# Privacy Engineering (70018)

## Zero-Knowledge Proofs

**Problem 1.** *Sequential Composition.* Consider an arbitrary interactive proving system $\pi = (p, v)$. Let $\Pi_N = (P_N, V_N)$ be an interactive proving system in which $\pi$ is executed $N$ independent times in sequence such that $V_N$ accepts iff $v$ accepts when invoked on the same common input in all $N$ runs, and $P_N$ invokes $p$ on the same common input in all $N$ runs.

- If the completeness and soundness errors of $\pi$ are the constants $c$ and $s$ respectively, what are the completeness and soundness errors, $C_N$ and $S_N$ respectively, of $\Pi_N$?
- If $p$ achieves perfect zero-knowledge, what level, if any, of zero-knowledge does $P_N$ achieve for all $N$?
- If $v$ has a knowledge error equal to the constant $k$, what is the knowledge error, $K_N$, of $V_N$?
- If $s = \frac{1}{2}$, what is the minimum value of $N$ required for $S_N$ to be strictly less than $10^{-40}$?

**Problem 2.** *Non-interactive Arguments.* Assume that $\pi = (p, v)$ is the proving system for graph isomorphism knowledge defined in section 3.2 on page 11 of the lecture slides.

- What is the expected number of attempts for a cheating prover without knowledge of $\phi$ to construct a valid argument in $\pi$?
- Let $\Pi_N = (P_N, V_N)$ be the sequentially composed version of $N$ invocations to $\pi$ as done in Problem 1. Specify $\Pi_N$ in a pseudo-code style similar to that of $\pi$.
- Using $\Pi_N$ as a basis, specify a non-interactive argument version of it $\bar{\Pi}_N = (\bar{P}_N, \bar{V}_N)$ in pseudo-code. Make sure $\bar{\Pi}_N$ achieves the same soundness, completeness and knowledge error values as $\Pi_N$ for all values of $N \leq 256$.
- What is the expected number of attempts, in terms of $N$, for a cheating prover without knowledge of $\phi$ to construct a valid argument in $\bar{\Pi}_N$?
- Does $\bar{P}_N$ reveal *any* knowledge?