Cryptography

Lecture 13

Announcements

- HW5 due 3/9
- Midterm Upcoming on 3/16
  - Review sheet posted on course webpage and on Canvas
  - Solutions and Cheat Sheet posted soon on Canvas
  - Extra practice for midterm posted on Canvas

Agenda

- This time:
  - Domain Extension for CRHF
    - (Merkle-Damgard) (K/L 5.2)

Collision Resistant Hashing

Collision Resistant Hashing

Definition: A hash function (with output length ℓ) is a pair of ppt algorithms (Gen, H) satisfying the following:

- Gen takes as input a security parameter 1^n and outputs a key s. We assume that 1^n is implicit in s.
- H takes as input a key s and a string $x \in \{0,1\}^*$ and outputs a string $H^s(x) \in \{0,1\}^{\ell(n)}$.

If H^s is defined only for inputs $x \in \{0,1\}^{\ell'(n)}$ and $\ell'(n) > \ell(n)$, then we say that (Gen, H) is a fixed-length hash function for inputs of length ℓ'. In this case, we also call H a compression function.

The collision-finding experiment

$Hashcoll_{A,\Pi}(n)$:

1. A key s is generated by running $Gen(1^n)$.
2. The adversary A is given s and outputs x, x'. (If Π is a fixed-length hash function for inputs of length $\ell'(n)$, then we require $x, x' \in \{0,1\}^{\ell'(n)}$.)
3. The output of the experiment is defined to be 1 if and only if $x \neq x'$ and $H^s(x) = H^s(x')$. In such a case we say that A has found a collision.

Security Definition

Definition: A hash function $\Pi = (Gen, H)$ is collision resistant if for all ppt adversaries A there is a negligible function neg such that

$$\Pr[Hashcoll_{A,\Pi}(n) = 1] \leq neg(n).$$

Domain Extension

The Merkle-Damgard Transform

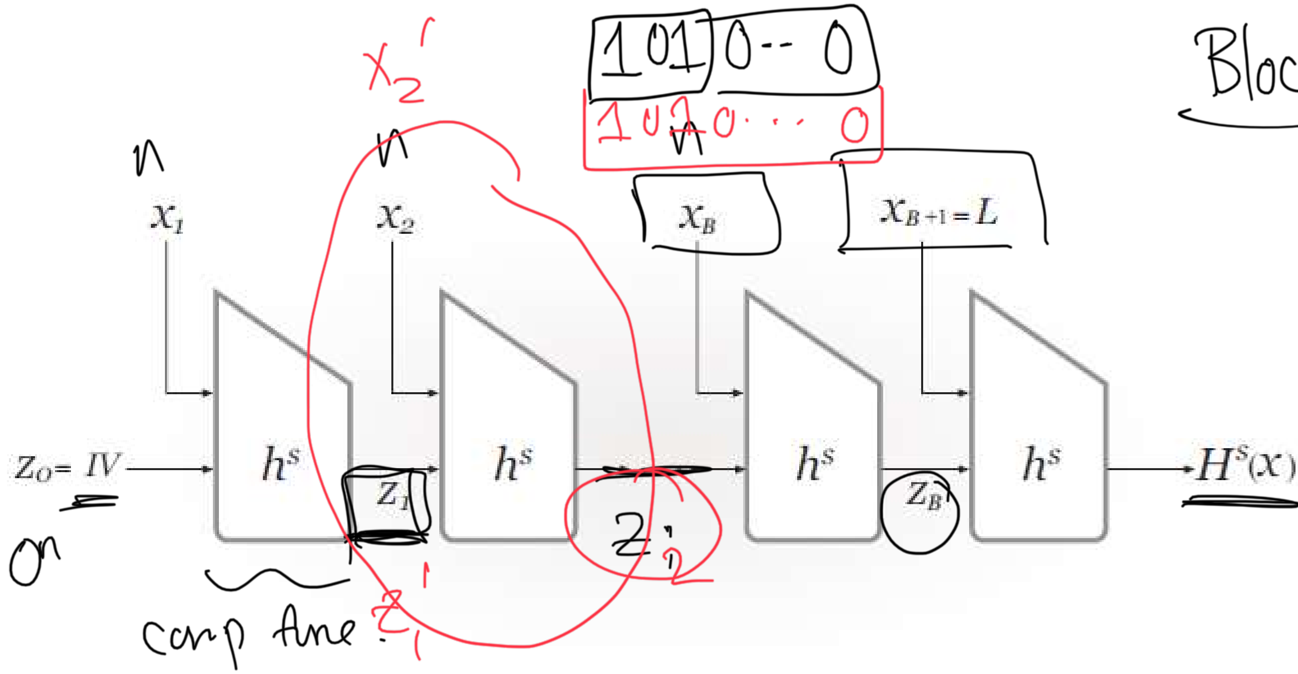

FIGURE 5.1: The Merkle-Damgård transform.

Blockchain.

SHA-1

SHA-2

~~SHA-3~~

$h^s : \{0,1\}^{512} \to \{0,1\}^{256}$.

$n = 256$

Prove: If comp. func is coll resist. then entire const is collision resistant.

The Merkle-Damgard Transform

Let (Gen, h) be a fixed-length hash function for inputs of length $2n$ and with output length n. Construct hash function (Gen, H) as follows:

- Gen: remains unchanged
- H: on input a key s and a string $x \in \{0,1\}^*$ of length $L < 2^n$, do the following:
  1. Set $B := \left\lceil \frac{L}{n} \right\rceil$ (i.e., the number of blocks in x). Pad x with zeros so its length is a multiple of n. Parse the padded result as the sequence of n-bit blocks $x_1, \ldots, x_B$. Set $x_{B+1} := L$, where L is encoded as an n-bit string.
  2. Set $z_0 := 0^n$. (This is also called the IV.)
  3. For $i = 1, \ldots, B+1$, compute $z_i := h^s(z_{i-1} || x_i)$.
  4. Output z_{B+1}.

Security of Merkle-Damgard

Theorem: If (Gen, h) is collision resistant, then so is (Gen, H).