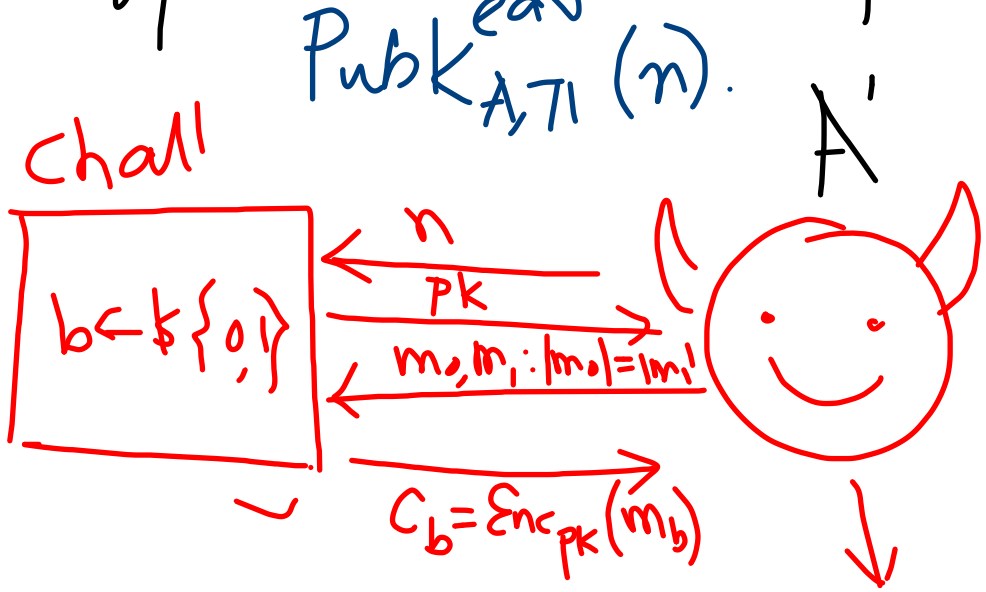
Thm: If PKE Π has indistinguishable encryption in the presence of an eavesdropper then Π has indistinguishable multiple encryption in the presence of an eavesdropper.

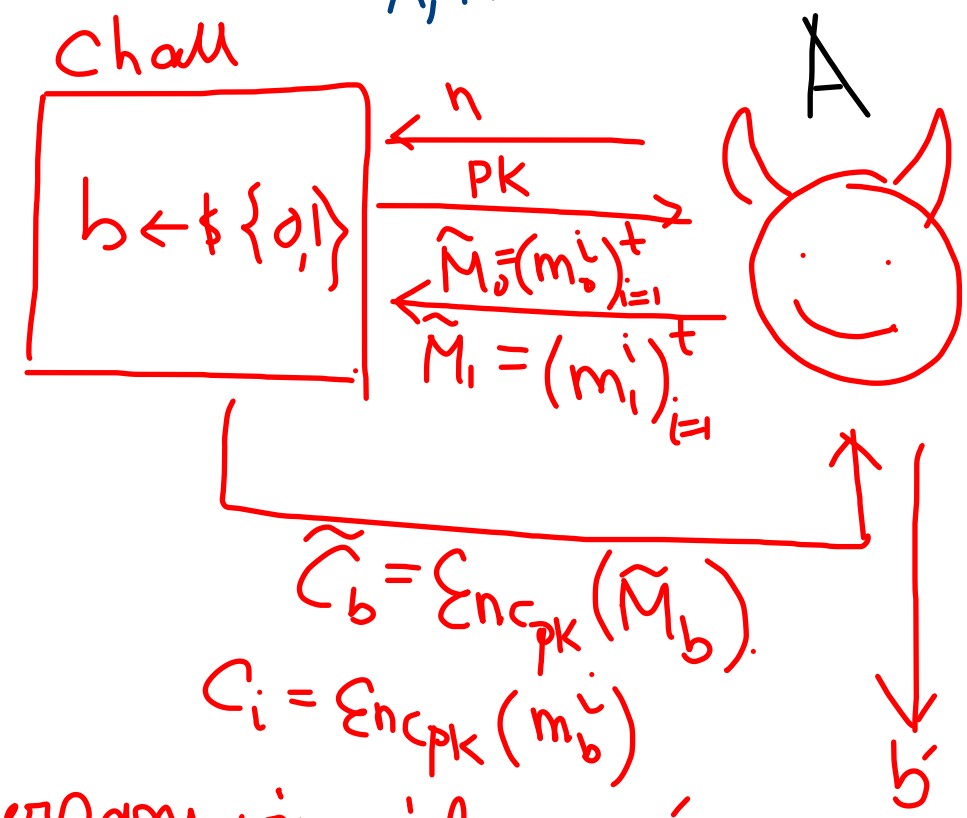
$PubK^{eav}_{A,\Pi}(n)$.



