MPRI - Module 2-12-1
Homework 1

1 ElGamal Encryption

The ElGamal public-key encryption scheme is as follows:

$\mathsf{KeyGen}(\mathbb{G}, p)$:	$\mathsf{Enc}(pk, m)$:	$\mathsf{Dec}(sk, C)$:
$g \stackrel{R}{\leftarrow} \mathbb{G}^*$	$r \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$; $C_1 \leftarrow g^r$	parse C as (C_1, C_2)
$x \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$; $X \leftarrow g^x$	$K \leftarrow X^r$	parse sk as x
$sk \leftarrow x$	$C_2 \leftarrow m \cdot K$	$m' \leftarrow C_2 / {C_1}^x$
$pk \leftarrow g, X$	Return (C_1, C_2)	Return m'
Return (pk, sk)		

1. Let $\hat{e} : \mathbb{G} \times \mathbb{G} \mapsto \mathbb{G}_{\mathrm{T}}$ be a symmetric bilinear map from $\mathbb{G} \times \mathbb{G}$ to $\mathbb{G}_{\mathrm{T}}$, where both $\mathbb{G}$ and $\mathbb{G}_{\mathrm{T}}$ are multiplicative groups of prime order p. Show that ElGamal is not IND-CPA-secure.

2. Assume that there exists an algorithm SQ that outputs g^{a^2} when given a pair (g, g^a). Show how to use SQ to break the IND-CPA security of ElGamal.

3. Assume that there exists an algorithm CUB that outputs g^{a^3} when given a pair (g, g^a). Show how to use CUB to break the IND-CPA security of ElGamal.

2 Decision Linear Problem (DLIN)

1. **DLIN.** Let DLIN be the problem of distinguishing the distribution $\{g_1, g_2, g_3, g_1^a, g_2^b, g_3^{a+b}\}$ from the distribution $\{g_1, g_2, g_3, g_1^a, g_2^b, g_3^c\}$, where the values a, b, c are chosen uniformly at random in $\mathbb{Z}_p$ and g_1, g_2, g_3 are three random generators for the group $\mathbb{G}$. Show that if there exists an algorithm $\mathcal{A}$ that breaks the DLIN problem, then one can construct an algorithm $\mathcal{B}$ that breaks the DDH problem.

2. Let $\hat{e} : \mathbb{G} \times \mathbb{G} \mapsto \mathbb{G}_{\mathrm{T}}$ be a symmetric bilinear map from $\mathbb{G} \times \mathbb{G}$ to $\mathbb{G}_{\mathrm{T}}$, where both $\mathbb{G}$ and $\mathbb{G}_{\mathrm{T}}$ are multiplicative groups of prime order p. Is the DLIN problem easy to solve in $\mathbb{G}$?

3. **Linear Encryption.** Similarly to the relation between the ElGamal and DDH problem, there exists a very natural public-key encryption scheme based on the DLIN problem. Please describe a decryption algorithm for this scheme.

$\mathsf{KeyGen}(\mathbb{G}, p)$:	$\mathsf{Enc}(pk, m)$:	$\mathsf{Dec}(sk, C)$:
$g_3 \stackrel{R}{\leftarrow} \mathbb{G}^*$	$a \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$; $C_1 \leftarrow g_1^a$	$\cdots$
$x \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$; $g_1 \leftarrow g_3^x$	$b \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$; $C_2 \leftarrow g_2^b$	$\cdots$
$y \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$; $g_2 \leftarrow g_3^y$	$K \leftarrow g_3^{a+b}$	$\cdots$
$sk \leftarrow (x, y)$	$C_3 \leftarrow m \cdot K$	$\cdots$
$pk \leftarrow (g_1, g_2, g_3)$	Return (C_1, C_2, C_3)	Return m'
Return (pk, sk)		

4. Show that the public-key encryption scheme above is IND-CPA-secure based on the hardness of the DLIN problem in $\mathbb{G}$.

3 Decision k-Linear problem (k-LIN)

1. **k-LIN.** Let k-LIN be the problem of distinguishing the distribution $\{g_1, \ldots, g_k, g_0, g_1^{r_1}, \ldots, g_k^{r_k}, g_0^{\sum_{i=1}^{k} r_i}\}$ from the distribution $\{g_1, \ldots, g_k, g_0, g_1^{r_1}, \ldots, g_k^{r_k}, g_0^{r_0}\}$, where the values $r_0, r_1, \ldots, r_k$ are chosen uniformly at random in $\mathbb{Z}_p$ and $g_0, g_1, \ldots, g_k$ are random generators for the group $\mathbb{G}$. Show that if there exists an algorithm $\mathcal{A}$ that breaks the k-LIN problem, then one can construct an algorithm $\mathcal{B}$ that breaks the $(k-1)$-LIN problem.

2. **Relation to BDDH.** Show that that if there exists an algorithm $\mathcal{A}$ that breaks the BDDH problem, then one can construct an algorithm $\mathcal{B}$ that breaks the 2-LIN problem.

4 IBE security notions

1. Let $\mathsf{IBE} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Enc}, \mathsf{Dec})$ be an identity-based encryption (IBE) scheme . Now let $\overline{\mathsf{IBE}} = (\overline{\mathsf{Setup}}, \overline{\mathsf{KeyDer}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ be an IBE scheme, where $\overline{\mathsf{Setup}} = \mathsf{Setup}$, $\overline{\mathsf{KeyDer}} = \mathsf{KeyDer}$, $\overline{\mathsf{Dec}} = \mathsf{Dec}$, and $\overline{\mathsf{Enc}}$ is defined as follows:

   $\overline{\mathsf{Enc}}(mpk, id, m)$:
   $C_1 \xleftarrow{R} \mathsf{Enc}(mpk, id, m)$
   $C_2 \leftarrow m$
   Return (C_1, C_2)

   Show that if IBE is ANO-ID-CPA, then so is $\overline{\mathsf{IBE}}$ (please refer to the lecture notes for the definition of ANO-ID-CPA).

2. Show that $\overline{\mathsf{IBE}}$ is not IND-ID-CPA. Also explain why this demonstrates that the IND-ID-CPA security of an IBE scheme does not follow from its ANO-ID-CPA security.

3. Provide a counterexample which shows that the ANO-ID-CPA security of an IBE scheme does not follow from its IND-ID-CPA security and explain why.