Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1

Kazumaro Aoki and Yu Sasaki

NTT

Contents

- **Results**
- **Preparation**
- **Problem and idea**
- **Application to SHA-0 and SHA-1**
- **Conclusion**

Results

		[3]		Ours	
	type	step	comp	step	comp
SHA-0	PPI	50	2^{158}	52	$2^{151.2}$
	PI	49	2^{159}	52	$2^{156.6}$
SHA-1	PPI	45	2^{157}	48	$2^{156.7}$
	PI	44	2^{157}	48	$2^{159.3}$

PPI: pseudo-preimage, PI: preimage

- # of SHA-0/1 steps is 80.

Recent progress for (MitM) PI attack

Conversion from PPI attack to PI attack:

- ***MitM [Fact 9.99@HAC]***
- **Tree [Leurent@FSE08]**
- **P3graph [Cannière&Rechberger@C08]**

Finding a preimage of compression function:

- **FORK-256 [Saarinen@I07]**
- **MD4 [Leurent@FSE08]**
- ***One-block MD4 and MD5 [Ours@SAC08]***
- ⋮
- **Reduced SHA-0/1 [This talk]**

SHA-b compression function

CF: (H_i (160-bit), M_i (512-bit))$\mapsto$ H_{i+1} (160-bit)

Message schedule:

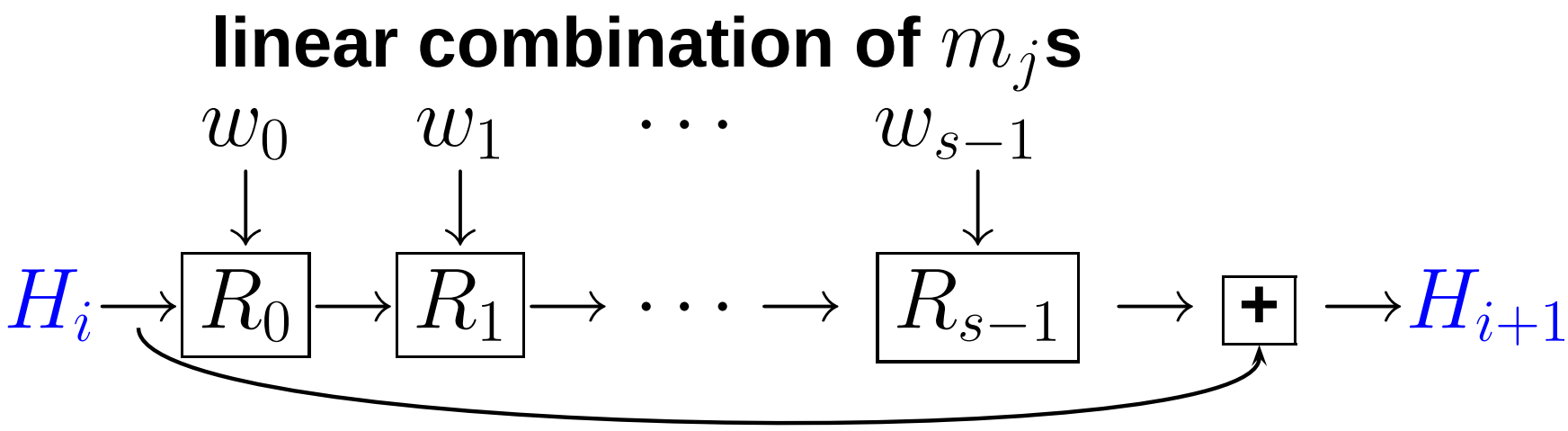
$$(m_0, m_1, \ldots, m_{15}) \leftarrow M_i \qquad (m_j \in \{0,1\}^{32})$$

$$\begin{cases} (w_0, w_1, \ldots, w_{15}) \leftarrow (m_0, m_1, \ldots, m_{15}) \\ w_j \leftarrow (\bigoplus_{k \in \{3,8,14,16\}} w_{j-k})^{\lll b} \quad (j \geq 16) \end{cases}$$

Iteration of step function ($s = 80$)

$$\begin{cases} p_0 \leftarrow H_i \\ p_{j+1} \leftarrow R_j(p_j, w_j) \quad j = 0, 1, \ldots, s-1 \\ H_{i+1} \leftarrow H_i + p_s \end{cases}$$

MitM attack for compression function



	$w_0, \ldots, w_{t-1}$	$w_t, \ldots, w_{s-1}$
m_v	**independent**	**may dependent**
m_u	**may dependent**	**independent**

meet between R_{t-1} and R_t

Q: How to find t and neutral words m_v and m_u?

