ZKP IAP: Session 3 Homework

Brian Justin Stout*

September 13, 2023

Problem 1. *Prove the quadratic non-residue interactive protocol is complete and sound.*

Suppose m, x are positive integers. Assume that $QR(m, x) = 0$, i.e. that x is not a quadratic residue, mod m. Assume the prover is honest. Let $s \in \mathbb{Z}_m$ and b be arbitrary. If $b = 0$, then $y = s^2x$. In this case y is also not a quadratic residue mod m (if it were, then x would be too), so Prover sends back 0, which matches b.

If $b = 1$, then Verifier sends $y = s^2$. This is a quadratic residue, so $QR(y, m) = 1$ and Prover sends back 1, matching b. The protocol is complete.

To show soundness, Verifier selects b as 0 or 1 with probability of $\frac{1}{2}$ each. Lets say that Prover responsds with 0 with probability p and 1 with probability $1-p$. Then the probability verifier rejects is $\frac{1}{2}p + \frac{1}{2}(1-p) = \frac{1}{2}$.

Problem 2. *Prove the quadratic residue interactive protocol is complete, sound, knowledge sound, and zero knowledge.*

The proof of soundness and completeness are identical to the previous problem.

To prove knowledge soundness, assume that the Verifier could query both $b = 0$ and $b = 1$ at the same time. In this case, Verifier receives both t and st. He recovers $s = t * t^{-1}$, so Prover does indeed know s.

To prove zero knowledge we argue as follows. Half of integers modulo m are quadratic resiudes. Verifier learns the following during his interaction with Prover: $y = xt^2$. Because t^2 is a quadratic resiude, the map $y \mapsto yt^2$ is a permutation of the set of resides and non-residues, respectively. Verifier then learns either $(0, t)$ or $(1, st)$ with probabilities of $\frac{1}{2}$ and $\frac{1}{2}$. So with probability $\frac{1}{2}$ Verifier knows $x, m, xt^2, 0, t$ and with probability $\frac{1}{2}$ Verifier knows $x, m, xt^2, 1, st$. The distribution of these elements is identical.

Problem 3. *Suppose a group G has an efficiently computable nondegenerate bilinear self pairing. Give an efficient algorithm for deciding given $\alpha G, \beta G, H \in \mathbb{G}$ whether $\alpha\beta G = H$.*

Let e be the pairing. Check $e(\alpha G, \beta G) = e(H, G)$

*email: bjstout@proton.me

Problem 4. *Check the BLS signature scheme accepts a correctly signed signaure. Argue it is computationally infeasible to to find a forged signature of any message m if the forger is given pk but not sk. What are come computational hardness assumptions?*

Assume σ is a a correct signature for a message m. Then

$$e(g_0, \sigma) = e(g_0, \alpha H(m)) = e(\alpha g_0, H(m)) = e(pk, H(m))$$

This requires the DDH assumption for the pairing and groups. It also requires a secure hash function. For any message m to create a forged signature requires solving the discrete log problem for $\mathbb{G}_0$, which is assumed hard.