Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 13
October 16, 1997

Problem Set 6

This problem set is due on *Thursday, October 25, 1997* at the end of class. Late homeworks will *not* be accepted.

Mark the top of each sheet with your name, 6.857, the problem set number, and the date. Type up your solutions, and be clear. Points may be deducted if your TA has problems understanding your solution.

If you collaborate with other students, you MUST write up solutions on your own and acknowledge the people you work with.

Problem 6-1. ZK proof of Satisfying Assignment

In class we proved that a Prover can demonstrate in zero-knowledge to a Verifier that the Prover knows a satisfying assignment for a boolean circuit f. That is, he knows a vector $x = x_1 x_2 \ldots x_n$ which, when given as input to the ciruit f, causes the circuit f to output 1 (true). The technique used by the prover relied upon *blobs* (commitments with equality testing), such as provided by Chaum-van Heijst-Pfitzmann commitments.

Now show that the same result can be obtained by using ordinary commitments instead of *blobs*. That is, demonstrate the same result using a commitment scheme that does not provide for equality testing.

You may prove this in any manner you like. But here is a hint that you may consider using.

Hint: The Prover commits, for each wire, a "wire coding type" for that wire. The wire coding type is either AB (that is, 0 is coded as A, and 1 as B) or BA (the reverse). These coding types are chosen independently for each wire. He also commits to a coded value (either A or B) for each wire. Finally, he commits to a coded truth table for each gate, where the rows are coded using A's and B's. Given this idea, explain how the Prover convinces the Verifier that he knows a satisfying assignment. Iterate portions of the above as necessary in various rounds.

Make your protocol zero-knowledge: be careful not to leak **any** information about the true values on each wire to the Verifier! (Proofs not necessary, although you should sketch the reasoning behind your construction.) Be sure to explain carefully what your protocol is, including the checks made by the Verifier.

Problem 6-2. User identification

Paranoid Corp is considering the following as a new user identification system for its computer system. Please write a short evaluation of this system, discussing its pros and cons, especially potential weaknesses. Paranoid Corp has about 5000 employees. The company

likes the fact that this system requires no passwords or hand-held devices that must be kept secure.

Each user has a PC on his desk, with a TV camera on top. The PC's are all connected by a corporate network. When the user initially registers to use the system, he must name a number (up to twelve) other users who have already registered with the system as his "checkers". He can add more "checkers" to his list at any time, by running a software program after he has logged in.

When the user logs in (by giving his name, but no password), the system automatically checks to see if any of his "checkers" are already logged in. (If not, the user can't log in unless he is the system administrator.) If so, then the system automatically intitiates a video linkup between the user and (a randomly chosen) one of his on-line checkers. They can exchange pleasantries or whatever, until the checker is satisfied that the user is who he claims to be. The checker indicates that the user is OK, and then the system allows the user to log in, and the video link is terminated. An audit record is made of the login, including who the user and the checker were.