MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (SNM-CPA implies IND-CPA). *Let $\mathfrak{C} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public key cryptosystem. We say that the crypto-system is $(t, t_\pi, t_m, \varepsilon)$-non-malleable against statically chosen relations (SNM-CPA) if for all t-time adversaries $\mathcal{A}$ the advantage*

$$\mathsf{Adv}^{\mathsf{s\text{-}nm\text{-}cpa}}_{\mathfrak{C}}(\mathcal{A}) = \left|\Pr\left[\mathcal{G}^{\mathcal{A}}_0 = 1\right] - \Pr\left[\mathcal{G}^{\mathcal{A}}_1 = 1\right]\right| \leq \varepsilon$$

where the security games are defined as follows

$\mathcal{G}^{\mathcal{A}}_0$
$\pi(\cdot) \leftarrow \mathcal{A}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
$\hat{c}_1, \ldots \hat{c}_n \leftarrow \mathcal{A}(c)$
if $c \in \{\hat{c}_1, \ldots \hat{c}_n\}$ then ***return*** 0
return $\pi(m, \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n))$

$\mathcal{G}^{\mathcal{A}}_1$
$\pi(\cdot) \leftarrow \mathcal{A}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
$\hat{c}_1, \ldots \hat{c}_n \leftarrow \mathcal{A}(\overline{c})$
if $\overline{c} \in \{\hat{c}_1, \ldots \hat{c}_n\}$ then ***return*** 0
return $\pi(m, \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n))$

and the sampling algorithm $\mathcal{M}_0$ is guaranteed to be a t_m-time algorithm and the predicate π is guaranteed to be t_π-time algorithm. Show that SNM-CPA security implies IND-CPA security by giving an explicit definition of the target relation π. Also, give the explicit quantification of running-time bounds. Interpret the results.

Solution. Let $\mathcal{B}$ be an adversary against IND-CPA. Then we construct the tree stage adversary $\mathcal{A}$. The first stage of the adversary $\mathcal{A}$ always outputs the binary relation $\pi(x, y) = [x = y]$ and the second and the third stage of the adversary are defined as follows

$\mathcal{A}(\mathsf{pk})$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$\mathcal{M}_0 = \{m_0, m_1\}$
return $\mathcal{M}_0$

$\mathcal{A}(c)$
$g \leftarrow B(c)$
$\hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_g)$
return $\hat{c}_1$

where $\mathcal{M}_0$ denotes the uniform distribution over m_0 and m_1.

As the predicate π is fixed, we can omit the predicate selection stage and replace the definition of the predicate into the games $\mathcal{G}_0$ and $\mathcal{G}_1$. As a result, we get the following simplification of the games:

$\mathcal{G}^{\mathcal{A}}_2$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
$\hat{c}_1, \ldots \hat{c}_n \leftarrow \mathcal{A}(c)$
if $c \in \{\hat{c}_1, \ldots \hat{c}_n\}$ then **return** 0
return $[m \neq \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1)]$

$\mathcal{G}^{\mathcal{A}}_3$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
$\hat{c}_1, \ldots \hat{c}_n \leftarrow \mathcal{A}(\overline{c})$
if $\overline{c} \in \{\hat{c}_1, \ldots \hat{c}_n\}$ then **return** 0
return $[m \neq \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1)]$

As the second stage of $\mathcal{A}$ returns $\mathcal{M}_0$ that is a uniform distribution over $\{m_0, m_1\}$, we can replace sample generation by uniform choice of index bits $i, j \leftarrow \{0, 1\}$. We can also replace the query $\mathcal{A}(c)$ by the explicit

description of the third stage of the adversary. This leads us to the following games:

$\mathcal{G}_4^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$i \leftarrow \{0,1\}$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_i)$
$g \leftarrow B(c)$
$\hat{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_g)$
if $c = \hat{c}$ then **return** 0
return $[m_i \neq \mathsf{Dec}_{\mathsf{sk}}(\hat{c})]$

$\mathcal{G}_5^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$i \leftarrow \{0,1\}, j \leftarrow \{0,1\}$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_j)$
$g \leftarrow B(c)$
$\hat{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_g)$
if $\overline{c} = \hat{c}$ then **return** 0
return $[m_i \neq \mathsf{Dec}_{\mathsf{sk}}(\hat{c})]$

