Attacks for Finding Collision in Reduced Versions of 3-PASS and 4-PASS HAVAL

Her, Yong-Sork
Graduate School of Information Science and Electrical Engineering, Kyushu University

Sakurai, Kouichi
Faculty of Computer Science and Communication Engineering, Kyushu University

Kim, Shin-Hwan
School of Computer and Communication Engineering, Daegu University, KOREA

https://hdl.handle.net/2324/6794463

出版情報：Proc. of 2003 International Conference on Computers, Communications and Systems. 1, pp.75-78, 2003-02. BK21 IT Division, Daegu University
バージョン：
権利関係：

Attacks for Finding Collision in Reduced Versions of 3-PASS and 4-PASS HAVAL

Yong-Sork HER[†]**, Kouichi SAKURAI**[††]**, Shin-Hwan KIM**[†††]

[†]Graduate School of Information Science and Electrical Engineering
Kyushu University, JAPAN
e-mail : ysher@tcslab.csce.kyushu-u.ac.jp
[††]Faculty of Computer Science and Communication Engineering
Kyushu University, JAPAN
e-mail : sakurai@csce.kyushu-u.ac.jp
[†††]School of Computer and Communication Engineering,
Daegu University, KOREA
e-mail : shkim@daegu.ac.kr

Abstract

HAVAL is a hash function, which was proposed by Zheng *et al.* HAVAL has the first flexiable variable output lengths, namely 128, 160, 192, 224 or 256 bits, and consists of 3-pass, 4-pass and 5-pass. Differences of these types are the number of step, permutations order and boolean functions. P. R. Kasselman *et al.* and Park *et al.* found collisions of 3-pass HAVAL. In order to find a collision, they used two successive passes of 3-pass. To verify the security of HAVAL, we try to find a collision in two non-successive passes and 4-pass HAVAL. We can evaluate on the security of HAVAL through results of our attack. That is, we can know whether permutations order and boolean functions have an influence on the security of HAVAL or not. For this evaluation, we introduce the scheme of Park *et al.*

Keyword: Cryptography, Cryptographic hash function, HAVAL, MD4, Security

1. Introduction

1.1 Motivation

A cryptographic hash function can be divided two by the output length. One is a hash function with the fixed output length as MD4, MD5, SHA-1 and so on [2] [5]. The other is a hash function with a variable output length as HAVAL. HAVAL was proposed by Zheng et al. as the dedicated hash function of MD4 family [2]. HAVAL is first hash function with variable output lengths, namely 128, 160, 192, 224 or 256 bits, and consists of 3-pass, 4-pass and 5-pass. One pass of HAVAL has one boolean function, 32 constants (only, the first pass has not constants), one permutation and so on. The advantage of HAVAL can create five variable output lengths by 3-pass, 4-pass and 5-pass. So, HAVAL has 15 output-type. Moreover, HAVAL plays an important role as the standard of a hash function with a variable output length. For example, there is HAS-V[6] which was proposed by N. K. Park *et al.* Now, we explain previous attack models of HAVAL by Kass elman *et al.* and Park *et al.* P.R. Kasselman and W.T. Penzhorn found a collision of the last two passes of 3-pass HAVAL[3]. Park et al. found a collision of the first two passes and of the last two passes of 3-pass HAVAL [4]. In order to find a collision, they used the disadvantage of HAVAL which only one chaining variable of eight chaining variables is changed at next step. That is, the chaining variable is kept the value till +8th. Their attacks enables only when HAVAL has output length of 256 bits in two successive passes of 3-pass HAVAL. That is, their attacks are partially attacks. So, it is difficult to analyze the security of HAVAL only by results of their attacks. We need the result of the attack on 4-pass or 5-pass HAVAL for the exactly analysis on HAVAL. In this paper, we try to find a collision in two non-successive passes and 4-pass HAVAL (See table 1). Differences of 3-pass and 4-pass HAVAL are the number of step, permutations order and boolean functions. We choose <1,3> of 3-pass HAVAL to find whether a collision is found in condition of two non-successive passes or not. To find the relationship of permutations order and boolean functions on the security of HAVAL, we choose 4-pass HAVAL.

