CS 171: Discussion Section 9 (April 1)

1 Group Operations

Definitions: Let $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$ be the description of a cyclic group for which the discrete log problem is hard. $|\mathbb{G}| = q \approx 2^n$, and $g \in \mathbb{G}$ is a generator of $\mathbb{G}$. Next, let $h \in \mathbb{G}$ be an arbitrary group element, and sample $a, x, y \leftarrow \mathbb{Z}_q$ independently and uniformly.

Question: For each of the following tasks, describe how it can be performed efficiently (in $\mathsf{poly}(n)$ time) or prove that it cannot be performed efficiently.

1. Given x, g, compute g^x.
2. Sample a uniformly random element of $\mathbb{G}$.
3. Given h, compute h^{-1}.
4. Given a, y, g^x, compute $g^{a \cdot x - y}$.
5. Given $a, g^{a \cdot x}$, compute $a \cdot x$.

2 Another PKE Construction from DDH

Consider the following public-key encryption scheme, which is based on El Gamal encryption.

1. $\mathsf{Gen}(1^n)$: Sample $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$ and $x \leftarrow \mathbb{Z}_q$. Then compute $h = g^x$. Next,

$$\begin{aligned} \text{let } \mathsf{pk} &= (\mathbb{G}, q, g, h) \\ \mathsf{sk} &= (\mathbb{G}, q, g, x) \end{aligned}$$

2. $\mathsf{Enc}(\mathsf{pk}, m)$: Let $m \in \{0, 1\}$. First, sample $y \leftarrow \mathbb{Z}_q$. Next:

   (a) If $m = 0$, compute and output the following ciphertext:

   $$c = (c_1, c_2) = (g^y, h^y)$$

   (b) If $m = 1$, then sample $z \leftarrow \mathbb{Z}_q$ and output the following ciphertext:

   $$c = (c_1, c_2) = (g^y, g^z)$$

3. $\mathsf{Dec}(\mathsf{sk}, c)$: TBD

Questions:

1. Fill in the algorithm $\mathsf{Dec}(\mathsf{sk}, c)$ so that the scheme is efficient and correct, up to negligible error.

2. Prove that this encryption scheme is CPA-secure if DDH is hard.