Problem Set 7 Solutions

Problem 1. [30 points] Let $G = \langle g \rangle$ be a cyclic group of order $m \geq 2^{2k}$.

1. **[10 points]** Show that the ElGamal scheme over G succumbs to a CCA in which an adversary given the public key and a decryption oracle succeeds in decrypting a target ciphertext (Y, W) without querying (Y, W) to its oracle.

The adversary has input public key $X = g^x$ and ciphertext $(Y, W) \xleftarrow{\$} \mathcal{E}_X(M)$, and has access to a decryption oracle **Dec**. It works as follows:

adversary $A(X, (Y, W))$
$\Delta \xleftarrow{\$} G - \{\mathbf{1}\}$
$W' \leftarrow W\Delta$; $M' \leftarrow \mathbf{Dec}((Y, W'))$
return $M'\Delta^{-1}$

This works because

$$M' = \frac{W'}{Y^x} = \frac{W\Delta}{Y^x} = \frac{W}{Y^x} \cdot \Delta = M\Delta\,.$$

The adversary makes one decryption query and has running time dominated by that of one group operation, so is very efficient. The fact that $\Delta \neq \mathbf{1}$ ensures that $(Y, W') \neq (Y, W)$, meaning the decryption query is allowed.

2. **[20 points]** Here is a modified scheme that attempts to get around this. Let $\mathsf{e}\colon \{0,1\}^{2k} \to G$ be an injective map that encodes a $2k$-bit string as a group element, and let $\mathsf{e}^{-1}\colon G \to \{0,1\}^{2k}$ be its inverse, extended to return 0^{2k} if its input is not in the range of e. Let $H\colon \{0,1\}^k \to \{0,1\}^k$ be a public hash function. Let asymmetric encryption scheme $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be defined via

algorithm $\mathcal{K}$	algorithm $\mathcal{E}_X(M)$	algorithm $\mathcal{D}_x((Y, W))$
$x \xleftarrow{\$} Z_m$	if $M \notin \{0,1\}^k$ then return $\perp$	if $Y \notin G$ OR $W \notin G$ then return $\perp$
$X \leftarrow g^x$	$P \leftarrow \mathsf{e}(M \,\|\, H(M))$	$K \leftarrow Y^x$; $P \leftarrow WK^{-1}$
return (X, x)	$y \xleftarrow{\$} Z_m$; $Y \leftarrow g^y$	$M \,\|\, R \leftarrow \mathsf{e}^{-1}(P)$
	$K \leftarrow X^y$; $W \leftarrow KP$	if $R \neq H(M)$ then return $\perp$
	return (Y, W)	else return M

The notation $M \,\|\, R \leftarrow Z$, where Z is a $2k$-bit string, means M is the first k bits of Z and R is the rest.

An adversary is given a decryption oracle $\mathcal{D}_x((\cdot, \cdot))$, the public key X, and a target ciphertext $(Y, W) \xleftarrow{\$} \mathcal{E}_X(M)$ obtained by encrypting some target message $M \in \{0,1\}^k$. The adversary is

not allowed to query (Y, W) to its oracle and is successful if it outputs M.

Determine whether the scheme is secure. If you say NO, give an adversary that is successful in the above sense. If you say YES, justify your answer assuming H is a random oracle and the DDH problem is hard in G.

NO, the scheme is not secure. The adversary has input public key $X = g^x$ and ciphertext $(Y, W) \xleftarrow{\$} \mathcal{E}_X(M)$, and has access to a decryption oracle **Dec**. It works as follows:

adversary $A(X, (Y, W))$
$Y' \leftarrow gY$; $W' \leftarrow XW$; $M' \leftarrow \mathbf{Dec}((Y', W'))$
return M'

Let $P = \mathsf{e}(M \,\|\, H(M))$. Then

$$\frac{W'}{(Y')^x} \;=\; \frac{XW}{(gY)^x} \;=\; \frac{XW}{g^x Y^x} \;=\; \frac{XW}{XY^x} \;=\; \frac{W}{Y^x} \;=\; P$$

and hence $\mathbf{Dec}((Y', W')) = \mathbf{Dec}((Y, W))$. The adversary makes one decryption query and has running time dominated by that of two group operations, so is very efficient. Clearly $(Y'W') \neq (Y, W)$ so the decryption query is allowed.

