Theoretical Cryptography Homework Set No. 2

Date Due: February 7th 2012

1. The goal of this exercise is to examine proposals for increasing the domain size of pseudo-random functions, that is constructions of a pseudo-random function F' on a large domain, from one F on a smaller domain. Let $\mathcal{F}$ be a family of pseudo-random function where members of the family $F_S : \{0,1\}^n \mapsto \{0,1\}^n$ and where $|S|$, the key length, is n as well. Our goal is to construct a family $\mathcal{F}'$ of functions with double the input length. That is $F'_S : \{0,1\}^{2n} \mapsto \{0,1\}^n$ for $F'_S \in \mathcal{F}'$.

   For input $X \in \{0,1\}^{2n}$ denote by X_L the first n bits and by X_R the last n bits.

   What can you say about the quality of the following constructions for F', that is either show that they are insecure or give a bound on the security:

   (a) The set of keys for F' is as in F and $F'_S(X_L, X_R) = F_{F_S(X_R)}(X_L)$.

   (b) The set of keys for F' is as in F and $F'_S(X_L, X_R) = F_S(F_S(X_R) \oplus X_L)$.

   (c) The set of keys for F' is as in F and $F'_S(X_L, X_R) = F_{F_{X_R}(S)}(X_L)$.

   (d) Let H be a family of pair-wise independent functions s.t. $h : \{0,1\}^{2n} \mapsto \{0,1\}^n$ for $h \in H$. The keys for F' consist of a key S to F and a function $h \in H$ and $F'_{S,h}(X) = F_S(h(X))$.

2. **Encrypting the secret key.** A key-dependent chosen-plaintext attack is a generalization of chosen-plaintext attack, in which the attacker is also allowed to provide a polynomial-time computable function g and to receive an encryption of the message $m = g(sk)$, where sk is the secret key.

   (a) Give an example of an encryption scheme which is semantically secure against a chosen-plaintext attack but is *totally insecure* in the sense that it allows retrieving the secret key when given an encryption of the secret key. Either public-key or shared-key schemes are valid.

   (b) Length preserving encryption: Show that *any* length preserving encryption scheme is totally insecure against an adaptive key-dependent chosen plain-text attack. I.e., show that by adaptively choosing functions g_i, an attacker can retrieve the secret key.

3. **Combiner for public-key encryption schemes.** Given two candidate public-key encryption schemes, E_1 and E_2, construct a third scheme that is semantically secure against a chosen-plaintext attack if and only if at least one of E_1 and E_2 is semantically secure against a chosen-plaintext attack.

4. **Arbitrary Domains.** Given a family of pseudo-random permutations on domains D which are powers of 2, suggest a family of pseudo-random permutation on any domain size.

5. **Zero-Knowledge for subset Sum.** Suggest a direct protocol (i.e. *not* through a reduction to Hamiltonicity) for the subset sum problem. Recall that the Subset sum problem is: given n numbers $0 \leq a_1, a_2, \ldots a_n \leq 2^\ell$ and a target sum T, is there a subset $S \subseteq \{1, \ldots n\}$ such that

$$\sum_{i \in S} a_i = T \bmod 2^\ell.$$