Homework 4

Posted: Mar 3, Due: Mar 11 (Note unusual due date!)

Task 1 — Public-Key Encryption

Let $PKE = (Kg, Enc, Dec)$ be a public-key encryption scheme with message space $M = \{0, 1\}$, i.e., $PKE$ can only encrypt one-bit messages. We want to use $PKE$ to encrypt longer messages — say $\ell$-bit long. To this end, we consider the construction $PKE' = (Kg, Enc', Dec')$ which encrypts $\ell$-bit messages bit-by-bit using $PKE$. More precisely, it behaves as follows. (Here, $M[i]$ denotes the $i$-th bit of a string $M$ and $v[i]$ the $i$-th component of a vector $v$.)

\begin{align*}
\text{Procedure } Kg: & \\
& \text{For } i = 1 \text{ to } \ell \text{ do} \\
& (SK_i, PK_i) \leftarrow Kg \\
& PK \leftarrow [PK_1, \ldots, PK_n] \\
& SK \leftarrow [SK_1, \ldots, SK_n] \\
& \text{Return } (PK, SK) \\
\end{align*}

\begin{align*}
\text{Procedure } Enc_{PK}(M): & & \text{// } M \in \{0, 1\}^\ell \\
& \text{For } i = 1 \text{ to } \ell \text{ do} \\
& C[i] \leftarrow Enc_{PK[i]}(M[i]) \\
& \text{Return } C \\
\end{align*}

\begin{align*}
\text{Procedure } Dec_{SK}(C): & \\
& \text{For } i = 1 \text{ to } \ell \text{ do} \\
& M[i] \leftarrow Dec_{SK[i]}(C[i]) \\
& \text{Return } M[1] \| . . . \| M[\ell] \\
\end{align*}

In particular, ciphertexts $C$ for $PKE'$ are $\ell$-dimensional vectors whose components are ciphertexts for $PKE$.

a) [5 pts] Prove that $PKE$ is not IND-CCA secure.

Hint: Give a concrete attack breaking IND-CCA-security.

Assume that $\ell \geq 2$. Moreover, we assume that $PKE$ is perfectly correct, i.e., decryption is always correct with probability one. (This is the only assumption we need to make to disprove the claim, and it is not really necessary, but makes the presentation somewhat easier.)

We consider the following adversary $A$ which operates as follows, given access to $LR_b$ and $DEC$, as well as the public key $PK$.

\begin{align*}
\text{Adversary } A^{LR_b, DEC}(PK): & \\
& C \leftarrow LR_b(0^\ell, 1^\ell) \\
& C' \leftarrow Enc_{PK[1]}(1) \\
& C'[1] \leftarrow C' \\
& \text{For } i = 2 \text{ to } \ell \text{ do} \\
& C'[i] \leftarrow C[i] \\
& M' \leftarrow Dec(C') \\
& \text{If } M' = 10^{\ell-1} \text{ then} \\
& \text{Return } 1 \\
& \text{Else return } 0 \\
\end{align*}

In particular, $A$ replaces the first component of $C$ with a fresh encryption of 1, and then submits the resulting ciphertext $C'$ for decryption. Note that the query $C'$ does not return $\bot$ if $C \neq C'$ (or equivalently, $C[1] \neq C'[1]$), and in particular if $b = 0$, whenever $C \neq C'$, $A$ gets the answer $M' = 10^{\ell-1}$. Overall, this means that

$$Pr\left[(PK, SK) \leftarrow Kg : A^{LR_0, DEC}(PK) = 1\right] = 1 - Pr\left[C' = C[1]\right].$$  \quad (1)
Recall however that we have assumed that PKE is perfectly correct and never decrypt incorrectly, and thus since $C'$ encrypts 1, yet $C[1]$ encrypts 0 when $b = 0$, we must have $C' \neq C[1]$, for otherwise decryption for PKE would be incorrect on $C'$ or $C[1]$. Therefore, $\Pr [C' = C[1]] = 0$, and the above probability is always one.

In contrast, if $b = 1$, $A$ always receives either $M' = \bot$ (when $C' = C[1]$) or $M' = 1^\ell$ (when $C' \neq C[1]$), and thus $M' \neq 1^{\ell-1}$ no matter what. Hence,

$$\Pr [(PK, SK) \leftarrow K^g : A^{LR_1, DEC}(PK) = 1] = 0.$$  \hfill (2)

To conclude, combining (1) and (2) yields

$$\text{Adv}_{\text{PKE}}^{\text{ind-cca}}(A) = 1.$$  

b) [15 pts] Assume that PKE is IND-CPA secure. Prove that $\overline{\text{PKE}}$ is also IND-CPA secure.

Hint: Proceed as follows:

- Formally describe a sequence of games $G_0, G_1, \ldots, G_\ell$ where the adversary $A$ asks a single query $(M_0, M_1)$ to the LR$_b$ oracle, for $M_0, M_1 \in \{0, 1\}^\ell$. For this query, Game $G_i$ returns $C$ such that

  $$C[j] \leftarrow \operatorname{Enc}_{PK}[j](M_0[j])$$

  for all $i < j \leq \ell$, and

  $$C[j] \leftarrow \operatorname{Enc}_{PK}[j](M_1[j])$$

  for all $1 \leq j \leq i$.

