Homework 5

Due: October 20, 2023

CS 1510: Intro. to Cryptography and Computer Security

1 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 $H(x_1 \| x_2) := x_1 \oplus_p H^{s_1}(x_2)$ 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, $1010 \oplus_p 110011 = 101000 \oplus 110011 = 011011$.

2 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 $G : \{0,1\}^k \to \{0,1\}^{2k}$.

a. Does it follow that the function $H^s(G(x))$ (where $H^s : \{0,1\}^{2k} \to \{0,1\}^k$) is indistinguishable from a random function, for $s \leftarrow \mathsf{Gen}(1^k)$? Consider a distinguisher $\mathcal{A}$ who can query its challenger on polynomially-many inputs $x \in \{0,1\}^k$ and observe the outputs before trying to distinguish whether the challenger is using $H^s(G(x))$ for a hidden s or a random function f.

b. Does it follow that it is 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 $G(H^s(x)) = G(H^s(x'))$.

3 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^s) for $H : \{0,1\}^* \to \{0,1\}^n$ described in class (Lecture 11 Slide 9).

a. What are the domain and range of MT_t? Show that $(\mathsf{Gen}, \mathsf{MT}_t)$ is a family of collision-resistant hash functions for these domain and range, assuming that (Gen, H) is a collision-resistant hash function family.

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 family, $(\mathsf{Gen}, \mathsf{MT}_t)$ 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

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

4 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 collision resistant.

5 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)?

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. 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.