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

Exercise (Semantic security for binding). *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*

$\mathcal{G}_0$

$\mathsf{pk} \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0$
$\pi(\cdot), \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing)$
$\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(m)$
For $i \in \{1, \ldots, n\}$ do
  $\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)$
if $\exists \hat{m}_i = \perp$ ***return*** 0
return $\pi(m, \hat{m}_1, \ldots, \hat{m}_n)$

$\mathcal{G}_1$

$\mathsf{pk} \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$\pi(\cdot), \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing)$
$\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(\overline{m})$
For $i \in \{1, \ldots, n\}$ do
  $\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)$
if $\exists \hat{m}_i = \perp$ ***return*** 0
return $\pi(m, \hat{m}_1, \ldots, \hat{m}_n)$

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 ordinary binding implies semantic binding and find the exact relation between advantages.

Solution. Before going any further let analyse when $\mathcal{A}$ can succeed in the game $\mathcal{G}_0$. First, $\mathcal{A}$ can define a relation π and messages $\overline{m}_1, \ldots, \overline{m}_n$ such that $\pi(m, \overline{m}_1, \ldots, \overline{m}_n)$ holds with high probability for $m \leftarrow \mathcal{M}_0$. Then it is straightforward to commit and later open $\overline{m}_1, \ldots, \overline{m}_n$ to win the game. Unfortunately, with this simplistic strategy the adversary wins the game $\mathcal{G}_1$ equally probably and the advantage cancels out. Intuitively, the advantage $\mathsf{Adv}^{\mathsf{sem\text{-}bind}}_{\mathfrak{C}}(\mathcal{A})$ can be high only if the relation is rarely satisfied when $\overline{m}_1, \ldots, \overline{m}_n$ is fixed and m is chosen from $\mathcal{M}_0$. On the same time, it should be possible for any message m choose $\overline{m}_1, \ldots, \overline{m}_n$ such that the relation $\pi(m, \overline{m}_1, \ldots, \overline{m}_n)$ holds. Consequently, a commitment scheme is not semantically binding if the adversary can adaptively modify the decommitment values.

Fixed target relation. To illustrate this insight a little further let us first consider the sematic binding against fixed relation π. The corresponding security games are without adaptive choice of π:

$\mathcal{G}_2$

$\mathsf{pk} \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0$
$\hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing)$
$\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(m)$
For $i \in \{1, \ldots, n\}$ do
  $\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)$
if $\exists \hat{m}_i = \perp$ **return** 0
return $\pi(m, \hat{m}_1, \ldots, \hat{m}_n)$

$\mathcal{G}_3$

$\mathsf{pk} \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$\hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing)$
$\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(\overline{m})$
For $i \in \{1, \ldots, n\}$ do
  $\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)$
if $\exists \hat{m}_i = \perp$ **return** 0
return $\pi(m, \hat{m}_1, \ldots, \hat{m}_n)$.

Formally, we say that a commitment scheme is semantically (t,ε)-binding with respect to the relation π if for any t-time adversary $\mathcal{A}$ the following advantage is bounded:

$$\mathsf{Adv}^{\mathsf{sem\text{-}bind}}_{\mathfrak{C},\pi}(\mathcal{A}) = \Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_3^{\mathcal{A}} = 1\right] \leq \varepsilon \ .$$

A commitment scheme might be semantically binding for the relation cause the relation is unsuitable for the attack. Let us define trivial attack setting through the following games:

$\mathcal{Q}_2$
$\mathcal{M}_0 \leftarrow \mathcal{B}$
$m \leftarrow \mathcal{M}_0$
$\hat{m}_1, \ldots, \hat{m}_n \leftarrow \mathcal{B}(m)$
return $\pi(m, \hat{m}_1, \ldots, \hat{m}_n)$

$\mathcal{Q}_3$
$\mathcal{M}_0 \leftarrow \mathcal{B}$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$\hat{m}_1, \ldots, \hat{m}_n \leftarrow \mathcal{B}(m)$
return $\pi(m, \hat{m}_1, \ldots, \hat{m}_n)$.