1.2 Our contribution

We try to find collisions in <1,2>, <2,3>, <3,4> of 4-pass HAVAL and <1,3> of 3-pass HAVAL. Previously, S.W.Park *et al.* found collisions in <1,2> and <2,3> of 3-pass HAVAL. Table 2 shows our results on attack of HAVAL. In this paper, we analyze the disadvantage of HAVAL through the finding of a collision of 4-pass HAVAL and the comparison on attacks of 3-pass HAVAL and 4-pass HAVAL.

In this paper, our contribution is large divided two. First, we attempt the attack of <1,3> of 3-pass HAVAL. The previous attack method by Kasselman *et al.* and Park *et al.* used successive two passes in 3-pass HAVAL. But, we try to the attack of <1,3> of 3-pass HAVAL that is not successive passes. Second, we analyze the disadvantage of HAVAL through results of attack of 4-pass HAVAL. The common point in reduced two round of HAVAL is the derived equation based on the changed variable in next step. HAVAL consist of three kinds, that is, 3-pass, 4-pass and 5-pass HAVAL. The differences of each HAVAL are the sequence of permutation and the number of boolean function. We find a factor that have an influence on attack of HAVAL through the finding of a collision on 4-pass HAVAL. If we find a collision of 4-pass HAVAL, we can know that the fourth boolean function is not secure, too. To conclude, the sequence of permutation has an influence on attack of HAVAL. Especially, when we compare <2,3>of 3-pass HAVAL with <2,3> of 4-pass HAVAL, we can know that it is different to the number of collisions. This is the result that is caused by the permutation sequence. In case of <1,2> of 3-pass HAVAL and <1,2> of 4-pass HAVAL, the number of collisions is the same. In case of the boolean function, it is used three boolean functions in 3-pass HAVAL, and add to one boolean function in 4-pass HAVAL. Although the boolean function is very important factor to keep the security of HAVAL, we could find the collision of 4-pass HAVAL. To raise the efficiency and the fairness of the verification on the security of HAVAL, we attempted the attack of three kinds in 4-pass HAVAL. When we see this result, the finding of a collision on <1,2>, <2,3>, <3,4> of 4-pass HAVAL can be shown the possibility of the attack on 5-pass HAVAL. In HAVAL, only one chaining variable of eight chaining variables is changed at next step. This is the disadvantage of HAVAL.

Table 1. Attacks of HAVAL

	3-pass HAVAL	**4-pass HAVAL**	**5-pass HAVAL**
Penzhorn	<2,3>	Nothing	Nothing
Park *et.al*	<1,2>,<2,3>	Nothing	Nothing
Our attacks	<1,3>	<1,2>,<2,3> <3,4>	

Table 2. Results of collisions

3-pass HAVAL	**Collisions**	**Probability**
<1,2>	12 pairs	0.375 %
<2,3>	9 pairs	0.28 %
<1,3>	6 pairs	0.186 %
4-pass HAVAL	**Collisions**	**Probability**
<1,2>	12 pairs	0.375 %
<2,3>	5 pairs	0.156 %
<3,4>	13 pairs	0.406 %

(<X,Y>: X-pass and X-pass)

2. Construction of HAVAL

There are three kinds of HAVAL. That is 3-pass of 96 steps, 4-pass of 128 steps and 5-pass of 160 steps. HAVAL has a message block of 1024-bit and eight 32-bit chaining variables, twice those of MD5 [9]. The important character of HAVAL is first hash function with variable output length.