Adversary wins if $b = b'$

$C_b^i = Enc_{pk}(m_b^i)$.

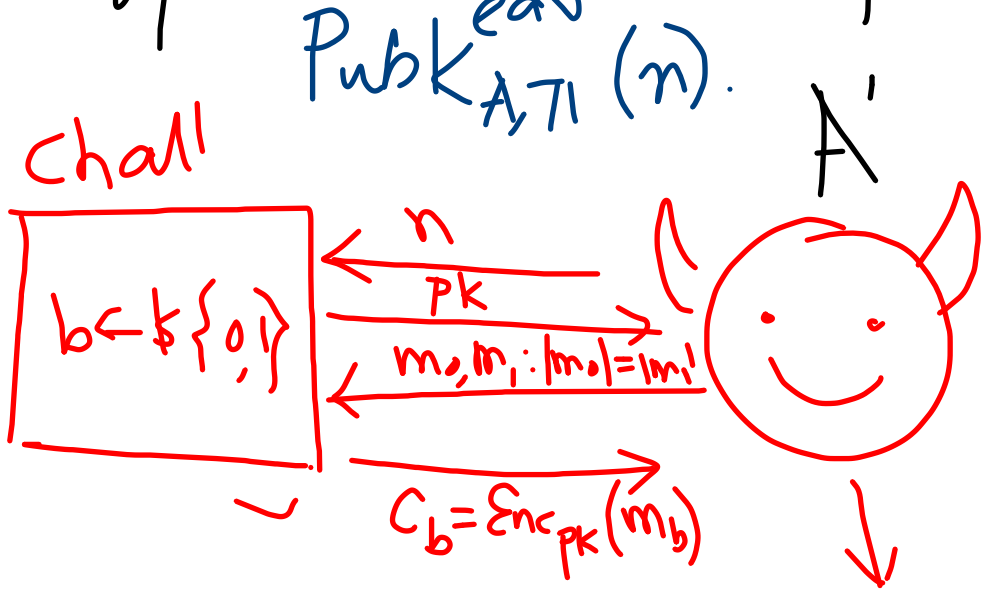
$PubK^{mult}_{A,\Pi}(n)$.



Adversary wins if $b = b'$

Thm: If PKE Π has indistinguishable encryption in the presence of an eavesdropper then Π has indistinguishable multiple encryption in the presence of an eavesdropper.

