CS 427/519: Homework 4

Due: Friday February 10, 10pm; typed and submitted electronically.

1. Let $F : \{0,1\}^\lambda \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure PRF.

   (a) Let $H$ be a 1-round Feistel network of $F$:
   
   $H(k,X_0\|X_1)$:
   
   $X_2 := F(k,X_1) \oplus X_0$
   
   return $X_1\|X_2$

   Show that $H$ is not a secure PRF.

   (b) Let $H$ be a 2-round Feistel network of $F$:
   
   $H((k_1,k_2),X_0\|X_1)$:
   
   $X_2 := F(k_1,X_1) \oplus X_0$
   
   $X_3 := F(k_2,X_2) \oplus X_1$
   
   return $X_2\|X_3$

   Show that $H$ is not a secure PRF.

2. Let $F$ be a secure PRF with $\lambda$-bit outputs, and let $G$ be a length-doubling PRG. Define

   $F'(k,r) = G(F(k,r))$.

   So $F'$ has outputs of length $2\lambda$. Prove that $F'$ is a secure PRF. Show the sequence of hybrid libraries and briefly justify each step.

3. Let $F$ be a secure PRP with blocklength $\lambda$. Below is the Enc algorithm of an encryption scheme with $\mathcal{K} = \mathcal{M} = \{0,1\}^\lambda$ and $\mathcal{C} = \{0,1\}^{2\lambda}$.

   Enc($k,m$) :
   
   $s_1 \leftarrow \{0,1\}^\lambda$
   
   $s_2 := s_1 \oplus m$
   
   $x := F(k,s_1)$
   
   $y := F(k,s_2)$
   
   return $(x,y)$

   Note: the idea is to secret-share the plaintext in the 2-out-of-2 secret-sharing scheme, and send each share through the PRP.

   ◀ Describe the corresponding Dec algorithm.

   ◀ Show that the scheme is not CPA-secure, by describing an attack.

grad. In all of the CPA-secure encryption schemes that we’ll ever see, ciphertexts are at least $\lambda$ bits longer than plaintexts. This problem shows that such ciphertext expansion is essentially unavoidable for CPA security.

Let $\Sigma$ be an encryption scheme with plaintext space $\mathcal{M} = \{0,1\}^n$ and ciphertext space $\mathcal{C} = \{0,1\}^{n+\ell}$. Show that there exists a distinguisher that distinguishes the two CPA libraries with advantage $\Omega(1/2^\ell)$.

Hint: As a warmup, consider the case where each plaintext has exactly $2^\ell$ possible ciphertexts. However, this need not be true in general. For the general case, choose a random plaintext $m$ and argue that with “good probability” (that you should precisely quantify) $m$ has at most $2^{\ell+1}$ possible ciphertexts.