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

Exercise (IND-FPA ⇒ IND-CPA). *In a fixed plaintext attack (FPA), an adversary has to fix the queried messages ahead of other interactions. Consequently, it might be possible to achieve a security goal against fixed plaintext attacks (CPA) that is infeasible against chosen ciphertext attacks. This separation manifests already if we consider indistinguishability as a security goal. Recall that a cryptosystem is (t, ε)-IND-FPA if for all t-time adversaries $\mathcal{B}$ the advantage is bounded:*

$$\mathsf{Adv}^{\mathsf{ind\text{-}fpa}}(\mathcal{B}) = |\Pr[\mathcal{Q}_0^{\mathcal{B}} = 1] - \Pr[\mathcal{Q}_1^{\mathcal{B}} = 1]| \leq \varepsilon$$

where

$$\begin{array}{ll} \mathcal{Q}_0 & \mathcal{Q}_1 \\ \left[\begin{array}{l} (m_0, m_1) \leftarrow \mathcal{B} \\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ \textbf{return } \mathcal{B}(\mathsf{pk}, \mathsf{Enc}_{\mathsf{pk}}(m_0)) \end{array}\right. & \left[\begin{array}{l} (m_0, m_1) \leftarrow \mathcal{B} \\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ \textbf{return } \mathcal{B}(\mathsf{pk}, \mathsf{Enc}_{\mathsf{pk}}(m_1)) \end{array}\right. . \end{array}$$

Prove that if the message space $\mathcal{M}$ consist of two elements then IND-FPA security implies IND-CPA security. Generalise the proof for the general case when the message space consists on n elements. How does the security bound depend on the size of the message space?

Solution. Message space with two elements. For the proof we must bound the advantage of a t-time IND-CPA adversary $\mathcal{A}$ that plays against the following IND-CPA games:

$$\begin{array}{ll} \mathcal{G}_0 & \mathcal{G}_1 \\ \left[\begin{array}{l} (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \textbf{return } \mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_0)) \end{array}\right. & \left[\begin{array}{l} (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \textbf{return } \mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_1)) \end{array}\right. . \end{array}$$

Under our assumption the message space $\mathcal{M}$ consists of two messages m_0 and m_1. Consequently, the adversary $\mathcal{A}$ can output only these two messages. The IND-FPA adversary $\mathcal{B}$ can also output messages m_0 and m_1, but differently from $\mathcal{A}$ it cannot change the order of messages based on the public key pk and this poses a problem in the reduction. The most naive reduction

$$\begin{array}{ll} \mathcal{B} & \mathcal{B}(\mathsf{pk}, c) \\ \left[\textbf{return } (m_0, m_1)\right. & \left[\begin{array}{l} (\overline{m}_0, \overline{m}_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \textbf{return } \mathcal{A}(c) \end{array}\right. \end{array}$$

is not very good. The inlining of $\mathcal{B}$ into the games $\mathcal{Q}_0$ and $\mathcal{Q}_1$ gives

$$\begin{array}{ll} \mathcal{Q}_0 & \mathcal{Q}_1 \\ \left[\begin{array}{l} (m_0, m_1) \leftarrow \mathcal{B} \\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ (\overline{m}_0, \overline{m}_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \textbf{return } \mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_0)) \end{array}\right. & \left[\begin{array}{l} (m_0, m_1) \leftarrow \mathcal{B} \\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ (\overline{m}_0, \overline{m}_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \textbf{return } \mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_1)) \end{array}\right. \end{array}$$

and thus $\mathcal{A}$ gives answer for switched games if $(\overline{m}_0, \overline{m}_1)$ is in the the opposite order as (m_0, m_1). The latter might completely destroy the advantage $\mathsf{Adv}^{\mathsf{ind\text{-}fpa}}(\mathcal{B})$. This problem can be solved by checking the order of messages and inverting the outcomes when messages are switched:

$$\begin{array}{ll} \mathcal{B} & \mathcal{B}(\mathsf{pk}, c) \\ \left[\textbf{return } (m_0, m_1)\right. & \left[\begin{array}{l} (\overline{m}_0, \overline{m}_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \mathsf{if}\ (\overline{m}_0 \stackrel{?}{=} m_0)\ \mathsf{then}\ \textbf{return } \mathcal{A}(c) \\ \mathsf{else}\ \textbf{return } \neg\mathcal{A}(c) \end{array}\right. . \end{array}$$