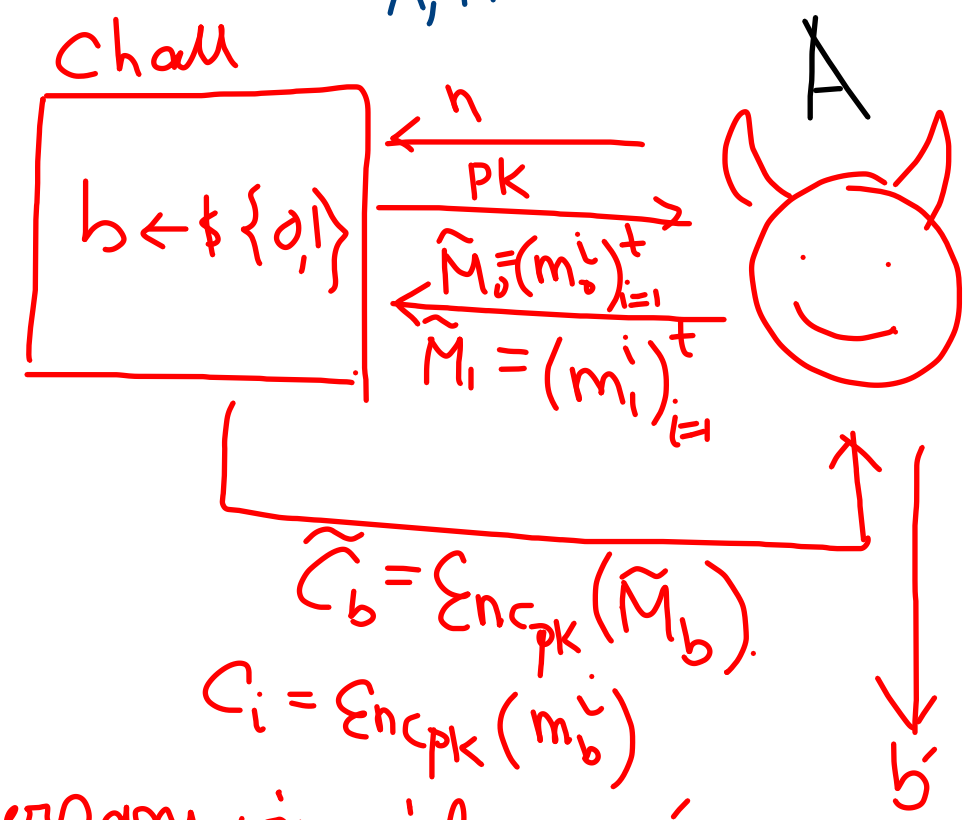
$PubK^{eav}_{A,\Pi}(n)$.



Adversary wins if $b = b'$

$C_b^i = Enc_{pk}(m_b^i)$.

$PubK^{mult}_{A,\Pi}(n)$.



Adversary wins if $b = b'$

Pf: Let A be a PPT adversary and consider the experiment "$PubK^{mult}_{A,\Pi}(n)$." Let $t(n)$ be the upper bound on the no. of messages in each of the two vectors output by A.

For a given public key pk, and two vectors $\tilde{M}_0 = (m_0^1, m_0^2, \ldots, m_0^t)$ $\tilde{M}_1 = (m_1^1, m_1^2, \ldots, m_1^t)$ output by A, we define.

$$\tilde{C}^i = \left(Enc_{pk}(m_0^1), \cdots Enc_{pk}(m_0^i), Enc_{pk}(m_1^{i+1}), \ldots Enc_{pk}(m_1^t)\right)$$

for all $0 \le i \le t$

Pf: Let A be a PPT adversary and consider the experiment "$PubK^{mult}_{A,\Pi}(n)$." Let $t(n)$ be the upper bound on the no. of messages in each of the two vectors output by A.

For a given public key pk, and two vectors $\tilde{M}_0 = (m_0^1, m_0^2, \ldots, m_0^t)$ $\tilde{M}_1 = (m_1^1, m_1^2, \ldots, m_1^t)$ output by A, we define.

$$\tilde{C}^i = \left(Enc_{pk}(m_0^1), \cdots Enc_{pk}(m_0^i), Enc_{pk}(m_1^{i+1}), \ldots Enc_{pk}(m_1^t)\right)$$

for all $0 \le i \le t$

$\tilde{C}^i$ is called a "hybrid" random variable.

Suppose $i=0$

$\tilde{C}^0 \equiv \tilde{C}_1$

Suppose $i=t$

$\tilde{C}^t \equiv \tilde{C}_0$

$1 \le i \le t$ s.t

A can distinguish $\tilde{C}^i$ from $\tilde{C}^{i-1}$

If adversary can't distinguish $\tilde{C}_0$ from $\tilde{C}_1$, then.

