Theoretical Foundations of Cryptography **Instructor: Chris Peikert**
Georgia Tech, Spring 2011 **Student: YOUR NAME HERE**

Homework 5

This homework is due by the **start of class on April 14** via the course page on T-Square. Start early!

Instructions. Solutions must be typeset in LaTeX (a template for this homework is available on the course web page). Your work will be graded on *correctness*, *clarity*, and *conciseness*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea.

You may collaborate with others on this problem set and consult external sources. However, you must ***write your own solutions*** and ***list your collaborators/sources*** for each problem.

1. *(Interactive proofs and zero-knowledge.)*

   (a) (5 points) *(Soundness error is necessary.)* Suppose that a language L has an interactive proof system (P, V) with *perfect* soundness, i.e., V never accepts an $x \notin L$ (no matter what P^* does). Prove that L must be in NP. That is, prove that there is a *deterministic* algorithm W, running in time polynomial in the length of its first argument x, such that $x \in L$ if and only if there exists some "witness" $w \in \{0,1\}^*$ making $W(x, w)$ accept. (*Hint*: consider a witness consisting of V's entire view.)

   In other words, to prove a language that lies outside NP, we must live with some chance of accepting a "false theorem."

   (b) (15 points) An undirected graph G is said to have a *Hamiltonian cycle* if it contains a cycle that passes through every vertex exactly once. (That is, the graph has a "closed loop.") The Hamiltonian Cycle Problem HCP is the language of all graphs G having a Hamiltonian cycle, and is known to be NP-complete.

   Consider the following sketch of an interactive proof (P, V) for HCP: on a graph $G = (V, E)$ having a Hamiltonian cycle, the prover first chooses a random permutation G' of G. For each pair of vertices $(i, j) \in V \times V$, the prover sends a (perfectly binding, computationally hiding) commitment to the bit $e'_{i,j}$, which is 1 if (i, j) is an edge in G', and is 0 otherwise. The verifier replies with a uniformly random challenge bit $b \leftarrow \{0, 1\}$. The prover answers the challenge, and the verifier checks the answer.

   Complete the description of the protocol: describe how P answers V's challenge in both cases ($b = 0$ and $b = 1$), and how V checks P's answer. Then prove that the protocol is complete and has soundness error $1/2$. (Why is this an advantage over the interactive proof for 3-colorability that we saw in class?) Finally, describe a (black-box) simulator and sketch a proof that the protocol is zero-knowledge.

2. (10 points) *(Final project status report.)* Write a short summary (of at most a couple of paragraphs) of your progress so far on your final project: what specific topic/problem you are investigating, your findings so far, any obstacles that you have encountered or foresee, etc. (The more you have accomplished on your project, the better your report will be!)