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

Exercise (NM-OPEN⇒SEM-BIND). *A commitment scheme* $\mathfrak{C}$ *is* (t,ε)*-semantically secure with respect to the binding property if the advantage of any* t*-time adversary* $\mathcal{A}$ *against the following games*

$$\mathcal{G}_0\quad\left[\begin{array}{l}\mathsf{pk}\leftarrow\mathsf{Gen}\\ \mathcal{M}_0\leftarrow\mathcal{A}(\mathsf{pk})\\ m\leftarrow\mathcal{M}_0\\ \pi(\cdot),\hat{c}_1,\ldots,\hat{c}_n\leftarrow\mathcal{A}(\varnothing)\\ \hat{d}_1,\ldots,\hat{d}_n\leftarrow\mathcal{A}(m)\\ \ \text{For } i\in\{1,\ldots,n\}\text{ do}\\ \ \left[\ \hat{m}_i\leftarrow\mathsf{Open}_{\mathsf{pk}}(\hat{c}_i,\hat{d}_i)\right.\\ \mathsf{if}\ \exists\hat{m}_i=\perp\ \textbf{\textit{return}}\ 0\\ \textbf{\textit{return}}\ \pi(m,\hat{m}_1,\ldots,\hat{m}_n)\end{array}\right.\qquad
\mathcal{G}_1\quad\left[\begin{array}{l}\mathsf{pk}\leftarrow\mathsf{Gen}\\ \mathcal{M}_0\leftarrow\mathcal{A}(\mathsf{pk})\\ m\leftarrow\mathcal{M}_0,\overline{m}\leftarrow\mathcal{M}_0\\ \pi(\cdot),\hat{c}_1,\ldots,\hat{c}_n\leftarrow\mathcal{A}(\varnothing)\\ \hat{d}_1,\ldots,\hat{d}_n\leftarrow\mathcal{A}(\overline{m})\\ \ \text{For } i\in\{1,\ldots,n\}\text{ do}\\ \ \left[\ \hat{m}_i\leftarrow\mathsf{Open}_{\mathsf{pk}}(\hat{c}_i,\hat{d}_i)\right.\\ \mathsf{if}\ \exists\hat{m}_i=\perp\ \textbf{\textit{return}}\ 0\\ \textbf{\textit{return}}\ \pi(m,\hat{m}_1,\ldots,\hat{m}_n)\end{array}\right.$$

is bounded

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

Show that non-malleability with respect to the opening implies restricted notion of semantic binding that additionally requires $\mathrm{supp}(\mathcal{M}_0)\subseteq\mathcal{M}_{\mathsf{pk}}$.

Solution. Recall that non-malleability with respect to opening is defined through the security games:

$$\mathcal{Q}_0\quad\left[\begin{array}{l}\mathsf{pk}\leftarrow\mathsf{Gen}\\ \mathcal{M}_0\leftarrow\mathcal{B}(\mathsf{pk})\\ m\leftarrow\mathcal{M}_0\\ (c,d)\leftarrow\mathsf{Com}_{\mathsf{pk}}(m)\\ \pi(\cdot),\hat{c}_1,\ldots,\hat{c}_n\leftarrow\mathcal{B}(c)\\ \hat{d}_1,\ldots,\hat{d}_n\leftarrow\mathcal{B}(d)\\ \mathsf{if}\ c\in\{\hat{c}_1,\ldots,\hat{c}_n\}\ \textbf{return}\ 0\\ \hat{m}_i\leftarrow\mathsf{Open}_{\mathsf{pk}}(\hat{c}_i,\hat{d}_i)\ \textbf{for}\ i\in\{1,\ldots,n\}\\ \mathsf{if}\ \exists\hat{m}_i=\perp\ \textbf{return}\ 0\\ \textbf{return}\ \pi(m,\hat{m}_1,\ldots,\hat{m}_n)\end{array}\right.\qquad
\mathcal{Q}_1\quad\left[\begin{array}{l}\mathsf{pk}\leftarrow\mathsf{Gen}\\ \mathcal{M}_0\leftarrow\mathcal{B}(\mathsf{pk})\\ m\leftarrow\mathcal{M}_0,\overline{m}\leftarrow\mathcal{M}_0\\ (\overline{c},\overline{d})\leftarrow\mathsf{Com}_{\mathsf{pk}}(\overline{m})\\ \pi(\cdot),\hat{c}_1,\ldots,\hat{c}_n\leftarrow\mathcal{B}(\overline{c})\\ \hat{d}_1,\ldots,\hat{d}_n\leftarrow\mathcal{B}(\overline{d})\\ \mathsf{if}\ \overline{c}\in\{\hat{c}_1,\ldots,\hat{c}_n\}\ \textbf{return}\ 0\\ \hat{m}_i\leftarrow\mathsf{Open}_{\mathsf{pk}}(\hat{c}_i,\hat{d}_i)\ \textbf{for}\ i\in\{1,\ldots,n\}\\ \mathsf{if}\ \exists\hat{m}_i=\perp\ \textbf{return}\ 0\\ \textbf{return}\ \pi(m,\hat{m}_1,\ldots,\hat{m}_n)\ .\end{array}\right.$$

