15-859(I) Theoretical Foundations of Cryptography

Homework 6 **due: April 21, 2003**

Ground Rules. You may speak with other students about these problems, and you may use any source you can find, but you must reference any source you use in your write-up. Please hand in a computer-generated hard copy of your solutions at the beginning of class on the due date.

1. **Non-malleable encryption and signatures** One natural question to ask regarding non-malleability of public-key encryption is whether digital signatures can be combined with semantically secure encryption in a way similar to the results of [BN00]. We will consider two composition models:

   (a) *Encrypt and Sign*: To encrypt message m, output $E(m), S(m)$. Show that if E is malleable with respect to the identity relation, then E&S is also malleable wrt $=$.

   (b) *Sign-then-Encrypt*: To encrypt message m, output $E(m||S(m))$. Show that if there exists any semantically secure PKC (G, E, D) there is a semantically secure PKC (G', E', D') and a EUF-CMA secure signature scheme S so that StE with E' and S is malleable with respect to the identity relation.

2. **Efficient CCA2-secure PKC in the RO model** Bellare and Rogaway [BR93] show that if $G : \{0,1\}^k \rightarrow \{0,1\}^*$ and $H : \{0,1\}^* \rightarrow \{0,1\}^k$ are random oracles and $f : \{0,1\}^k \rightarrow \{0,1\}^k$ is a trapdoor OWP, then the PKC given by $E(f, x; r) = f(r)||G(r) \oplus x||H(rx)$ is a IND-CCA2 secure PKC. We will play with this idea a bit more.

   (a) Show that if E_S is any IND-CCA2-secure symmetric key encryption scheme, then $E(f, x; r) = f(r)||E_S(H(r), x)$ is an IND-CCA2 secure PKC.

   (b) Let E_P denote the encryption function for any semantically secure PKC, and let E_S denote the encryption function for an IND-CCA2 secure symmetric encryption scheme. Let $H : \{0,1\}^* \rightarrow \{0,1\}^k$ be a random oracle. Show how to extend the idea in the previous question to use $E_P(r)$ in place of $f(r)$. (Note that in this case, E_P may be malleable wrt identity, so the previous construction does not prevent malleability wrt identity of the resulting cryptosystem)

3. **Random Oracles are Cheating for Symmetric Crypto** In these exercises, we will consider adversaries which are *computationally unbounded* Oracle turing machines but that make only a polynomial number of oracle queries. Call a machine a $q(n)$-COTM if it is an (probabilistic) oracle TM which queries its oracle at most $q(n)$ times on inputs of size n. We will see that making the random oracle assumption on a hash function is "cheating" for symmetric primitives because it gives all of symmetric crypto for free:

   (a) Let $R : \{0,1\}^k \rightarrow \{0,1\}^k$ be a random oracle. Show that the function $G(r) : R(r)||R(r+1)$ is pseudorandom against $poly(k)$-COTMs.

   (b) Let $R : \{0,1\}^{2k} \rightarrow \{0,1\}^k$ be a random oracle. Show that the function family $F : \{0,1\}^k \times \{0,1\}^k \rightarrow \{0,1\}^k$ defined by $F(k, x) = R(k||x)$ is pseudorandom $poly(k)$-COTMs.

   (c) Let $R : \{0,1\}^{2k} \rightarrow \{0,1\}^k$ be a random oracle. Show that R is collision-resistant against $poly(k)$-COTMs.