TD 9: CCA security in PKE and ROM

Exercise 1. [*CPA secure scheme that is not CCA secure*]

We define the LWE-based public key encryption scheme, instantiated to encrypt only 1-bit messages.

Keygen: Let m, n, q, B be some integers such that $m > n$ and $q > 8mB^2$. Let χ be the distribution $\mathcal{U}([-B, B-1] \cap \mathbb{Z})$. Sample $A \leftarrow \mathcal{U}(\mathbb{Z}_q^{m \times n})$ and $pk = (A, b)$ with $b = As + e$.

Enc(pk, m)**:** for any message $m \in G$, sample $t \leftarrow \chi^m$, $f \leftarrow \chi^n$ and $f' \leftarrow \chi$. Output $(c_1, c_2) = (t \cdot A + f, t \cdot b + f' + \lfloor q/2 \rfloor m) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Dec(sk, c)**:** for any $c = (c_1, c_2) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, compute $x = c_2 - c_1 \cdot s$, and take x the representative in $\left[-\frac{q}{2}, \frac{q}{2}\right]$. If $x \in \frac{q}{4}$ output 0, otherwise output 1.

1. Show that the scheme is CPA-secure
2. Show that the scheme is not CCA2-secure.

Exercise 2. [*Cramer-Shoup*]

We consider the following encryption scheme, proposed by Cramer and Shoup (and called "lite Cramer-Shoup") in 1998.

Keygen (1^λ)**:** Choose a cyclic group $\mathbb{G}$ of large prime order $q > 2^\lambda$. Choose generators $g, h \leftarrow U(\mathbb{G})$. Choose $\alpha, \beta, \gamma, \delta \leftarrow U(\mathbb{Z}_q)$ and compute $X = g^\alpha h^\beta$ and $Y = g^\gamma h^\delta$.

Define $PK := (g, h, X, Y)$, $SK := (\alpha, \beta, \gamma, \delta) \in \mathbb{Z}_q^4$.

Encrypt(PK, M)**:** In order to encrypt $M \in \mathbb{G}$, do the following.

1. Choose a random $r \leftarrow U(\mathbb{Z}_q)$ and compute

$$C = (C_0, C_1, C_2, C_3) = (M \cdot X^r,\ g^r,\ h^r,\ Y^r).$$

2. Output $C = (C_0, C_1, C_2, C_3)$.

Decrypt(SK, C)**:** Parse C as $(C_0, C_1, C_2, C_3) \in \mathbb{G}^4$ (and return $\perp$ if C is not in $\mathbb{G}^4$). If $C_3 \neq C_1^\gamma \cdot C_2^\delta$, return $\perp$. Otherwise, output $M = C_0 / (C_1^\alpha \cdot C_2^\beta)$.

1. Show that the scheme is *not* secure in the IND-CCA2 sense.

We now consider the problem of proving that the scheme provides IND-CCA1 security under the DDH assumption in $\mathbb{G}$.

2. Show that, if $(g, h, C_1, C_2) = (g, h, g^r, h^r)$ for some random $r \leftarrow U(\mathbb{Z}_q)$, then

$$(C_0, C_1, C_2, C_3) = (M \cdot C_1^\alpha C_2^\beta,\ C_1,\ C_2,\ C_1^\gamma C_2^\delta)$$

is distributed as a valid ciphertext.

3. Show that, if $(g, h, C_1, C_2) = (g, h, g^r, h^{r'})$ for some random $r \leftarrow U(\mathbb{Z}_q)$, $r' \leftarrow U(\mathbb{Z}_q \backslash \{r\})$then

$$(C_0, C_1, C_2, C_3) = (M \cdot C_1^{\alpha} C_2^{\beta},\ C_1,\ C_2,\ C_1^{\gamma} C_2^{\delta})$$

   for some random $\alpha, \beta, \gamma, \delta \leftarrow U(\mathbb{Z}_q)$, is statistically independent of $M \in \mathbb{G}$, even conditionally on the information that PK reveals about $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}_q^4$.

4. We consider the following variant of DDH.

   DDH' consists in distinguishing between tuples of the form (g^a, g^b, g^{ab}) and $(g^a, g^b, g^{ab'})$ with a, b uniform modulo q and b' uniform in $\mathbb{Z}_q \backslash \{b\}$. Show that the scheme provides IND-CPA security under the DDH' assumption. (**Bonus:** Show that DDH reduces to DDH'.)

5. Show that, with high probability, decryption queries (which all occur before the adversary sees the challenge ciphertext) of the form $C = (C_0, g^r, h^{r'}, C_3)$ (with $r \neq r'$) always receive the response $\perp$. Deduce that the scheme is IND-CCA1-secure

Exercise 3. [*RO does not exist*]

In this exercise we show a scheme that can be proven secure in the random oracle model, but is insecure when the random oracle model is instantiated with SHA-1 (or any fixed hash function). Let Π be a encryption scheme that is secure in the standard model.
Construct a encryption scheme Π_y where signing is carried out as follows: if $H(0) = y$ then output the secret key, if $H(0) \neq y$ then return a encryption computed using Π.

1. Prove that for any value y, the scheme Π_y is secure in the random oracle model.

2. Show that there exists a particular y for which Π_y is insecure when the random oracle model is instantiated with SHA-1.