Midterm

Due: Oct 25, 2024

CS 1510: Intro. to Cryptography and Computer Security

- The midterm exam is due at 11:59 PM on October 25th (Friday). **No late days or extensions will be granted.**
- Try to answer all questions. Partial credit will be given if you have good intuitions/ideas. Before you answer any question, read the problem carefully. Be precise and concise in your answers.
- You may consult the course materials and textbooks, but you must write each answer in your own words/structure. Apart from that, you may *not* collaborate, ask the instructor or TAs.
- If you have any clarifying questions on the exam, please post a private post on EdStem, and we will respond as soon as we can (within a day).

1 Warm-Ups (10 points)

a. Perfect security [ ] (does/does not) imply randomized encryption.

b. CPA security [ ] (does/does not) imply semantic security.

c. CPA security [ ] (does/does not) imply randomized encryption.

d. CCA security [ ] (does/does not) imply perfect security.

e. CCA security [ ] (does/does not) imply CPA security.

f. CCA security [ ] (does/does not) imply unforgeability.

g. The pseudo-OTP encryption scheme [ ] (is/is not) perfectly secure.

h. The pseudo-OTP encryption scheme [ ] (is/is not) CPA-secure.

i. Give an example of a negligible function: $f(n) =$ [ ]

j. Consider a hash function $h : \{0,1\}^* \to \{0,1\}^{128}$. Assume that h operates ideally, i.e., each input to h is mapped to a random 128-bit output. Suppose an attacker tries to find a collision of h by computing it on distinct inputs. What is the expected number of tries (evaluations of h) the attacker needs in order to find a collision with probability roughly 50%? [ ]

2 PRFs and PRGs (10 points)

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function and $G : \{0,1\}^{n-1} \to \{0,1\}^n$ be a pseudorandom generator. Define $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^n$ as

$$F'_k(x) := F_k(G(x)).$$

Provide a countereaxmple to show that F' is *not* necessarily a PRF. You may assume PRFs and PRGs exist, and use another PRF and/or PRG in your construction.

3 Zero CPA Security (16 points)

Consider a new security definition of symmetric-key encryption schemes. We first introduce an experiment for any encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, adversary $\mathcal{A}$, and security parameter n. The experiment is defined as follows:

- The challenger $\mathcal{C}$ chooses a uniform bit $b \in \{0, 1\}$.
- $\mathcal{C}$ runs $\mathsf{Gen}(1^n)$ to generate the key k.
- The adversary $\mathcal{A}$ queries $\mathsf{poly}(n)$ number of messages m_i, one at a time. Upon receiving each message m_i from $\mathcal{A}$, $\mathcal{C}$ responds as follows:

  If $b = 0$, then $\mathcal{C}$ sends $\mathsf{Enc}_k(m_i)$ to $\mathcal{A}$;
  If $b = 1$, then $\mathcal{C}$ sends $\mathsf{Enc}_k(0)$ to $\mathcal{A}$.
- $\mathcal{A}$ outputs b'.

We say a symmetric-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is zero-CPA-secure if for any PPT adversary $\mathcal{A}$, there exists a negligible function negl such that

$$\Pr[b' = b] \le \frac{1}{2} + \mathsf{negl}(n).$$

In this problem, you will prove that this new security definition is equivalent to CPA-security.

a. (8 points) Prove that zero-CPA-security implies CPA-security. Namely, if an encryption scheme Π is zero-CPA-secure, then it is also CPA-secure.

b. (8 points) Prove that CPA-security implies zero-CPA-security. Namely, if an encryption scheme Π is CPA-secure, then it is also zero-CPA-secure.

4 Collision Resistant Hash Functions (10 points)

Construct a collision resistant hash function (Gen, H) with the property that, if one truncates the last bit of output of H then the new hash function is no longer collision resistant. Prove that your construction of H is a CRHF, and show how the adversary finds a collision if the last bit of output is removed. You may assume CRHFs exist, and use another CRHF in your construction.

5 Unforgeability of Authenticate-then-Encrypt (8 points)

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

b. (6 points) 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).

6 Block Cipher Modes of Operation (6 points)

Suppose you are a security engineer and would like to deploy symmetric-key encryption using a block cipher.

a. (3 points) Which mode of operation (among ECB/CBC/CTR/OFB modes) would you choose? Why?

b. (3 points) What do you need to pay attention to during the deployment?

Hints

Q2: *Hint 1:* Assuming another PRG $G' : \{0,1\}^{n-1} \to \{0,1\}^n$, try to construct PRG $G : \{0,1\}^{n-1} \to \{0,1\}^n$ with certain properties.

Hint 2: You may take inspiration from HW5 Q1.

Q3(b): You may consider doing a hybrid argument over the $Q(n)$ messages queried by $\mathcal{A}$ in the zero-CPA-security game.

Q4: Assuming another CRHF $H' : \{0,1\}^{2n} \to \{0,1\}^{n-1}$, try to construct CRHF $H : \{0,1\}^{2n} \to \{0,1\}^n$ that has the desired property. How can you use the extra bit to make sure that there is no collision on any two inputs x_1, x_2 to H, but there would be a collision when we remove the bit?