CS 171: Discussion Section 10 (April 8)

1 Which Tasks Become Easy With Bilinear Maps?

Let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a bilinear map for which the *decisional bilinear Diffie-Hellman* (DBDH) problem is hard.

1. For each of the following computational problems, indicate whether the following problems are hard:
   (a) DDH in $\mathbb{G}$
   (b) CDH in $\mathbb{G}$
   (c) DDH in $\mathbb{G}_T$
2. Will the Diffie-Hellman key-exchange protocol be secure if we use group $\mathbb{G}$? How about if we use $\mathbb{G}_T$?

2 Bounded Collusion Identity-Based Encryption

In lecture 18, we used a bilinear map to construct IBE (identity-based encryption). Here, we will use DDH and a random oracle $H : \mathbb{Z}_q \to \mathbb{Z}_q$ to construct a weaker version of IBE that is secure if the attacker only receives a single $\mathsf{sk}_{\mathsf{ID}}$.

A random oracle is a truly random function that all parties have query access to. In this problem, H is sampled uniformly at random from all functions mapping $\mathbb{Z}_q \to \mathbb{Z}_q$. Random oracles are idealized objects, and they don't exist in the real world. In practice, we replace random oracles with sufficiently complex hash functions, such as SHA-256.

Let the IBE scheme $\Pi = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be constructed as follows:

1. $\mathsf{Setup}(1^n)$:
   (a) Sample the parameters of a cyclic group $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$. Let $\mathsf{pp} = (\mathbb{G}, q, g)$.
   (b) Sample $a, b \leftarrow \mathbb{Z}_q$ independently. Compute $h_0 = g^a$ and $h_1 = g^b$.
   (c) Output $\mathsf{mpk} = (\mathsf{pp}, h_0, h_1)$ and $\mathsf{msk} = (\mathsf{pp}, a, b)$.
2. $\mathsf{KeyGen}(\mathsf{msk}, \mathsf{ID})$:
   (a) Let $\mathsf{ID} \in \mathbb{Z}_q$.
   (b) Compute $r = H(\mathsf{ID})$ and $s = r \cdot a + b \mod q$.
   (c) Output $\mathsf{sk}_{\mathsf{ID}} = (\mathsf{ID}, s)$.
3. $\mathsf{Enc}(\mathsf{mpk}, \mathsf{ID}, m)$:
   (a) Let $m \in \mathbb{G}$.
   (b) Compute $r = H(\mathsf{ID})$.
   (c) Sample $y \leftarrow \mathbb{Z}_q$.
   (d) Output $\mathsf{ct} = (g^y, h_0^{y \cdot r} \cdot h_1^y \cdot m)$.
4. $\mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}}, \mathsf{ct})$: TBD

It is implied that all functions can make queries to H.

Questions:

1. Fill in $\mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}}, \mathsf{ct})$, and prove that any valid ciphertext will be decrypted correctly.
2. Show that Π is not a CPA-secure IBE scheme.

It turns out that any adversary that breaks the CPA-security of this IBE scheme needs to make at least 2 queries to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$. This IBE scheme is CPA-secure against any adversary that never makes more than 1 query to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$.