we say that the relation π is (t, ε)-non-controllable if for any t-time adversary $\mathcal{B}$ we can bound the advantage

$$\mathsf{Adv}^{\mathsf{non\text{-}cont}}_{\pi}(\mathcal{B}) = \Pr\left[\mathcal{Q}_2^{\mathcal{B}} = 1\right] - \Pr\left[\mathcal{Q}_3^{\mathcal{B}} = 1\right] \leq \varepsilon \ .$$

As we can inline the entire commitment generation procedure inside the adversary

$\mathcal{B}$
$\mathsf{pk} \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
return $\mathcal{M}_0$

$\mathcal{B}(m)$
$\hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing)$
$\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(m)$
For $i \in \{1, \ldots, n\}$ do
  $\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)$
if $\exists \hat{m}_i = \perp$ **return** $\perp$
return $(\hat{m}_1, \ldots, \hat{m}_n)$

we can easily establish that

$$\mathsf{Adv}^{\mathsf{sem\text{-}bind}}_{\mathfrak{C},\pi}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{non\text{-}cont}}_{\pi}(\mathcal{B})$$

and thus non-controllable relations are indeed also semantically binding.

Let us now study how close to the upper bound we can get if the commitment is binding. Recall that the binding property is defined through the following game

$\mathcal{Q}$
$\mathsf{pk} \leftarrow \mathsf{Gen}$
$(c, d_0, d_1) \leftarrow \mathcal{B}(\mathsf{pk})$
$m_0 \leftarrow \mathsf{Open}_{\mathsf{pk}}(c, d_0)$
$m_1 \leftarrow \mathsf{Open}_{\mathsf{pk}}(c, d_1)$
if $\perp \in \{m_0, m_0\}$ **return** 0
return $[m_0 \neq m_1]$

More precisely, a commitment scheme $\mathfrak{C}$ is (t, ε)-binding if the advantage of any t-time adversary $\mathcal{B}$ against game $\mathcal{Q}$ is bounded

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

As our intuition suggest that $\mathcal{A}$ chooses decommitment values adaptively based on the value of m, it makes sense to run it twice for with different messages m and $\overline{m}$. This should provoke the adversary to release decommitments for different values of $\hat{m}_1, \ldots, \hat{m}_n$ which itself would reveal double opening. The corresponding

adversarial construction is following

$$
\begin{array}{l}
\mathcal{B}(\mathsf{pk}) \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk}) \\
\hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing) \\
m \leftarrow \mathcal{M}_0, m_* \leftarrow \mathcal{M}_0 \\
\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(m) \\
\hat{d}^*_1, \ldots, \hat{d}^*_n \leftarrow \mathcal{A}(\overline{m}) \\
\quad \text{For } i \in \{1, \ldots, n\} \text{ do} \\
\quad \left[\begin{array}{l}
\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i) \\
\hat{m}^*_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}^*_i) \\
\quad \text{if } \ \perp \notin \{\hat{m}_i, \hat{m}^*_i\} \wedge \hat{m}_i \neq \hat{m}^*_i \text{ then} \\
\quad \left[\begin{array}{l} \textbf{return } (\hat{c}_i, \hat{d}_i, \hat{d}^*_i) \end{array}\right.
\end{array}\right. \\
\textbf{return } \perp
\end{array}\right.
\end{array}
$$

where $\mathcal{B}$ always rewinds $\mathcal{A}$ back to the previous state before calling $\mathcal{A}(\overline{m})$. Let Valid denote the event that messages $\hat{m}_1, \ldots, \hat{m}_n$ are valid and Valid_* denote the event that messages $\hat{m}^*_1, \ldots, \hat{m}^*_n$ are valid:

$$
\begin{aligned}
\mathsf{Valid} \quad &\Leftrightarrow \quad \perp \notin \{\hat{m}_1, \ldots, \hat{m}_n\} \ , \\
\mathsf{Valid}_* \quad &\Leftrightarrow \quad \perp \notin \{\hat{m}^*_1, \ldots, \hat{m}^*_n\} \ .
\end{aligned}
$$

