Homework 5

Due: October 18, 2024

CS 1510: Intro. to Cryptography and Computer Security

1 CRHFs and PRGs

Suppose that we are given a family of length-halving collision-resistant hash functions H with parameters generated by Gen, and a pseudorandom generator $G : \{0,1\}^k \to \{0,1\}^{2k}$. Are the following statements necessarily true?

a. Statement 1: The function $H^s(G(x))$ (where $H^s : \{0,1\}^{2k} \to \{0,1\}^k$) is computationally indistinguishable from a random function, for $s \leftarrow \mathsf{Gen}(1^k)$.
Here, consider a distinguisher $\mathcal{A}$ who can query its challenger on polynomially many inputs $x \in \{0,1\}^k$ and observe the outputs. $\mathcal{A}$ eventually tries to distinguish whether the challenger is using $H^s(G(x))$ for a hidden s or a random function f.

b. Statement 2: It is computationally hard to find $2k$-bit $x \neq x'$ such that $G(H^s(x)) = G(H^s(x'))$ for $s \leftarrow \mathsf{Gen}(1^k)$.
This time, consider an adversary $\mathcal{A}$ who obtains s from the challenger and tries to find a pair $x \neq x'$ such that $G(H^s(x)) = G(H^s(x'))$.

For each of the above statements, if you believe the statement is true, you must prove that for *any* CRHF H and *any* PRG G, the statement is true (e.g., by showing a reduction or hybrid argument reducing to G and H). If you believe the statement if false, you must show that for *some* CRHF H and *some* PRG G, the composition does not satisfy the property. For instance, you may follow a three-step approach: (1) construct a specific H and G, (2) prove that H is a CRHF and that G is a PRG (e.g., by showing a reduction proof), and (3) show that there is a polynomial-time attack when we instantiate the composition with the specific H and G.

2 Merkle Trees

Let $(\mathsf{Gen}, \mathsf{MT}_t)$ (for a fixed $t = 2^k$ where k is a constant) be the construction of a Merkle tree based on a hash function (Gen, H) for $H : \{0,1\}^* \to \{0,1\}^n$ described in class (Lecture 11, Slide 3).

a. What are the domain and range of MT_t? Show that $(\mathsf{Gen}, \mathsf{MT}_t)$ is a collision-resistant

hash function for these domain and range, assuming that (Gen, H) is a collision-resistant hash function.

b. Let $\mathsf{MTVerify}_t^s(v, x, i, a)$ be the verification algorithm for a Merkle tree with root v, x being the i-th document, and a being the authenticating path for x (sibling nodes of the root-to-leaf path of x). Prove that, assuming that (Gen, H) is a collision-resistant hash function, $(\mathsf{Gen}, \mathsf{MT}_t)$ is sound. Namely, no PPT $\mathcal{A}$ can produce an authenticating path for the same Merkle root v but conflicting i-th documents x and x'. More formally, show that, for every PPT $\mathcal{A}$ there exists a negligible function ν such that

$$\Pr[s \leftarrow \mathsf{Gen}(1^n); (v, x, x', i, a, a') \leftarrow \mathcal{A}(1^n, s) : \\ x \neq x' \wedge \mathsf{MTVerify}_t^s(v, x, i, a) \wedge \mathsf{MTVerify}_t^s(v, x', i, a')] \leq \nu(n)$$

3 Modifying the Merkle-Damgård Transform

Consider the following modification of $H^s(x)$ in the Merkle-Damgård transform. Instead of outputting $Z_{B+1} = h^s(Z_B \| |x|)$, output $Z_B \| |x|$. (Now $H^s(x)$ has output length $2n$.) Prove or disprove that the resulting hash function (Gen, H) is necessarily collision resistant.

4 Feistel Network

Consider an r-round Feistel network with input (L_0, R_0).

a. What is its output if each round function outputs all 0s, regardless of the input?

b. What is its output if each round function is the identity function (i.e., output equals input)?

5 Block Cipher Modes of Operation

In this problem, we will explore the differences in errors between the block cipher CBC, OFB, and CTR modes of operation.

a. Consider the case in which there is a single-bit error in the ciphertext. What is the effect on the decryption output of the CBC, OFB, and CTR modes of operation?

b. Consider the case in which there is a dropped ciphertext block (in other words, if the transmitted ciphertext $c_0, c_1, c_2, c_3, \ldots$ is received as $c_0, c_1, c_3, \ldots$). What is the effect on the decryption output of the CBC, OFB, and CTR modes of operation?

6 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.