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

Exercise (Security against partial double-opening). *Let* $\mathfrak{C} = (\mathsf{Gen}, \mathsf{Com}, \mathsf{Open})$ *be commitment scheme and* $\mathcal{H}$ *be a collision resistant hash function family with an appropriate domain. Then we can build a list commitment scheme on top of the ordinary commitment scheme:*

$$\begin{array}{ll}
\mathsf{Gen}^\star & \mathsf{Com}^\star_{\mathsf{pk},h}(x_1,\ldots,x_\ell) \\
\left[\begin{array}{l} \mathsf{pk} \leftarrow \mathsf{Gen} \\ h \xleftarrow{u} \mathcal{H} \\ \textbf{\textit{return}}\ (\mathsf{pk}, h) \end{array}\right. &
\left[\begin{array}{l} (c_i, d_i) \leftarrow \mathsf{Com}_{\mathsf{pk}}(x_i),\ i \in \{1,\ldots,\ell\} \\ c_* \leftarrow h(c_1,\ldots,c_\ell) \\ \textbf{\textit{return}}\ (c_*, (c_1,\ldots,c_\ell,d_1,\ldots,d_\ell)) \end{array}\right.
\end{array}$$

where the decommitment procedure just verifies $c_* = h(c_1,\ldots,c_\ell)$ *and restores* $x_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(c_i, d_i)$ *for* $i \in \{1,\ldots,\ell\}$*. Prove that the commitment scheme is secure against partial double openings defined through the following security game*

$$\begin{array}{l}
\mathcal{G} \\
\left[\begin{array}{l}
(\mathsf{pk}, h) \leftarrow \mathsf{Gen}^\star \\
(c_*, c_1, \ldots c_\ell, \hat{c}_1, \ldots \hat{c}_\ell) \leftarrow \mathcal{A}(\mathsf{pk}, h) \\
(i, d_i, \hat{d}_i) \leftarrow \mathcal{A}(\mathsf{pk}, h) \\
\mathsf{if}\ c_* \neq h(c_1,\ldots c_\ell) \vee c_* \neq h(\hat{c}_1,\ldots \hat{c}_\ell)\ \mathsf{then}\ \textbf{\textit{return}}\ 0 \\
\textbf{\textit{return}}\ \bot \neq \mathsf{Open}_{\mathsf{pk}}(c_i, d_i) \neq \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i) \neq \bot
\end{array}\right.
\end{array}$$

provided that the base commitment is (t, ε_1)*-binding and the hash function family is* (t, ε_2)*-collision resistant.*

Solution. Intuitively, there are two possible ways how the adversary $\mathcal{A}$ can breach the security. First, the adversary $\mathcal{A}$ may find a double opening for the base commitment scheme $\mathfrak{C}$. Second, the adversary $\mathcal{A}$ can breaking collision resistant hash function $h \in \mathcal{H}$.

Given the output $(c_*, c_1, \ldots c_\ell, \hat{c}_1, \ldots \hat{c}_\ell)$ is straightforward to decide whether the adversary found a hash collision or not. Namely, the collision occurs if $h(c_1, \ldots c_\ell) = h(\hat{c}_1, \ldots \hat{c}_\ell)$ and there exists $c_i \neq \hat{c}_i$. Thus, we can convert the original adversary $\mathcal{A}$ into two adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$. The adversary $\mathcal{A}_1$ runs internally $\mathcal{A}$ and outputs $(c_*, c_1, \ldots c_\ell, \hat{c}_1, \ldots \hat{c}_\ell)$ only if the event $\mathsf{Collision}$ does not occur, otherwise it halts. The adversary $\mathcal{A}_2$ also runs internally $\mathcal{A}$ but continues only if the event $\mathsf{Collision}$ occurs. By the construction it is straightforward to note that

$$\Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right] = \Pr\left[\mathcal{G}^{\mathcal{A}_1} = 1\right] + \Pr\left[\mathcal{G}^{\mathcal{A}_2} = 1\right]$$

and thus it is sufficient if we analyse the success of both adversaries separately.

Note that $\mathcal{A}_1$ can succeed only if $\mathcal{A}$ double opens some commitment value c_i, since it always outputs $c_i = \hat{c}_i$ for all $i \in \{1, \ldots, \ell\}$. More formally, let

$$\begin{array}{l}
\mathcal{Q}^{\mathcal{B}} \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
(c, d, \hat{d}) \leftarrow \mathcal{B}(\mathsf{pk}) \\
\textbf{return}\ \bot \neq \mathsf{Open}_{\mathsf{pk}}(c, d) \neq \mathsf{Open}_{\mathsf{pk}}(c, \hat{d}) \neq \bot
\end{array}\right.
\end{array}$$

be the binding game. Then we can use the following a reduction construction

$$\begin{array}{l}
\mathcal{B}(\mathsf{pk}) \\
\left[\begin{array}{l}
h \xleftarrow{u} \mathcal{H} \\
(c_*, c_1, \ldots c_\ell, \hat{c}_1, \ldots \hat{c}_\ell) \leftarrow \mathcal{A}_1(\mathsf{pk}, h) \\
(i, d_i, \hat{d}_i) \leftarrow \mathcal{A}_1(\mathsf{pk}, h) \\
\textbf{return}\ (c_i, d_i, \hat{d}_i)\ .
\end{array}\right.
\end{array}$$

