Handout 7: Zero Knowledge

Boaz Barak

Total of 110 points.
Exercises due November 15th, 2005 1:30pm.

Exercise 1 (Interaction is necessary, 15 points)**.** Let L be a language that is not decidable by polynomial-sized circuits. Show that there is no *non-interactive* zero knowledge proof system for L. That is, show that if a language L has a proof system that consists of a single message from the prover to the verifier then L is decidable by polynomial-sized circuits.

Exercise 2 (Randomness is necessary, 15 points)**.** Let L be a language that is not decidable by polynomial-sized circuits. Show that there is no *deterministic* zero knowledge proof system for L. That is, show that if a language L has a proof system where the verifier is deterministic then L is decidable by polynomial-sized circuits.

Exercise 3 (80 points)**.** Consider the following more sophisticated identification problem: we want to have a box that decides whether or not to allow people inside a building but every person may be authorized to enter the building at *different times*.

Design and prove security for an identification protocol with the following properties: (If you design a correct protocol but can't or don't have time to prove everything, you will still get partial credit)

- Assume that each person is authorized for a particular range of hours every day. That is, the range of each person is two numbers $t_1 \leq t_2$ between 0 and 24. For simplicity assume that every one has access to perfectly synchronized clocks.
- There is some central trusted algorithm that provides each person with some secret data corresponding to her authorized range. She can use this secret data when interacting with the box. This algorithm also provides the public information for the box.
- The box contains only a clock and some public information. The box does *not* contain the list of authorized people and their authorized time periods.
- Even if a cheating box interacts with a person authorized to enter at a particular time, it should not learn anything about her secret information. It should not even learn anything about the range of that person (other than that this range contains that particular time).
- A person that has authorization for a particular time period can not (with non-negligible probability) convince an honest box to allow her to enter in another time period. This holds even if that person is given the contents of data in the box and even in previous days managed to install a cheating box that interacted with other people that are authorized for that period.

See footnote for hint[1]

Clarification: You should try to design your system to achieve all the above security goals. However, to keep things simple when *proving security*, consider only the following simplified attack scenario: we have Alice a user that is authorized to enter the building at all hours (e.g., range 0 to 23) and Bob a user that is authorized to enter the building only at specified times (say between 1 and 2). We think of the following attack: Bob gets all the information contents of the valid box. Then he has Alice interact once with a fake box of its own design. Then, he needs to interact with the real box and convince it to let him in at a time that is not in his range. We say the system is secure of the probability of Bob's success is at most $1/n^{\omega(1)}$.

[1] **Hint:** For starters you might want to think how you would do that if you could put secret information in the box, but did not want to store there the long list of all people and their time ranges. Use the following components: zero-knowledge proofs for NP, commitment schemes, message authentication codes. Note that if you have some secret information, you can make a commitment to that secret public.