MD Transform

Murat Kantarcioglu

MD Paradigm

- SHF1 uses shf1 as the compression function
- If we prove that if shf1 is secure then SHF1 is secure then we need to attack shf1 only
- MD paradigm shows how to use collision resistant compression function to built collision resistant hash function

MD Paradigm: Definitions

$H(K, M)$

  $y \leftarrow \mathsf{pad}(M)$

  Parse y as $M_1 \| M_2 \| \cdots \| M_n$ where $|M_i| = b \ (1 \le i \le n)$

  $V \leftarrow \mathtt{IV}$

  for $i = 1, \ldots, n$ **do**

    $V \leftarrow h(K, M_i \| V)$

Return V

- Given suitable pad() function and collision resistant h(), we can prove that H is collision resistant.

MD-compliant Padding

- Let D be some subset of $\{0,1\}^{2^b}$
- Let b be an integer called the block length
- Let $\mathrm{h}\colon \mathrm{K} \times \{0,1\}^{b+v} \mapsto \{0,1\}^{v}$
- Let s be in B if |s|=0 mod b
- A function "pad" from D to B is MD-compliant if for all $M, M_1, M_2 \in D$
  - M is a prefix of $pad(M)$
  - If $|M_1| = |M_2| \Rightarrow |pad(M_1)| = |pad(M_2)|$
  - $|M_1| \neq |M_2| \Rightarrow$ last blocks of $pad(M_1), pad(M_2)$ are equal → not

shapad(M)

$d \leftarrow (447 - |M|) \bmod 512$

$\ell \leftarrow$ be the 64-bit repsentation of size M

$y \leftarrow M \| 1 \| 0^d \| \ell$

MD- Security

Theorem 5.8 Let $h: \mathcal{K} \times \{0,1\}^{b+v} \to \{0,1\}^v$ be a family of functions and let $H: \mathcal{K} \times D \to \{0,1\}^v$ be built from h as described above. Suppose we are given an adversary A_H that attempts to find collisions in H. Then we can construct an adversary A_h that attempts to find collisions in h, and

$$\mathbf{Adv}_H^{\text{cr2-kk}}(A_H) \leq \mathbf{Adv}_h^{\text{cr2-kk}}(A_h) . \tag{5.9}$$

Furthermore, the running time of A_h is that of A_H plus the time to perform $(|\mathsf{pad}(x_1)| + |\mathsf{pad}(x_2)|)/b$ computations of h where (x_1, x_2) is the collision output by A_H. ■

Proof of Thm 5.8

Adversary $A_h(K)$

Run $A_H(K)$ to get its output (x_1, x_2) ← we use A_H

$y_1 \leftarrow \mathsf{pad}(x_1)$; $y_2 \leftarrow \mathsf{pad}(x_2)$

Parse y_1 as $M_{1,1} \| M_{1,2} \| \cdots \| M_{1,n[1]}$ where $|M_{1,i}| = b$ $(1 \le i \le n[1])$

Parse y_2 as $M_{2,1} \| M_{2,2} \| \cdots \| M_{2,n[2]}$ where $|M_{2,i}| = b$ $(1 \le i \le n[2])$

$V_{1,0} \leftarrow \mathrm{IV}$; $V_{2,0} \leftarrow \mathrm{IV}$

for $i = 1, \ldots, n[1]$ **do** $V_{1,i} \leftarrow h(K, M_{1,i} \| V_{1,i-1})$ → $H(x_1) = V_{1,n[1]}$

for $i = 1, \ldots, n[2]$ **do** $V_{2,i} \leftarrow h(K, M_{2,i} \| V_{2,i-1})$ → $H(x_2) = V_{2,n[2]}$

if $(V_{1,n[1]} \ne V_{2,n[2]}$ OR $x_1 = x_2)$ **return** FAIL → whether A_H is successful

if $|x_1| \ne |x_2|$ **then return** $(M_{1,n[1]} \| V_{1,n[1]-1}, M_{2,n[2]} \| V_{2,n[2]-1})$

$n \leftarrow n[1]$ // $n = n[1] = n[2]$ since $|x_1| = |x_2|$

for $i = n$ downto 1 **do**

  if $M_{1,i} \| V_{1,i-1} \ne M_{2,i} \| V_{2,i-1}$ **then return** $(M_{1,i} \| V_{1,i-1}, M_{2,i} \| V_{2,i-1})$

$V_{1,n[1]} = h(K, M_{1,n[1]} \| V_{1,n[1]-1})$

$V_{1,n[1]} = V_{2,n[2]}$

Proof of Thm 5.8

- We will show if A_H finds a collision then A_h finds a collision
- Note if $x_1 = x_2$ or $H(K, x_1) \neq H(K, x_2)$ then A_h fails
- If $|x_1| \neq |x_2|$ then $M_{1,n[1]}||V_{1,n[1]-1}$ and $M_{2,n[2]}||V_{2,n[2]-1}$ will be a collision for h
- Else, we need to have some $M_{1,i}||V_{1,i-1}$ and $M_{2,i}||V_{2,i-1}$ that forms a collision for h

We can conclude $Adv_H^{cr2-kk}(A_H) \leq Adv_h^{cr2-kk}(A_h)$