Cryptanalysis of 4-Pass HAVAL*

Zhangyi Wang[1], Huanguo Zhang[1], Zhongping Qin [2], Qingshu Meng[1]

1. School of Computer Science, Wuhan University, Wuhan, China;
2. School of software, Huazhong University of Science and Technology, Wuhan, China

Email: wzy@whu.edu.cn

Abstract. HAVAL is a cryptographic hash function proposed by Zheng *et al*. Van Rompay *et al* and Wang *et al* found collisions of full 3-Pass HAVAL. In this paper, we study the security of 4-Pass HAVAL. By analyzing the expanding of subtraction difference and differential characters of Boolean functions, we find collisions of full versions of 4-Pass HAVAL. The form of collisions is similar to the two-block collisions of MD5 proposed by Wang *et al*. With fixed carry method instead of multi-message modification, the computational complexity of the attack is about 2^{30}-2^{32} for the first block and 2^{27}-2^{29} for the second block. We use this method to find collisions of 4-Pass HAVAL in 3-4 hour on a common PC.

Keywords. HAVAL, differential attack, collision

1. Introduction

Cryptographic hash functions are important cryptographic primitives and used in authentication, non-repudiation, electronic commerce and encryption schemes. Cryptographic hash functions have to satisfy requirements of onewayness and collision resistance[1-3]. One such family of hash functions is the MDx family. This family includes hash functions such as

*This work was supported by the National Natural Science Foundation of China (69973034，60373087) and the Ph.D. Programs Foundation of Ministry of Education of China（20020486046）

MD5, SHA and HAVAL.

HAVAL [2] is a cryptographic hash function proposed by Zheng *et al* in 1992. HAVAL compresses a message of arbitrary length into a hash value of 128,160,192,224, or 256 bits. The specification of HAVAL allows for a trade-off between efficiency and security margin by means of a parameter, the number of passes, which can be chosen equal to 3,4,or 5. Her *et al* [4], Kasselman *et al* [5], Park *et al* [6] found collisions when the number of passes is reduced to two. Yoshida *et al* [7] gave a theoretic differentials attack with probabilities $>2^{-125}$ for the full 4-Pass HAVAL and $>2^{-168}$ for the full 5-Pass HAVAL. Van Rompay *et al* [8] found collisions of full 3-Pass HAVAL in ASIACRYPT2003 while the complexity is about 2^{29}. In 2004, Wang *et al* [9] proposed another attack to full 3-Pass HAVAL which only need 2^7 computations of 3-Pass HAVAL.

In this paper we show a cryptanalysis of full version of 4-Pass HAVAL, using the correct initial value as specified for the algorithm. This attack also works for all possible output lengths of the algorithm. The form of collisions is similar to the two-block collisions of MD5 proposed by Wang *et al* [10]. The computational complexity of the attack is about 2^{30}-2^{32} for the first block and 2^{27}-2^{29} for the second block with fixed carry method instead of multi-message modification. We use this method to collisions of 4-Pass HAVAL in 3-4 hour using a common PC.

Note: An attack on 4 and 5 passes of Haval was presented at FSE 2006 (FSE 2006 : "Cryptanalysis of the Full HAVAL with 4 and 5 Passes" by H.Yu, X.Wang, A.Yun, and S.Park) , which provides a stronger attack on HAVAL than this paper.

We were ill-informed about the result already obtained on FSE2006 as well as the specific method of this research when independently carrying on our research. In fact until now we still can't retrieve the corresponding abstract or the full text document from the FSE2006 homepage and the LNCS database of Springer Press.

Though acknowledging that the publication of the result on FSE2006 is prior to ours and the specific attack result is also superior to ours, we are still willing to share our method in this paper with everyone on eprint. My email address: wzy@whu.edu.cn

2. Description of HAVAL

The hash function HAVAL is defined as an iteration of a compression function as follows: $H_0 = IV, H_j = HAVAL(H_{j-1}, M_j)$, where $1 \le j \le t$. The message is divided into *t* blocks M_j of 1024 bits each. The 256 bits input is loaded into eight registers (A, B, C, D, E, F, G, H) and the 1024 bits message block M_i is divided into 32 words$\{X_0, X_1, \ldots, X_{31}\}$. The compression function of HAVAL is composed of addition mod 2^{32}, Boolean functions and shift rotation. The processing of 4-Pass HAVAL involves 128 steps, and each step performs above three

basic operations.

For description convenience, we use following notation:

1.（A_i ,B_i ,C_i ,D_i ,E_i ,F_i ,G_i ,H_i）respectively denote the outputs of the i-th step, $i \in [0,127]$;

2. $X_{i,j}$ represent the j-th bit of X_i，where the least significant bit is the 0-th bit，the most significant bit is the 31-th bit ;

3. $X_{i,(j,k)}$ denotes keep from the j-th to k-th bit of X_i, other bits set to 0. Then the whole 32 bit of X_i can be represented as composing of blocks，for example：$X_i = X_{i,(31,k)} + X_{i,(k-1,0)}$;

4. $X_{i,[j,k]}$ denotes the j-th, (j+1)-th,… , (k-1)-th, k-th bit of X_i ;

5. $X^{>>k}$ denotes the result of shift-right rotation of X (32 bits).