It can't distinguish the two extreme hybrid random variables. namely $\tilde{C}^0, \tilde{C}^t$

Let us consider a PPT A'

Algorithm A'

- On i/p pk, A' will run A with pk and A' will obtain two vectors

$$\tilde{M}_0 = (m_0^1, m_0^2, \ldots, m_0^t)$$

$$\tilde{M}_1 = (m_1^1, m_1^2, \ldots, m_1^t) \text{ with } t = t(n).$$

- A' will choose a random index $i \leftarrow_R \{1, \ldots, t\}$ and outputs the pair of messages (m_0^i, m_1^i) to its own challenger. Let C' be the obtained ciphertext.

Let us consider a PPT A'

Algorithm A'

- On i/p pk, A' will run A with pk and A' will obtain two vectors

$$\tilde{M}_0 = (m_0^1, m_0^2, \ldots, m_0^t)$$

$$\tilde{M}_1 = (m_1^1, m_1^2, \ldots, m_1^t) \text{ with } t = t(n).$$

- A' will choose a random index $i \leftarrow_R \{1, \ldots, t\}$ and outputs the pair of messages (m_0^i, m_1^i) to its own challenger. Let c^i be the obtained ciphertext.

- for $j < i$, computes $c^j \leftarrow Enc_{pk}(m_0^j)$
  for $j > i$, computes $c^j \leftarrow Enc_{pk}(m_1^j)$.
  returns $c = (c^1, c^2, \uparrow_{i^*}, c^t)$. $c^{i^*} = Enc_{pk}(m_0^{i^*})$.
- outputs b' if A output b'

- In the experiment $Pubk^{eav}_{A',\pi}(n)$, when $b = 0$ and $i = i^*$, then A runs on an i/p which is distributed according to $\tilde{C}^{i^*}$.
- In the experiment $Pubk^{eav}_{A',\pi}(n)$, when $b = 1$ and $i = i^*$, then A runs on an i/p which is distributed according to $\tilde{C}^{(i^*-1)}$

- for $j < i$, computes $c^j \leftarrow Enc_{pk}(m_0^j)$
  for $j > i$, computes $c^j \leftarrow Enc_{pk}(m_1^j)$.
  returns $c = (c^1, c^2, \uparrow_{i^*}, c^t)$.
- outputs b' if A output b'

- In the experiment $Pubk^{eav}_{A',\Pi}(n)$, when $b = 0$ and $i = i^*$, then A runs on an i/p which is distributed according to $\tilde{C}^{i^*}$.
- In the experiment $Pubk^{eav}_{A',\Pi}(n)$, when $b = 1$ and $i = i^*$, then A runs on an i/p which is distributed according to $\tilde{C}^{(i^*-1)}$

$$\Pr\left[\mathrm{PubK}^{eav}_{A',\pi}(n)=1\right]$$

$$= \Pr\left[\mathrm{PubK}^{eav}_{A',\pi}(n)=1 \wedge b=0\right]$$

$$+ \Pr\left[\mathrm{PubK}^{eav}_{A',\pi}(n)=1 \wedge b=1\right].$$

$$= \frac{1}{2}\cdot \boxed{\Pr\left[A' \text{ outputs } 0 \mid b=0\right]}$$

$$+ \frac{1}{2}\cdot \Pr\left[A' \text{ outputs } 1 \mid b=1\right].$$

$$\Pr\left[A' \text{ outputs } 0 \mid b=0\right] = \sum_{i^*=1}^{t} \Pr\left[A' \text{ outputs } 0 \wedge i=i^* \mid b=0\right].$$

$$\Rightarrow \Pr[A' \text{ outputs } 0 \mid b=0]$$

$$= \sum_{i^*=1}^{t} \Pr[A' \text{ outputs } 0 \mid b=0 \wedge i=i^*] \times \Pr[i=i^*]$$

$$= \frac{1}{t} \sum_{i^*=1}^{t} \Pr[A' \text{ outputs } 0 \mid b=0 \wedge i=i^*].$$

$$= \frac{1}{t} \sum_{i^*=1}^{t} \Pr_{y \leftarrow \tilde{C}^{i^*}}[A(y)=0]$$

Similarly, $\Pr[A' \text{ outputs } 1 \mid b=1] = \frac{1}{t} \sum_{i^*=1}^{t} \Pr_{y \leftarrow \tilde{C}^{(i^*-1)}}[A(y)=1]$ ∧

