Foundations of Cryptography

Homework Set No. 5

Date Due: Dec 18th 2003

1. Prove the following regarding the one-time n-bit signature scheme seen in class:

Theorem 1 *If there is an Adversary $\mathcal{A}$ that with probability at least ε succeeds in the following*

- *chooses a message $m \in 0, 1^n$ for Alice to legitimately authenticate and*
- *forges a message $m' \neq m$, i.e. Alice accepts a message $m' \neq m$.*

Then there is an Adversary $\mathcal{B}$ that

- *can invert the function f with probability at least $\varepsilon/2n$ (where is over choice of image and internal coin flips of $\mathcal{B}$)*
- *operates in time roughly the same as $\mathcal{A}$*

2. Show that the existence of UOWHFs implies the existence of one-way functions

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

4. 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.