For example the first step of the compression function update the value of the A register in the following manner:

$$A_0 = F_1 (\text{IV-B, IV-C, IV-D, IV-E, IV-F, IV-G, IV-H})^{>>7} + \text{IV-A}^{>>11} + X_0 ,$$

where F_i is a Boolean function used in the *i*-th pass.

3. Differential Analysis of HAVAL

For the 4-Pass HAVAL, four functions are employed by each pass, and each pass has a different permutation on coordinates. The differential characters of Boolean functions with permutation in each pass are list as follows: ‘0’ denotes input without difference, ‘1’ denotes input with difference, and $\triangle F_i$ denote output differential. For example:

$$\triangle F_1(0,0,0,0,0,0,1) = F_1(x_6, x_5, x_4, x_3, x_2, x_1, x_0) \oplus F_1(x_6, x_5, x_4, x_3, x_2, x_1, x_0 \oplus 1)$$

Pass1:

$$f_1(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_1 x_4 \oplus x_2 x_5 \oplus x_3 x_6 \oplus x_0 x_1 \oplus x_0$$

$$\phi_{4,1}(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = (x_2, x_6, x_1, x_4, x_5, x_3, x_0)$$

the composition of f_1 and $\phi_{4,1}$ is $F_1 = f_1 \circ \phi_{4,1}$, then

$$F_1(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = f_1(\phi_{4,1}(x_6, x_5, x_4, x_3, x_2, x_1, x_0)) = x_1 x_3 \oplus x_5 x_6 \oplus x_2 x_4 \oplus x_0 x_3 \oplus x_0$$

The differential characters of $F_1 = f_1 \circ \phi_{4,1}$ is:

$$\triangle F_1(0,0,0,0,0,0,1) = x_3 \oplus 1 \qquad \triangle F_1(0,0,0,0,1,0,1) = x_3 \oplus x_4 \oplus 1$$
$$\triangle F_1(0,0,0,0,0,1,0) = x_3 \qquad \triangle F_1(0,0,0,1,0,1,0) = x_0 \oplus x_1 \oplus x_3 \oplus 1$$
$$\triangle F_1(0,0,0,0,1,0,0) = x_4 \qquad \triangle F_1(0,0,1,0,1,0,0) = x_2 \oplus x_4 \oplus 1$$
$$\triangle F_1(0,0,0,1,0,0,0) = x_0 \oplus x_1 \qquad \triangle F_1(0,1,0,1,0,0,0) = x_0 \oplus x_1 \oplus x_6$$
$$\triangle F_1(0,0,1,0,0,0,0) = x_2 \qquad \triangle F_1(1,0,1,0,0,0,0) = x_2 \oplus x_5$$
$$\triangle F_1(0,1,0,0,0,0,0) = x_6$$
$$\triangle F_1(1,0,0,0,0,0,0) = x_5$$

Pass2:

$$f_2(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5 \oplus x_0x_2 \oplus x_0$$

$$\phi_{4,2}(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = (x_3,x_5,x_2,x_0,x_1,x_6,x_4)$$

the composition of f_2 and $\phi_{4,2}$ is $F_2 = f_2 \circ \phi_{4,2}$, then

$$F_2(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = f_2(\phi_{4,2}(x_6,x_5,x_4,x_3,x_2,x_1,x_0))$$
$$= x_0x_1x_6 \oplus x_1x_2x_5 \oplus x_1x_6 \oplus x_2x_6 \oplus x_1x_3 \oplus x_0x_5 \oplus x_2x_5 \oplus x_1x_4 \oplus x_4$$

The differential characters of $F_2 = f_2 \circ \phi_{4,2}$ is:

$$\triangle F_2(0,0,0,0,0,0,1) = x_1x_6 \oplus x_5$$
$$\triangle F_2(0,0,0,0,0,1,0) = x_0x_6 \oplus x_2x_5 \oplus x_3 \oplus x_4 \oplus x_6$$
$$\triangle F_2(0,0,0,0,1,0,0) = x_1x_5 \oplus x_5 \oplus x_6$$
$$\triangle F_2(0,0,0,1,0,0,0) = x_1$$
$$\triangle F_2(0,0,1,0,0,0,0) = x_1 \oplus 1$$
$$\triangle F_2(0,1,0,0,0,0,0) = x_1x_2 \oplus x_0 \oplus x_2$$
$$\triangle F_2(1,0,0,0,0,0,0) = x_0x_1 \oplus x_1 \oplus x_2$$