- **Initial value**

$A_0 = 0xEC\,4E6C89$, $B_0 = 0x082\,EFA\,98$, $C_0 = 0x299\,F31D0$

$D_0 = 0xA4093822$, $E_0 = 0x03707344$, $F_0 = 0x13198\,A2E$

$G_0 = 0x85\,A308\,D3$, $H_0 = 0x243\,F6A88$

- **Boolean functions** (See Table 3)

We describe the step function of the HAVAL. Let $T_{i,j}\,(j = 0,\ldots,7)$ be the input of the step function at step i.

$$P = \begin{cases} f_r\,(P_{3,r}\,(T_{i,6}, T_{i,5}, T_{i,4}, T_{i,3}, T_{i,2}, T_{i,1}, T_{i,0})),\ for\,3 - pass \\ f_r\,(P_{4,r}\,(T_{i,6}, T_{i,5}, T_{i,4}, T_{i,3}, T_{i,2}, T_{i,1}, T_{i,0})),\ for\,4 - pass \\ f_r\,(P_{5,r}\,(T_{i,6}, T_{i,5}, T_{i,4}, T_{i,3}, T_{i,2}, T_{i,1}, T_{i,0})),\ for\,5 - pass \end{cases}$$

$$R = P^{>>7} + T_{i,7}{}^{>>11} + W_{ord_r(i)} + K_i$$

$$T_{i+1,7} = T_{i,6}; T_{i+1,6} = T_{i,5}; T_{i+1,5} = T_{i,4}; T_{i+1,4} = T_{i,3};$$

$$T_{i+1,3} = T_{i,2}; T_{i+1,2} = T_{i,1}; T_{i+1,1} = T_{i,0}; T_{i+1,0} = R;$$

, where $W_{ord_r(i)}$ denotes the world processing order.

3. Attack of <1, 3> pass on 3-pass HAVAL

In this paper, we describes the attack method of <1,3> pass on 3-pass HAVAL. The other attack methods are skipped, and the only results are shown in the Section 4. To find a collision in <1,3> pass of 3-passHAVAL, we select the message block X_{29} .The message block X_{29} is used in step 30 of the first pass and step 73 of the third pass. We define the difference X and $\overline{X}$ as follows.

$$\Delta X = X - \overline{X} \pmod{2^{32}}$$

$A_i, B_i, C_i, D_i, E_i, F_i, G_i$ and H_i are chaining variables in step i, and a message block is $X = (X_0, X_1, \ldots, X_{31})$. $\overline{A}_i, \overline{B}_i, \overline{C}_i, \overline{D}_i, \overline{E}_i, \overline{F}_i\ \overline{G}_i$ and $\overline{H}_i$ in step i are chaining variables for a message block $\overline{X} = (\overline{X}_0, \overline{X}_1, \ldots, \overline{X}_{31})$.

- **Our goal**

In order to find a collision in the first and the last passes of 3-pass HAVAL, we must find two distinct message blocks X and $\overline{X}$. Then, X and $\overline{X}$ must same the chaining variable between step 32 and step 63.

Table 3. Boolean Functions of HAVAL

$f_1(x_6, x_5, x_4, x_3, x_2, x_1, x_0)$	$x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_0x_1 \oplus x_0$
$f_2(x_6, x_5, x_4, x_3, x_2, x_1, x_0)$	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5 \oplus x_0x_2 \oplus x_0$
$f_3(x_6, x_5, x_4, x_3, x_2, x_1, x_0)$	$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_0x_3 \oplus x_0$
$f_4(x_6, x_5, x_4, x_3, x_2, x_1, x_0)$	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6$ $\oplus x_4x_5 \oplus x_4x_6 \oplus x_0x_4 \oplus x_0$
$f_5(x_6, x_5, x_4, x_3, x_2, x_1, x_0)$	$x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_0x_1x_2x_3 \oplus x_0x_5 \oplus x_0$

($\oplus$: *bitwise exclusive OR*)

For example,

$$A_{32} = \overline{A}_{32}, B_{32} = \overline{B}_{32}, C_{32} = \overline{C}_{32}, D_{32} = \overline{D}_{32},$$

$$E_{32} = \overline{E}_{32}, F_{32} = \overline{F}_{32}, G_{32} = \overline{G}_{32}, H_{32} = \overline{H}_{32}$$

To finding a collision in <1,3> pass of HAVAL, we should be satisfied the equation (1).

