Math 480A2, Homework 10

Due November 3, 2022

Homework is graded out of a total of 10 points. Collaboration is permitted, but you must list all coauthors on a problem's solution at the top of the page, and your writing must be your own.

Problem 1. (5 points) Let $G_0 = \mathbb{Z}/83\mathbb{Z}$ be the integers modulo 83, and let G be the prime order cyclic subgroup of G_0 generated by $g = 3$, which has order $p = 41$. Suppose that the following transcripts are produced by Schnorr's protocol over G with public input $h = 33$: $\tau = (37, 18, 22)$, and $\tau' = (37, 29, 23)$.

A. Show that τ and τ' are accepting transcripts for Schnorr's protocol.

B. Using these two transcripts, find a witness w such that $33 = 3^w \pmod{83}$.

Problem 2. (3 points) Recall that a Pedersen commitment in a cyclic group G with prime order p and hard discrete logarithms is defined for a random pair of generators $g, h \in G$ by

$$\textsc{Commit}(m) = g^m h^z$$

where z is chosen randomly in $\{0, \ldots, p-1\}$. Suppose that instead of random generators g and h, you are given generators such that you know a discrete logarithm relation between them, say $h = g^k$ for some $k \in \{0, \ldots, p-1\}$. How can this knowledge be used to break the binding property of the commitment scheme?

Problem 3. (2 points) Pick a topic for your final project, and give a brief (non-binding) summary of several specific aspects of your topic that you might want to explore in your write-up and presentation. Also decide if you would like to work with a partner, and if so, indicate who you will be working with.