Homework 4

Due: Oct 11, 2024

CS 1510: Intro. to Cryptography and Computer Security

Feel free to use the lecture notes to help with 1 and 2, but note that you should at least rewrite each answer in your own words/structure.

1 CPA Security of Authenticate-then-Encrypt

Let $\Pi^E = (\mathsf{Gen}^E, \mathsf{Enc}^E, \mathsf{Dec}^E)$ be an encryption scheme and $\Pi^M = (\mathsf{Gen}^M, \mathsf{Mac}^M, \mathsf{Verify}^M)$ be a MAC scheme.

a. Formalize the construction of the "authenticate-then-encrypt" scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ given Π^E and Π^M.

b. Prove that Π is CPA-secure for any MAC scheme Π^M (even if not secure) and any CPA-secure encryption scheme Π^E.

2 Unforgeability of Encrypt-then-Authenticate

Let $\Pi^E = (\mathsf{Gen}^E, \mathsf{Enc}^E, \mathsf{Dec}^E)$ be an encryption scheme and $\Pi^M = (\mathsf{Gen}^M, \mathsf{Mac}^M, \mathsf{Verify}^M)$ be a MAC scheme.

a. Formalize the construction of the "encrypt-then-authenticate" scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ given Π^E and Π^M.

b. Prove that Π is unforgeable for any encryption scheme Π^E (even if not CPA-secure) and any secure MAC scheme Π^M (even if not strongly secure).

3 CCA Security from Strong PRPs

Consider the following definition of a pseudorandom permutation.

Definition 1 (Pseudorandom Permutation) *Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be an efficient, keyed, length-preserving function. F is a* pseudorandom permutation *if $F_k(\cdot)$ is a permutation for any k (i.e. $F_k(\cdot)$ is a bijection from $\{0,1\}^n$ to $\{0,1\}^n$) and that for all probabilistic polynomial-time distinguishers D, there is a negligible function* negl *such that*

$$|\Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1]| \leq \mathsf{negl}(n),$$

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 $f \in \mathsf{Perm}_n$ and the randomness of D. Perm_n denotes the set of all permutations from $\{0,1\}^n$ to $\{0,1\}^n$.

Now consider the following definition of a *strong* pseudorandom permutation.

Definition 2 (Strong Pseudorandom Permutation) *Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be an efficient, keyed, length-preserving function. F is a* strong pseudorandom permutation *if $F_k(\cdot)$ is a permutation for any k and that for all probabilistic polynomial-time distinguishers D, there is a negligible function negl such that*

$$|\Pr[D^{F_k(\cdot),F_k^{-1}(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot),f^{-1}(\cdot)}(1^n) = 1]| \leq \mathsf{negl}(n),$$

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 $f \in \mathsf{Perm}_n$ and the randomness of D.

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a strong pseudorandom permutation. Define the following fixed-length encryption scheme: On input a message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, Enc picks a uniform random $r \xleftarrow{\$} \{0,1\}^{n/2}$ and outputs $c := F_k(m\|r)$.

a. Discuss the difference between the two definitions. What is the "strength" of a strong PRP? Why might it be a useful notion in cryptography?

b. Describe how Dec works.

c. Prove that this scheme is CCA-secure.

d. Show that this scheme is *not* unforgeable.

Hint: For any pseudorandom permutation F, given a key k, the inverse function F_k^{-1} is also a deterministic polynomial-time computable function. For more discussion on PRPs, please see the Katz-Lindell textbook section 3.5.1.

4 Collision Resistant Hash Functions

Let (Gen_1, H_1) and (Gen_2, H_2) be two hash functions, where at least one of them is collision resistant. Define (Gen, H) in the following. Prove or disprove that (Gen, H) is necessarily collision resistant.

a. Gen runs Gen_1 and Gen_2 to obtain keys s_1 and s_2, respectively. Then define $H^{s_1,s_2}(x) := H_1^{s_1}(x)\|H_2^{s_2}(x)$.

b. Gen runs Gen_1 and Gen_2 to obtain keys s_1 and s_2, respectively. Then define $H^{s_1,s_2}(x) := H_1^{s_1}(H_2^{s_2}(x))$.

c. For this problem, assume (Gen_1, H_1) is a CRHF. Gen runs Gen_1 to obtain key s_1. Then define $H(x_1 \| x_2) := x_1 \oplus_p H_1^{s_1}(x_2)$ where $\oplus_p$ denotes "padded XOR," where if we're XORing strings of unequal length, we pad the shorter string with as many 0s on the right hand-side as is needed to make it the correct length. For example, $1010 \oplus_p 110011 = 101000 \oplus 110011 = 011011$.

5 Summary Question

Summarize the most important insights from this week's material, including from the lectures, notes, textbooks, homework problems, and other resources you find helpful, into a one-page resource. We expect that these summary pages will help you with the take-home midterm and final. Please note this question is graded based on completion—we will not be checking it for correctness. However, we will be checking it for relevance to the week's content and length.