In any attack, say how many oracle queries your adversary makes and what is its running time. (The lower these are, the more points you get.)

Problem 2. [30 points] Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an asymmetric encryption scheme whose message space includes $\{0,1\}^k$. Define the KEM $\mathcal{KEM} = (\mathcal{K}, \mathcal{EK}, \mathcal{D})$ with keylength k via

algorithm $\mathcal{EK}$
$K \xleftarrow{\$} \{0,1\}^k$
$C \xleftarrow{\$} \mathcal{E}_{pk}(K)$
return (K, C)

Show that if $\mathcal{AE}$ is IND-CCA secure, then so is $\mathcal{KEM}$. This means you must state a reduction-style theorem and then prove it. The better your bounds, the more points you get.

Theorem: Let A be an ind-cca adversary against $\mathcal{KEM}$. Then there is an ind-cca adversary B against $\mathcal{AE}$ such that

$$\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{KEM}}(A) \;\le\; \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(B)\,.$$

The running time of B is that of A.

The proof begins by considering games G_0, G_1 of Fig. 1, which differ only in their **Enc** procedures. We claim that

$$\mathbf{Adv}^{\text{ind-cca}}_{\mathcal{KEM}}(A) \;=\; \Pr\left[G_0^A \Rightarrow \mathsf{true}\right] \;=\; \Pr\left[G_1^A \Rightarrow \mathsf{true}\right]\,.$$

The first equality is true because G_0 is exactly game $\text{INDCPA}_{\mathcal{KEM}}$. For the second, consider separately the cases $b = 1$ and $b = 0$. In the first case, the **Enc** procedures of the two games are identical. In the second case, they are equivalent, by swapping of the variable names K_0, K_1. Now

Game G_0	Game G_1
procedure Initialize	**procedure Initialize**
$(pk, sk) \xleftarrow{\$} \mathcal{KK}$; $b \xleftarrow{\$} \{0,1\}$	$(pk, sk) \xleftarrow{\$} \mathcal{KK}$; $b \xleftarrow{\$} \{0,1\}$
$S \leftarrow \emptyset$; return pk	$S \leftarrow \emptyset$; return pk
procedure Enc	**procedure Enc**
$K_0 \xleftarrow{\$} \{0,1\}^k$; $K_1 \xleftarrow{\$} \{0,1\}^k$	$K_0 \xleftarrow{\$} \{0,1\}^k$; $K_1 \xleftarrow{\$} \{0,1\}^k$
$C_a \xleftarrow{\$} \mathcal{E}_{pk}(K_1)$	$C_a \xleftarrow{\$} \mathcal{E}_{pk}(K_b)$
$S \leftarrow S \cup \{C_a\}$	$S \leftarrow S \cup \{C_a\}$
return (K_b, C_a)	return (K_1, C_a)
procedure Dec(C_a)	**procedure Dec**(C_a)
if $C_a \in S$ then $K \leftarrow \perp$	if $C_a \in S$ then $K \leftarrow \perp$
else $K \leftarrow \mathcal{DK}_{sk}(C_a)$	else $K \leftarrow \mathcal{DK}_{sk}(C_a)$
return K	return K
procedure Finalize(b')	**procedure Finalize**(b')
return $(b = b')$	return $(b = b')$

Figure 1: Games G_0, G_1 for Problem 2.

adversary $B(pk)$	**subroutine** EncSIM()
$K_0, K_1 \xleftarrow{\$} \{0,1\}^k$	$C_a \xleftarrow{\$} \mathbf{LR}(K_0, K_1)$
$b' \xleftarrow{\$} A^{\text{EncSIM},\mathbf{Dec}}(pk)$	return (K_1, C_a)
return b'	

Figure 2: Adversary B for Problem 2.

we define our adversary B in Fig. 2. It answers A's **Enc** query as shown via its **LR** oracle, and answers A's **Dec** queries directly via its own **Dec** oracle. Then

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(B) \;=\; \Pr\left[G_1^A \Rightarrow \mathsf{true}\right] .$$

This concludes the proof.