Pass3:

$$f_3(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_0x_3 \oplus x_0$$

$$\phi_{4,3}(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = (x_1,x_4,x_3,x_6,x_0,x_2,x_5)$$

the composition of f_3 and $\phi_{4,3}$ is $F_3 = f_3 \circ \phi_{4,3}$, then

$$F_3(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = f_3(\phi_{4,3}(x_6,x_5,x_4,x_3,x_2,x_1,x_0))$$
$$= x_0x_2x_6 \oplus x_2x_3 \oplus x_0x_4 \oplus x_1x_6 \oplus x_5x_6 \oplus x_5$$

The differential characters of $F_3 = f_3 \circ \phi_{4,3}$ is:

$$\triangle F_3(0,0,0,0,0,0,1) = x_2x_6 \oplus x_4$$
$$\triangle F_3(0,0,0,0,0,1,0) = x_6$$
$$\triangle F_3(0,0,0,0,1,0,0) = x_0x_6 \oplus x_3$$
$$\triangle F_3(0,0,0,1,0,0,0) = x_2$$
$$\triangle F_3(0,0,1,0,0,0,0) = x_0$$
$$\triangle F_3(0,1,0,0,0,0,0) = x_6 \oplus 1$$
$$\triangle F_3(1,0,0,0,0,0,0) = x_0x_2 \oplus x_1 \oplus x_5$$

Pass4:

$$f_4(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus$$
$$x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_0x_4 \oplus x_0$$

$$\phi_{4,4}(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = (x_6,x_4,x_0,x_5,x_2,x_1,x_3)$$

the composition of f_4 and $\phi_{4,4}$ is $F_4 = f_4 \circ \phi_{4,4}$, then

$$F_4(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = f_4(\phi_{4,4}(x_6, x_5, x_4, x_3, x_2, x_1, x_0))$$
$$= x_1x_2x_5 \oplus x_0x_2x_4 \oplus x_0x_5x_6 \oplus x_0x_1 \oplus x_2x_6 \oplus x_0x_5 \oplus$$
$$x_4x_5 \oplus x_5x_6 \oplus x_0x_4 \oplus x_0x_6 \oplus x_0x_3 \oplus x_3$$

The differential characters of $F_4 = f_4 \circ \phi_{4,4}$ is:

$$\triangle F_4(0,0,0,0,0,0,1) = x_2x_4 \oplus x_5x_6 \oplus x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6$$
$$\triangle F_4(0,0,0,0,0,1,0) = x_2x_5 \oplus x_0$$
$$\triangle F_4(0,0,0,0,1,0,0) = x_1x_5 \oplus x_0x_4 \oplus x_6$$
$$\triangle F_4(0,0,0,1,0,0,0) = x_0 \oplus 1$$
$$\triangle F_4(0,0,1,0,0,0,0) = x_0x_2 \oplus x_0 \oplus x_5$$
$$\triangle F_4(0,1,0,0,0,0,0) = x_1x_2 \oplus x_0x_6 \oplus x_0 \oplus x_4 \oplus x_6$$
$$\triangle F_4(1,0,0,0,0,0,0) = x_0x_5 \oplus x_0 \oplus x_2 \oplus x_5$$
$$\triangle F_4(0,0,0,0,1,0,1) = x_0x_4 \oplus x_2x_4 \oplus x_1x_5 \oplus x_5x_6 \oplus x_1 \oplus x_3 \oplus x_5$$

4. Differential Attack on 4-Pass HAVAL

The original initial value *IV* of HAVAL is:

IV = 243f6a88 85a308d3 13198a2e 03707344 a4093822 299f31d0 082efa98 ec4e6c89

We select a collision differential with two iterations as follows:

$$H_0 = IV, H_1 = HAVAL(H_0, M_1), H_2 = HAVAL(H_1, M_2)$$
$$H_0' = IV, H_1' = HAVAL(H_0', M_1'), H_2' = HAVAL(H_1', M_2')$$
$$\Delta H_0 = 0 \rightarrow \Delta H_1 = (0,0,0,0,2^{31},0,2^{31},0) \rightarrow \Delta H_2 = 0, \text{ where } \Delta H_i = H_i' - H_i$$

The first block input differential is $\Delta X_8 = +2^{10}$, $\Delta X_{16} = 2^{31}$, and the second block input differential is $\Delta X_8 = -2^{10}$, $\Delta X_{16} = 2^{31}$. The detail differential path is list in Table1 and Table2:

For the each block, there are two inner collisions: inner collision I (step8-47 for the first block and step0-47 for the second block) and inner collision II (step70-78), and one inner near-collision: step116-step127. The final near-collision in step127 of second block is turned to full collision with the feed-forward of the initial difference.