$$A_{73} = \overline{A}_{73}, B_{73} = \overline{B}_{73}, C_{73} = \overline{C}_{73}, D_{73} = \overline{D}_{73}, \qquad (1)$$

$$E_{73} = \overline{E}_{73}, F_{73} = \overline{F}_{73}, G_{73} = \overline{G}_{73}, H_{73} = \overline{H}_{73}$$

■ Conditions

From the equation (1), we can get the following equation.

$$\Delta A_{73} = \Delta A_{72}, \Delta B_{73} = \Delta B_{71}, \Delta C_{73} = \Delta C_{70}, \Delta D_{73} = \Delta D_{69}$$ A

$$\Delta E_{73} = \Delta E_{68}, \Delta F_{73} = \Delta F_{67}, \Delta G_{73} = \Delta G_{66}$$

nd then, we can obtain the following equation.

$$\Delta A_{72} = 0, \Delta B_{71} = 0, \Delta C_{70} = 0, \Delta D_{69} = 0$$

$$\Delta E_{68} = 0, \Delta F_{67} = 0, \Delta G_{66} = 0, \Delta H_{73} = 0$$

The standard message word is X_{29} which is used in step 30 and step 73. We can get as follows.

$$X_{29} \neq \overline{X}_{29}, \quad X_i = \overline{X}_i \quad (i \neq 29)$$

Table 4 shows the chaining variables and message words that are employed at step 30, 31, 32, 65, 66, 67, 68, 69, 70, 71, 72, 73. The boxed variables represent the chaining varia ble which is updated at each step.

■ Equations (Step30 – Step73)

- Step 30

$$C_{30} = (F_{29}G_{29} \oplus B_{29}D_{29} \oplus A_{29}E_{29} \oplus H_{29}F_{29} \oplus H_{29})^{>>7} + C_{29}^{>>11} + X_{29}$$

$$\overline{C}_{30} = (\overline{F}_{29}\overline{G}_{29} \oplus \overline{B}_{29}\overline{D}_{29} \oplus \overline{A}_{29}\overline{E}_{29} \oplus \overline{H}_{29}\overline{F} \oplus \overline{H}_{29})^{>>7} + \overline{C}_{29}^{>>11} + \overline{X}_{29}$$

Since

$$A_{29} = \overline{A}_{29}, B_{29} = \overline{B}_{29}, C_{29} = \overline{C}_{29}, D_{29} = \overline{D}_{29},$$

$$E_{29} = \overline{E}_{29}, F_{29} = \overline{F}_{29}, G_{29} = \overline{G}_{29}, H_{29} = \overline{H}_{29},$$

And then, we can get the following equation:

$$\Delta C_{30} = \Delta X_{29} \neq 0$$

- Step 31

$$B_{31} = (E_{30}F_{30} \oplus A_{30}C_{30} \oplus H_{30}D_{30} \oplus F_{30}E_{30} \oplus G_{30})^{>>7} + B_{30}^{>>11} + X_{30}$$

$$\overline{B}_{31} = (\overline{E}_{30}\overline{F}_{30} \oplus \overline{A}_{30}\overline{C}_{30} \oplus \overline{H}_{30}\overline{D}_{30} \oplus \overline{F}_{30}\overline{E}_{30} \oplus \overline{G}_{30})^{>>7} + \overline{B}_{30}^{>>11} + \overline{X}_{30}$$

$$B_{31} - \overline{B}_{31} = (E_{30}F_{30} \oplus A_{30}C_{30} \oplus H_{30}D_{30} \oplus F_{30}E_{30} \oplus G_{30})^{>>7}$$

$$-(E_{30}F_{30} \oplus A_{30}\overline{C}_{30} \oplus H_{30}D_{30} \oplus F_{30}E_{30} \oplus G_{30})^{>>7}$$

