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

Exercise (Alternative NM-CPA security definition). *Prove that the standard non-malleability definition specified by the games*

$$
\begin{array}{l}
\mathcal{Q}_0\\
\left[\begin{array}{l}
(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\
\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})\\
m \leftarrow \mathcal{M}_0\\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)\\
\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{B}(c)\\
\text{if } c \in \{\hat{c}_1, \ldots, \hat{c}_n\} \text{ then } \textbf{\textit{return}}\ 0\\
\hat{m}_1 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \hat{m}_n \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n)\\
\textbf{\textit{return}}\ \pi(m, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
\end{array}
$$

$$
\begin{array}{l}
\mathcal{Q}_0\\
\left[\begin{array}{l}
(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\
\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})\\
m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0\\
\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})\\
\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{B}(\overline{c})\\
\text{if } c \in \{\hat{c}_1, \ldots, \hat{c}_n\} \text{ then } \textbf{\textit{return}}\ 0\\
\hat{m}_1 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \hat{m}_n \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n)\\
\textbf{\textit{return}}\ \pi(m_i, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
\end{array}
$$

is equivalent to the simplified definition specified by the following games

$$
\begin{array}{l}
\mathcal{G}_0\\
\left[\begin{array}{l}
(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})\\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0)\\
\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(c)\\
\text{if } c \in \{\hat{c}_1, \ldots, \hat{c}_n\} \text{ then } \textbf{\textit{return}}\ 0\\
\hat{m}_1 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \hat{m}_n \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n)\\
\textbf{\textit{return}}\ \pi(m_0, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
\end{array}
$$

$$
\begin{array}{l}
\mathcal{G}_0\\
\left[\begin{array}{l}
(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})\\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)\\
\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(c)\\
\text{if } c \in \{\hat{c}_1, \ldots, \hat{c}_n\} \text{ then } \textbf{\textit{return}}\ 0\\
\hat{m}_1 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \hat{m}_n \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n)\\
\textbf{\textit{return}}\ \pi(m_0, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
\end{array}
$$

Solution. For clarity we split the proof into three smaller steps.

First step. Show that standard definition is equivalent to the definition specified by the following games

$$
\begin{array}{l}
\mathcal{G}_0\\
\left[\begin{array}{l}
(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})\\
i \leftarrow \{0,1\}\\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_i)\\
\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{B}(c)\\
\text{if } c \in \{\hat{c}_1, \ldots, \hat{c}_n\} \text{ then } \textbf{return}\ 0\\
\hat{m}_1 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \hat{m}_n \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n)\\
\textbf{return}\ \pi(m_i, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
\end{array}
$$

$$
\begin{array}{l}
\mathcal{G}_0\\
\left[\begin{array}{l}
(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})\\
i \leftarrow \{0,1\}, j \leftarrow \{0,1\}\\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_j)\\
\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{B}(c)\\
\text{if } c \in \{\hat{c}_1, \ldots, \hat{c}_n\} \text{ then } \textbf{return}\ 0\\
\hat{m}_1 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \hat{m}_n \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n)\\
\textbf{return}\ \pi(m_i, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
\end{array}
$$

Second step. Show that the alternative definition is equivalent to the definition specified by the following games

$$
\begin{array}{l}
\mathcal{G}_0 \\
\left\lfloor\begin{array}{l}
(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1) \\
\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(c) \\
\text{if } c \in \{\hat{c}_1, \ldots, \hat{c}_n\} \text{ then } \mathbf{return}\ 0 \\
\hat{m}_1 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \hat{m}_n \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n) \\
\mathbf{return}\ \pi(m_1, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
\end{array}
\qquad
\begin{array}{l}
\mathcal{G}_0 \\
\left\lfloor\begin{array}{l}
(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\
(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0) \\
\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(c) \\
\text{if } c \in \{\hat{c}_1, \ldots, \hat{c}_n\} \text{ then } \mathbf{return}\ 0 \\
\hat{m}_1 \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots, \hat{m}_n \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_n) \\
\mathbf{return}\ \pi(m_1, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
\end{array}
$$

THIRD STEP. Show that the results obtained in the second and third step are sufficient to conclude the desired result.