We can further simplify the games, as $\mathsf{Dec}_{\mathsf{sk}}(\hat{c}) = m_g$ by the perfect functionality of the cryptosystem:

$\mathcal{G}_6^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$i \leftarrow \{0,1\}$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_i)$
$g \leftarrow B(c)$
if $c = \mathsf{Enc}_{\mathsf{pk}}(m_g)$ then **return** 0
return $[m_i \neq m_g]$

$\mathcal{G}_7^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$i \leftarrow \{0,1\}, j \leftarrow \{0,1\}$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_j)$
$g \leftarrow B(\overline{c})$
if $\overline{c} = \mathsf{Enc}_{\mathsf{pk}}(m_g)$ then **return** 0
return $[m_i \neq m_g]$

As the if branch makes the analysis of the games more difficult, we first analyse the without these branches. This a good approximation. A cryptosystem can be IND-CPA secure only if such ciphertext collisions occur with a negligible probability. We will later analyse this issue in further.

$\mathcal{G}_8^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$i \leftarrow \{0,1\}$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_i)$
$g \leftarrow B(c)$
return $[m_i \neq m_g]$

$\mathcal{G}_9^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$i \leftarrow \{0,1\}, j \leftarrow \{0,1\}$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_j)$
$g \leftarrow B(\overline{c})$
return $[m_i \neq m_g]$

Since i is not used before the last line in the game $\mathcal{G}_9$, we can rewrite the game as follows:

$\mathcal{G}_9^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$j \leftarrow \{0,1\}$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_j)$
$g \leftarrow B(\overline{c})$
$i \leftarrow \{0,1\}$
return $[m_i \neq m_g]$

From this game construction it is very tempting to say that $\Pr\left[\mathcal{G}_9^{\mathcal{B}} = 1\right] = \frac{1}{2}$. However, this is not true! For example consider an adversary $\mathcal{A}$ that always outputs $m_0 = m_1$. Then clearly $\Pr\left[\mathcal{G}_9^{\mathcal{B}} = 1\right] = 1$.

Intuitively, an adversary $\mathcal{B}$ that return $m_0 = m_1$ with high probability is not useful, as this event diminishes their success against the IND-CPA games. However, we must prove this formally. Let us consider the advantage of $\mathcal{B}$ against IND-CPA games:

$$\begin{array}{ll}\mathcal{Q}_0^{\mathcal{B}} & \mathcal{Q}_0^{\mathcal{B}} \\ \left\lceil\begin{array}{l}(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0,m_1) \leftarrow \mathcal{B}(\mathsf{pk}) \\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0) \\ \textbf{return } \mathcal{B}(c)\end{array}\right. & \left\lceil\begin{array}{l}(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0,m_1) \leftarrow \mathcal{B}(\mathsf{pk}) \\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1) \\ \textbf{return } \mathcal{B}(c)\end{array}\right.\end{array}$$

Now we can express the success of $\mathcal{B}$ against IND-CPA games by exhaustive decomposition:

$$\begin{aligned}\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] &= \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 = m_1\right] + \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 \neq m_1\right] \\ \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right] &= \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1 \wedge m_0 = m_1\right] + \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1 \wedge m_0 \neq m_1\right]\end{aligned}$$

If $m_0 = m_1$ then the ciphertext in both games has identical distribution and thus we can prove

$$\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 = m_1\right] = \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1 \wedge m_0 = m_1\right] \ .$$

As a consequence,

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathfrak{C}}(\mathcal{B}) = \left|\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 \neq m_1\right] - \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1 \wedge m_0 \neq m_1\right]\right| \ .$$

There are now two ways how to proceed with the proof. First, we could do the same decomposition for the games $\mathcal{G}_8$ and $\mathcal{G}_9$. However, this would lead us to the lengthy probability calculations. Instead, we use a shortcut. Note that given $\mathcal{B}$ which can occasionally output $m_0 = m_1$, we can define $\mathcal{B}^\circ$ that runs $\mathcal{B}$ and filters out these unfortunate events:

$$\begin{array}{ll}\mathcal{B}^\circ(\mathsf{pk}) & \mathcal{B}^\circ(c) \\ \left\lceil\begin{array}{l}(m_0,m_1) \leftarrow \mathcal{B}(\mathsf{pk}) \\ \mathsf{if}\ (m_0 = m_1)\ \mathsf{then}\ \textbf{return}\ (m_0^*, m_1^*) \\ \mathsf{else}\ \textbf{return}\ (m_0,m_1)\end{array}\right. & \left\lceil\begin{array}{l}\mathsf{if}\ (m_0 = m_1)\ \mathsf{then}\ \textbf{return}\ 0 \\ \mathsf{else}\ \textbf{return}\ \mathcal{B}(c)\ .\end{array}\right.\end{array}$$