Then by the construction

$$
\begin{aligned}
\Pr\left[\mathcal{G}^{\mathcal{A}}_2 = 1\right] &= \Pr\left[\mathsf{pk} \leftarrow \mathsf{Gen}, \mathcal{B}(\mathsf{pk}) : \mathsf{Valid} \wedge \pi(m, \hat{m}_1, \ldots, \hat{m}_n) = 1\right] \\
\Pr\left[\mathcal{G}^{\mathcal{A}}_3 = 1\right] &= \Pr\left[\mathsf{pk} \leftarrow \mathsf{Gen}, \mathcal{B}(\mathsf{pk}) : \mathsf{Valid}_* \wedge \pi(m, \hat{m}^*_1, \ldots, \hat{m}^*_n) = 1\right]
\end{aligned}
$$

whereas the binging advantage can be lower bounded

$$
\mathsf{Adv}^{\mathsf{bind}}_{\mathfrak{C}}(\mathcal{B}) \geq \Pr\left[\mathsf{pk} \leftarrow \mathsf{Gen}, \mathcal{B}(\mathsf{pk}) : \mathsf{Valid} \wedge \mathsf{Valid}_* \wedge \pi(m, \hat{m}_1, \ldots, \hat{m}_n) = 1 \wedge \pi(m, \hat{m}^*_1, \ldots, \hat{m}^*_n) = 0\right]
$$

since the output of the relation can be different only of some argument is different. Each such difference gives us a double opening as both versions of decommitments are valid. As a result, we have structural mismatch between the probability that we want to estimate and the probabilities that determine the success of $\mathcal{A}$.

As the next step, we need to decompose the lower bound probability into simpler terms. First note that for fixed public key pk and randomness ω of $\mathcal{A}$, the events

$$
\mathsf{Valid} \wedge \pi(m, \hat{m}_1, \ldots, \hat{m}_n) = 1 \qquad \text{and} \qquad \mathsf{Valid}_* \wedge \pi(m, \hat{m}^*_1, \ldots, \hat{m}^*_n) = 0
$$

are independent by the construction. Thus, we can expand the bound further

$$
\mathsf{Adv}^{\mathsf{bind}}_{\mathfrak{C}}(\mathcal{B}) \geq \sum_{\mathsf{pk}, \omega} \Pr\left[\omega, \mathsf{pk}\right] \cdot \Pr\left[\mathsf{Valid} \wedge \pi(m, \hat{m}_1, \ldots, \hat{m}_n) = 1 | \omega, \mathsf{pk}\right] \cdot \Pr\left[\mathsf{Valid}_* \wedge \pi(m, \hat{m}^*_1, \ldots, \hat{m}^*_n) = 0 | \omega, \mathsf{pk}\right]
$$

However, this is not enough and we have split this probability into more elementary terms. For that we introduce the following notions:

$$
\begin{aligned}
\delta(\mathsf{pk}, \omega) &= \Pr\left[\mathsf{Valid} | \mathsf{pk}, \omega\right] = \Pr\left[\mathsf{Valid}_* | \mathsf{pk}, \omega\right] \\
\alpha(\mathsf{pk}, \omega) &= \Pr\left[\pi(m, \hat{m}_1, \ldots, \hat{m}_n) = 1 | \mathsf{pk}, \omega, \mathsf{Valid}\right] \\
\beta(\mathsf{pk}, \omega) &= \Pr\left[\pi(m, \hat{m}^*_1, \ldots, \hat{m}^*_n) = 1 | \mathsf{pk}, \omega, \mathsf{Valid}_*\right]
\end{aligned}
$$

where the first equality in the definition follows form the symmetry of Valid and Valid_* events. Armed with this definition we can express the advantage against semantic binding as

