Homework 4

1. (5 + 15 points) Let $L = \mathbb{QR}_n$ and consider the 3-round ZK protocol taught in the class to prove that $x \in L$. We had seen that this protocol has completeness 1 and soundness 1/2.

   (a) Formally write the protocol that sequentially runs this protocol t-times.

   (b) This new protocol has completeness 1 and soundness $1/2^t$. Prove that this protocol is also ZK.

2. (5 + 15 points) In this question we shall define *witness indistinguishable proofs*, referred to as WI proofs, and their relation to ZK proofs.

   (a) Consider a language $L \in \mathsf{NP}$. Let R_L be the set of all (x, w) such that w is a witness for $x \in L$.

   A WI proof is a proof system with the following intuitive property. Consider $x \in L$ and any two distinct witnesses w and w' such that $(x, w) \in R_L$ and $(x, w') \in R_L$. The distribution of the transcripts produced by the interaction between an honest prover and any arbitrary efficient verifier when the prover uses the witness w is computationally indistinguishable from the case when the prover uses the witness w'. Formalize this intuition to define witness indistinguishable proofs.

   (b) Prove that every ZK proof is also a WI proof.