Foundations of Cryptography

Homework Set No. 3

Date Due: Dec 20th 2006

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 that if family of UOWHFs exist, then there are family of UOWHFs which are *not* collision intractable.

3. Show that if the $(n, \beta \cdot n)$-subset sum assumption holds for $\beta < 1$, then the corresponding subset function defines a family of UOWHFs

You may use the fact that for $m = beta \cdot n$ for most $a_1, a_2, \ldots a_n \in \{0,1\}^m$ the distribution of $T = \sum_{i \in S} a_i$ is close to uniform, when S is random.

You may consult Russell Impagliazzo and Moni Naor, Efficient Cryptographic Schemes Provably as Secure as Subset Sum, J. of Cryptology 9(4), 1996.

4. 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

5. Assume one-way functions exist.

   1. Show that the last bit/first bit are not necessarily hardcore predicates.

   2. Generalization: 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.

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