$$\begin{aligned}\mathsf{Adv}^{\mathsf{sem\text{-}bind}}_{\mathfrak{C},\pi}(\mathcal{A}) &= \sum_{\mathsf{pk},\omega} \Pr\left[\mathsf{pk},\omega\right] \delta(\mathsf{pk},\omega)\alpha(\mathsf{pk},\omega) - \sum_{\mathsf{pk},\omega} \Pr\left[\mathsf{pk},\omega\right] \delta(\mathsf{pk},\omega)\beta(\mathsf{pk},\omega) \\ &= \sum_{\mathsf{pk},\omega} \Pr\left[\mathsf{pk},\omega\right] \delta(\mathsf{pk},\omega)(\alpha(\mathsf{pk},\omega) - \beta(\mathsf{pk},\omega))\end{aligned}$$

and the advantage against biding as

$$\mathsf{Adv}^{\mathsf{bind}}_{\mathfrak{C}}(\mathcal{B}) \geq \sum_{\mathsf{pk},\omega} \Pr\left[\mathsf{pk},\omega\right] \delta(\mathsf{pk},\omega)^2(\alpha(\mathsf{pk},\omega) - \beta(\mathsf{pk},\omega))$$

Probably wrong here We must consider dependence on m here instead! The dependence on pk and ω might be constant an we still have problems

Siim

We will now make a reduction to the ordinary binding game by considering an optimal adversary $\mathcal{A}$ against the semantic binding games and constructing an adversary $\mathcal{B}$ against game $\mathcal{Q}$. We construct the adversary $\mathcal{B}$ in the following way:

$\mathcal{B}(\mathsf{pk})$
- $\mathsf{pk} \leftarrow \mathsf{Gen}$
- $\mathcal{M}_0 \leftarrow \mathcal{A}(\mathsf{pk})$
- $\pi(\cdot), \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{A}(\varnothing)$
- $m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
- $\hat{d}_1, \ldots, \hat{d}_n \leftarrow \mathcal{A}(m)$
- $\overline{d}_1, \ldots, \overline{d}_n \leftarrow \mathcal{A}(\overline{m})$
- For $i \in \{1, \ldots, n\}$ do
  - $\hat{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i)$
  - $\overline{m}_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \overline{d}_i)$
  - if $\hat{m}_i \neq \perp \ \wedge\ \overline{m}_i \neq \perp \ \wedge\ \hat{m}_i \neq \overline{m}_i$ **return** $(\hat{c}_i, \hat{d}_i, \overline{d}_i)$
- **return** $\perp$

Without loss of generality, we can assume an optimal adversary in the semantic binding games, given inputs $m \neq \overline{m}$ for some fixed $\mathcal{M}_0$, always produces the sets of decommitments $\hat{d}_1, \ldots, \hat{d}_n$ and $\overline{d}_1, \ldots, \overline{d}_n$ such, that at least one pair $\hat{d}_i, \overline{d}_i$ opens to a different message (or one or both fail to open). Otherwise, the adversary increases the probability that both games $\mathcal{G}_0$ and $\mathcal{G}_1$ return the same result, possibly reducing the overall advantage.

We can also assume that the call $\mathcal{A}(m)$ does not affect the behavior of the adversary in the next call $\mathcal{A}(\overline{m})$, as $\mathcal{B}$ can always rewind the adversary to the previous state. Also, since the predicate $\pi(\cdot)$ is fixed by the adversary before these calls, both calls will surely produce an equal amount of decommitment values, otherwise the opened messages would not be a valid input to the predicate in games $\mathcal{G}_0, \mathcal{G}_1$, since the domain of $\pi(\cdot)$ is fixed. Altogether the construction of $\mathcal{B}$ is valid, since all operations can be executed and $\mathcal{A}$ receives valid inputs.

