Tutorial 9: Random Oracle

Exercise 1.  

In this exercise we show a scheme that can be proven secure in the random oracle model, but is insecure when the random oracle model is instantiated with SHA-1 (or any fixed hash function). Let $\Pi$ be a signature scheme that is secure in the standard model.

Construct a signature scheme $\Pi_y$ where signing is carried out as follows: if $H(0) = y$ then output the secret key, if $H(0) \neq y$ then return a signature computed using $\Pi$.

1. Prove that for any value $y$, the scheme $\Pi_y$ is secure in the random oracle model.

2. Show that there exists a particular $y$ for which $\Pi_y$ is insecure when the random oracle model is instantiated with SHA-1.

Exercise 2.  

We define a new signature scheme which uses an encoding function $F : M \to \mathbb{Z}_N^*$ (where $M$ is the set of messages). The key generation is the same as in the naive RSA signature scheme: let $N = pq$ with $p$ and $q$ primes of identical bit-length, and $\phi$ be the Euler function. We recall that $\phi(N) = (p-1)(q-1)$.

The integers $e$ and $d$ are chosen as in the RSA scheme such that $e \cdot d \equiv 1 \mod \phi(N)$.

The public key of the signature scheme is $(N,e)$ and the secret key is $d$.

- To sign $m \in M$, compute $\sigma = F(m)^d \mod N$.
- To verify $(m,\sigma) \in M \times \mathbb{Z}_N^*$, accept if and only if $\sigma^e = F(m) \mod N$.

This exercise studies the properties of the function $F$ needed to guarantee the security of this scheme.

1. Assume that $F$ is a hash function which is not pre-image resistant. Give a key only attack against existential unforgeability.

2. Assume that $F$ is a hash function which is not collision resistant. Give an adaptive chosen message attack against existential unforgeability.

Remark: If the function $F$ is a hash function in $\mathbb{Z}_N^*$ which is indistinguishable from a random function, then this scheme is existentially unforgeable under an adaptive chosen-message attack in the random oracle model.

Instead of using a hash function for $F$, we now consider that $F$ is a linear redundancy function. A linear redundancy function is an invertible function which takes as input a message $m$ and outputs a bit string. Let $\omega \in \mathbb{Z}_N^*$ be fixed, we define $F$ as follows: $m \mapsto \omega \cdot m$.

3. Assume that we use this function $F$. Give an adaptive chosen message attack against existential unforgeability.

Exercise 3.  

Let $H : \{0,1\}^{2n} \to \{0,1\}^n$ be a random oracle. For $x \in \{0,1\}^n$ and $k \in \{0,1\}^n$, we define $F_k$ as follows:

$$F_k(x) = H(k\|x).$$

The security of a PRF $F_k$ is defined by the following game:

- A random function $H$, a random $k \in \{0,1\}^n$ and a uniform bit $b$ are chosen.
• If \( b = 0 \), the adversary \( \mathcal{A} \) is given access to an oracle for evaluating \( F_k(\cdot) \). If \( b = 1 \) then \( \mathcal{A} \) is given access an oracle for evaluating a random function mapping \( n \)-bit inputs to \( n \)-bit outputs (which is independent of \( H \)).

• \( \mathcal{A} \) outputs a bit \( b' \), and succeeds if \( b = b' \).

Note that during the second step, \( \mathcal{A} \) can access \( H \) in addition to the function oracle provided by the experiment.

The function \( F_k \) is a PRF if for any polynomial-time adversary \( \mathcal{A} \), the success probability of \( \mathcal{A} \) in the preceding experiment is at most negligibly greater than \( 1/2 \).

1. Show that \( F_k \) is a PRF.

Exercise 4. Security of the CTR encryption scheme

Let \( F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \) be a PRF. To encrypt a message \( M \in \{0,1\}^d \) under the key \( k \in \{0,1\}^n \), CTR proceeds as follows:

- Write \( M = M_0 \parallel M_1 \parallel \ldots \parallel M_{d-1} \) with each \( M_i \in \{0,1\}^n \);
- Sample \( IV \) uniformly in \( \{0,1\}^n \);
- Return \( IV \parallel C_0 \parallel C_1 \parallel \ldots \parallel C_{d-1} \) with \( C_i = M_i \oplus F(k, IV + i \mod 2^n) \) for all \( i \).

The goal of this exercise is to prove the security of CTR encryption mode against chosen ciphertext attacks, when the PRF \( F \) is secure.

1. Assume an attacker makes \( q \) encryption queries. Let \( IV_1, \ldots, IV_q \) be the corresponding \( IV \)'s. Let \( \text{Twice} \) denote the event “there exist \( i, j \leq q \) such that \( IV_i + k_i = IV_j + k_j \mod 2^n \).” Show that the probability of \( \text{Twice} \) is upper bounded by \( q^2 d / 2^{n-1} \).

2. Assume the PRF \( F \) is replaced by an uniformly chosen function \( f : \{0,1\}^n \rightarrow \{0,1\}^n \). Bound the distinguishing advantage of an adversary \( \mathcal{A} \) against this idealized version of CTR, as a function of \( d \) and the number of encryption queries \( q \).

3. Show that there exists a probabilistic polynomial-time adversary \( \mathcal{A} \) against CTR based on PRF \( F \), then there exists a probabilistic polynomial time adversary \( \mathcal{B} \) against the PRF \( F \). Give a lower bound on the advantage degradation incurred by the reduction.