Multiple encryptions + CPA Security

* Ind security holds only if adversary sees exactly one encryption] ⇒ the same key can be used only once [like perfect secrecy] even though key can be smaller then message

Consider following experiment for scheme $\mathcal{E} = (G, E, D)$ and adversary A

Multiple $Ind_A^{\mathcal{E}}(n)$

$A \leftrightarrow \bar{m}_0, \bar{m}_1$ vectors of t messages of same length
$k \leftarrow \{0,1\}^n$; $b \leftarrow \{0,1\}$
$b' \leftarrow A(E(k, m_b^1), \dots, E(k, m_b^t))$
if $b = b'$ return 1 else return 0

Def. $\mathcal{E}$ is multi ind secure if
$\forall$ PPT A $\exists \nu$ negligible s.t.

$$Prob[Multiple\,Ind_A^{\mathcal{E}}(n) = 1] \leq \frac{1}{2} + \nu(n)$$

Obs. Previous scheme (based on PRG) is not MIND-secure. Consider A outputs
$\bar{m}_0 = (0^n, 0^n)$ and $\bar{m}_1 = (0^n, 1^n)$
if $b=0$ A receives $(E(k,0^n), E(k,0^n))$
if $b=1$ $(E(k,0^n), E(k,1^n))$

Consider following attack (experiment)

$CPA_A^{\mathcal{E}}(n)$

1. $k \leftarrow \{0,1\}^n$
2. Query phase
   A asks for $m \in \{0,1\}^*$ and obtains $E(k,m)$
3. A returns (m_0, m_1)
4. $b \leftarrow \{0,1\}$
5. $c \leftarrow E(k, m_b)$ is given to A
6. 2nd Query phase
7. $b' \leftarrow A(c)$
8. If $b = b'$ return 1
   else return 0

$MCPA_A^{\mathcal{E}}(n)$

1.
2.
3. A return $(\bar{m}_0, \bar{m}_1)$ (vectors)
5. $\bar{c} = (E(k, m_b^1), \dots, E(k, m_b^t))$ is given to A
7. $b' \leftarrow A(\bar{c})$

Def. $\mathcal{E}$ is CPA-secure (MCPA-secure) if for all A PPT $\exists \nu$ s.t.

$$Prob[CPA_A^{\mathcal{E}}(n) = 1] \leq \frac{1}{2} + \nu(n)$$

$$\left(Prob[MCPA_A^{\mathcal{E}}(n) = 1] \leq \frac{1}{2} + \nu(n)\right)$$

Obs. No deterministic encryption scheme can be CPA-secure
in 2 ask for $E(k, m_0) = c_0$
$E(k, m_1) = c_1$
in 3 return (m_0, m_1)
in 5 receive c_0 or c_1

Thm $\mathcal{E}$ is CPA secure iff $\mathcal{E}$ is MCPA secure

Proof One direction is trivial. We prove the other.

Let $\bar{m}_0$ and $\bar{m}_1$ be the two vectors output by adversary A in $MCPA_A^{\mathcal{E}}(n)$
Let M_i be the vector $(m_0^1 \ldots m_0^i, m_1^{i+1} \ldots m_1^t)$
Observe that $\bar{m}_0 = M_t$ and $\bar{m}_1 = M_1$.
Let $MCPA_A^{\mathcal{E}}(n,i)$ be the experiment in which at step 5 A receives an encryption of M_i
Let $OutMCPA_A^{\mathcal{E}}(n,i)$ be the random variable of A's output in $MCPA_A^{\mathcal{E}}(n,i)$ and
let $p_i = Prob[OutMCPA_A^{\mathcal{E}}(n,i) = 1]$.

Now we have that $p_0 = Prob[MCPA_A^{\mathcal{E}}(n) = 1 \mid b=1] =$
$p_t = Prob[OutMCPA_A^{\mathcal{E}}(n) = 1] = 1 - Prob[MCPA_A^{\mathcal{E}}(n) = 1 \mid b=0]$

If A wins the MCPA game then we have

$$\frac{1}{2} + \frac{1}{p(n)} \le Prob[MCPA_A^{\mathcal{E}}(n) = 1] = \frac{1}{2}\left[Prob[MCPA_A^{\mathcal{E}}(n)=1 \mid b=0] + Prob[MCPA_A^{\mathcal{E}}(n)=1 \mid b=1]\right]$$

$$= \frac{1}{2}[1 - p_t + p_0] \Rightarrow p_0 - p_t \ge \frac{2}{p(n)} \quad \text{for a poly } p(n)$$

$\Rightarrow \exists i$ s.t. $|p_i - p_{i+1}| \ge \frac{2}{t \cdot p(n)}$. Assume $p_i \ge p_{i+1} + \frac{2}{t \cdot p(n)}$

Now we construct B that uses A and breaks CPA
B runs A and in Query phase 1, B makes the same queries of A
When A outputs $\bar{m}_0$ and $\bar{m}_1$ B returns m_0^{i+1} and m_1^{i+1} and obtain c

B uses oracle for obtaining encryption

$m_0^1 \ldots m_0^i \quad m_1^{i+2} \ldots m_1^t$ and runs A on $\bar{c}$
$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$ and returns A's output
$\bar{c} \quad (c_1 \quad e_i \quad c \quad e_{i+2} \quad c_t)$

If c is encryption of m_1^{i+1} then $\bar{c}$ is like in $MCPA_A^{\mathcal{E}}(n,i)$ and prob A gives 1 is p_i
m_0^{i+1} $MCPA_A^{\mathcal{E}}(n,i+1)$ 1 is p_{i+1}

$$Prob[CPA_B^{\mathcal{E}}(n)=1] = \frac{1}{2}[1 - p_{i+1} + p_i] \ge \frac{1}{2} + \frac{2}{t \cdot p(n)}$$