Namely, a commitment scheme $\mathfrak{C}$ is (t,ε)-non-malleable with respect to opening if the advantage of any t-time adversary $\mathcal{B}$ against the games $\mathcal{Q}_0,\mathcal{Q}_1$ is bounded:

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

As the games defining security against semantic binding are structurally very close to non-malleability games, it is not hard to morph an adversary $\mathcal{A}$ against games $\mathcal{G}_0$ and $\mathcal{G}_1$ to an adversary $\mathcal{B}$ against games $\mathcal{Q}_0$ and $\mathcal{Q}_0$. The corresponding construction is following:

$$\mathcal{B}(\mathsf{pk})\quad\left[\begin{array}{l}\mathcal{M}_0\leftarrow\mathcal{A}(\mathsf{pk})\\ \textbf{return}\ \mathcal{M}_0\end{array}\right.\qquad
\mathcal{B}(c)\quad\left[\begin{array}{l}\pi(\cdot),\hat{c}_1,\ldots,\hat{c}_n\leftarrow\mathcal{A}(\varnothing)\\ \textbf{return}\ \pi(\cdot),\hat{c}_1,\ldots,\hat{c}_n\end{array}\right.\qquad
\mathcal{B}(d)\quad\left[\begin{array}{l}m_*\leftarrow\mathsf{Open}_{\mathsf{pk}}(c,d)\\ \hat{d}_1,\ldots,\hat{d}_n\leftarrow\mathcal{A}(m_*)\\ \textbf{return}\ \hat{d}_1,\ldots,\hat{d}_n\end{array}\right.$$

This construction is valid since $\mathcal{A}$ receives correct inputs and $\mathcal{B}$ can open the message m since it can store c in the second block and open it with decommitment value d. By inlining the adversary $\mathcal{B}$ into the games $\mathcal{Q}_0$ and $\mathcal{Q}_1$, we get a pair of games that are not yet identical to games $\mathcal{G}_0^{\mathcal{A}}$ and $\mathcal{G}_1^{\mathcal{A}}$:

$$
\begin{array}{ll}
\mathcal{Q}_0^{\mathcal{B}} & \mathcal{Q}_1^{\mathcal{B}} \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk}) \\
m \leftarrow \mathcal{M}_0 \\
(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m) \\
\pi(\cdot), \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing) \\
m_* \leftarrow \mathsf{Open}_{\mathsf{pk}}(c, d) \\
\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(m_*) \\
\mathsf{if}\ c \in \{\hat{c}_1, \ldots, \hat{c}_n\}\ \mathbf{return}\ 0 \\
\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)\ \mathbf{for}\ i \in \{1, \ldots, n\} \\
\mathsf{if}\ \exists \hat{m}_i = \perp\ \mathbf{return}\ 0 \\
\mathbf{return}\ \pi(m, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
&
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk}) \\
m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0 \\
(\overline{c}, \overline{d}) \leftarrow \mathsf{Com}_{\mathsf{pk}}(\overline{m}) \\
\pi(\cdot), \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing) \\
\overline{m}_* \leftarrow \mathsf{Open}_{\mathsf{pk}}(\overline{c}, \overline{d}) \\
\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(\overline{m}_*) \\
\mathsf{if}\ \overline{c} \in \{\hat{c}_1, \ldots, \hat{c}_n\}\ \mathbf{return}\ 0 \\
\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)\ \mathbf{for}\ i \in \{1, \ldots, n\} \\
\mathsf{if}\ \exists \hat{m}_i = \perp\ \mathbf{return}\ 0 \\
\mathbf{return}\ \pi(m, \hat{m}_1, \ldots, \hat{m}_n)\ .
\end{array}\right.
\end{array}
$$

Under the assumption that the commitment scheme $\mathfrak{C}$ is functional we get

$$
\begin{aligned}
m_* &= \mathsf{Open}_{\mathsf{pk}}(\mathsf{Com}_{\mathsf{pk}}(m)) = m\ , \\
\overline{m}_* &= \mathsf{Open}_{\mathsf{pk}}(\mathsf{Com}_{\mathsf{pk}}(\overline{m})) = \overline{m}\ .
\end{aligned}
$$

Thus, we can delete these lines from the above games and give m and $\overline{m}$ directly as input to $\mathcal{A}$ without changing the success probabilities. Also, we can move the line where m or $\overline{m}$ is commited right before the check $\overline{c} \in \{c_1, \ldots, \hat{c}_n\}$ since previous lines do not depend on (c, d). We thus obtain the following games