$$= \frac{1}{2} \quad \frac{1}{t}\left[\sum_{i^*=1}^{t} \Pr_{y \leftarrow \tilde{C}^{i^*}}[A(y)=0] + \sum_{i^*=1}^{t} \Pr_{y \leftarrow \tilde{C}^{(i^*-1)}}[A(y)=1]\right]$$

$$= \frac{1}{2t}\left[\sum_{i^*=1}^{t} \Pr_{y \leftarrow \tilde{C}^{i^*}}[A(y)=0] + t - \sum_{i^*=1}^{t} \Pr_{y \leftarrow \tilde{C}^{(i^*-1)}}[A(y)=0]\right]$$

$$= \frac{1}{2} + \frac{1}{2t}\left[\sum_{i^*=1}^{t} \left\{\Pr_{y \leftarrow \tilde{C}^{i^*}}[A(y)=0] - \Pr_{y \leftarrow \tilde{C}^{(i^*-1)}}[A(y)=0]\right\}\right]$$

$$= \frac{1}{2} + \frac{1}{2t}\left[\Pr_{y \leftarrow \tilde{C}^{t}}[A(y)=0] - \Pr_{y \leftarrow \tilde{C}^{0}}[A(y)=0]\right]$$

$$= \frac{1}{2} + \frac{1}{2t}\left[\Pr_{y \leftarrow \tilde{C}^{t}}[A(y)=0] - 1 + \Pr_{y \leftarrow \tilde{C}^{0}}[A(y)=1]\right]$$

$$P_\gamma\left[\mathrm{PubK}^{\mathrm{mult}}_{A,\pi}(n)=1\right] > \frac{1}{2}+\varepsilon(n)$$

$$\| \text{(by def.)}$$

$$= \frac{1}{2}\cdot P_\gamma\left[A(y)=0\right] + \frac{1}{2}\cdot P_\gamma\left[A(y)=1\right]$$

$$y\leftarrow \tilde{C}^t \qquad\qquad y\leftarrow \tilde{C}^\circ$$

$$> \frac{1}{2}+\varepsilon(n) \quad \text{where } \varepsilon(n)=\text{non-negl. fn.}$$

$$P_0\left[\mathrm{PubK}^{\mathrm{mult}}_{A,\pi}(n)=1\right] > \frac{1}{2}+\varepsilon(n)$$

$$= \frac{1}{2}\cdot P_0\left[A(y)=0\right] + \frac{1}{2}\cdot P_1\left[A(y)=1\right]$$

$y \leftarrow \tilde{C}^t$ $\qquad$ $y \leftarrow \tilde{C}^0$

$$> \frac{1}{2}+\varepsilon(n) \quad \text{where } \varepsilon(n) = \text{non-negl. fn}$$

$$= \frac{1}{2}\left[P_0\left[A(y)=0\right] + P_1\left[A(y)=1\right]\right] > \frac{1}{2}+\varepsilon(n)$$

$$= \frac{1}{2} - \frac{1}{2t} + \frac{1}{2t}\Big[\underbrace{\Pr_{y \leftarrow \tilde{C}^t}[A(y)=0] + \Pr_{y \leftarrow \tilde{C}^*}[A(y)=1]}_{> \frac{1}{2} + \varepsilon(n)} \Big]$$

$$> \frac{1}{2t} + \frac{\varepsilon(n)}{t} + \frac{1}{2} - \frac{1}{2t}$$

$$\Rightarrow \quad \frac{1}{2t}\Big[\qquad \Big] > \frac{1}{2t} + \varepsilon(n).$$

$$= \frac{1}{2} + \frac{\varepsilon(n)}{t}$$

$$\Rightarrow \quad \frac{1}{2}\Big[\Pr_{y \leftarrow \tilde{C}^t}[A(y)=0] + \Pr_{y \leftarrow \tilde{C}^*}[A(y)=1] \Big] > \frac{1}{2} + t\varepsilon(n)$$

$$= \Pr\Big[Priv^{mult}_{A,\Pi}(n) = 1 \Big] > \frac{1}{2} + t \cdot \varepsilon(n)$$