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

Exercise (Security of user-aided key agreement). *Consider the following simple user-aided key agreement protocol. The public key* pk *of a server* $\mathcal{P}_1$ *is known to all participants. If a participant* $\mathcal{P}_2$ *wants to connect to* $\mathcal{P}_1$ *it generates a random session key* $k \xleftarrow{u} \mathcal{K}$ *and a short authentication nonce* $r \xleftarrow{u} \{0, \ldots, 9999\}$ *and sends* $\mathsf{Enc}_{\mathsf{pk}}(k\|r)$ *to* $\mathcal{P}_1$. *Next* $\mathcal{P}_1$ *recovers* k *and* r *and sends* r *as an SMS back to* $\mathcal{P}_2$. *The client* $\mathcal{P}_2$ *halts if the SMS does not correspond to his or her authentication nonce. Prove that a* t*-time adversary can alter the ciphertext without being detected with probability at most* $10^{-4} + \varepsilon$ *provided that the cryptosystem is* (t, ε)*-IND-CCA2 secure and no adversary cannot alter the SMS message.*

Solution. For brevity, let $\mathcal{R} = \{0000, \ldots, 9999\}$ denote the nonce space. Then we can formalise the security goal through the following game:

$$
\begin{array}{l}
\mathcal{G} \\
\left[\begin{array}{l}
(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen} \\
k \xleftarrow{u} \mathcal{K}, r \xleftarrow{u} \mathcal{R} \\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(k||r) \\
\hat{c} \leftarrow \mathcal{A}(c) \\
\hat{k}||\hat{r} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(c) \\
\mathsf{if}\ r \neq \hat{r}\ \mathbf{return}\ 0 \\
\mathbf{return}\ \neg[k \stackrel{?}{=} \hat{k}]\ .
\end{array}\right.
\end{array}
$$

Note that if the adversary return $\hat{c} = c$, he or she is guaranteed to loose the game. Hence, we can consider only adversaries that always return $\hat{c} \neq c$. More formally, it is straightforward to modify any adversary to output a different encryption if $\hat{c} = c$. This would only increase the adversaries success probability with the cost of constant overhead in running time.

Now let $\mathcal{A}$ be an adversary interacting with game $\mathcal{G}$. Then our goal is to construct an adversary $\mathcal{B}^{\mathcal{A}}$ against IND-CCA2 games

$$
\begin{array}{l}
\mathcal{Q}_0 \\
\left[\begin{array}{l}
(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen} \\
(m_0, m_1) \leftarrow \mathcal{B}^{\mathcal{O}_1}(\mathsf{pk}) \\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0) \\
\mathbf{return}\ \mathcal{B}^{\mathcal{O}_2}(c)
\end{array}\right.
\end{array}
\qquad
\begin{array}{l}
\mathcal{Q}_1 \\
\left[\begin{array}{l}
(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen} \\
(m_0, m_1) \leftarrow \mathcal{B}^{\mathcal{O}_1}(\mathsf{pk}) \\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1) \\
\mathbf{return}\ \mathcal{B}^{\mathcal{O}_2}(c)
\end{array}\right.
\end{array}
$$

so that $\mathcal{Q}_0^{\mathcal{B}}$ would be identical to the game $\mathcal{G}^{\mathcal{A}}$. The latter is straightforward, we must just define:

$$
\begin{array}{l}
\mathcal{B}^{\mathcal{O}_1}(\mathsf{pk}) \\
\left[\begin{array}{l}
k_0, k_1 \xleftarrow{u} \mathcal{K} \\
r_0, r_1 \xleftarrow{u} \mathcal{R} \\
m_0 \leftarrow k_0||r_0 \\
m_1 \leftarrow k_1||r_1 \\
\mathbf{return}\ (m_0, m_1)
\end{array}\right.
\end{array}
\qquad
\begin{array}{l}
\mathcal{B}^{\mathcal{O}_2}(c) \\
\left[\begin{array}{l}
\hat{c} \leftarrow \mathcal{A}(c) \\
\hat{k}||\hat{r} \leftarrow \mathcal{O}_2(\hat{c}) \\
\mathbf{return}\ [r_0 \stackrel{?}{=} \hat{r}] \wedge \neg[k_0 \stackrel{?}{=} \hat{k}]\ .
\end{array}\right.
\end{array}
$$