- Step 32

$$\Delta A_{32} = 0$$

$$\Leftrightarrow D_{31}E_{31} \oplus H_{31}B_{31} \oplus G_{31}C_{31} \oplus F_{31}D_{31} \oplus F_{31}$$

$$= D_{31}E_{31} \oplus H_{31}\overline{B}_{31} \oplus G_{31}\overline{C}_{31} \oplus F_{31}D_{31} \oplus F_{31}$$

$$\Leftrightarrow G_{31} \bullet (C_{31} \oplus \overline{C}_{31}) = H_{31} \bullet (B_{31} \oplus \overline{B}_{31})$$

- From Step 65 to Step 73

$$C_{30} - \overline{C}_{30} = X_{29} - \overline{X}_{29} \qquad (2)$$

$$B_{31} - \overline{B}_{31} =$$
$$(E_{28}F_{27} \oplus A_{24}C_{\underline{30}} \oplus H_{25}D_{29} \oplus F_{27}E_{28} \oplus G_{26})^{>>7} \qquad (3)$$
$$-(E_{28}F_{27} \oplus A_{24}C_{30} \oplus H_{25}D_{29} \oplus F_{27}E_{28} \oplus G_{26})^{>>7}$$

$$(C_{30} \oplus \overline{C}_{30})G_{26} = (B_{31} \oplus \overline{B}_{31})H_{25} \qquad (4)$$

$$(C_{30} \oplus \overline{C}_{30})F_{27} = (B_{31} \oplus \overline{B}_{31})E_{28} \qquad (5)$$

$$(H_{65} \oplus \overline{H}_{65})(G_{26}D_{29}) \oplus F_{27}(C_{30} \oplus \overline{C}_{30}) = E_{28}(B_{31} \oplus \overline{B}_{31}) \qquad (6)$$

$$(C_{30} \oplus \overline{C}_{30})(G_{66}F_{27} \oplus F_{27}) \oplus E_{28}(B_{31} \oplus \overline{B}_{31}) \qquad (7)$$
$$= C_{30}H_{65} \oplus \overline{C}_{30}\overline{H}_{65}$$

$$(F_{67}E_{68} \oplus G_{66} \oplus E_{28})(B_{31} \oplus \overline{B}_{31}) = C_{30}H_{65} \oplus \overline{C}_{30}\overline{H}_{65} \qquad (8)$$

$$(B_{31} \oplus \overline{B}_{31})G_{66} = C_{30}H_{65} \oplus \overline{C}_{30}\overline{H}_{65} \qquad (9)$$

$$(D_{69}C_{30}H_{65} \oplus B_{31}G_{66} \oplus A_{32}F_{67} \oplus H_{65}E_{68} \oplus H_{65}C_{30} \oplus C_{30})^{>>7}$$
$$+C_{30}^{>>11} \qquad (10)$$
$$=(\overline{D}_{69}\overline{C}_{30}\overline{H}_{65} \oplus \overline{B}_{31}\overline{G}_{66} \oplus \overline{A}_{32}\overline{F}_{67} \oplus \overline{H}_{65}\overline{E}_{68} \oplus \overline{H}_{65}\overline{C}_{30} \oplus \overline{C}_{30})^{>>7}$$
$$+\overline{C}_{30}^{>>11}$$

$$H_{65}^{>>11} + X_{29} = H_{65}^{>>11} + X_{29} \qquad (11)$$

Table 4. Chaining variable for the finding collision on <1,3> pass of 3-pass HAVAL

