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

Exercise (Tradeoffs for IND-FPA ⇒ IND-CPA transformation). *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 there exists a simple reduction that proves that for any t-time IND-CPA adversary $\mathcal{A}$ the advantage is bounded:*

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) \leq \frac{n(n-1)}{2} \cdot \varepsilon$$

provided that the cryptosystem is (t, ε)-IND-FPA secure. Give a corresponding construction that converts any IND-FPA secure encryption scheme to the IND-CPA secure encryption scheme so that the advantage bound decreases logarithmically with respect to the message space size.

Solution. Security of vectorised encryption. A vectorised encryption rule is defined as follows:

$$\overline{\mathsf{Enc}}_{\mathsf{pk}}(m_1, \ldots, m_k) = (\mathsf{Enc}_{\mathsf{pk}}(m_1), \ldots, \mathsf{Enc}_{\mathsf{pk}}(m_k)) \ .$$

and the corresponding IND-CPA games are following with non-standard indices:

$\mathcal{G}_k^{\mathcal{A}}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_1^0, \ldots, m_k^0), (m_1^1, \ldots, m_k^1) \leftarrow \mathcal{A}(\mathsf{pk})$
$c_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1^0), \ldots, c_k \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_k^0)$
return $\mathcal{A}(c_1, \ldots, c_k)$

$\mathcal{G}_0^{\mathcal{A}}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_1^0, \ldots, m_k^0), (m_1^1, \ldots, m_k^1) \leftarrow \mathcal{A}(\mathsf{pk})$
$c_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1^1), \ldots, c_k \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_k^1)$
return $\mathcal{A}(c_1, \ldots, c_k)$

To bound the distance, we can consider hybrid games

$\mathcal{G}_i^{\mathcal{A}}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_1^0, \ldots, m_k^0), (m_1^1, \ldots, m_k^1) \leftarrow \mathcal{A}(\mathsf{pk})$
$c_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1^0)$
$\ldots$
$c_i \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_i^0)$
$c_{i+1} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{i+1}^1)$
$\ldots$
$c_k \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_k^1)$
return $\mathcal{A}(c_1, \ldots, c_k)$

$\mathcal{G}_{i+1}^{\mathcal{A}}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_1^0, \ldots, m_k^0), (m_1^1, \ldots, m_k^1) \leftarrow \mathcal{A}(\mathsf{pk})$
$c_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1^0)$
$\ldots$
$c_i \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_i^0)$
$c_{i+1} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{i+1}^0)$
$\ldots$
$c_k \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_k^1)$
return $\mathcal{A}(c_1, \ldots, c_k)$.

Note that the games $\mathcal{G}_i$ and $\mathcal{G}_{i+1}$ differ only by a single line and thus we can do a direct reduction to IND-CPA games of the original cryptosystem:

$\mathcal{Q}_0$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
return $\mathcal{B}(\mathsf{Enc}_{\mathsf{pk}}(m_0))$

$\mathcal{Q}_1$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{B}(\mathsf{pk})$
return $\mathcal{B}(\mathsf{Enc}_{\mathsf{pk}}(m_1))$.

The corresponding reduction is following:

$\mathcal{B}(\mathsf{pk})$
$(m_1^0, \ldots, m_k^0), (m_1^1, \ldots, m_k^1) \leftarrow \mathcal{A}(\mathsf{pk})$
return (m_{i+1}^0, m_{i+1}^1)

$\mathcal{B}(c)$

$\lceil$ For $j \in \{1, \ldots, i\}$ do
$\lceil\, c_j \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_j^0)$
$c_{i+1} \leftarrow c$
For $j \in \{i+2, \ldots, k\}$ do
$\lceil\, c_j \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_j^1)$
$\lfloor$ **return** $\mathcal{A}(c_1, \ldots, c_k)$

It is straightforward to see that $\mathcal{Q}_0^{\mathcal{B}} \equiv \mathcal{G}_i^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{B}} \equiv \mathcal{G}_{i+1}^{\mathcal{A}}$. Since the running time of $\mathcal{B}$ is only by $\mathrm{O}(k)$ steps longer we get

$$|\Pr[\mathcal{G}_i^{\mathcal{A}} = 1] - \Pr[\mathcal{G}_{i+1}^{\mathcal{A}} = 1]| \leq \varepsilon$$

and thus triangle inequality yields

$$|\Pr[\mathcal{G}_k^{\mathcal{A}} = 1] - \Pr[\mathcal{G}_0^{\mathcal{A}} = 1]| \leq k \cdot \varepsilon.$$

Tradeoffs. The size of the message space of the vectorised encryption depends on the number of potential values n for each slot and the length of the vector k. Similarly, the security depends on both parameter as we start with IND-FPA secure cryptosystem. By noting that IND-FPA security cannot decrease if we reduce the message space and by combining two bounds, we get

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\overline{\mathsf{Enc}}}(\mathcal{A}) \leq \frac{kn(n-1)\varepsilon}{2} \ .$$

The size of vectorised message space is obviously n^k and thus the security degradation per available bits is

$$\delta = \frac{kn(n-1)\varepsilon}{\varepsilon k \log n} = \frac{n(n-1)}{2 \log n} \ ,$$

which increases when we use more than two states for each slot. If we consider length blowup (encoding rate), we get a different measure

$$\varrho = \frac{kc}{k \log n} = \frac{c}{\log n}$$

where c is the length of an individual ciphertext. In other words, the larger the number of available states for each slot means less communication. Since δ and ϱ find their optimum in different ends of the set of feasible solutions, the problem has no unique solution. One has either fix the maximum security degradation level and based on that choose the largest n to minimise the communication overhead or fix the maximum communication overhead and then find the minimal n that meets this demand to reduce security degradation.