Clearly, game $\mathcal{Q}^{\mathcal{B}}$ ends with 1 iff $\mathcal{B}$ returns the triplet $(\hat{c}_i, \hat{d}_i, \overline{d}_i)$, since then $\hat{d}_i$ and $\overline{d}_i$ decommit to different messages. Thus, the advantage of the adversary against ordinary binding game is

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

We will now analyze the probability $\Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right]$. Let us first define two events Valid_1 and Valid_2:

$$\mathsf{Valid}_1 := \forall i \in \{1, \ldots, n\}\, \hat{m}_i \neq \perp$$
$$\mathsf{Valid}_2 := \forall i \in \{1, \ldots, n\}\, \overline{m}_i \neq \perp$$

If events Valid_1 and Valid_2 occur together and there exists some i for which $\hat{m}_i \neq \overline{m}_i$, then $\mathcal{B}$ successfully finds a triplet to return. Therefore, we have

$$\Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right] \geq \Pr\left[\mathsf{Valid}_1 \wedge \mathsf{Valid}_2 \wedge \exists \hat{m}_i \neq \overline{m}_i\right] = \Pr\left[\mathsf{Valid}_1 \wedge \mathsf{Valid}_2\right] \cdot \Pr\left[\exists \hat{m}_i \neq \overline{m}_i \mid \mathsf{Valid}_1 \wedge \mathsf{Valid}_2\right].$$

Since we assumed that for two different messages $m \neq \overline{m}$, a pair of different openings always exists, then

$$\Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right] \geq \Pr\left[\mathsf{Valid}_1 \wedge \mathsf{Valid}_2\right] \cdot \Pr\left[m \neq \overline{m} \mid \mathsf{Valid}_1 \wedge \mathsf{Valid}_2\right].$$

By manipulating the conditional probabilities we can arrive at

$$\Pr\left[m \neq \overline{m} \mid \mathsf{Valid}_1 \wedge \mathsf{Valid}_2\right] = 1 - \frac{\Pr\left[m = \overline{m}\right] \cdot \Pr\left[\mathsf{Valid}_1 \wedge \mathsf{Valid}_2 \mid m = \overline{m}\right]}{\Pr\left[\mathsf{Valid}_1 \wedge \mathsf{Valid}_2\right]}$$

Notice that if $m = \overline{m}$, then the events Valid_1 and Valid_2 coincide, which means

$$\Pr\left[\mathsf{Valid}_1 \wedge \mathsf{Valid}_2 \mid m = \overline{m}\right] = \Pr\left[\mathsf{Valid}_1\right]$$

and we have thus arrived at

$$\Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right] \geq \Pr\left[\mathsf{Valid}_1 \wedge \mathsf{Valid}_2\right] - \Pr\left[m = \overline{m}\right] \cdot \Pr\left[\mathsf{Valid}_1\right].$$

Notice that Valid_1 and Valid_2 are independent events, since they depend only on the values of m and $\overline{m}$, since all other parameters are fixed up to that point. Also, since we can assume $\mathcal{A}(m)$ and $\mathcal{A}(\overline{m})$ are independent calls and use the same randomness, then actually

$$\Pr\left[\mathsf{Valid}_1\right] = \Pr\left[\mathsf{Valid}_2\right]$$

and thus we have

$$\Pr\left[\mathsf{Valid}_1 \wedge \mathsf{Valid}_2\right] = \Pr\left[\mathsf{Valid}_1\right] \cdot \Pr\left[\mathsf{Valid}_2\right] = \Pr\left[\mathsf{Valid}_1\right]^2.$$

From the definition of Valid_1 and our $\mathcal{B}$ construction, it is easy to see that

$$\Pr\left[\mathsf{Valid}_1\right] \geq \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] + \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 0 \wedge \mathsf{Valid}_1\right] \geq \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] = \varepsilon_1$$

We finally need to analyze the probability $\Pr\left[m = \overline{m}\right]$.
And now I got stuck... I have

$$\Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right] \geq \varepsilon_1^2 - \Pr\left[m = \overline{m}\right] \cdot \Pr\left[\mathsf{Valid}_1\right]$$

but I can't seem to get this into something like $\varepsilon_1^2 - \varrho \cdot \varepsilon_1$, which would give me $\varepsilon_1 \leq \varrho + \varepsilon$.