

Public-Key-Encryption:

Defn: A public key encryption is a tuple of three algorithms:-

(a) Key-Generation algorithm:-

on input 1^n , it outputs (pk, sk) . - probabilistic algorithm.

(b) Encryption algorithm:- on input a public key pk , a message m , it outputs a ciphertext $ct \leftarrow \text{Enc}_{pk}(m)$ probabilistic algorithm.

(c) Decryption algorithm:- on input a secret key sk , and a ciphertext ct , it outputs either a message m or abort, i.e., $m / \textcircled{1} \leftarrow \text{Dec}_{sk}(ct)$.

Correctness condition:-

Decryption error.

$$P_r \left[\text{Dec}_{sk}(\text{Enc}_{pk}(m)) = m \right] \geq 1 - \delta, \text{ where } \delta \text{ is negligible}$$

$\forall m \in \mathcal{M}, \forall (pk, sk) \leftarrow \text{Key-Gen}(1^n)$.

Security notion:

$\text{PubK}_{A,\Pi}^{\text{eav}}(n)$

1. $\text{Gen}(1^n)$ is run to obtain (PK, SK) .
2. A is given PK ; A outputs two msg. m_0, m_1 and sends it to the challenger.
3. Challenger samples $b \leftarrow \{0, 1\}$ and computes $c \leftarrow \text{Enc}_{PK}^{\$}(m_b)$ and sends it to A .
4. A returns a bit $\hat{b}$
5. output 1 if $b = \hat{b}$

Defn $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ has indistinguishable encryption in the presence of an eavesdropper if $\forall$ PPT algorithm A , $\exists$ a negl fn $\text{negl}()$ such that

$$\Pr[\text{PubK}_{A,\Pi}^{\text{eav}}(n) = 1] \leq \frac{1}{2} + \text{negl}(n).$$

Security against multiple encryptions:

LR-oracle experiment $\text{PubK}_{A,\pi}^{\text{LR-CPA}}(n)$.

1. $\text{Gen}(1^n)$ is run to obtain (PK, SK) .
2. A uniform bit $b \xleftarrow{\$} \{0,1\}$ is chosen.
3. A is given PK and is given oracle access to $\text{LR}_{PK,b}(\cdot, \cdot)$.
4. A outputs a bit $\hat{b}$.
5. output 1 if $\hat{b} = b$.

Thm: If public key encryption Π is CPA-secure, then Π has indistinguishable multiple encryptions.

Pf: $(m_{1,0}, m_{1,1})$:- 1st query
 $(m_{2,0}, m_{2,1})$:- 2nd query

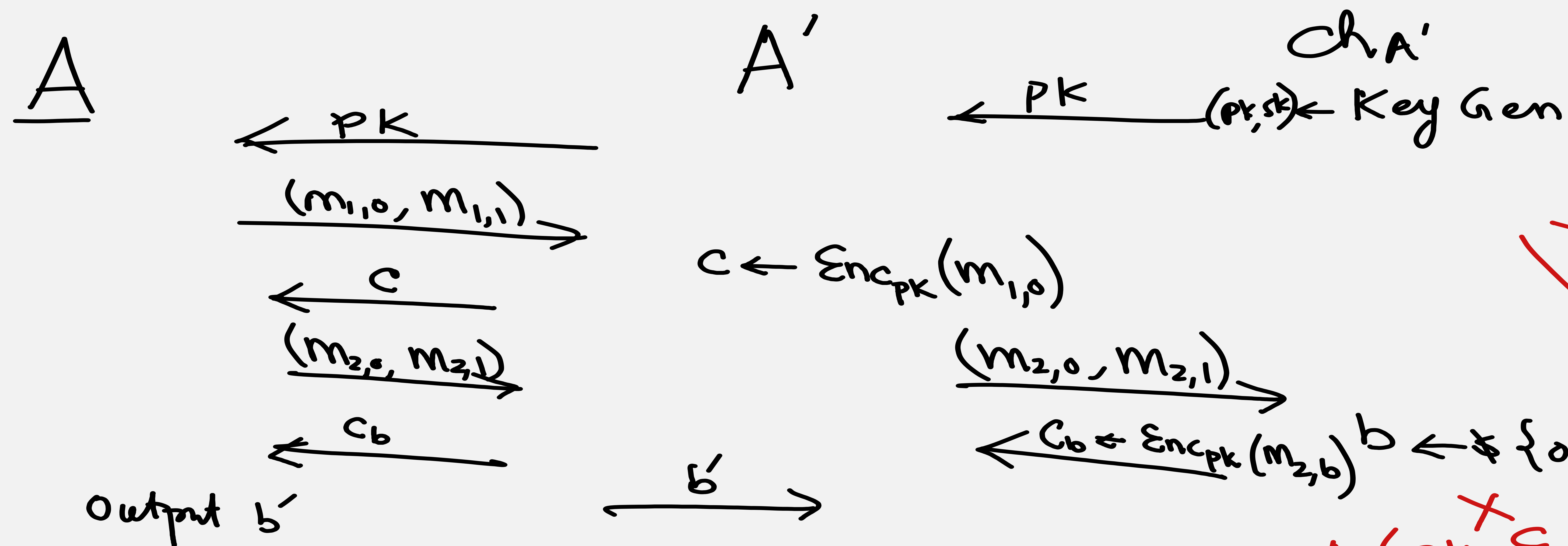
A breaks multiple encryption
 we construct A' breaks CPA of Π

