6.875/18.425J Cryptography and Cryptanalysis April 1, 2005

Handout 10: Problem Set #5

This problem set is due on: April 15, 2005.

Problem 1 - Fun With Pseudorandom Functions

Suppose that $\{F_S\}$ is a pseudorandom family of functions from k-bit input to k-bit output, indexed by a k-bit key ("seed"). Consider the following constructions, and for each say whether it is is pseudorandom or not. If it is, give a proof; if not, demonstrate a counterexample. Below, "$\circ$" denotes concatenation, "$\oplus$" denotes exclusive-or, and $\bar{x}$ denotes the bitwise complement of x.

- $G_S(x) = F_S(x) \circ F_S(\bar{x})$.
- $G_S(x) = F_{0^k}(x) \circ F_S(x)$.
- $G_S(x) = F_{S_1}(x) \circ F_{S_2}(x)$, where $S_1 = F_S(0^k)$ and $S_2 = F_S(1^k)$.
- $G_S(x) = F_x(S)$.
- $G_S(x) = F_S(x) \oplus S$.
- $G_{S_1,S_2}(x) = F_{S_1}(x) \circ (F_{S_2}(x) \oplus S_1)$ (where $|S_1| = |S_2| = k$; consider only even-length seeds for G).

Problem 2 - Another Definition of Pseudorandom Functions

We define $f_s(\cdot)$ to be a NEW-PRF family if: $\forall$ $PPTA$, $\forall$ M, $\forall$ sufficiently large k,

$$\begin{aligned} Prob[s \leftarrow \{0,1\}^k; (x_1,\alpha_1) \leftarrow A(1^k); (x_2,\alpha_2) \leftarrow A(\alpha_1, f_s(x_1)); \ldots ; \\ (x_M,\alpha_M) \leftarrow A(\alpha_{M-1}, f_s(x_{M-1})); (x^*,\alpha^*) \leftarrow A(\alpha_M, f_s(x_M)); \\ b \leftarrow \{0,1\}; z_0 \leftarrow f_s(x^*); z_1 \leftarrow \{0,1\}^k : b = A(\alpha^*, z_b)] < neg(k) \end{aligned}$$

Flip a fair coin. If your coin comes up heads, prove that the existence of a NEW-PRF family implies the existence of a PRF family. If your coin comes up tails, prove that the existence of a PRF family implies the existence of a NEW-PRF family.

Informal Explanation: We say that $f_s(\cdot)$ is a NEW-PRF family if no probabilistic polynomial-time adversary is able to win the following game between an adversary and an oracle. First, the oracle randomly selects a seed, s. Then, the adversary is allowed to adaptively select inputs x_i and the oracle returns to him $f_s(x_i)$. Once the adversary is satisfied that he has learned something about the function, he outputs a challenge input x^* (which is not one of the x_i's that he previously asked the oracle about). Next, the oracle randomly selects a bit b and if $b = 0$ he gives the adversary $z_0 = f_s(x^*)$ and if $b = 1$ he gives the adversary a truly random value z_1. The adversary wins if he can guess b non-negligibly better than 1/2.

[Note: The role of the α's in the above definition is to allow the adversary to remember information between invocations. Without loss of generality, we can think of α_i as the complete state of the adversary after he finishes selecting x_i.]

Problem 3 - Private Key Encryption

Give a formal definition of private-key encryption. Your definition should embody security against chosen-message attacks. (That is, a private-key cryptosystem should remain secure even if the adversary picks the messages to be encrypted). Additionally, your definition should require that a private-key cryptosystem be secure even if the same key is used for an arbitrary number of messages. (That is, the one-time-pad system should not achieve your definition).

Prove that the existence of PRF's implies the existence of secure private-key encryption schemes.[1]

Problem 4 - An Active Attack on Blum-Goldwasser

Provide an active attack against the Blum-Goldwasser cryptosystem. Recall your definition of Active-Security from Problem Set 3. Does your definition rule out the the active attack you just provided? (Why or Why Not?)

[1]Note that since $OWF \Rightarrow PRF$, you have also proved that One-Way functions suffice for private-key encryption.