Step	A	B	C	D	E	F	G	H	X
30	A_{30}	B_{30}	$\boxed{C_{30}}$	D_{30}	E_{30}	F_{30}	G_{30}	H_{30}	X_{29}
31	A_{31}	$\boxed{B_{31}}$	C_{31}	D_{31}	E_{31}	F_{31}	G_{31}	H_{31}	X_{30}
32	$\boxed{A_{32}}$	B_{32}	C_{32}	D_{32}	E_{32}	F_{32}	G_{32}	H_{32}	X_{31}
65	A_{65}	B_{65}	C_{65}	D_{65}	E_{65}	F_{65}	G_{65}	$\boxed{H_{65}}$	X_{19}
66	A_{66}	B_{66}	C_{66}	D_{66}	E_{66}	F_{66}	$\boxed{G_{66}}$	H_{66}	X_{9}
67	A_{67}	B_{67}	C_{67}	D_{67}	E_{67}	$\boxed{F_{67}}$	G_{67}	H_{67}	X_{4}
68	A_{68}	B_{68}	C_{68}	D_{68}	$\boxed{E_{68}}$	F_{68}	G_{68}	H_{68}	X_{20}
69	A_{69}	B_{69}	C_{69}	$\boxed{D_{69}}$	E_{69}	F_{69}	G_{69}	H_{69}	X_{28}
70	A_{70}	B_{70}	$\boxed{C_{70}}$	D_{70}	E_{70}	F_{70}	G_{70}	H_{70}	X_{17}
71	A_{71}	$\boxed{B_{71}}$	C_{71}	D_{71}	E_{71}	F_{71}	G_{71}	H_{71}	X_{8}
72	$\boxed{A_{72}}$	B_{72}	C_{72}	D_{72}	E_{72}	F_{72}	G_{72}	H_{72}	X_{22}
73	A_{73}	B_{73}	C_{73}	D_{73}	E_{73}	F_{73}	G_{73}	$\boxed{H_{73}}$	X_{29}

Table 5. The results of equations

A_{24}	$0x=80$	$\overline{A}_{24}$	
H_{25}	0	$\overline{H}_{25}$	
G_{26}	0	$\overline{G}_{26}$	
F_{27}	0	$\overline{F}_{27}$	
E_{28}	0	$\overline{E}_{28}$	
D_{29}	0	$\overline{D}_{29}$	
C_{30}	$0xffffffff$	$\overline{C}_{30}$	0
B_{31}	0	$\overline{B}_{31}$	$0xffffffff$
A_{32}	0	$\overline{A}_{32}$	
H_{65}	0	$\overline{H}_{65}$	$0xffffffff$
G_{66}	0	$\overline{G}_{66}$	
F_{67}	0	$\overline{F}_{67}$	
E_{68}	0	$\overline{E}_{68}$	
D_{69}	0	$\overline{D}_{69}$	
C_{70}	$0xfffffffe$	$\overline{C}_{70}$	

Table 6. Collisions of <1,3> pass on 3-pass HAVAL

$X_i(\overline{X_i})$	The values of $X_i(\overline{X_i})$	$X_i(\overline{X_i})$	The values of $X_i(\overline{X_i})$
$X_4(\overline{X_4})$	Ox3a2e4fdd	$X_{19}(\overline{X_{19}})$	Ox63cf2ac7
$X_9(\overline{X_9})$	Oxd50d9fed	$X_{20}(\overline{X_{20}})$	Ox d79f7a10
$X_{17}(\overline{X_{17}})$	Ox4724c7df	$X_{28}(\overline{X_{28}})$	Ox35be86e8

4. Results of attacks on 4-pass HAVAL

In this section, we show only results of attacks on 4-pass HAVAL

Table 7. Collisions of <1,2> pass on 4-pass HAVAL

$X_i(\overline{X_i})$	The values of $X_i(\overline{X_i})$	$X_i(\overline{X_i})$	The values of $X_i(\overline{X_i})$
$X_5(\overline{X_5})$	Oxbad7de19	$X_{26}(\overline{X_{26}})$	Ox41ab9930
$X_{14}(\overline{X_{14}})$	Oxc72fec89	$X_{27}(\overline{X_{27}})$	Oxb9107999
$X_{18}(\overline{X_{18}})$	Oxcb16f394	$X_{28}(\overline{X_{28}})$	Ox260791c2
$X_{23}(\overline{X_{23}})$	Ox2d8e2ef4		Ox 260791c3
$X_{24}(\overline{X_{24}})$	Oxcd6f4a4a	$X_{29}(\overline{X_{29}})$	Ox92102afd
$X_{25}(\overline{X_{25}})$	Ox4a45d2f3	$X_{30}(\overline{X_{30}})$	Oxf0000000

