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

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 $h: K \times \{0,1\}^{b+v} \rightarrow \{0,1\}^v$
- 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 $\text{pad}(M)$
  - If $|M_1| = |M_2|$ then $|\text{pad}(M_1)| = |\text{pad}(M_2)|$
  - $|M_1| \neq |M_2|$ implies the last blocks of $\text{pad}(M_1), \text{pad}(M_2)$ are equal
  \[ \text{pad}(M) \triangleq (4u7 - 1M_1) \mod 512 \]
  \( u \) be the 64-bit representation of $s$ with $m$ zeros
  \( y \) is the first 1110 bits of $y$
Theorem 5.8 Let $h: \mathcal{K} \times \{0,1\}^{b+u} \to \{0,1\}^u$ be a family of functions and let $H: \mathcal{K} \times \mathcal{D} \to \{0,1\}^u$ 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

$$\text{Adv}^{cr^2-kk}_H(A_H) \leq \text{Adv}^{cr^2-kk}_h(A_h).$$

(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 $A_H$. \hfill \blacksquare$
Proof of Thm 5.8

Adversary $A_h(K)$
Run $A_H(K)$ to get its output $(x_1, x_2)$
y_1 ← pad(x_1); y_2 ← pad(x_2)

Parse $y_1$ as $M_{1,1} \| M_{1,2} \| \cdots \| M_{1,n[1]}$ where $|M_{1,i}| = b (1 \leq i \leq n[1])$
Parse $y_2$ as $M_{2,1} \| M_{2,2} \| \cdots \| M_{2,n[2]}$ where $|M_{2,i}| = b (1 \leq i \leq n[2])$

$V_{1,0} ← IV; V_{2,0} ← IV$
for $i = 1, \ldots, n[1]$ do $V_{1,i} ← h(K, M_{1,i} \| V_{1,i-1})$
for $i = 1, \ldots, n[2]$ do $V_{2,i} ← h(K, M_{2,i} \| V_{2,i-1})$
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 $(M_{1,n[1]} \| V_{1,n[1]-1}, M_{2,n[2]} \| V_{2,n[2]-1})$

$n ← n[1]$ // $n = n[1] = n[2]$ since $|x_1| = |x_2|$ for $i = n$ downto 1 do
if $M_{1,i} \| V_{1,i-1} \neq M_{2,i} \| V_{2,i-1}$ then return $(M_{1,i} \| V_{1,i-1}, M_{2,i} \| V_{2,i-1})$

We use $A_H$

$H(x_1) = U_{1 \cup C_1}$
$H(x_2) = U_{2 \cup C_2}$
whether $A_H$ is successful

$V_{1,1} \cup C_1 = h(K, M_{1,1} \| V_{1,0})$
$V_{1,1} \cup C_2 = U_{2 \cup C_2}$
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 $M_{1,i} || V_{1,i1}$ and $M_{2,i} || V_{2,i1}$ that forms a collision for $h$.

We can conclude

$$\text{Adv}_{H}^{cr, 2-2k}(A_H) \leq \text{Adv}_{h}^{cr, 2-kk}(A_h)$$