One-Way Hash Functions

Notes by Srini Devadas

MIT - 6.5610
Lecture 1 (February 2, 2026)

> ***Warning:*** This document is a rough draft, so it may contain bugs. Please feel free to email me with corrections.

Administrivia

- Homeworks in groups
- Midterm
- Projects in groups

Cryptographic Hash Functions

A *cryptographic hash function* maps arbitrary-length strings of data to a fixed-length output in a deterministic, public, and "random-looking" manner.

$$h : \{0,1\}^* \to \{0,1\}^d.$$

Random Oracle Intuition. The ideal functionality of a random oracle is as follows: $h(x)$ for a new x is computed by flipping coins d times, returning the bit-string, and recording the input–output pair in a table. Upon receiving x, prior to flipping coins, the table is checked for an $(x, h(x))$ pair, and if it exists, the stored $h(x)$ is returned. Many cryptographic schemes are proven secure in the *random oracle (RO) model*. In practice, since true random oracles do not exist, we use *pseudorandom* hash functions.

Desirable Properties

Notation. We write $\{0,1\}$ for the set of bits, and use $\mathrm{negl}(\cdot)$ for $\mathrm{negl}(\lambda)$ functions.

One-Wayness (Preimage Resistance)

It should be infeasible, given $y \in_R 0,1^d$, to find any x such that $h(x) = y$.

Collision Resistance (CR)

It should be infeasible to find two distinct inputs $x \neq x'$ such that

$$h(x) = h(x').$$

Target Collision Resistance (TCR)

Given a target input x, it should be infeasible to find $x' \neq x$ such that $h(x) = h(x')$. This is also called 2^{nd} pre-image resistance.

Generic Attacks. Collisions can be found in time approximately $2^{n/2}$ via the birthday attack. Inversion can be done in time $O(2^n)$.

Relations.

Collision resistance implies target collision resistance, but not vice versa. One-wayness does not imply collision resistance, and collision resistance does not imply one-wayness.

Collision resistance does not imply one-wayness Suppose $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ is collision resistant. Define $H(x) = f(x) \parallel x$, where $\parallel$ denotes concatenation. This is *not* one-way. If $H(x) = H(x')$, then $x = x'$, so $H(x)$ is collision resistant.

One-wayness does not imply collision resistance Suppose $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ is one-way. Define $H(x_1, x_2) = f(x_1)$. This remains one-way. Collisions are trivial, just vary x_2 for any x_1.

Applications

Password Storage

Store $h(\mathsf{PW})$ instead of the password itself. Disclosure of the hash should not reveal the password. Need one-wayness.

File Integrity

For each file F, store $h_F = h(F)$ securely. To detect modification, recompute the hash and compare with the stored h_F. Target collision resistance suffices.

Digital Signatures

To sign a large message M, sign its hash:

$$\sigma = \mathsf{Sign}(\mathsf{sk}, h(M)).$$

Collision resistance is required to prevent substitution attacks. Do not need one-wayness if we assume M is public.

Commitments

Alice commits to a value x by publishing $c = h(r \parallel x)$ for random r. To open, she reveals (r, x). Commitments require one-wayness and collision resistance, and additional properties for secrecy.

One-Way Functions: Formal Definition

Definition 1. A negligible function $\mu(\lambda)$ satisfies the property that for all polynomials p, $\exists \lambda_0$ such that $\forall \lambda > \lambda_0$, we have $\mu(\lambda) < 1/p(\lambda)$.

Definition 2. $H : \{0,1\}^* \to \{0,1\}^n$ is a one-way function if given any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, there exists a negligible function μ such that for every security parameter $\lambda \in \mathbb{N}$,

$$Pr[H(x) = H(x')] \leq \mu(\lambda)$$

where $x \xleftarrow{R} \{0,1\}^\lambda$, and $x' \leftarrow \mathcal{A}(H(x))$.

The probability is taken over the randomness of x and the adversary. The definition prevents the adversary from choosing an "easy" input.

The adversary does not need to recover the original input x in this definition.

Collision Resistance: Formal Definition

A family of hash functions H_λ is collision resistant if for every $\lambda \in \mathbb{N}$, for every PPT adversary $\mathcal{A}$, the probability that $A(1^\lambda)$ outputs distinct x, x' such that $H_\lambda(x) = H_\lambda(x')$ is negligible.

The probability space is the internal randomness of the adversary, and any randomness in H, which can be deterministic.

Exercises

OWF Question

Let f be a one-way function and define $g(x_1, x_2) = f(x_1) \oplus x_2$. Analyze the one-wayness of g.

CR Question

Given collision-resistant h_1, h_2, analyze whether $h(x, y) = h_1(x, h_2(y))$ is collision resistant. Consider cases based on whether collisions arise in h_1 or h_2.

References