1 Zero-knowledge and discrete logarithm

Fix a group $G$ of prime order $q$ with generator $g$. ($G$, $q$, and $g$ may depend on some implicit security parameter but are considered publicly known.) Let $R := \{(x, w): g^w = x, w \in \{0, \ldots, q-1\}\}$.

Consider the following proof system for $R$ (Schnorr’s proof system for discrete logarithms):

- The prover $P$ gets input $(x, w) \in R$.
- The verifier $V$ gets input $x \in R$.
- The prover $P$ chooses $b \overset{\$}{\leftarrow} \{0, \ldots, q-1\}$ and sends $a := g^b$ to the verifier $V$.
- The verifier chooses $r \overset{\$}{\leftarrow} \{0, \ldots, q-1\}$ and sends $r$ to the prover $P$.
- The prover $P$ computes $s := b + rw \mod q$ and sends $s$ to the verifier $V$.
- The verifier $V$ checks whether $x, a \in G$ and $g^s = ax^r$.

This proof system is well-known to be a proof system. However, in the classical setting, it is unknown whether this proof system is zero-knowledge!

(a) Knowlets: ProofSys

ProblemID: ZKDisLogSound

Time: 

Difficulty:

Show that $(P, V)$ is a proof system with soundness-error $1/q$.

(b) Knowlets: QZK, DlogAlgo

ProblemID: ZKDisLogShor

Time: 

Difficulty:

Show that $(P, V)$ is statistical quantum zero-knowledge.

Hint: This has nothing to do with rewinding! It has a lot to do with Shor’s algorithm. Think of what information the simulator is missing for making everything easy, and how to get it.

---

1 It is however “honest-verifier zero-knowledge”. This is a weaker notion where the verifier is considered to behave honestly.