$$
\begin{array}{ll}
\mathcal{G}_2^{\mathcal{A}} & \mathcal{G}_3^{\mathcal{A}} \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk}) \\
m \leftarrow \mathcal{M}_0 \\
\pi(\cdot), \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing) \\
\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(m) \\
(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m) \\
\mathsf{if}\ c \in \{\hat{c}_1, \ldots, \hat{c}_n\}\ \mathbf{return}\ 0 \\
\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)\ \mathbf{for}\ i \in \{1, \ldots, n\} \\
\mathsf{if}\ \exists \hat{m}_i = \perp\ \mathbf{return}\ 0 \\
\mathbf{return}\ \pi(m, \hat{m}_1, \ldots, \hat{m}_n)
\end{array}\right.
&
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk}) \\
m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0 \\
\pi(\cdot), \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing) \\
\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(\overline{m}) \\
(\overline{c}, \overline{d}) \leftarrow \mathsf{Com}_{\mathsf{pk}}(\overline{m}) \\
\mathsf{if}\ \overline{c} \in \{\hat{c}_1, \ldots, \hat{c}_n\}\ \mathbf{return}\ 0 \\
\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)\ \mathbf{for}\ i \in \{1, \ldots, n\} \\
\mathsf{if}\ \exists \hat{m}_i = \perp\ \mathbf{return}\ 0 \\
\mathbf{return}\ \pi(m, \hat{m}_1, \ldots, \hat{m}_n)\ .
\end{array}\right.
\end{array}
$$

that satisfy $\mathcal{Q}_0^{\mathcal{B}} \equiv \mathcal{G}_2^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{B}} \equiv \mathcal{G}_3^{\mathcal{A}}$. It is clear that the games $\mathcal{G}_2$ and $\mathcal{G}_3$ differ from the semantic security games $\mathcal{G}_0$ and $\mathcal{G}_1$ only by the additional checks $c \in \{\hat{c}_1, \ldots, \hat{c}_n\}$ and $\overline{c} \in \{\hat{c}_1, \ldots, \hat{c}_n\}$. Thus, we can estimate

$$
\begin{aligned}
\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[c \in \{\hat{c}_1, \ldots, \hat{c}_n\}\right] \le \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] \le \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right]\ , \\
\Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] - \Pr\left[\overline{c} \in \{\hat{c}_1, \ldots, \hat{c}_n\}\right] \le \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right] \le \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\ .
\end{aligned}
$$

Note that the probabilities $\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right]$ and $\Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right]$ can indeed be anywhere in the specified range. For instance, if the relation $\pi(m, \hat{m}_1, \ldots, \hat{m}_n) = [\forall i : m \neq \overline{m}_i]$ then events $\mathcal{G}_0^{\mathcal{A}} = 1$ and $c \in \{\hat{c}_1, \ldots, \hat{c}_n\}$ are mutually exclusive and we achieve upper bound. Similarly, the relation $\pi(m, \hat{m}_1, \ldots, \hat{m}_n) = [\forall i : m = \overline{m}_i]$ assures that events occur simultaneously and we achieve the lower bound.

By combining the inequalities derived above, we can conclude

$$\mathsf{Adv}^{\mathsf{nm\text{-}cpa}}_{\mathfrak{C}}(\mathcal{B}) \geq \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] - \Pr\left[c \in \{\hat{c}_1, \ldots, \hat{c}_n\}\right] \quad .$$

To go further with the analysis, we must make additional assumptions about the commitment scheme. Let δ be the upper bound on the probability that by committing the message twice we get the same digest:

$$\delta = \max_{\substack{(\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{Gen}\\ m\in\mathcal{M}_{\mathsf{pk}}}} \Pr\left[(c_0, d_0) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m), (c_1, d_1) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m) : c_1 = c_0\right] \quad .$$

Then we can use union bound to upper bound the probability

$$\Pr\left[c \in \{\hat{c}_1, \ldots, \hat{c}_n\}\right] \leq n \cdot \Pr\left[c = \hat{c}_i\right] \leq n \cdot \delta$$

and thus

$$\mathsf{Adv}^{\mathsf{nm\text{-}cpa}}_{\mathfrak{C}}(\mathcal{B}) \geq \mathsf{Adv}^{\mathsf{sem\text{-}bind}}_{\mathfrak{C}}(\mathcal{A}) - n \cdot \delta$$

As the final step, we must analyse the time-complexity of our constructed adversary $\mathcal{B}$. The only additional operation $\mathcal{B}$ does is open the commitment. Thus, the overhead is a constant c. Thus, we have proven, that if a commitment scheme is $(t + c, \varepsilon)$-non-malleable wrt opening, then it is also $(t, \varepsilon + n\delta)$-semantically secure with respect to the binding property. For practical commitment schemes, the value δ is much smaller than ε, as it is usually one over the randomness size used to commit a message. One can formally derive the bound on δ solely from the non-malleability assumption, as non-malleability implies hiding and commitment scheme with high δ value is not very hiding.

Remark on the restriction. The formal definition of semantic binding does not require that the support of $\mathcal{M}_0$ is always inside the message space $\mathcal{M}_{\mathsf{pk}}$ or otherwise we cannot pass the information about m to $\mathcal{A}$. This restriction is artificial, as the distribution of future messages $\mathcal{M}_0$ that might influence the the decommitment procedure might be arbitrary. If the messages is short enough, we can still pack it inside a single commitment. Otherwise, we can pack it into several commitments. The latter leads to a different definition of non-malleability where the adversary sees many commitments $c_1, \ldots, c_n$ before it creates related commitments $\hat{c}_1, \ldots, \hat{c}_n$. As this definition is more complex, we do not pursue this issue further.