CSA E0 235: Cryptography 30/08/2019

Tutorial 4

Instructor: Arpita Patra *Question Set*

1. Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $l(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

   (a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

   (b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

   (c) To encrypt $m \in \{0,1\}^{n+1}$, output the ciphertext $F_k(m + G(k+1))$ where F is a pseudorandom permutation.

2. Let $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a length-preserving pseudorandom function. For the following constructions of a keyed function F', state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

   (a) $F' : \{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^n$ such that

   $$F'_K(x_1||x_2) = F_K(x_1) \oplus F_K(x_2)$$

   for all $x_1, x_2 \in \{0,1\}^n$ and $K \in \{0,1\}^k$.

   (b) $F' : \{0,1\}^{2k} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ such that

   $$F'_{K_1||K_2}(x_1||x_2) = F_{K_1}(x_1) \oplus F_{K_2}(x_2)$$

   for all $x_1, x_2 \in \{0,1\}^n$ and $K_1, K_2 \in \{0,1\}^k$.

   (c) $F' : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ such that

   $$F'_K(x) = F_K(x) \oplus x$$

   for all $x \in \{0,1\}^n$ and $K \in \{0,1\}^k$.