EE 720: Introduction to Number Theory and Cryptography (Autumn 2024)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 2: 20 points — Date: August 23, 2024

1. [5 points] Let F be a length-preserving pseudorandom function having key length, input length, and output length all equal to n bits. Consider the following keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \mapsto \{0,1\}^{2n}$ defined as

$$F'_k(x) = F_k(0\|x)\|F_k(x\|1).$$

Prove that the F' is **not** a pseudorandom function. Here $F'_k(x) = F'(k,x)$, $F_k(y) = F(k,y)$, and $\|$ is the string concatenation operator.

Note 1: All pseudorandom functions are not necessarily length-preserving. We defined pseudorandomness for length-preserving functions in class just for the sake of convenience. See the note below for the definition of pseudorandomness for F'.

Note 2: F' is a pseudorandom function if for any PPT distinguisher D, there is a negligible function $\texttt{negl}$ such that:

$$\left|\Pr\left[D^{F'_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| \leq \texttt{negl}(n),$$

where the first probability is taken over uniform choice of $k \in \{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $f \in \texttt{Func}_{n-1,2n}$ and the randomness of D. The set $\texttt{Func}_{n-1,2n}$ is the set of all functions with domain equal to $\{0,1\}^{n-1}$ and range equal to $\{0,1\}^{2n}$. By $D^{F'_k(\cdot)}(1^n)$ and $D^{f(\cdot)}(1^n)$, we mean distinguishers D who have oracle access to F'_k and f respectively.

2. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a keyed pseudorandom permutation (the first argument is the key). Consider the keyed function $F' : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined for all $x, x' \in \{0,1\}^n$ by

$$F'_k(x\|x') = F_k(x)\|F_k(x \oplus x').$$

   (a) [1 point] Prove that F'_k is a permutation for all $k \in \{0,1\}^n$.

   (b) [4 points] Prove that F' is **not** a pseudorandom permutation.

Note: F' is a pseudorandom permutation if for any PPT distinguisher D, there is a negligible function $\texttt{negl}$ such that:

$$\left|\Pr\left[D^{F'_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| \leq \texttt{negl}(n),$$

where the first probability is taken over uniform choice of $k \in \{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $f \in \texttt{Perm}_{2n}$ and the randomness of D. The set $\texttt{Perm}_{2n}$ is the set of all permutations (bijections) with domain and range equal to $\{0,1\}^{2n}$. By $D^{F'_k(\cdot)}(1^n)$ and $D^{f(\cdot)}(1^n)$, we mean distinguishers D who have oracle access to F'_k and f respectively.

3. [10 points] Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom permutation. Suppose messages of size dn bits have to be encrypted where $d > 1$. The message m is divided into d blocks of n bits each where m_i is the ith block. Consider the mode of operation in which a uniform value $\texttt{ctr} \in \{0,1\}^n$ is chosen, and the ith ciphertext block c_i is computed as $c_i := F_k(\texttt{ctr} + i + m_i)$. The value $\texttt{ctr}$ is sent in the clear, i.e. the eavesdropper observes $\texttt{ctr}$, $c_1, c_2, c_3, \ldots, c_d$. The sum $\texttt{ctr} + i + m_i$ is calculated modulo 2^n ensuring that the argument of F_k belongs to $\{0,1\}^n$. Show that this scheme is **not** EAV-secure.