To construct inner collision II in pass3, $\Delta X_8 = \pm 2^{10}$ and $\Delta X_{16} = 2^{31}$ are chosen. Since $\Delta X_8 = \pm 2^{10}$ in step70 produce difference $\Delta G_{70} = \pm 2^{10}$, $\Delta X_{16} = 2^{31}$ will eliminate the difference: $\Delta G_{78} = (\Delta G_{70} = \pm 2^{10})^{>>11} + \Delta X_{16} = \pm 2^{31} + 2^{31} = 0 \bmod 2^{32}$.

Table1. The Differential Path for the First Block

Pass	Step	Message	Boolean	Output register differential	
1	8	$\Delta X_8=+2^{10}$	$\Delta F_1 = 0$	$\Delta A_8=+2^{11}-2^{10}$	
	9	0	$\Delta F_1 = 0$	$\Delta B_9=0$	
	10	0	$\Delta F_1 = 0$	$\Delta C_{10}=0$	
	11	0	$\Delta F_1 = 0$	$\Delta D_{11}=0$	
	12	0	$\Delta F_1 = 0$	$\Delta E_{12}=0$	
	13	0	$\Delta F_1 = -2^{11}$	$\Delta F_{13}=-2^7+2^6+2^5+2^4$	
	14	0	$\Delta F_1 = -2^4$	$\Delta G_{14} = -2^{29}$	
	15	0	$\Delta F_1 = -2^{29}-2^7$	$\Delta H_{15}=-2^{25}+2^{24}+2^{23}+2^{22}-2^0$	
	16	$\Delta X_{16}=2^{31}$	$\Delta F_1 = -2^7$	$\Delta A_{16} = 0$	Inner collision I
	17	0	$\Delta F_1 = 0$	$\Delta B_{17} = 0$	
	18	0	$\Delta F_1 = 0$	$\Delta C_{18} = 0$	
	19	0	$\Delta F_1 = 0$	$\Delta D_{19} = 0$	
	20	0	$\Delta F_1 = 0$	$\Delta E_{20} = 0$	
	21	0	$\Delta F_1 = +2^0$	$\Delta F_{21} = 0$	
	22	0	$\Delta F_1 = +2^{25}$	$\Delta G_{22} = 0$	
	23	0	$\Delta F_1 = 0$	$\Delta H_{23} = -2^{21}-2^{11}$	
	24-30	0	$\Delta F_1 = 0$	$\Delta (A_{24},B_{25},C_{26},D_{27},E_{28},F_{29},G_{30})=0$	
	31	0	$\Delta F_1 = 0$	$\Delta H_{31} = -2^{10}-2^0$	
2	32-38	0	$\Delta F_2 = 0$	$\Delta (A_{32},B_{33},C_{34},D_{35},E_{36},F_{37},G_{38})=0$	
	39	$\Delta X_{16}=2^{31}$	$\Delta F_2 = 0$	$\Delta H_{39} = -2^{21}$	
	40-46	0	$\Delta F_2 = 0$	$\Delta (A_{40},B_{41},C_{42},D_{43},E_{44},F_{45},G_{46})=0$	
	47	$\Delta X_8=+2^{10}$	$\Delta F_2 = 0$	$\Delta H_{47} = 0$	
	…				
3	70	$\Delta X_8=+2^{10}$	$\Delta F_3 = 0$	$\Delta G_{70} = +2^{10}$	Inner collision II
	71-77	0	$\Delta F_3 = 0$	$\Delta (H_{71},A_{72},B_{73},C_{74},D_{75},E_{76},F_{77})=0$	
	78	$\Delta X_{16}=2^{31}$	$\Delta F_3 = 0$	$\Delta G_{78} = 0$	
	…				
4	116	$\Delta X_8=+2^{10}$	$\Delta F_4 = 0$	$\Delta E_{116} = +2^{10}$	
	116-123	0	$\Delta F_4 = 0$	$\Delta (F_{117},G_{118},H_{119},A_{120},B_{121},C_{122},D_{123})=0$	Inner near collision
	124	0	$\Delta F_4 = 0$	$\Delta E_{124} = 2^{31}$	
	125	0	$\Delta F_4 = 0$	$\Delta F_{125} = 0$	
	126	$\Delta X_{16}=2^{31}$	$\Delta F_4 = 0$	$\Delta G_{126} = 2^{31}$	
	127	0	$\Delta F_4 = 0$	$\Delta H_{127} = 0$	

By analyzing the expanding of subtraction difference, differential characters of Boolean functions, the sufficient conditions for keeping desired path could be obtained. Sufficient conditions for the desired differential path of first block are listed in Table3. Besides the first 15 steps, sufficient conditions for the second block are similar to the first block.

