Tutorial 2: Pseudorandom Objects

Submission Guidelines All problems must be solved in class today. Searching on the internet for solutions is strictly discouraged.

1. Prove that an efficient pseudorandom function with lengths of the input and key being $\log_2 n$ and $p(n)$ respectively (for some polynomial p) exist *unconditionally*. State any assumptions you make about p and also specify what the output length of the PRF should be.

   A: Assume $n|p(n)$. We will define a random function F_k with output length $m(n) = p(n)/(2^{\log_2 n})$ bits. Define $F_k(x)$ for $k \in \{0,1\}^{p(n)}$ and $x \in \{0,1\}^{\log_2 n}$ as follows: divide k into $n = 2^{\log_2 n}$ blocks $k_1, k_2, \ldots, k_n$ of $m(n)$ bits each; output will be k_x which is $m(n)$ bits long. Since k is uniformly distributed in $\{0,1\}^{p(n)}$, so is k_x in $\{0,1\}^{m(n)}$.

   Even when $n \nmid p(n)$, one can choose $m(n) = \lceil p(n)/n \rceil$ (assuming $p(n) \geq n$), discarding the last $p(n) \bmod n$ bits of k.

2. Let $G : \{0,1\}^n \to \{0,1\}^\ell$ be a pseudorandom generator. Define $G'(s)$ (for $s \in \{0,1\}^n$) to be the first n bits of $G(s)$. Is the function $F_k : \{0,1\}^n \to \{0,1\}^n$ (where $k \in \{0,1\}^n$) defined as $F_k(x) = G'(k) \oplus x$ pseudorandom? Justify your answer.

   A: F_k is not pseudorandom when more than one query is allowed. An attacker can query $F_k(0^n)$, obtain $G'(k)$ and compute the $F_k(x)$ for any input x of its choice without knowledge of k (thus making it completely deterministic).

3. Let $F = \{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ be a pseudorandom function and G a pseudorandom generator with input length n and output length $\ell = n + 1$. For each of the following encryption schemes, state whether the scheme has IND-EAV-secure and whether it is IND-CPA-secure. In each case, the shared key k is chosen uniformly at random from $\{0,1\}^n$.

   (a) To encrypt $m \in \{0,1\}^{2n+2}$, parse m as $m_1 || m_2$ with $|m_1| = |m_2|$ and send $\langle G(k) \oplus m_1, G(k+1) \oplus m_2 \rangle$.

   A: Essentially, the key stream of length $2n + 2$ masking the message is generated as $G(k)||G(k + 1)$. This string need not be pseudorandom since $k+1$ is not uniformly distributed in $\{0,1\}^n$ conditioned on k. Hence, we cannot say that the scheme has indistinguishable encryptions in the presence of an eavesdropper i.e., IND-EAV security.

   (b) For a message $m \in \{0,1\}^{n+1}$, choose a random $r \xleftarrow{R} \{0,1\}^n$ and compute the ciphertext as $\langle r, G(r) \oplus m \rangle$.

   A: This scheme is not secure at all since there is no secret key used in encryption. Using r (given in the clear), one can compute $G(r)$ and unmask the message.

   (c) Encrypt $m \in \{0,1\}^n$ as $m \oplus F_k(0^n)$.

   A: $F_k(0^n)$ is pseudorandom but produces the same output each time the function is evaluated, it can be used for one encryption. Thus the scheme is IND-EAV-secure.

   (d) Parse message $m \in \{0,1\}^{2n}$ as $m_1 || m_2$ with $|m_1| = |m_2|$, choose $r \xleftarrow{R} \{0,1\}^n$ and encrypt as $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r + 1) \rangle$.

   A: Since k is chosen at random and F_k is a pseudorandom function, $F_k(r)$ and $F_k(r+1)$ are uniformly and independently distributed in $\{0,1\}^n$. Hence, the scheme is IND-CPA-secure (detailed proof may be worked out in class).

4. Assume that F is a pseudorandom permutation. Show that there exists a function F' that is a PRP but is not a strong PRP.

A: Define

$$F'_k(x) = \begin{cases} 0^n & \text{if } x = k \\ F_k(k) & \text{if } x = F_k^{-1}(0) \\ F_k(x) & \text{otherwise} \end{cases},$$

so that F'_k remains a permutation. The inverse of F'_k would be defined as follows.

$$(F'_k)^{-1}(y) = \begin{cases} k & \text{if } y = 0^n \\ F_k^{-1}(0) & \text{if } y = F_k(k) \\ F_k^{-1}(y) & \text{otherwise} \end{cases}$$

So, given $(F'_k)^{-1}$, a distinguisher can completely recover the key by querying on 0^n and detect whether or not the function is random.