By our assumption $\hat{c}$ is always different form c and thus the call to the decryption oracle never fails. As a result, the direct substitution of the construction of $\mathcal{B}$ leads to the game

$$
\begin{array}{l}
\mathcal{G}_0^{\mathcal{B}} \\
\left[\begin{array}{l}
\mathsf{sk}, \mathsf{pk} \leftarrow \mathsf{Gen} \\
k \xleftarrow[u]{} \mathcal{K} \\
r_0, r_1 \xleftarrow[u]{} \mathcal{R} \\
m_0 \leftarrow k || r_0 \\
m_1 \leftarrow k || r_1 \\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0) \\
\hat{c} \leftarrow A(c) \\
\hat{k} || \hat{r} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}) \\
\textbf{return } [r_0 \stackrel{?}{=} \hat{r}] \wedge \neg [k \stackrel{?}{=} \hat{k}]
\end{array}\right.
\end{array}
$$

which identical to the game $\mathcal{G}^{\mathcal{A}}$. The only syntactical difference becomes from the extra lines that are needed to compute m_1 that is not used to create outcome of the game. Now if we substitute the construction of $\mathcal{B}$ into the other game $\mathcal{Q}_1$, we get

$$
\begin{array}{l}
\mathcal{G}_1^{\mathcal{B}} \\
\left[\begin{array}{l}
\mathsf{sk}, \mathsf{pk} \leftarrow \mathsf{Gen} \\
k \xleftarrow[u]{} \mathcal{K} \\
r_0, r_1 \xleftarrow[u]{} \mathcal{R} \\
m_0 \leftarrow k || r_0 \\
m_1 \leftarrow k || r_1 \\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1) \\
\hat{c} \leftarrow A(c) \\
\hat{k} || \hat{r} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}) \\
\textbf{return } [r_0 \stackrel{?}{=} \hat{r}] \wedge \neg [k \stackrel{?}{=} \hat{k}]
\end{array}\right.
\end{array}
$$

which can be further converted into the semantically identical form

$$
\begin{array}{l}
\mathcal{G}_2^{\mathcal{B}} \\
\left[\begin{array}{l}
\mathsf{sk}, \mathsf{pk} \leftarrow \mathsf{Gen} \\
k \xleftarrow[u]{} \mathcal{K} \\
r_1 \xleftarrow[u]{} \mathcal{R} \\
m_1 \leftarrow k || r_1 \\
c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1) \\
\hat{c} \leftarrow A(c) \\
\hat{k} || \hat{r} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c}) \\
r_0 \leftarrow \mathcal{R} \\
\textbf{return } [r_0 \stackrel{?}{=} \hat{r}] \wedge \neg [k \stackrel{?}{=} \hat{k}] \ .
\end{array}\right.
\end{array}
$$

For this game, it is easy to estimate the success probability

$$\Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right] \leq \frac{1}{|\mathcal{R}|} \ ,$$

since r_0 value is randomly chosen after the value $\hat{r}$ is fixed. By our construction

$$\left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| = \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{ind\text{-}cca\text{-}2}}(\mathcal{B}) \ .$$

Hence, we can estimate the success of the original game

$$\Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right] \leq \mathsf{Adv}^{\text{ind-cca-2}}_{\mathfrak{E}}(\mathcal{B}) + \Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right] \leq \mathsf{Adv}^{\text{ind-cca-2}}_{\mathfrak{E}}(\mathcal{B}) + \frac{1}{|\mathcal{R}|} \enspace .$$

As the running-time $\mathcal{B}$ is only by a constant larger than the running time of $\mathcal{A}$, the usage of (t, ε)-IND-CCA2 secure cryptosystem guarantees that

$$\Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right] \leq \frac{1}{|\mathcal{R}|} + \varepsilon \enspace .$$