Following three extra conditions in the first block are requested for keeping the differential path of second block:

$H=H_{127}+IV-H=0$(the 31^{th} bit)； $F=F_{125}+IV-F=0$(the 31^{th} bit)；

$(E=E_{124}+IV-E)\neq(G=G_{126}+IV-G)$ (the 31^{th} bit)

Table2. The Differential Path for the Second Block

Pass	Step	Message	Boolean	Output register differential	
1	0			$\Delta A_0=0$	
	1			$\Delta B_1=0$	
	2			$\Delta C_2=0$	
	3			$\Delta D_3=0$	
	4			$\Delta E_4=-2^{20}$	
	5			$\Delta F_5=0$	
	6			$\Delta G_6= +2^{20}$	
	7			$\Delta H_7=0$	
	8	$\Delta X_8=-2^{10}$	$\Delta F_1 = 0$	$\Delta A_8=-2^{16}+2^{15}+2^{14}+2^{13}+2^{12}+2^{11}+2^{10}$	
	9	0	$\Delta F_1 = 0$	$\Delta B_9=0$	
	10	0	$\Delta F_1 = 0$	$\Delta C_{10}=0$	
	11	0	$\Delta F_1 = 0$	$\Delta D_{11}=0$	Inner collision I
	12	0	$\Delta F_1 = +2^{16}$	$\Delta E_{12}=0$	
	13	0	$\Delta F_1 = +2^{11}$	$\Delta F_{13}=+2^7-2^6-2^5-2^4$	
	14	0	$\Delta F_1 = -2^{16}+2^4$	$\Delta G_{14} = +2^{29}$	
	15	0	$\Delta F_1 = +2^{29}+2^7$	$\Delta H_{15}=+2^{25}-2^{24}-2^{23}-2^{22}+2^0$	
	16	$\Delta X_{16}=2^{31}$	$\Delta F_1 = +2^7$	$\Delta A_{16} = 0$	
	17	0	$\Delta F_1 = 0$	$\Delta B_{17} = 0$	
	18	0	$\Delta F_1 = 0$	$\Delta C_{18} = 0$	
	19	0	$\Delta F_1 = 0$	$\Delta D_{19} = 0$	
	20	0	$\Delta F_1 = 0$	$\Delta E_{20} = 0$	
	21	0	$\Delta F_1 = -2^0$	$\Delta F_{21} = 0$	
	22	0	$\Delta F_1 = -2^{25}$	$\Delta G_{22} = 0$	
	23	0	$\Delta F_1 = 0$	$\Delta H_{23} = +2^{21}+2^{11}$	
	24-30	0	$\Delta F_1 = 0$	$\Delta (A_{24},B_{25},C_{26},D_{27},E_{28},F_{29},G_{30})=0$	
	31	0	$\Delta F_1 = 0$	$\Delta H_{31} = +2^{10}+2^0$	
2	32-38	0	$\Delta F_2 = 0$	$\Delta (A_{32},B_{33},C_{34},D_{35},E_{36},F_{37},G_{38})=0$	
	39	$\Delta X_{16}=2^{31}$	$\Delta F_2 = 0$	$\Delta H_{39} = +2^{21}$	
	40-46	0	$\Delta F_2 = 0$	$\Delta (A_{40},B_{41},C_{42},D_{43},E_{44},F_{45},G_{46})=0$	
	47	$\Delta X_8=-2^{10}$	$\Delta F_2 = 0$	$\Delta H_{47} = 0$	
	…				
3	70	$\Delta X_8=-2^{10}$	$\Delta F_3 = 0$	$\Delta G_{70} = -2^{10}$	Inner collision II
	71-77	0	$\Delta F_3 = 0$	$\Delta (H_{71},A_{72},B_{73},C_{74},D_{75},E_{76},F_{77})=0$	
	78	$\Delta X_{16}=2^{31}$	$\Delta F_3 = 0$	$\Delta G_{78} = 0$	
	…				
4	116	$\Delta X_8=-2^{10}$	$\Delta F_4 = 0$	$\Delta E_{116} = -2^{10}$	
	116-123	0	$\Delta F_4 = 0$	$\Delta (F_{117},G_{118},H_{119},A_{120},B_{121},C_{122},D_{123})=0$	
	124	0	$\Delta F_4 = 0$	$\Delta E_{124} = 2^{31}$	Inner near collision
	125	0	$\Delta F_4 = 0$	$\Delta F_{125} = 0$	
	126	$\Delta X_{16}=2^{31}$	$\Delta F_4 = 0$	$\Delta G_{126} = 2^{31}$	
	127	0	$\Delta F_4 = 0$	$\Delta H_{127} = 0$	

