CO 485/685: Assignment #5 Due date: December 1 (Friday)

Some of these exercises are from the textbook. In such cases, the corresponding exercise number from the textbook is provided.

1. (Exercise 6.40.) Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and let ℓ be a prime. Suppose that we are given four points $P, aP, bP, cP \in E(\mathbb{F}_q)[\ell]$. The (elliptic) decision Diffie-Hellman problem is to determine whether cP is equal to abP. Of course, if we could solve the Diffie-Hellman problem itself, then we could compute abP and compare it with cP, but the Diffie-Hellman problem is often difficult to solve.

   Suppose that there exists a distortion map ϕ for $E[\ell]$. Show how to use the modified Weil pairing to solve the elliptic decision Diffie-Hellman problem without actually having to compute abP.

2. (Exercise 6.43.) Let E be the elliptic curve

$$E : y^2 = x^3 + 1$$

   over a field K, and suppose that K contains an element $\beta \neq 1$ satisfying $\beta^3 = 1$. (We say that β is a *primitive cube root of unity.*) Define a map ϕ by

$$\phi(x, y) = (\beta x, y) \quad \text{and} \quad \phi(\mathcal{O}) = \mathcal{O}.$$

   (a) Let $P \in E(K)$. Prove that $\phi(P) \in E(K)$.

   (b) Prove that ϕ respects the addition law on E, i.e., $\phi(P_1+P_2) = \phi(P_1)+\phi(P_2)$ for all $P_1, P_2 \in E(K)$.

3. (Exercise 6.44.) Let $E : y^2 = x^3 + 1$ be the elliptic curve in Exercise 6.43.

   - Let $p \geq 3$ be a prime with $p \equiv 2 \pmod 3$. Prove that $\mathbb{F}_p$ does not contain a primitive cube root of unity, but that $\mathbb{F}_{p^2}$ does contain a primitive cube root of unity.
   - Let $\beta \in \mathbb{F}_{p^2}$ be a primitive cube root of unity and define a map $\phi(x, y) = (\beta x, y)$ as in Exercise 6.43. Suppose that $E(\mathbb{F}_p)$ contains a point P of prime order $\ell \geq 5$. Prove that ϕ is an ℓ-distortion map for P.

4. On page 359 of your textbook, the text suggests to use the following hash function for the Boneh-Franklin ID-based public-key cryptosystem:

   > ...take a given User ID I, convert it to a binary string β, apply a hash function to β that takes values uniformly in $\{1, 2, \ldots, \ell - 1\}$ to get an integer m, and set $H_1(I) = mP$.

   Show that the Boneh-Franklin ID-based public-key cryptosystem is insecure under this hash function, using any reasonable security definition of your choice (and state which such security definition you choose).