The Secure Hash Algorithm

Truong Tuan Anh
CSE-HCMUT

Outline

- Iterated Hash Functions
- SHA-1
- …

Recall: Iterated Hash Functions

- Preprocessing step

Given an input string x, where $|x| \geq m + t + 1$

Construct a string y, using a public algorithm, such that $|y| \equiv 0 \pmod{t}$. Denote

$$y = y_1 \,||\, y_2 \,||\, \cdots \,||\, y_r,$$

where $|y_i| = t$ for $1 \leq i \leq r$.

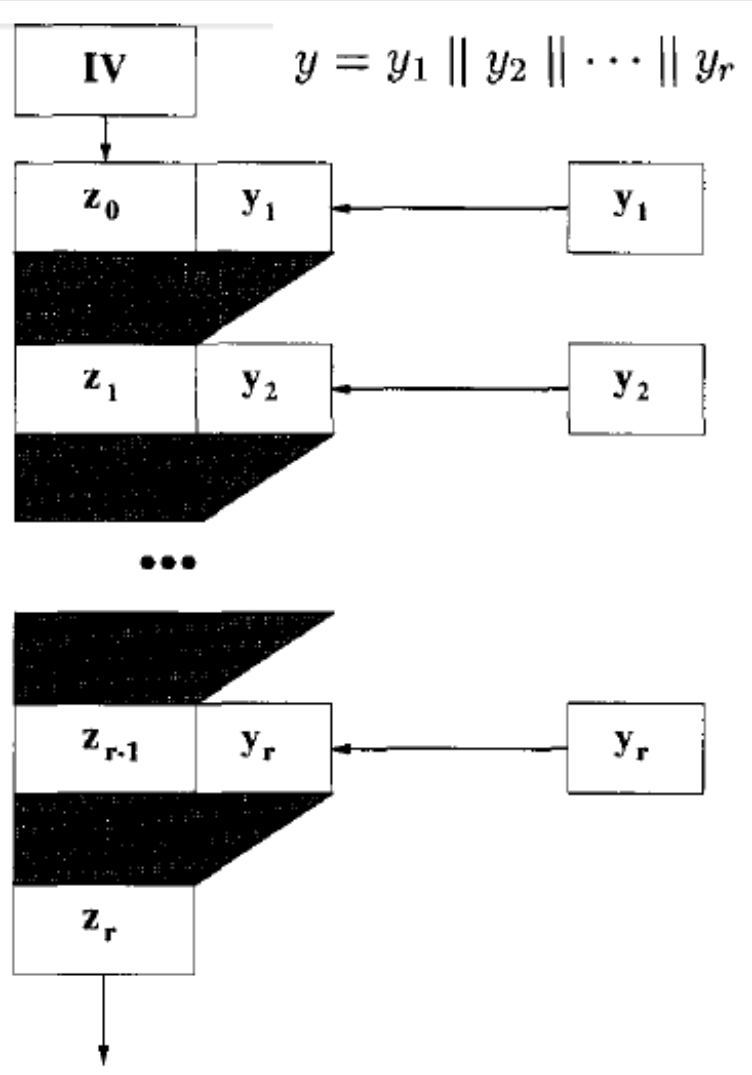
Recall: Iterated Hash Functions

- Processing step

Let IV be a public initial value which is a bitstring of length m. Then compute the following:

$$
\begin{aligned}
z_0 &\leftarrow \mathrm{IV} \\
z_1 &\leftarrow \mathbf{compress}(z_0 \,||\, y_1) \\
z_2 &\leftarrow \mathbf{compress}(z_1 \,||\, y_2) \\
&\vdots \quad \vdots \quad \vdots \\
z_r &\leftarrow \mathbf{compress}(z_{r-1} \,||\, y_r).
\end{aligned}
$$

Recall: Iterated Hash Functions



Recall: Iterated Hash Functions

- Output Transformation (Optional)

Let $g : \{0,1\}^m \rightarrow \{0,1\}^\ell$ be a public function.

