# 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 $\Pi_N$?

  $C_N = c^N$

  $S_N = s^N$

- If $p$ achieves perfect zero-knowledge, what level, if any, of zero-knowledge does $P_N$ achieve for all $N$?

  Perfect zero-knowledge.

- If $v$ has a knowledge error equal to the constant $k$, what is the knowledge error, $K_N$, of $V_N$?

  $K_N = k^N$

- If $s = \frac{1}{2}$, what is the minimum value of $N$ required for $S_N$ to be strictly less than $10^{-40}$?

  $N = 133$

**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 $\pi$?

  2

- 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 $\pi$.

  Repeat N times or until first failure:

  $P \rightarrow V : H = \psi(G_2)$

  $V \rightarrow P : c \in \{1, 2\}$

  $P \rightarrow V : \omega = \psi \circ \phi \text{ if } c = 1 \text{ else } \omega = \psi$

  $V \rightarrow P : \text{ pass if } \omega(G_c) = H \text{ else fail}$

  End repeat.

- 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 $N \leq 256$.

  $P : H_n \leftarrow \psi_n(G_2) \forall n \in \mathbb{Z}_N$

  $P : c_n \leftarrow R(n, G_1, G_2, H_0, ..., H_{N-1}) \forall n \in \mathbb{Z}_N$

  $P : \omega_n \leftarrow \psi_n \circ \phi \text{ if } c_n = 1 \text{ else } \psi_n \forall n \in \mathbb{Z}_N$

  $P \rightarrow V : H_0, ..., H_{N-1}, \omega_0, ..., \omega_{N-1}$

- 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 $\bar{\Pi}_N$?

  $2^N$

- Does $\bar{P}_N$ reveal *any* knowledge?

  Arguably the argument itself.