^b)$.

Security : $\forall \rho_1, \rho_2$

$$\left| \Pr\left[\tilde{b}=1 \mid pk, \mathrm{Enc}(pk,\rho_1)\right] - \Pr\left[\tilde{b}=1 \mid pk, \mathrm{Enc}(pk,\rho_2)\right] \right| \leq \mathrm{negl}(\lambda)$$

$pk, \mathrm{Enc}(pk,\rho_1)$ | $pk, \mathrm{Enc}(pk,\rho_2)$

$pk, \mathrm{Enc}_{pk}(a,b), X^a Z^b \rho_1 (X^a Z^b)^\dagger$ | $pk, \mathrm{Enc}_{pk}(a,b), X^a Z^b \rho_2 (X^a Z^b)^\dagger$

$(a,b) \xleftarrow{\$} \{0,1\}^2$ | $(a,b) \leftarrow \{0,1\}^2$.

$\approx_c$ By security of classical encryption | $\approx_c$ By security of classical encryption

$pk, \mathrm{Enc}_{pk}(0,0), X^a Z^b \rho_1 (X^a Z^b)^\dagger$ | $pk, \mathrm{Enc}_{pk}(0,0), X^a Z^b \rho_2 (X^a Z^b)^\dagger$

$(a,b) \xleftarrow{\$} \{0,1\}^2$ | $(a,b) \xleftarrow{\$} \{0,1\}^2$

$=$ | $=$

$pk, \mathrm{Enc}_{pk}(0,0), \frac{\mathbb{I}}{2}$ | $=$