By inlining the definition of $\mathcal{B}$ into the game $\mathcal{Q}$ we obtain a slightly modified game

$$\begin{array}{l}\mathcal{G}_1\\ \left[\begin{array}{l}\mathsf{pk}, \leftarrow \mathsf{Gen}, h \xleftarrow{u} \mathcal{H}\\ (c_*, c_1, \dots c_\ell, \hat{c}_1, \dots \hat{c}_\ell) \leftarrow \mathcal{A}_1(\mathsf{pk}, h)\\ (i, d_i, \hat{d}_i) \leftarrow \mathcal{A}_{\mathsf{Com}}(\mathsf{pk}, h)\\ \mathbf{return}\ \bot \neq \mathsf{Open}_{\mathsf{pk}}(c_i, d_i) \neq \mathsf{Open}_{\mathsf{pk}}(c_i, \hat{d}_i) \neq \bot\end{array}\right.\end{array}$$

which is more liberal compared to the original security game $\mathcal{G}$ due to omitted tests. As a result, we get

$$\Pr\left[\mathcal{G}^{\mathcal{A}_1} = 1\right] \leq \Pr\left[\mathcal{G}_1^{\mathcal{A}_1} = 1\right] = \Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right] = \mathsf{Adv}^{\mathsf{bind}}_{\mathfrak{C}}(\mathcal{B}) \ .$$

Now note that the time needed to check whether the collision exists or not is $\Theta(\ell)$ and thus the running time of $\mathcal{A}_1$ and $\mathcal{B}$ is only $\Theta(\ell)$ bigger that the running time for $\mathcal{A}$. Hence for $(t - \mathrm{O}(\ell))$-time adversaries $\mathcal{A}$, we can conclude that $\Pr\left[\mathcal{G}^{\mathcal{A}_1} = 1\right] \leq \varepsilon_1$ if the commitment is (t, ε_1)-binding.

By the construction, $\mathcal{A}_2$ can succeed only if $\mathcal{A}_1$ finds a hash collision and thus its success is bounded by ε_2. Formally, we must still prove it by providing an explicit reduction to the collision-resistance game

$$\begin{array}{l}\mathcal{G}'\\ \left[\begin{array}{l}h \xleftarrow{u} \mathcal{H}\\ (m_1, m_2) \leftarrow \mathcal{B}(h)\\ \mathbf{return}\ m_1 \neq m_2 \wedge h(m_1) = h(m_2) \ .\end{array}\right.\end{array}$$

The reduction is trivial

$$\begin{array}{l}\mathcal{B}(h)\\ \left[\begin{array}{l}\mathsf{pk} \leftarrow \mathsf{Gen}\\ (c_*, c_1, \dots c_\ell, \hat{c}_1, \dots \hat{c}_\ell) \leftarrow \mathcal{A}_2(\mathsf{pk}, h)\\ m_1 \leftarrow (c_1, \dots, c_\ell)\\ m_2 \leftarrow (\hat{c}_1, \dots, \hat{c}_\ell)\\ \mathbf{return}\ (m_1, m_2) \ .\end{array}\right.\end{array}$$

By inlining this adversary definition in to the game $\mathcal{Q}$, we obtain a more liberal game

$$\begin{array}{l}\mathcal{G}_2\\ \left[\begin{array}{l}\mathsf{pk}, \leftarrow \mathsf{Gen}, h \xleftarrow{u} \mathcal{H}\\ (c_1, \dots, c_\ell, \hat{c}_1, \dots, \hat{c}_\ell) \leftarrow \mathcal{A}_2(\mathsf{pk}, h)\\ \mathbf{return}\ h(c_1, \dots, c_\ell) = h(\hat{c}_1, \dots, \hat{c}_\ell) \wedge (c_1, \dots, c_\ell) \neq (\hat{c}_1, \dots, \hat{c}_\ell)\end{array}\right.\end{array}$$

compared to the game $\mathcal{G}$. Thus, we arrive at

$$\Pr\left[\mathcal{G}^{\mathcal{A}_2} = 1\right] \leq \Pr\left[\mathcal{G}_2^{\mathcal{A}_2} = 1\right] = \Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right] = \mathsf{Adv}^{\mathsf{cr}}_{\mathcal{H}}(\mathcal{B}) \ .$$

Again, the overhead in the running-time of $\mathcal{B}$ is $\mathrm{O}(\ell)$ and thus for all $(t - \mathrm{O}(\ell))$-time adversaries $\mathcal{A}$, we can conclude that $\Pr\left[\mathcal{G}^{\mathcal{A}_2} = 1\right] \leq \varepsilon_2$ if the hash function family is (t, ε_2)-collision resistant.