Theoretical Cryptography

Homework Set No. 1

Date Due: January 9th 2011

1. Construction of one-time signature schemes: let $f : \{0,1\}^n \mapsto \{0,1\}^n$ be a one-way function. We saw a one-time signature schemes based on one-way function where to sign m bits the public key size was $2nm$ bits. Suggest a tradeoff with more evaluations but fewer bits in the public key. Hint: you may assume that f is one-way on its iterates.

2. Show how to construct from a signature scheme that is existentially unforgeable against random message attack a signature scheme that is existentially unforgeable against adaptively chosen message attacks
Hint: use two schemes of the first type

3. Assume one-way functions exist.

1. Show that for any fixed function $h : \{0,1\}^* \mapsto \{0,1\}$ there is a one-way function $f : \{0,1\}^* \mapsto \{0,1\}^*$ such that h is not a hardcore predicate of f.

2. Show a one-way function f such that given $y = f(x)$ each input bit of x can be guessed with probability at least $3/4$.

3. Suppose that the function g maps a given a seed into a sequence of blocks. Let $\ell(n)$ be the number of blocks a given a seed of length n is mapped to ($\ell(n) > n$). If the input (seed) is random, then the output *passes the next-block unpredicatability* test: For any prefix $0 < i < \ell(n)$, for any probabilistic polynomial time adversary A that receives the first i blocks of $y = g(x)$ and tries to guess the next block y_{i+1}, for any polynomial $p(n)$ and sufficiently large n

$$|\Pr[A(y_1, y_2, \ldots, y_i) = y_{i+1}]| < 1/p(n)$$

Show how to convert a next-block unpredictable generator into a pseudo-random generator.

4. A function $S : \{0,1\}^* \times \{0,1\}^* \mapsto \{0,1\}^*$ is called a *pseudo-random synthesizer* if (i) it is polynomial time computable and (ii) For any m polynomial in n, if $\langle x_1, \ldots, x_m \rangle$ and $\langle y_1, \ldots, y_m \rangle$ are chosen uniformly at random from $\{0,1\}^n$, then the output of S on all the combinations of these assignments, $(S(x_i, y_j))_{i,j=1}^m$, is indistinguishable from a random $m \times m$ matrix with entries of size $|S(x_i, y_j)|$ to a polynomial-time observer.

1. Show how to construct a synthesizer from the Diffie-Hellman assumption.

2. Show how to construct a synthesizer from trapdoor permutations.