NYU COMPUTER SCIENCE FALL 2026

Introduction to Cryptography

CSCI-GA.3210-001 Instructor: Nir Bitansky

Problem Set 5

Due: Wednesday, December 2, 2026, at 11:59 p.m.

Instructions:

- Turn in your solutions in LaTeX and submit a PDF through Gradescope.
(You don't have to know latex, can use AI tools like Prism.)
- Solutions will be graded for both correctness and clarity. If you do not know how to solve a question, you may write "I don't know how to do this" to receive 15% credit for that question.
- Discussion with peers is strongly encouraged, but you must write up your solutions on your own and list your discussion partners. Cite any external sources you use.
- AI use is permitted. If you use AI to solve the homework, list the exact model as a collaborator and include your prompts in an appendix. We strongly recommend solving the questions yourself: the final exam will mostly contain variants of homework questions.
- Use the course forum for clarification questions, but do not post solutions there.

1. In this question, we'll construct a two-message bit commitment scheme based on PRGs. Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a length-tripling PRG. Consider the following protocol between a sender S and a receiver R:

   - R samples a random string $r \leftarrow \{0,1\}^{3n}$ and sends it to S.
   - S samples $s \leftarrow \{0,1\}^n$, and commits to a bit b, by sending $Com_r(b;s)$ defined by:
     - $G(s)$ if $b = 0$,
     - $G(s) \oplus r$ if $b = 1$.

   Show that the commitment is:

   - (15 pts) **Binding:** with overwhelming probability over the choice of r, the commitment is binding:

   $$\Pr_{r \leftarrow \{0,1\}^{3n}} [\exists s_0, s_1 : Com_r(0;s_0) = Com_r(1;s_1)] \leq 2^{-n} \ .$$

   - (15 pts) **Hiding:** for every (even malicious) choice of r, the sender's message is computationally-hiding:

   $$\{Com_r(0;U_n)\}_{\substack{n\in\mathbb{N} \\ r\in\{0,1\}^{3n}}} \approx_c \{Com_r(1;U_n)\}_{\substack{n\in\mathbb{N} \\ r\in\{0,1\}^{3n}}} \ .$$

2. (30 pts) Consider the NP language of solvable Soduko puzzles. That is, all $n^2 \times n^2$ matrices over values $\{\perp\} \cup [n^2]$ for which the values $\perp$ can be replaced with values in $[n^2]$, so that every line , column, or $n \times n$ subsquare contain the values $[n^2]$. (By subsquare here we mean the entries corresponding to the intersection of rows $i \cdot n + 1, \ldots, i \cdot n + n$ with columns $in + 1, \ldots, in + n$ for some $i, j \in \{0, \ldots, n-1\}$.)

   Describe a zero-knowledge proof for this language, based on non-interactive commitments, with perfect completeness, soundness error $s \leq 1 - n^{-O(1)}$, and expected poly-time simulator. Re zero-knowledge, you can describe the simulator, without writing the proof of its validity and run-time.

3. A proof system (P, V) for a language L is *zero knowledge with a universal simulator* if there is one simulator that can simulate the interaction with any given verifier. That is, there exists a PPT simulator S such that for every poly-size V^*:

$$\left\{\langle P, V^* \rangle(x)\right\}_{x \in L} \approx_c \left\{S([V^*], x)\right\}_{x \in L},$$

   where $[V^*]$ is a description of the circuit V^* as a string.

   (a) Prove that if L has a zero knowledge proof with a universal simulator in one message (from prover to verifier) then $L \in \text{BPP}$.

   (b) Prove that if L has a zero knowledge proof with a universal simulator in two messages (first from verifier to prover and second from prover to verifier) then $L \in \text{BPP}$.

   (c) Prove that if L has a zero knowledge proof with a universal simulator where the honest prover is deterministic (in any number of messages) then $L \in \text{BPP}$.

4. Show that any two-message $(1, 2)$-OT (that is semi-honestly secure) implies public-key encryption.