- Prove that $\text{Adv}_{\text{PKE}}^{\text{ind-cca}}(A) = \Pr [G_0 \Rightarrow 1] - \Pr [G_\ell \Rightarrow 1]$.

- For all $1 \leq i \leq \ell$, prove that there exists an adversary $B_i$ such that

  $$\text{Adv}_{\text{PKE}}^{\text{ind-cca}}(B_i) = \Pr [G_{i-1} \Rightarrow 1] - \Pr [G_i \Rightarrow 1].$$

- Conclude IND-CPA security of $\overline{\text{PKE}}$ from the above.

To prove the claim, we fix an adversary $A$ against IND-CPA security of $\overline{\text{PKE}}$ issuing exactly one query to its LR$_b$ oracle. We are going to prove that there exist adversaries $A_1, \ldots, A_\ell$ such that

$$\text{Adv}_{\text{PKE}}^{\text{ind-cca}}(A) = \sum_{i=1}^\ell \text{Adv}_{\text{PKE}}^{\text{ind-cca}}(A_i),$$

and moreover, $A_1, \ldots, A_\ell$ are all PPT when $A$ is PPT. This implies the claim, because all advantages $\text{Adv}_{\text{PKE}}^{\text{ind-cca}}(A_i)$ are all negligible when $A$ is PPT by our assumption that PKE is IND-CPA secure, and moreover, $\ell$ is small (i.e., polynomial in the security parameter) for $\overline{\text{PKE}}$ to be efficient. (The latter assumption was somewhat implicit, but the scheme does not make sense otherwise if it cannot be executed.)

We start by defining the games $G_0, G_1, \ldots, G_\ell$ as requested:
Game $G_i$: // $i \in \{0, 1, \ldots, \ell\}$

\[
\begin{align*}
(PK, SK) & \xleftarrow{\$} Kg \\
b & \xleftarrow{\$} ALR_0(PK) \\
\text{Return } b
\end{align*}
\]

Procedure $LR_0(M_0, M_1)$: // $M_0, M_1 \in \{0, 1\}^\ell$

\[
\begin{align*}
\text{For } j = 1 \text{ to } \ell \text{ do} \\
\text{If } j \leq i \text{ then} \\
\quad C[j] & \xleftarrow{\$} \text{Enc}_{PK[j]}(M_1[j]) \\
\text{Else} \\
\quad C[j] & \xleftarrow{\$} \text{Enc}_{PK[j]}(M_0[j]) \\
\text{Return } C
\end{align*}
\]

It is easy to verify that

\[
Pr[G_0 \Rightarrow 1] = Pr[(PK, SK) \xleftarrow{\$} Kg : ALR_0 = 1]
\]

as well as

\[
Pr[G_\ell \Rightarrow 1] = Pr[(PK, SK) \xleftarrow{\$} Kg : ALR_1 = 1].
\]

In other words, we can rewrite $A$'s advantage as

\[
\text{Adv}^{\text{ind-cpa}}_{\text{PKE}}(A) = Pr[G_0 \Rightarrow 1] - Pr[G_\ell \Rightarrow 1] = \sum_{i=1}^{\ell} Pr[G_{i-1} \Rightarrow 1] - Pr[G_i \Rightarrow 1].
\]

To conclude the proof, we now give the adversaries $A_i$ explicitly. Note that these adversaries live in the IND-CPA experiment for PKE. The idea, as usual, is that we let $A_i$ use the underlying experiment to simulate either of $G_{i-1}$ or $G_i$ to $A$ depending on whether $b = 0$ or $b = 1$. In particular, the adversaries $A_i$ internally run an execution of $A$ with some simulate public key $PK$, and access to a simulated $LR'_0$ oracle which is obtained by using, as a sub-routine, the actual $LR_0$ oracle $A_i$ is given access to. Formally:

\[
\text{Adversary } A_i^{LR_0}(PK): \text{ // } i \in \{0, 1, \ldots, \ell\}
\]

\[
\begin{align*}
\text{For } j = 1 \text{ to } \ell \text{ do} \\
\text{If } j = i \text{ then} \\
\quad PK[j] & \leftarrow PK \\
\text{Else} \\
\quad (PK[j], SK[j]) & \xleftarrow{\$} Kg \\
b & \xleftarrow{\$} ALR'_0(PK) \\
\text{Return } b
\end{align*}
\]

Procedure $LR'_0(M_0, M_1)$: // $M_0, M_1 \in \{0, 1\}^\ell$

\[
\begin{align*}
\text{For } j = 1 \text{ to } \ell \text{ do} \\
\text{If } j < i \text{ then} \\
\quad C[j] & \xleftarrow{\$} \text{Enc}_{PK[j]}(M_1[j]) \\
\text{Else if } j = i \text{ then} \\
\quad C[j] & \xleftarrow{\$} LR_0(M_0[j], M_1[j]) \\
\text{Else} \\
\quad C[j] & \xleftarrow{\$} \text{Enc}_{PK[j]}(M_0[j]) \\
\text{Return } C
\end{align*}
\]

It is not hard to check by inspection that

\[
\text{Adv}^{\text{ind-cpa}}_{\text{PKE}}(A_i) = Pr[G_{i-1} \Rightarrow 1] - Pr[G_i \Rightarrow 1],
\]

which concludes the proof. (The fact that $A_i$ is PPT if $A$ is PPT is obvious.)