Then clearly $\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathfrak{C}}(\mathcal{B}^\circ) = \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathfrak{C}}(\mathcal{B}\circ)$ and the running times differ by a constant.

Hence, we can assume that $\mathcal{B}$ never returns $m_0 = m_1$ and proceed further with the analysis. Under the assumption $m_0 \neq m_1$, the condition $m_i \neq m_g$ is equivalent to the condition $i \neq g$ and we can indeed conclude that $\Pr\left[\mathcal{G}_9^{\mathcal{B}} = 1\right] = \frac{1}{2}$. The game $\mathcal{G}_8$ simplifies to

$$\mathcal{G}_8^{\mathcal{B}}$$
$$\left\lceil\begin{array}{l}(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0,m_1) \leftarrow \mathcal{B}(\mathsf{pk}) \\ i \leftarrow \{0,1\} \\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_i) \\ g \leftarrow B(c) \\ \textbf{return}\ [i \neq g]\ ,\end{array}\right.$$

for which we know from previous exercises that $\Pr\left[\mathcal{G}_8^{\mathcal{B}} = 1\right] = \frac{1}{2} \pm \frac{1}{2} \cdot \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathfrak{C}}(\mathcal{B})$. Thus, we have proved

$$\left|\Pr\left[\mathcal{G}_8^{\mathcal{B}} = 1\right] - \Pr\left[\mathcal{G}_9^{\mathcal{B}} = 1\right]\right| = \frac{1}{2} \cdot \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathfrak{C}}(\mathcal{B}) \ .$$

To complete the proof, we must relate this difference to the difference between the games $\mathcal{G}_6$ and $\mathcal{G}_7$. First note that if $c = \mathsf{Enc}_{\mathsf{pk}}(m_g)$ then $m_i = m_g$ and the adversary cannot win the game $\mathcal{G}_8$. Thus, we have proved

$$\Pr\left[\mathcal{G}_6^{\mathcal{B}} = 1\right] = \Pr\left[\mathcal{G}_8^{\mathcal{B}} = 1\right] \ .$$

For the game $\mathcal{G}_7$, we can conclude only that

$$\Pr\left[\mathcal{G}_7^{\mathcal{B}} = 1\right] \leq \Pr\left[\mathcal{G}_9^{\mathcal{B}}\right] \leq \frac{1}{2} \ .$$

Without loss of generality we can assume that the $\mathcal{B}$ is such that

$$\Pr\left[\mathcal{G}_8^{\mathcal{B}} = 1\right] \geq \frac{1}{2} \ .$$

If the inequality does not hold we can invert the the outcome of $\mathcal{B}$ to make it hold. The running time will increase only by constant. Now combining all inequalities we obtain

$$\Pr\left[\mathcal{G}_6^{\mathcal{B}} = 1\right] - \Pr\left[\mathcal{G}_7^{\mathcal{B}} = 1\right] \geq \Pr\left[\mathcal{G}_8^{\mathcal{B}} = 1\right] - \frac{1}{2} = \left|\Pr\left[\mathcal{G}_8^{\mathcal{B}} = 1\right] - \Pr\left[\mathcal{G}_9^{\mathcal{B}} = 1\right]\right| = \frac{1}{2} \cdot \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{B}) \ .$$

Hence, we have proved that

$$\mathsf{Adv}_{\mathfrak{C}}^{\mathsf{s\text{-}nm\text{-}cpa}}(\mathcal{A}) \geq \frac{1}{2} \cdot \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{B})$$

for the adversary $\mathcal{A}$ for which the running time is only constant times larger than the running time of $\mathcal{B}$. Thus, $(t, t_\pi, t_m, \varepsilon)$-non-malleablity against statically chosen relations implies $(t, 2\varepsilon)$-IND-CPA security.