$A(PK, \text{Enc}_{PK}(m_{1,0}), \text{Enc}_{PK}(m_{2,0}))$
 or $A(PK, \text{Enc}_{PK}(m_{1,1}), \text{Enc}_{PK}(m_{2,1}))$.

$$\left| \Pr \left[A(PK, \overset{= C_0}{\text{Enc}_{PK}(m_{1,0})}, \text{Enc}_{PK}(m_{2,0})) = 1 \mid b=0 \right] - \Pr \left[A(PK, \underset{= C_1}{\text{Enc}_{PK}(m_{1,1})}, \text{Enc}_{PK}(m_{2,1})) = 1 \mid b=1 \right] \right| \leq \text{negl}(n).$$

$C_0 \sim C_{0,1}$
 $C_{0,1} \sim C_1$

A' is given pk



$$\begin{aligned}
 & |x - y| \\
 &= |x - w + w - y| \\
 &\leq |x - w| + |w - y|
 \end{aligned}$$

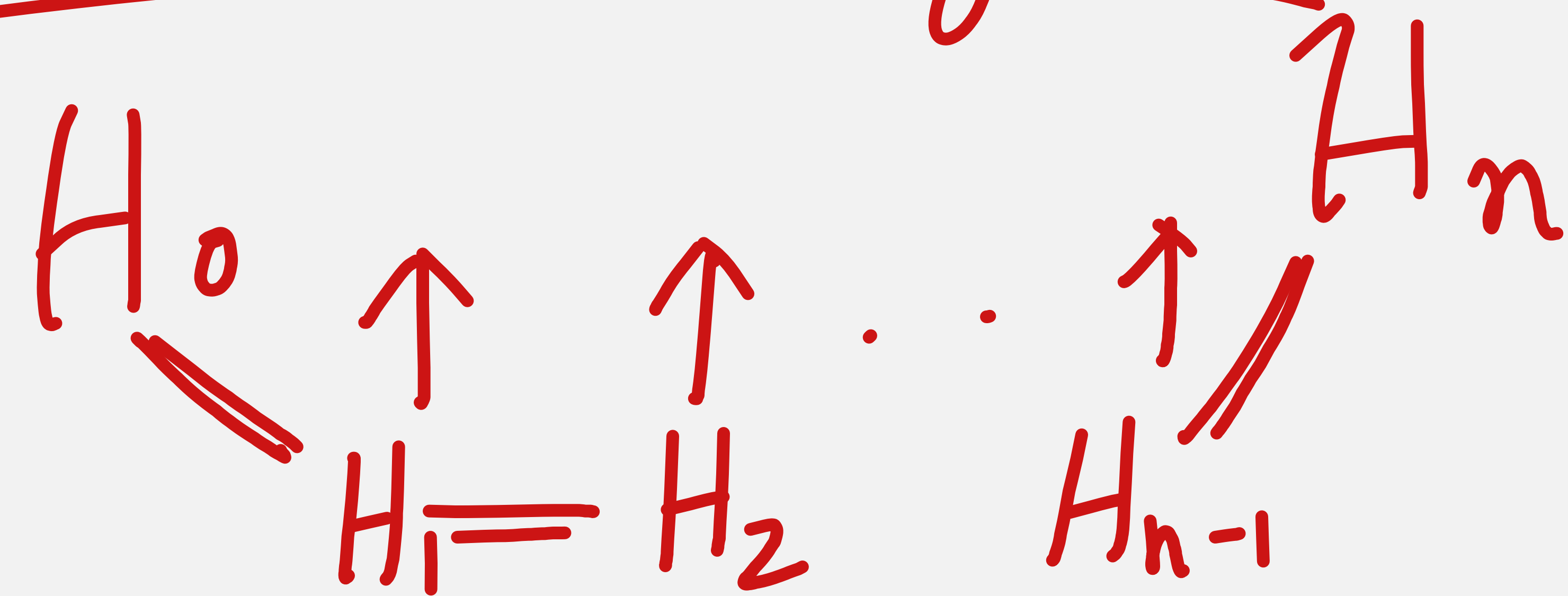
$$\begin{aligned}
 & A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) \text{ when } b=0 \\
 & A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,1})) \text{ when } b=1
 \end{aligned}$$

$$\begin{aligned}
 & A(pk, \text{Enc}(m_{1,0}), \text{Enc}(m_{2,0})) \\
 & (pk, \text{Enc}(m_{1,1}), \text{Enc}(m_{2,1}))
 \end{aligned}$$