Under the assumption that $\mathcal{A}$ outputs always different messages $\overline{m}_0 \neq \overline{m}_1$, we get

$$\begin{aligned}\Pr\left[\mathcal{Q}_i^{\mathcal{B}} = 1\right] &= \Pr\left[\mathcal{Q}_i^{\mathcal{B}} = 1 \wedge m_0 = \overline{m}_0\right] + \Pr\left[\mathcal{Q}_i^{\mathcal{B}} = 1 \wedge m_0 \neq \overline{m}_0\right] \\ &= \Pr\left[\mathcal{G}_i^{\mathcal{A}} = 1 \wedge m_0 = \overline{m}_0\right] + \Pr\left[\mathcal{G}_{1-i}^{\mathcal{A}} = 0 \wedge m_0 \neq \overline{m}_0\right] \\ &= \Pr\left[\mathcal{G}_i^{\mathcal{A}} = 1 \wedge m_0 = \overline{m}_0\right] + 1 - \Pr\left[\mathcal{G}_{1-i}^{\mathcal{A}} = 1 \wedge m_0 \neq \overline{m}_0\right]\end{aligned}$$

and thus the advantages are identical:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{ind\text{-}fpa}}(\mathcal{B}) = \big|&\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1 \wedge m_0 = \overline{m}_0\right] + 1 - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1 \wedge m_0 \neq \overline{m}_0\right] \\ &- \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1 \wedge m_0 = \overline{m}_0\right] - 1 + \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1 \wedge m_0 \neq \overline{m}_0\right]\big| \\ = \big|&\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\big| = \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) \ .\end{aligned}$$

To complete the proof we must extend the argument to the adversaries $\mathcal{A}$ that sometimes output identical messages $\overline{m}_0 = \overline{m}_1$. It is straightforward to see that

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) = \big|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1 \wedge \overline{m}_0 \neq \overline{m}_1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1 \wedge \overline{m}_0 \neq \overline{m}_1\right]\big| \ ,$$

since the execution steps in the games $\mathcal{G}_0$ and $\mathcal{G}_1$ are identical if $\overline{m}_0 = \overline{m}_1$. As a result, it is straightforward to convert an adversary $\mathcal{A}$ into an adversary $\mathcal{A}_*$ that is guaranteed to output different messages:

$\mathcal{A}_*(\mathsf{pk})$
$(\overline{m}_0, \overline{m}_1) \leftarrow \mathcal{A}(\mathsf{pk})$
if $(\overline{m}_0 \stackrel{?}{=} \overline{m}_1)$ then **return** (m_0, m_1)
else **return** (m_0, m_1)

$\mathcal{A}_*(c)$
if $(\overline{m}_0 \stackrel{?}{=} \overline{m}_1)$ then **return** 0
else **return** $\mathcal{A}(c)$

and to have the same advantage. As a result, we have specified the reduction in two steps. First, we convert $\mathcal{A}$ to $\mathcal{A}_*$ and then use the construction of $\mathcal{B}$ with the adversary $\mathcal{A}_*$. The resulting adversary is clearly valid, since both conversion steps do not contain any undefined operations. Similarly, the overhead in the running time is constant as both transformations add constant overhead.

Generalisation to arbitrary message space. First note that we can always decompose the advantage of IND-CPA adversary as sum of pairwise advantages:

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) \leq \sum_{m_0^*, m_1^* \in \mathcal{M}} \big|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1 \wedge m_0 = m_0^* \wedge m_1 = m_1^*\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1 \wedge m_0 = m_0^* \wedge m_1 = m_1^*\right]\big|$$

and thus we can concentrate our efforts on bounding

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{m_0^*, m_1^*}(\mathcal{A}) = \big|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1 \wedge m_0 = m_0^* \wedge m_1 = m_1^*\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1 \wedge m_0 = m_0^* \wedge m_1 = m_1^*\right]\big| \ .$$

This advantage is an IND-CPA advantage of the cryptosystem with the messages space $\mathcal{M}_* = \{m_0^*, m_1^*\}$. Obviously, the cryptosystem remains IND-FPA with the same parameters when we restrict the message space to $\mathcal{M}_*$ and thus the first part of the exercise allows us to deduce that

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) \leq \sum_{m_0^*, m_1^* \in \mathcal{M}} \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{m_0^*, m_1^*}(\mathcal{A}) \leq \frac{|\mathcal{M}| \cdot (|\mathcal{M}| - 1)}{2} \cdot \varepsilon \ .$$

Consequently, the effectiveness of IND-CPA $\Rightarrow$ IND-FPA reduction decreases quadratically with respect to the message space, which is too weak for (exponentially) large messages spaces.

Note that the reduction is tight. It is possible that the adversary chooses messages (m_0, m_1) deterministically based on the public key so that each message pair has the same probability. Now if the advantage for each message pair is same, then the upper bound is tight.