Exercise 3 – Foundations of Cryptography 89-856

Due Date: May 12, 2019

April 28, 2019

Exercise 1: Prove that if there exists an interactive proof for some language L with soundness error $1/3$ (and perfect completeness), then there exists an interactive proof for L with soundness error 2^{-n}. (Hint: Consider many sequential executions of the interactive proof and note that this is not exactly the same as error reduction for RP algorithms.)

Exercise 2: Prove that the existence of non-interactive perfectly-binding bit commitments implies the existence of one-way functions.

Exercise 3: Prove the following statements about zero-knowledge:

1. Every language $L \in \mathcal{BPP}$ has a zero-knowledge proof.

2. If a language L has a zero-knowledge proof with a deterministic verifier, then $L \in \mathcal{BPP}$.

3. If a language L has a non-interactive zero-knowledge proof (where the prover sends a message to the verifier and that is all), then $L \in \mathcal{BPP}$.

Exercise 4: Formulate a definition of perfect binding for string commitment. In addition, prove that the hiding for bit commitment implies hiding for string commitment, as defined in class. (Hint: use a hybrid argument to prove that the first definition implies the second.)

Exercise 5: Provide a proof sketch that the protocol below constitutes a zero-knowledge proof system for the language of directed graphs containing Hamiltonian cycles (HC). In particular, describe the simulator and sketch the analysis. Prove the soundness error of the proof system.

Protocol 1 (proof system for HC):

- **Common Input:** *a directed graph $G = (V, E)$ with $n \overset{\text{def}}{=} |V|$.*
- **Auxiliary Input to Prover:** *a directed Hamiltonian Cycle, $C \subset E$, in G.*
- **The protocol:**
    1. Prover's first step (P1): *The prover selects a random permutation π over the vertices V, and commits (using a perfectly-binding commitment scheme) to the entries of the adjacency matrix of the resulting permuted graph. That is, it sends an n-by-n matrix where the $(\pi(i), \pi(j))^{\text{th}}$ entry is a commitment to 1 if $(i, j) \in E$, and is a commitment to 0 otherwise.*
    2. Verifier's first step (V1): *The verifier uniformly selects $\sigma \in \{0, 1\}$ and sends it to the prover.*

3. Prover's second step (P2):

   (a) *If $\sigma = 0$, the prover sends π to the verifier and decommits to all of the commitments in the adjacency matrix.*

   (b) *If $\sigma = 1$, the prover decommits to the commitments of entries $(\pi(i), \pi(j))$ for which $(i, j) \in C$ (and only to these commitments).*

4. Verifier's second step (V2):

   (a) *If $\sigma = 0$, the verifier checks that the revealed graph is isomorphic to G via π.*

   (b) *If $\sigma = 1$, the verifier checks that all revealed values are 1 and that the corresponding entries form a simple n-cycle.*

   In both cases the verifier checks that the decommitments are proper (i.e., that they fits the corresponding commitments). The verifier accepts if and only if the corresponding condition holds.