Table3. Sufficient conditions for the desired differential path of first block

$\Delta F_5=0$	$F_{5,[11,10]} = 1$
$\Delta G_6=0$	$G_{6,[11,10]} = 0$
$\Delta H_7=0$	$H_{7,[11,10]} = 0, H_{7,4} = 1$
$\Delta A_8=+2^{11}-2^{10}$	$A_{8,11} = 0, A_{8,10} = 1, A_{8,4} = 1$
$\Delta B_9=0$	$B_{9,29} = 0, B_{9,[11,10]} = 0, B_{9,7} = 0,$
$\Delta C_{10}=0$	$C_{10,11}=1, C_{10,10}=0, C_{10,[7,5]}=1, C_{10,4}=0$
$\Delta D_{11}=0$	$D_{11,29}=0, D_{11,11}=1, D_{11,10}=0, D_{11,7}=1, D_{11,[6,4]}= 0$
$\Delta E_{12}=0$	$E_{12,29}=0, E_{12,[25,22]}=1, E_{12,11}=1, E_{12,[7,4]}=0, E_{12,0}=1$
$\Delta F_{13}=-2^7+2^6+2^5+2^4$	$F_{13,29}=0, F_{13,[25,22]}=0, F_{13,7}=1, F_{13,[6,4]}=0, F_{13,0}=0$
$\Delta G_{14} = -2^{29}$	$G_{14,29}=1, G_{14,[25,22]}=0, G_{14,[7,4]}=0, G_{14,0}=1$
$\Delta H_{15}=-2^{25}+2^{24}+2^{23}+2^{22}-2^0$	$H_{15,29}=0, H_{15,25}=1, H_{15,[24,22]}=0, H_{15,[7,4]}=0, H_{15,0}=1$
$\Delta A_{16} = 0$	$A_{16,29}=0, A_{16,25}=1, A_{16,[24,22]}=0, A_{16,[7,4]}=0, A_{16,0}=0$
$\Delta B_{17} = 0$	$B_{17,29}=0, B_{17,[25,22]}=0, B_{17,0}=0$
$\Delta C_{18} = 0$	$C_{18,[25,22]}=0, C_{18,0}=0$
$\Delta D_{19} = 0$	
$\Delta E_{20} = 0$	$E_{20,21}=1, E_{20,11}=1, E_{20,0}=1$
$\Delta F_{21} = 0$	$F_{21,25}=1, F_{21,21}=0, F_{21,21}=0$
$\Delta G_{22} = 0$	$G_{22,21}=0, G_{22,11}=0$
$\Delta H_{23} = -2^{21}-2^{11}$	$H_{23,21}=1, H_{23,11}=1$
$\Delta (A_{24},B_{25},C_{26},D_{27},E_{28},F_{29},G_{30})=0$	$A_{24,21}=0, A_{24,11}=0, B_{25,21}=0, B_{25,11}=0, C_{26,21}=0, C_{26,11}=0$
$\Delta H_{31} = -2^{10}-2^0$	$H_{31,10}=1, H_{31,0}=1$
$\Delta A_{32} = 0$	$B_{25}G_{30} \oplus C_{26}=0$(the 10^{th},0 th bit)
$\Delta B_{33} = 0$	$A_{32}C_{26} \oplus D_{27}G_{30} \oplus C_{26} \oplus E_{28} \oplus F_{29}=0$(the 10^{th},0 th bit)
$\Delta C_{34} = 0$	$A_{32}E_{28} \oplus D_{27} \oplus E_{28}=0$(the 10^{th},0 th bit)
$\Delta D_{35} = 0$	$B_{33}=0$(the 10^{th},0 th bit)
$\Delta E_{36} = 0$	$C_{34}=1$(the 10^{th},0 th bit)
$\Delta F_{37} = 0$	$C_{34}D_{35} \oplus C_{34} \oplus E_{36}=0$(the 10^{th},0 th bit)
$\Delta G_{38} = 0$	$E_{36}F_{37} \oplus D_{35} \oplus E_{36}=0$(the 10^{th},0 th bit)
$\Delta H_{39} = -2^{21}$	$H_{39} = 1$(the 21^{th} bit)
$\Delta A_{40} = 0$	$B_{33}G_{38} \oplus C_{34}=0$(the 21^{th} bit)
$\Delta B_{41} = 0$	$A_{40}C_{34} \oplus D_{35}G_{38} \oplus C_{34} \oplus E_{36} \oplus F_{37}=0$(the 21^{th} bit)
$\Delta C_{42} = 0$	$A_{40}E_{36} \oplus D_{35} \oplus E_{36}=0$(the 21^{th} bit)
$\Delta D_{43} = 0$	$B_{41}=0$(the 21^{th} bit)
$\Delta E_{44} = 0$	$C_{42}=1$(the 21^{th} bit)
$\Delta F_{45} = 0$	$C_{42}D_{43} \oplus C_{42} \oplus E_{44}=0$(the 21^{th} bit)
$\Delta G_{46} = 0$	$E_{44}F_{45} \oplus D_{43} \oplus E_{44}=0$(the 21^{th} bit)
$\Delta H_{47} = 0$	
…	
$\Delta G_{70} = +2^{10}$	$G_{70} = 0$(the 10^{th} bit)
$\Delta (H_{71},A_{72},B_{73},C_{74},D_{75},E_{76},F_{77})=0$	$A_{64}=1, B_{65}=0, C_{66}=1, E_{68}=1, F_{69}=1,$ $H_{71}=0, A_{72}=1, C_{74}=0, D_{75}=0$(the 10^{th} bit)
…	
$\Delta E_{116} = +2^{10}$	$E_{116} = 0$(the 10^{th} bit)
$\Delta F_{117} = 0$	$A_{112}C_{114} \oplus G_{110}H_{111} \oplus D_{115} \oplus B_{113} \oplus A_{112} \oplus H_{111} \oplus G_{110}=0$(the 10^{th} bit)
$\Delta G_{118} = 0$	$A_{112}D_{115} \oplus F_{117}=0$(the 10^{th} bit)
$\Delta H_{119} = 0$	$B_{113}F_{117} \oplus C_{114}G_{118} \oplus A_{112}=0$(the 10^{th} bit)
$\Delta A_{120} = 0$	$H_{119}=1$(the 10^{th} bit)
$\Delta B_{121} = 0$	$A_{120}G_{118} \oplus A_{120} \oplus D_{115}=0$(the 10^{th} bit)
$\Delta C_{122} = 0$	$A_{120} \oplus B_{121}D_{115} \oplus B_{121} \oplus F_{117} \oplus D_{115}=0$(the 10^{th} bit)
$\Delta D_{123} = 0$	$C_{122}F_{117} \oplus C_{122} \oplus A_{120} \oplus F_{117}=0$(the 10^{th} bit)
$\Delta E_{124} = 2^{31}$	
$\Delta F_{125} = 0$	$A_{120}C_{122} \oplus G_{118}H_{119} \oplus D_{123} \oplus B_{121} \oplus A_{120} \oplus H_{119} \oplus G_{118}=0$(the 31^{th} bit)
$\Delta G_{126} = 2^{31}$	$A_{120}D_{123} \oplus F_{125}=0$(the 31^{th} bit)
$\Delta H_{127} = 0$	$B_{121}F_{125} \oplus A_{120}B_{121} \oplus F_{125} \oplus D_{123} \oplus C_{122} \oplus B_{121}=0$(the 31^{th} bit)

