Homework 4

Due: October 13, 2023

CS 1510: Intro. to Cryptography and Computer Security

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*

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

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 $r \overset{\$}{\leftarrow} \{0,1\}^{n/2}$ 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 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. You will be permitted to use this one-page resource (along with the other weeks' resources) on the midterm and final.

Changes to this document prior to the exams are permitted, but for each change, you will be asked to state what you changed and why. For example, if you dropped something and replaced it with something else, justify why the thing you dropped wasn't as important as the thing you inserted, why you think it might be more useful for the exam, etc.

Please note that the purpose of this question is to help you organize and synthesize the material for your own future use. It will be graded based on completion—we will not be checking it for correctness.