CS60084: Foundations of Cryptography
Spring 2019 — February 15, 2019

CS60084: Foundations of Cryptography
Spring 2019

February 15, 2019

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.

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.

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 $\mathsf{IND\text{-}EAV}$-secure and whether it is $\mathsf{IND\text{-}CPA}$-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 $\langle G(k) \oplus m_1, G(k+1) \oplus m_2 \rangle$.

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

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

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

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.