5. A Fast Attack Algorithm

5.1 How to fulfill the conditions in Pass1

If the initial vector are fixed in HAVAL, the value of input message $X_0,X_1…X_{31}$ and register $A_0,B_1,…H_{31}$ are corresponding: register $A_0,B_1,…H_{31}$ and initial vector can be used to compute $X_0,X_1…X_{31}$ in step0-31 . So special register value can be chosen to fulfill Table3, and be used to compute $X_0,X_1…X_{15}$. This method can avoid Single-message Modification [9,10] in Pass1, and speedup searching process. For example, for the first block we can set the register value according to Table3, remain free bits set to 0:

A_0=0x00000000	B_1=0x00000000	C_2=0x00000000	D_3=0x00000000
E_4=0x00000000	F_5=0x00000c00	G_6=0x00000000	H_7=0x00000010
A_8=0x00000410	B_9=0x00000000	C_{10}=0x000008e0	D_{11}=0x00200880
E_{12}=0x03c00801	F_{13}=0x00000080	G_{14}=0x20000001	F_{15}=0x02000001
A_{16}=0x02000000	B_{17}=0x00000000	C_{18}=0x00000000	D_{19}=0x00000000
E_{20}=0x00200801	F_{21}=0x02000000	G_{22}=0x00000000	H_{23}=0x00200800
A_{24}=0x00000000	B_{25}=0x00000000	C_{26}=0x00000000	D_{27}=0x00200800
E_{28}=0x00000000	F_{29}=0x00000000	G_{30}=0x00000000	H_{31}=0x00000401

5.2 How to fulfill the conditions in Pass2

For the desired differential path, there are 22 conditions in Pass2, 10 conditions in Pass3, 11 conditions in Pass4, and 3 extra conditions for the first block. Then the computational complexity of the attack is about 2^{46} for the first block and 2^{43} for the second block.

The 22 conditions in Pass2 are as follows:

(1)$B_{25}G_{30} \oplus C_{26}=0$ (10^{th} and 0^{th} bit)
(2)$A_{32}C_{26} \oplus D_{27}G_{30} \oplus C_{26} \oplus E_{28} \oplus F_{29}=0$ (10^{th} and 0^{th} bit)
(3)$A_{32}E_{28} \oplus D_{27} \oplus E_{28}=0$ (10^{th} and 0^{th} bit)
(4)$B_{33}=0$ (10^{th} and 0^{th} bit)
(5)$C_{34}=1$ (10^{th} and 0^{th} bit)
(6)$C_{34}D_{35} \oplus C_{34} \oplus E_{36}=0$ (10^{th} and 0^{th} bit)
(7)$E_{36}F_{37} \oplus D_{35} \oplus E_{36}=0$ (10^{th} and 0^{th} bit)
(8)$H_{39} = 1$ (21^{th} bit)
(9)$B_{33}G_{38} \oplus C_{34}=0$ (21^{th} bit)
(10)$A_{40}C_{34} \oplus D_{35}G_{38} \oplus C_{34} \oplus E_{36} \oplus F_{37}=0$ (21^{th} bit)
(11)$A_{40}E_{36} \oplus D_{35} \oplus E_{36}=0$ (21^{th} bit)
(12)$B_{41}=0$ (21^{th} bit)
(13)$C_{42}=1$ (21^{th} bit)
(14)$C_{42}D_{43} \oplus C_{42} \oplus E_{44}=0$ (21^{th} bit)
(15)$E_{44}F_{45} \oplus D_{43} \oplus E_{44}=0$ (21^{th} bit)