Define $h(x) = g(z_r)$

SHA-1: Overview

- The Secure Hash Algorithm
- An iterated hash function
- 160 –bit message digest
- Word-oriented operations on bitstrings
- A word consists of 32 bits (8 hexadecimal digits)

Operations

$X \wedge Y$	bitwise "and" of X and Y
$X \vee Y$	bitwise "or" of X and Y
$X \oplus Y$	bitwise "xor" of X and Y
$\neg X$	bitwise complement of X
$X + Y$	integer addition modulo 2^{32}
$\mathbf{ROTL}^s(X)$	circular left shift of X by s positions
	$(0 \leq s \leq 31)$

Padding Scheme

SHA-1-PAD(x)

$d \leftarrow (447 - |x|) \bmod 512$
$\ell \leftarrow$ the binary representation of $|x|$, where $|\ell| = 64$
$y \leftarrow x \parallel 1 \parallel 0^d \parallel \ell$

Note: $|x| \leq 2^{64} - 1$

Padding Scheme

- *y* has length divisible by 512, including *n* blocks

$$y = M_1 \,||\, M_2 \,||\, \cdots \,||\, M_n$$

The Core Function

Define the functions $\mathbf{f}_0, \ldots, \mathbf{f}_{79}$:

$$\mathbf{f}_t(B, C, D) = \begin{cases} (B \wedge C) \vee ((\neg B) \wedge D) & \text{if } 0 \leq t \leq 19 \\ B \oplus C \oplus D & \text{if } 20 \leq t \leq 39 \\ (B \wedge C) \vee (B \wedge D) \vee (C \wedge D) & \text{if } 40 \leq t \leq 59 \\ B \oplus C \oplus D & \text{if } 60 \leq t \leq 79 \end{cases}$$

$\mathbf{f}_t$: input : B, C and D

output : one word

SHA-1

SHA-1(x)

external SHA-1-PAD
global $K_0, \ldots, K_{79}$
$y \leftarrow$ SHA-1-PAD(x)
denote $y = M_1 \parallel M_2 \parallel \cdots \parallel M_n$,
$H_0 \leftarrow$ 67452301 $H_3 \leftarrow$ 10325476
$H_1 \leftarrow$ EFCDAB89 $H_4 \leftarrow$ C3D2E1F0
$H_2 \leftarrow$ 98BADCFE

Compress Function

for $i \leftarrow 1$ **to** n
do { H_0, H_1, H_2, H_3, H_4 are modified }
return $(H_0 \parallel H_1 \parallel H_2 \parallel H_3 \parallel H_4)$

denote $M_i = W_0 \parallel W_1 \parallel \cdots \parallel W_{15}$, where each W_i is a word

for $t \leftarrow 16$ **to** 79

  do $W_t \leftarrow \mathbf{ROTL}^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16})$

$A \leftarrow H_0 \qquad D \leftarrow H_3$

$B \leftarrow H_1 \qquad E \leftarrow H_4$

$C \leftarrow H_2$

for $t \leftarrow 0$ **to** 79

do
$$\begin{cases} temp \leftarrow \mathbf{ROTL}^5(A) + \mathbf{f}_t(B, C, D) + E + W_t + K_t \\ E \leftarrow D \\ D \leftarrow C \\ C \leftarrow \mathbf{ROTL}^{30}(B) \\ B \leftarrow A \\ A \leftarrow temp \end{cases}$$

$H_0 \leftarrow H_0 + A \qquad H_3 \leftarrow H_3 + D$

$H_1 \leftarrow H_1 + B \qquad H_4 \leftarrow H_4 + E$

$H_2 \leftarrow H_2 + C$

Note: Word Constants

$$K_0, \ldots, K_{79}, :$$

$$K_t = \begin{cases} \texttt{5A827999} & \text{if } 0 \leq t \leq 19 \\ \texttt{6ED9EBA1} & \text{if } 20 \leq t \leq 39 \\ \texttt{8F1BBCDC} & \text{if } 40 \leq t \leq 59 \\ \texttt{CA62C1D6} & \text{if } 60 \leq t \leq 79 \end{cases}$$

SHA-1: Review

- The compress function maps 160+512 bits to 160 bits
- SHA-1 is one in a series of related iterated hash functions
  - MD4 (1990)
  - MD5 (1992)
  - SHA (1993, sometimes called SHA-0)
  - SHA-1 (1995)
  - SHA-2 (2002): SHA-224; SHA-256; SHA-384; SHA-512
  - SHA-3 (2012)

Presentations

- Message Authentication Code (Section 4.4)