Difficulties to find t, m_u, and m_v

- w_i is one of m_js for MD{4,5}.
  $\Rightarrow$ Their dependency is easy to analyze.
- Linear message schedule is adopted for SHA-0 $\Rightarrow$ How to analyze???

Presumable condition:

$$W_1 = [w_0, \ldots, w_{t-1}], \ \mathrm{rank}_M W_1 < 16 \ (\textbf{full})$$
$$W_2 = [w_t, \ldots, w_{s-1}], \ \mathrm{rank}_M W_2 < 16 \ (\textbf{full})$$

(This is the generalization of the case for MD{4,5}.)

How to decide neutral words

- **For MD$\{$4,5$\}$, neutral words are simply chosen from m_j which is not used. It can be interpreted using the notations from linear algebra,**

$$\langle [\overset{m_0}{0}, \ldots, \overset{m_{j-1}}{0}, \overset{m_j}{1}, \overset{m_{j+1}}{0}, \ldots, \overset{m_{15}}{0}]^T \rangle \subseteq \ker W_1$$

- **In the example from SHA-0 case,**

$$\ker W_1 = \langle [1,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0]^T \rangle$$
$$\ker W_2 = \langle [0,1,0,0,1,0,0,0,0,0,0,0,0,0,0,0]^T \rangle$$

1st chunk: $m_1 = m_4$

2nd chunk: $m_0 = m_2 = m_3$

How to decide neutral words (cont'd)

To see the another example of SHA-0, we may encounter

$$\ker W_1 = \left\langle [0,0,0,1,0,1,0,1,0,\mathbf{1},0,0,0,0,0,0]^T \right\rangle$$
$$\ker W_2 = \left\langle [0,0,0,0,0,0,1,0,1,\mathbf{1},0,0,0,1,1,1]^T \right\rangle$$

1st chunk: $m_6{=}m_8{=}m_9{=}m_{13}{=}m_{14}{=}m_{15}$

2nd chunk: $m_3 = m_5 = m_7 = m_9$

How to choose neutral words?

Idea

Apply linear transformation R to the input of CF: CF$(H, (RM'^T)^T)$, where $M^T = RM'^T$.
R should satisfy the followings.

- $$\begin{cases} (W_1 R)\mathbf{e}_0 = 0 \\ (W_2 R)\mathbf{e}_1 = 0 \end{cases}$$
  (Kernel vectors do not share 1 in the same position.)
  (Unit vector $\mathbf{e}_j = [0 \cdots \overset{j}{\overset{\smile}{1}} \cdots 0]^T$.)
- **Regular. (Converted message M' must be computed from the original message M.)**

Construction of R

$$\begin{cases} \ker W_1 &= \langle k_1 \rangle \\ \ker W_2 &= \langle k_2 \rangle \end{cases}, \quad R = T^{-1}B^{-1}S,$$

$$\left[\begin{array}{c} H \\ \hline \\ * \\ \\ \end{array}\right] = T[k_1\ k_2], \quad B = \left[\begin{array}{c|c} H^{-1} & 0 \\ \hline \\ 0 & \\ & E_{14} \end{array}\right],$$

$$S = \left[\begin{array}{c|c} BT[k_1\ k_2] & 0 \\ \hline \\ & E_{14} \end{array}\right].$$

Properties

Let $W_1' = W_1 R$ and $W_2' = W_2 R$, then we have

$$\begin{cases} W_1' \mathbf{e}_0 = W_1 R \mathbf{e}_0 = 0 \\ W_2' \mathbf{e}_1 = W_2 R \mathbf{e}_1 = 0 \end{cases}.$$

Regard $M' = [m_0', m_1', \ldots, m_{15}']$ as a message with

$$M^T = R M'^T.$$

$\Rightarrow m_0'$ and m_1' are natural words.

Hence, we can use MitM as the MD$\{$4,5$\}$ attacks.

Notes

- **The proposed method can be used with splice-and-cut, initial structure, partial-matching, and partial-fixing techniques used in the attacks against MD$\{4,5\}$.**
- **The same approach can be applied for SHA-1 using bit instead of word (32 bits).**

Application to SHA-{0,1}

of internal steps to attack SHA-{0,1}

	1C	IS	2C	PM+PF	total
SHA-0	15	2	21	14	52
SHA-1	15	4	15	14	48

1C: first chunk
2C: second chunk
IS: initial structure
PM: partial-matching
PF: partial-fixing

Conclusion

- **A similar MitM attack for MD$\{$4,5$\}$ can be established for SHA-b, whose message schedule is linear and not simply the permutations of message words.**
- **Attackable steps are increased.**
  SHA-0: 49$\longrightarrow$52, SHA-1: 44$\longrightarrow$48

Thank you for *your* attention!

Correction (page 72): *Memory complexities in Table 1 for [3] should be corrected to* “negligible”*.*

