



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 build collision resistant hash function



MD Paradigm: Definitions

$H(K, M)$

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

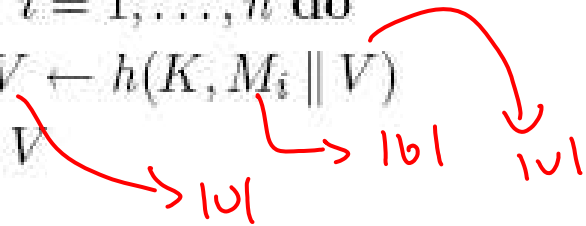
Parse y as $M_1 \parallel M_2 \parallel \dots \parallel M_n$ where $|M_i| = b$ ($1 \leq i \leq n$)

$V \leftarrow IV$

for $i = 1, \dots, n$ do

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

Return V



- Given suitable $\text{pad}()$ 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 $h: K \times \{0,1\}^{b+v} \mapsto \{0,1\}^v$
- Let s be in B if $|s| \equiv 0 \pmod b$
- 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)

$d \leftarrow (447 - |M|) \pmod{512}$

$f \leftarrow$ be the 64-bit representation of size M

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

MD- Security

Theorem 5.8 Let $h: \mathcal{K} \times \{0,1\}^{b+v} \rightarrow \{0,1\}^v$ be a family of functions and let $H: \mathcal{K} \times D \rightarrow \{0,1\}^v$ 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

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

Furthermore, the running time of A_h is that of A_H plus the time to perform $(|\text{pad}(x_1)| + |\text{pad}(x_2)|)/b$ 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

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

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

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

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

for $i = 1, \dots, n[1]$ do $V_{1,i} \leftarrow h(K, M_{1,i} \parallel V_{1,i-1})$

for $i = 1, \dots, n[2]$ do $V_{2,i} \leftarrow h(K, M_{2,i} \parallel V_{2,i-1})$

*$H(x_1) = \cup_{1, n[1]}$
 $H(x_2) = \cup_{2, n[2]}$
 \rightarrow whether A_H is successful*

if $(V_{1,n[1]} \neq V_{2,n[2]} \text{ OR } x_1 = x_2)$ return FAIL

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

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

for $i = n$ downto 1 do

if $M_{1,i} \parallel V_{1,i-1} \neq M_{2,i} \parallel V_{2,i-1}$ then return $(M_{1,i} \parallel V_{1,i-1}, M_{2,i} \parallel V_{2,i-1})$

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

$\cup_{2, n[2]} = \cup_{2, n[2]}$



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