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

Exercise (Dual-mode commitment). *Show that an multiplicatively homomorphic asymmetric IND-CPA secure cryptosystem* $\mathfrak{C} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with perfect decryption can be converted to perfectly hiding and computationally binding commitment by using the following construction:*

$\mathsf{Gen}^\star$
$\lceil (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$\quad c_\star \leftarrow \mathsf{Enc}_{\mathsf{pk}}(0)$
$\quad \boldsymbol{return}\ (\mathsf{pk}, c_\star)$

$\mathsf{Com}_{\mathsf{pk},c_\star}(m)$
$\lceil r \leftarrow_u \mathcal{R}$
$\quad c \leftarrow c_\star^m \cdot \mathsf{Enc}_{\mathsf{pk},c_\star}(0; r)$
$\quad \boldsymbol{return}\ (c, (m, r))$

$\mathsf{Open}_{\mathsf{pk},\star}(c, m, r)$
$\lceil \hat{c} \leftarrow c_\star^m \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r)$
$\quad \mathsf{if}\ c = \hat{c}\ \boldsymbol{return}\ m$
$\quad \mathsf{else}\ \boldsymbol{return}\ \perp$

and computationally hiding and perfectly binding commitment by using the following construction:

$\mathsf{Gen}^\star$
$\lceil (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$\quad c_\circ \leftarrow \mathsf{Enc}_{\mathsf{pk}}(1)$
$\quad \boldsymbol{return}\ (\mathsf{pk}, c_\circ)$

$\mathsf{Com}_{\mathsf{pk},c_\circ}(m)$
$\lceil r \leftarrow_u \mathcal{R}$
$\quad c \leftarrow c_\circ^m \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r)$
$\quad \boldsymbol{return}\ (c, (m, r))$

$\mathsf{Open}_{\mathsf{pk}}(c, m, r)$
$\lceil \hat{c} \leftarrow c_\circ^m \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r)$
$\quad \mathsf{if}\ c = \hat{c}\ \boldsymbol{return}\ m$
$\quad \mathsf{else}\ \boldsymbol{return}\ \perp\ .$

Solution. Let us prove simple security statements first. Since the encryption scheme is multiplicatively homomorphic, we get that the commitment value

$$c_\star^m \cdot \mathsf{Enc}_{\mathsf{pk}}(0) \equiv \mathsf{Enc}_{\mathsf{pk}}(0)^m \cdot \mathsf{Enc}_{\mathsf{pk}}(0) \equiv \mathsf{Enc}_{\mathsf{pk}}(0)$$

is a random encryption of a zero. Thus it is straightforward to prove that hiding games

$\mathcal{G}_0^{\mathcal{A}}$
$\lceil (\mathsf{pk}, c_\star) \leftarrow \mathsf{Gen}^\star$
$\quad (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}, c_\star)$
$\quad r \leftarrow_u \mathcal{R}$
$\quad c \leftarrow c_\star^{m_0} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r)$
$\quad \mathbf{return}\ \mathcal{A}(c)$

$\mathcal{G}_1^{\mathcal{A}}$
$\lceil (\mathsf{pk}, c_\star) \leftarrow \mathsf{Gen}^\star$
$\quad (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}, c_\star)$
$\quad r \leftarrow_u \mathcal{R}$
$\quad c \leftarrow c_\star^{m_1} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r)$
$\quad \mathbf{return}\ \mathcal{A}(c)$

are completely identical. Hence, the first commitment scheme is indeed perfectly hiding. By using the properties of homomorphic encryption, we can easily show that

$$c_\circ^m \cdot \mathsf{Enc}_{\mathsf{pk}}(0) \equiv \mathsf{Enc}_{\mathsf{pk}}(1)^m \cdot \mathsf{Enc}_{\mathsf{pk}}(0) \equiv \mathsf{Enc}_{\mathsf{pk}}(m)$$

is a random encryption of m. Consequently no commitment can be double opened. Indeed, a valid double opening c, m_0, r_0, m_1, r_1 means that

$$\mathsf{Enc}_{\mathsf{pk}}(m_0; \hat{r}_0) = c = \mathsf{Enc}_{\mathsf{pk}}(m_1; \hat{r}_1)$$

for some $r_0, r_1 \in \mathcal{R}$. Consequently, the cryptosystem cannot be perfectly decryptable.

Similarlty of commitment modes. Both commitment schemes are structurally very similar. First note that the commit and open functions are identical for both schemes. The difference lies only in the form of the public parameters. Moreover, the key generation algorithm returns elements pair that are computationally indistinguishable if the cryptosystem is IND-CPA secure. Thus, we can prove the remaining security properties by contrasting these two commitment schemes commonly references as commitment modes.

Contrasting for hiding. Let us prove first that the second commitment mode is computationally hiding.

