CS 127/CSCI E-127: Introduction to Cryptography

Problem Set 6

Assigned: Oct. 18, 2013 Due: Oct. 25, 2013 (5:00 PM)

Justify all of your answers. See the syllabus for collaboration and lateness policies. Submit solutions by email to `mbun@seas` (and please put the string "CS127PS6" somewhere in your subject line).

Problem 1. (The Hybrid Technique) In class, we saw a few methods for increasing the expansion function of a pseudorandom generator; here we give another. Let $G : \{0,1\}^* \to \{0,1\}^*$ be a pseudorandom generator with expansion function $\ell(n)$, and let $t(n)$ be a function. Consider the function

$$G'(x) = G^{(t(|x|))}(x) = \underbrace{G(G(G(\cdots G(}_{t(|x|)} x)))).$$

a) Show that when $\ell(n) = 2n$ and $t(n) = \lfloor \log n \rfloor$, G' is a pseudorandom generator. (Hint: use the hybrid technique.)

b) Does part a also hold for $t(n) = n$? Identify necessary and sufficient conditions on the relationship between $\ell(n)$ and $t(n)$ for G' to be a pseudorandom generator.

c) What are the advantages and disadvantages of this method for length expansion as compared to the one given in class?

Problem 2. (Separating Passive and Active Security) In class, we saw that every encryption scheme that satisfies indistinguishability under chosen plaintext attack also satisfies multiple-message indistinguishability. In this problem, you'll see that the converse is false. Let $\{f_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ be a family of pseudorandom functions (for security parameter n). Consider a probabilistic encryption scheme over message space $\{0,1\}^n$ where

$$E_k(m) = \begin{cases} (r, f_k(r) \oplus m, f_k(0^n)) & \text{if } m \neq f_k(0^n) \\ (r, f_k(r) \oplus m, k) & \text{if } m = f_k(0^n) \end{cases}$$

where $r \xleftarrow{\text{R}} \{0,1\}^n$ is chosen randomly for each encryption. Prove that this encryption scheme satisfies multiple-message indistinguishability, but is insecure against a chosen-plaintext attack.

Problem 3. (Secure Identification) Consider a setting where a user U needs to log on to a server S, and the user and server share a secret password $k \xleftarrow{\text{R}} \{0,1\}^n$ that was selected when the user's account was first created. To avoid having to remember k, the user holds it in a smartphone app which can also perform computations for the user.

The traditional way for the user to identify herself to the server is by sending k to the server, which can then verify that it received the correct key. However, an adversary listening in on the communication would learn k and could later impersonate the user.

a) Using pseudorandom functions, design a protocol between the user U and server S for identification that does not have this difficulty. That is, even after watching the user identify herself many times, a PPT adversary $\mathcal{A}$ should not be able to successfully impersonate the user (except with negligible probability).

b) Precisely define and prove the security property that your protocol achieves (assuming the security of the pseudorandom function family).