600.105 M&Ms October 30, 2009

Cryptography Homework

Instructor: Joanne Selinski *Speaker: Susan Hohenberger*

This assignment is due by the start of class on November 6, 2009. It should be completed on your own. If you use any reference materials, you **must** provide proper citations.

Recall that a *proof system* is a two-party protocol between a prover P and a verifier V with the following two properties, which we'll define informally:

1. *Correctness:* If the claim is true, then the honest prover P can convince the honest verifier V to accept with probability 1.
2. *Soundness:* If the claim is false, then when interacting with *any* malicious prover P^*, the honest verifier V will reject with probability $\geq 1/2$. (Recall that we can then repeated the protocol k times to reduce the soundness error to $1/2^k$.)

A *zero-knowledge proof system* has the two properties above, plus the property that the verifier "does not learn anything but the fact that the claim is true".

This is typically realized by the having the prover and verifier play a game. In class, we saw games that enable a zero-knowledge proof for:

1. proving that you can color an undirected graph with three colors,
2. proving that you can find Waldo in a picture,
3. proving that you can solve a Sudoku puzzle.

We learned the amazing fact that: *anything that can be proven can be proven in zero-knowledge*!" We discussed how zero-knowledge proofs are very important in modern cryptography, and enable many new applications such as:

1. proving that you are over 21 without revealing your birthdate,
2. proving that you are allowed access to a file, without revealing which access control criteria you satisfy,
3. proving that your public key is the product of two large primes.

Your assignment: In at most two pages (one page is optimal), complete *one* of the following assignments:

1. Think of something you would like to prove to someone else in zero-knowledge. Then describe a game that allows you to do this.
2. Describe a new application of zero-knowledge proofs. Be specific. Where could this technology be useful?

You will be judged on your creativity.