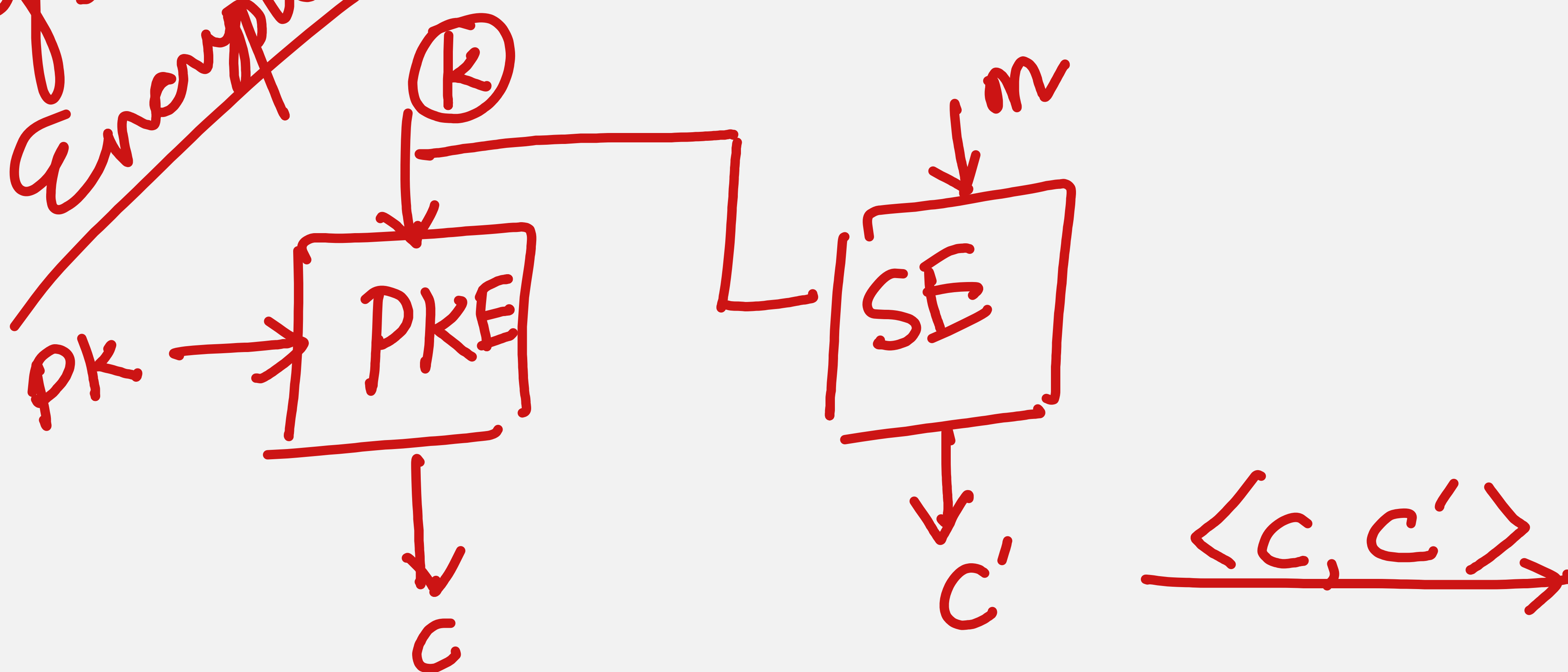
$$\Pr[A'(pk, \text{Enc}_{pk}(m_{2,0})) = 1] = \Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1]$$

$$\Pr[A'(pk, \text{Enc}_{pk}(m_{2,1})) = 1] = \Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,1})) = 1]$$

Two extreme hybrids.



Hybrid
Encryption



$$\begin{aligned}
 & \Pr[\hat{b} = b] \leq \frac{1}{2} + \text{negl}(n) \\
 & \Pr[\hat{b} = 0 \wedge b = 0] + \Pr[\hat{b} = 1 \wedge b = 1] \\
 & = \Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 0 \mid b = 0] \cdot \frac{1}{2} \\
 & \quad + \Pr[A(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1 \mid b = 1] \cdot \frac{1}{2} \\
 & \frac{1}{2} \left[1 - \Pr[A(pk, \dots) = 1 \mid b = 0] + \Pr[A(\dots) = 1 \mid b = 1] \right]
 \end{aligned}$$

Key-encapsulation Mechanism (KEM)

