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

Exercise (Characterisation of non-malleability). *Let* $(\mathsf{Gen}, \mathsf{Com}, \mathsf{Open})$ *be a commitment scheme with message space* $\mathbb{Z}_2$*. Then we can define a restricted form of non-malleability for fixed relation* $\pi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \{0, 1\}$ *through the following games*

$$\begin{array}{ll}
\mathcal{G}_0 & \mathcal{G}_1 \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
m_0, m_1, \sigma \leftarrow \mathcal{A}(\mathsf{pk}) \\
b \leftarrow \{0,1\} \\
c, d \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_b) \\
\hat{c} \leftarrow \mathcal{A}(c), \hat{d} \leftarrow \mathcal{A}(d) \\
\hat{m} \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}, \hat{d}) \\
\text{if } \hat{c} = c \vee \hat{m} = \bot \text{ then } \textbf{\textit{return}}\ 0 \\
\textbf{\textit{return}}\ \pi(m_b, \hat{m})
\end{array}\right.
&
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
m_0, m_1, \sigma \leftarrow \mathcal{A}(\mathsf{pk}) \\
b \leftarrow \{0,1\} \\
\hat{m} \leftarrow \mathcal{A}^*(\sigma) \\
\text{if } \hat{m} = \bot \vee \neg\mathcal{A}^*(m_b) \text{ then } \textbf{\textit{return}}\ 0 \\
\textbf{\textit{return}}\ \pi(m_b, \hat{m})
\end{array}\right.
\end{array}$$

where σ *is the state of* $\mathcal{A}$ *after the first execution step and* $\mathcal{A}^*$ *is another stateless algorithm which corresponds to honest actor that creates* $\hat{c}, \hat{d} \leftarrow \mathsf{Com}_{\mathsf{pk}}(\hat{m})$ *without looking at* c *and decides whether to release* $\hat{d}$ *based on* m_b*. A commitment scheme is* $(t, f(\cdot), \varepsilon)$*-nonmalleable if for any* t*-time* $\mathcal{A}$ *there exists* $f(t)$*-time* $\mathcal{A}^*$ *such that*

$$\mathsf{Adv}^{\mathsf{nm\text{-}open}}(\mathcal{A}, \mathcal{A}^*) = \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A},\mathcal{A}^*} = 1\right] \leq \varepsilon \enspace .$$

Prove that this security notion follows if the following games

$$\begin{array}{ll}
\mathcal{Q}_0 & \mathcal{Q}_1 \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
m_0, m_1, m_* \leftarrow \mathcal{B}(\mathsf{pk}) \\
c, d \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_0) \\
\hat{c} \leftarrow \mathcal{B}(c), \hat{d} \leftarrow \mathcal{B}(d) \\
\hat{m} \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}, \hat{d}) \\
\text{if } \hat{c} = c \vee \hat{m} = \bot \text{ then } \textbf{\textit{return}}\ 0 \\
\textbf{\textit{return}}\ [\hat{m} = m_*]
\end{array}\right.
&
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
m_0, m_1, m_* \leftarrow \mathcal{B}(\mathsf{pk}) \\
c, d \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_1) \\
\hat{c} \leftarrow \mathcal{B}(c), \hat{d} \leftarrow \mathcal{B}(d) \\
\hat{m} \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}, \hat{d}) \\
\text{if } \hat{c} = c \vee \hat{m} = \bot \text{ then } \textbf{\textit{return}}\ 0 \\
\textbf{\textit{return}}\ [\hat{m} \neq m_*]
\end{array}\right.
\end{array}$$

are computationally close enough.

Proof. Let us look at the matrix R defining the relation with rows corresponding to m_b and columns corresponding to $\hat{m}$.

Trivial case. Show that if there is a column of ones then it is trivial to get $\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] \leq \Pr\left[\mathcal{G}_1^{\mathcal{A},\mathcal{A}^*} = 1\right]$.

Non-trivial case. Let A be 2×2 matrix of potential outcome probabilities for the game $\mathcal{G}_0$ and what is the minimal difference between the games $\mathcal{G}_0$ and $\mathcal{G}_1$ if we allow optimal $\mathcal{A}^*$. Based on that define $\mathcal{B}$.

□