Table 8. Collisions of <2,3> pass on 4-pass HAVAL

$X_i(\overline{X_i})$	The values of $X_i(\overline{X_i})$	$X_i(\overline{X_i})$	The values of $X_i(\overline{X_i})$
$X_6(\overline{X_6})$	Oxa7891c3e	$X_{15}(\overline{X_{15}})$	Ox9a31cbb1
$X_9(\overline{X_9})$	Oxbe38682c	$X_{24}(\overline{X_{24}})$	Ox73e6fac2
$X_{13}(\overline{X_{13}})$	Oxe34933c9		

Table 9. Collisions of <3,4> pass on 4-pass HAVAL

$X_i(\overline{X_i})$	The values of $X_i(\overline{X_i})$	$X_i(\overline{X_i})$	The values of $X_i(\overline{X_i})$
$X_0(\overline{X_0})$	Oxc470b767	$X_{13}(\overline{X_{13}})$	Ox4c11ebef
$X_2(\overline{X_2})$	Ox93db30a3	$X_{14}(\overline{X_{14}})$	Ox94b44651
$X_4(\overline{X_4})$	Oxd76a7988	$X_{21}(\overline{X_{21}})$	Oxd4563aa3
$X_5(\overline{X_5})$	Ox502945cd	$X_{23}(\overline{X_{23}})$	Ox31a3c1ea
$X_6(\overline{X_6})$	Ox9c9043d6	$X_{24}(\overline{X_{24}})$	Ox85cdac7e
$X_{10}(\overline{X_{10}})$	Ox8be7ce0a	$X_{27}(\overline{X_{27}})$	Ox38d166c
$X_{11}(\overline{X_{11}})$	Ox64786ce2		

5. Conclusion

In this paper, we attempted attack methods of <1,3> of 3-pass HAVAL and 4-pass HAVAL with reduced 2-round based on the attack method of 3-pass HAVAL. HAVAL was first cryptographic hash function which has a variable output length. But, HAVAL has the disadvantage in step computation. That is, only one chaining variable of eight chaining variables is updated at each step. In reduced two-round of 3-pass and 4-pass HAVAL, it is not collision-free. The attack method will an influence reduced versions of 5-pass HAVAL

Acknowledgments

The first author has been supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 (Head of Researchers: Prof. Hiroto Yasuura, System LSI Research center, Kyushu University) of the Ministry of Education, Science, Sports and Culture (MEXT)

REFERENCES

[1] Y.Zheng, J. Pieprzyk and J. Seberry ”HAVAL-A One-Way Hashing Algorithm with Variable Length of Output” Auscrypt’92, LNCS 718, pp83-104, Springer, 1992

[2] Ronald L.Rivest ”The message digest algorithm” crypto’90 LNCS 537, pp303-311, Springe-Verlag, 1991

[3] P.R. Kasselman, W.T.Penzhorn ”Cryptanalysis of reduced version of HAVAL” 6th ELECTRONICS LETTERS, vol.36, No.1, Jan.2000

[4] S.W.Park, S.H. Sung, S.T. Chee and J.G Lim ”On the Security of Reduced Versions of 3-Pass HAVAL” ACISP 2002, LNCS 2384, pp 406-pp419, Springer-Verlag, 2002

[5] A.J. Menzs, P.C. Van Oorshot, S.A.Vanstone ”Handbook of Applied Cryptography” CRC Press, 1997

[6] N.K. Park, J.H. Hwang, P.J.Lee ”HAS-V: A new hash function with variable output length” SAC2000, LNCS2012, pp202-216, 2001

[7] H.Dobbertin ”Cryptanalysis of MD4” Fast Software Encryption, LNCS 1039, Springer-Verlag, pp53-69, 1996.

[8] B.Preneel ”Analysis and design of cryptographic hash functions” PhD thesis, Katholieke Universiteit Leuven, 1993

[9] B.Schneier ”Applied Cryptography” 2nd edition John Wiley & Sons Press, 1996

[10] H.Kuwakado, H. Tanaka ”New algorithm for finding preimages in a reduced version on the MD4 compression function” IEICE trans, Vol. E83-A, No.1. Jan. 2000.