COS 496: Cryptography	Due: Nov 15

Problem Set 4

Professor Amit Sahai

Please list everyone you collaborated with when solving the problems on this problem set. If you make use of outside material, make a note of that as well. Make sure you write up your solutions on your own.

Problem 1. Show that the existence of trapdoor functions implies the existence of one-way functions.

Problem 2. Recall our simplest construction of universal one-way hash functions: Given a one-way permutation $f_k : \{0,1\}^k \to \{0,1\}^k$ and a family $G_k : \{0,1\}^k \to \{0,1\}^{k-1}$ of universal hash functions, let g be a random element of G_k. We defined $h(x) = g(f_k(x))$.

1. Suppose we define $h'(x) = f_{k-1}(g(x))$. Is this a UOWHF?
2. How about $f_{k-1}(g(f_k(x)))$?

Problem 3. In class we developed a one-time digital signature scheme with the concept of "message windows." Given a one-way function f and a secret key $(x_1^0, \ldots, x_k^0, x_1^1, \ldots, x_k^1)$, the public key is $(f(x_1^0), \ldots, f(x_k^0), f(x_1^1), \ldots, f(x_k^1))$. To sign a message, the preimage $x_i^{m_i}$ to revealed for each bit m_i of the message.

Now consider an efficiently computable *subset selection function* σ which maps each message m to a distinct *arbitrary subset* of preimages. Furthermore, for any x, y $x \neq y$, both $\sigma(x) - \sigma(y)$ and $\sigma(y) - \sigma(x)$ are nonempty sets.

1. Prove that this function can be similarly used to produce a one-time secure digital signature scheme.
2. Now generalize this construction to produce a signature scheme that is secure for l signed messages rather than just one, where l is polynomially related to the security parameter k. **Hint:** Give an explicit signing algorithm with the needed properties. Think about the fact that different polynomials of degree d over a finite field can agree in at most d places. (If you're still confused, see the TA.)
3. Modify the many-message, UOWHF-based, linked-list based digital signature scheme given in class to use one window for both the message and the key. Give a proof of the security of this system.

Problem 4. We consider a new cryptographic operation known as *secret sharing*. The idea is to divide a secret key into pieces called "shares" and distribute them among n participants. A *k-out-of-n* secret sharing scheme is such that any k of the shares can be put together to recover the secret, but for any $k-1$ shares no information can be obtained about the secret.

Construct a k-out-of-n secret sharing scheme to hide an arbitrary bit b. Any k shares must uniquely determine b, but given only $k-1$ shares, $\Pr[b = 0] = \Pr[b = 1]$. Assume that the person who generates the shares is always honest. **Hint:** Think again about bounded-degree polynomials over finite fields.

PS4 Brought to you by Jason Perry