For that observe that corresponding hiding games

$$\begin{array}{ll}\mathcal{G}_2^{\mathcal{A}} & \mathcal{G}_3^{\mathcal{A}} \\ \left[\begin{array}{l}(\mathsf{pk}, c_\circ) \leftarrow \mathsf{Gen}^\circ \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}, c_\circ) \\ r \leftarrow_u \mathcal{R} \\ c \leftarrow c_\circ^{m_0} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r) \\ \textbf{return } \mathcal{A}(c)\end{array}\right. & \left[\begin{array}{l}(\mathsf{pk}, c_\circ) \leftarrow \mathsf{Gen}^\circ \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}, c_\circ) \\ r \leftarrow_u \mathcal{R} \\ c \leftarrow c_\circ^{m_1} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r) \\ \textbf{return } \mathcal{A}(c)\end{array}\right.\end{array}$$

are very similar to the hiding games $\mathcal{G}_0$ and $\mathcal{G}_1$. More precisely, consider the adversary construction

$$\begin{array}{ll}\mathcal{B}^{\mathcal{A}}(\mathsf{pk}) & \mathcal{B}^{\mathcal{A}}(c) \\ \left[\textbf{return } (0,1)\right. & \left[\begin{array}{l}(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}, c) \\ r \leftarrow_u \mathcal{R} \\ c \leftarrow c^{m_0} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r) \\ \textbf{return } \mathcal{A}(c)\ .\end{array}\right.\end{array}$$

Then direct substitution of the adversary into the IND-CPA security games

$$\begin{array}{ll}\mathcal{Q}_0^{\mathcal{B}} & \mathcal{Q}_1^{\mathcal{B}} \\ \left[\begin{array}{l}\mathsf{pk} \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{B}(pk) \\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0) \\ \textbf{return } \mathcal{B}(c)\end{array}\right. & \left[\begin{array}{l}\mathsf{pk} \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{B}(pk) \\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1) \\ \textbf{return } \mathcal{B}(c)\end{array}\right.\end{array}$$

yields games $\mathcal{G}_0^{\mathcal{A}}$ and $\mathcal{G}_2^{\mathcal{A}}$. The similar construction exists also for the games $\mathcal{G}_1^{\mathcal{A}}$ and $\mathcal{G}_3^{\mathcal{A}}$. Hence,

$$\begin{aligned}\left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right]\right| &= \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{B})\ , \\ \left|\Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_3^{\mathcal{A}} = 1\right]\right| &= \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{C})\ ,\end{aligned}$$

for algorithms $\mathcal{B}$ and $\mathcal{C}$ which have only constant overhead in the running time. Since $\mathcal{G}_0^{\mathcal{A}} \equiv \mathcal{G}_1^{\mathcal{A}}$, we can use the triangle inequality to get the boung

$$\left|\Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_3^{\mathcal{A}} = 1\right]\right| \leq \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{B}) + \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{C})\ .$$

Consequently, if the cryptosystem is (t, ε)-IND-CPA secure, the resulting commitment scheme is $(t, 2\varepsilon)$-hiding.

Contrasting for binding. We can us the same contrasting also for the binging games. Let us consider the binging game against the first commitment mode:

$$\begin{array}{l}\mathcal{G}_3^{\mathcal{A}} \\ \left[\begin{array}{l}\mathsf{pk} \leftarrow \mathsf{Gen} \\ c_\star = \mathsf{Enc}_{\mathsf{pk}}(0) \\ (c, m_0, r_0, m_1, r_1) \leftarrow \mathcal{A}(pk, c_\star) \\ c_0 \leftarrow c_\star^{m_0} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r_0) \\ c_1 \leftarrow c_\star^{m_1} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r_1) \\ \textbf{return } [c \stackrel{?}{=} c_0] \wedge [c \stackrel{?}{=} c_1] \wedge [m_0 \neq m_1]\end{array}\right.\end{array}$$

and he binging game against the second commitment mode:

$$
\begin{array}{l}
\mathcal{G}_4^{\mathcal{A}} \\
\left[\begin{array}{l}
\mathsf{pk} \leftarrow \mathsf{Gen} \\
c_\circ = \mathsf{Enc}_{\mathsf{pk}}(0) \\
(c, m_0, r_0, m_1, r_1) \leftarrow \mathcal{A}(pk, c_\circ) \\
c_0 \leftarrow c_\star^{m_0} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r_0) \\
c_1 \leftarrow c_\star^{m_1} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r_1) \\
\textbf{return } [c \stackrel{?}{=} c_0] \wedge [c \stackrel{?}{=} c_1] \wedge [m_0 \neq m_1] \ .
\end{array}\right.
\end{array}
$$

Again, we can give a reduction construction

$$
\begin{array}{ll}
\mathcal{B}^{\mathcal{A}}(\mathsf{pk}) & \mathcal{B}^{\mathcal{A}}(c) \\
\left[\textbf{return } (0,1)\right. & \left[\begin{array}{l}
(c, m_0, r_0, m_1, r_1) \leftarrow \mathcal{A}(pk, c_\circ) \\
c_0 \leftarrow c_\star^{m_0} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r_0) \\
c_1 \leftarrow c_\star^{m_1} \cdot \mathsf{Enc}_{\mathsf{pk}}(0; r_1) \\
\textbf{return } [c \stackrel{?}{=} c_0] \wedge [c \stackrel{?}{=} c_1] \wedge [m_0 \neq m_1] \ .
\end{array}\right.
\end{array}
$$

such that by substituting it to the IND-CPA games yields: $\mathcal{G}_3^{\mathcal{A}} \equiv \mathcal{Q}_0^{\mathcal{B}}$ and $\mathcal{G}_4^{\mathcal{A}} \equiv \mathcal{Q}_1^{\mathcal{B}}$. Thus, again we get

$$
\left|\Pr\left[\mathcal{G}_3^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_4^{\mathcal{A}} = 1\right]\right| = \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{B})
$$

Since the second commitment mode is perfectly binding, we can estimate

$$
\Pr\left[\mathcal{G}_3^{\mathcal{A}} = 1\right] \leq \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{B}) + \Pr\left[\mathcal{G}_4^{\mathcal{A}} = 1\right] \leq \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cpa}}(\mathcal{B}) \ .
$$

Again, the overhead in the running time of $\mathcal{B}$ is only constant and we get that (t, ε)-IND-CPA security assures that the first commitment mode is (t, ε)-binding.