Because Boolean functions used in HAVAL have 7 variables, part of input variables can determine the output by absent bits computation [11]. For example, condition(1) will always be hold when $B_{25}=0$ and $C_{26}=0$; condition(2) will always be hold when $B_{25}=0$, $C_{26}=0$, $D_{27}=0$, $E_{28}=0$, $F_{29}=0$; condition(3) will always be hold when $D_{27}=0$, $E_{28}=0$.

Condition(4-7) are equivalent to $B_{33}=0$, $C_{34}=1$, $D_{35}=0$, $E_{36}=1$, $F_{37}=1$; (the 10^{th} and 0^{th} bit)

Condition(9-11) always be hold when B_{33}=0, C_{34}=0, D_{35}=0, E_{36}=0, F_{37}=0;(the 21th bit)

Condition(12-15) are equivalent to B_{41}=0, C_{42}=1, D_{43}=0, E_{44}=1, F_{45}=1; (the 21th bit)

So the equivalent conditions are:

$B_{33,\ 21}$=0, $C_{34,\ 21}$=0, $D_{35,\ 21}$=0, $E_{36,\ 21}$=0, $F_{37,\ 21}$=0,

$B_{33,\ 10}$=0, $C_{34,\ 10}$=1, $D_{35,\ 10}$=0, $E_{36,\ 10}$=1, $F_{37,\ 10}$=1,

$B_{33,\ 0}$=0, $C_{34,\ 0}$=1, $D_{35,\ 0}$=0, $E_{36,\ 0}$=1, $F_{37,\ 0}$=1,

$H_{39,\ 21}$=1, $B_{41,\ 21}$=0, $C_{42,\ 21}$=1, $D_{43,\ 21}$=0, $E_{44,\ 21}$=1, $F_{45,\ 21}$=1

Here we show how to use the absent bits computation and fixed carry method instead of multi-message modification [9,10] to fulfill conditions from step32 to step37 in Pass2. Using fixed carry digit method and early abort method [11], the probability and the complexity to find a collision are greatly improved. These methods are especially suitable for hash functions such as HAVAL and SHA-2, which have a lot of registers.

The first 30 registers are fixed in search process, chosen according to §5.1; only some bits in G_{30} and H_{31} are free.

Step32: $A_{32} = F_2 (B_{25}, C_{26}, D_{27}, E_{28}, F_{29}, G_{30}, H_{31})^{>>7} + A_{24}{}^{>>11} + X_5 + 0x452821E6$;

From Pass1 we can get X_5=0xba3562be, R=0x452821E6, A_{24}=0, by absent bits computation, besides the 21th and 11th bit, remain bits of

$$F_2 = B_{25}G_{30}H_{31} \oplus C_{26}F_{29}G_{30} \oplus B_{25}G_{30} \oplus B_{25}F_{29} \oplus E_{28}G_{30} \oplus C_{26}H_{31} \oplus C_{26}F_{29} \oplus D_{27}G_{30} \oplus D_{27}$$

are 0, so $F_2 \approx 0$, and A_{32}≈0xff5d84a4.

Step33: $B_{33} = F_2 (C_{26}, D_{27}, E_{28}, F_{29}, G_{30}, H_{31}, A_{32})^{>>7} + B_{25}{}^{>>11} + X_{14} + 0x38D01377$;

From Pass1 we can get X_{14}=0xfffffff1, R=0x38d01377,B_{25}=0, by absent bits computation, besides the 21th and 11th bit, remain bits of

$$F_2 = C_{26}H_{31}A_{32} \oplus D_{27}G_{30}H_{31} \oplus C_{26}H_{31} \oplus C_{26}G_{30} \oplus F_{29}H_{31} \oplus D_{27}A_{32} \oplus D_{27}G_{30} \oplus E_{28}H_{31} \oplus E_{28}$$

are 0, so $F_2 \approx 0$, and B_{33}≈0x38d01368, conditions $B_{33,21}$=0,$B_{33,10}$=0,$B_{33,0}$=0 always be hold.

Step34: $C_{34} = F_2 (D_{27}, E_{28}, F_{29}, G_{30}, H_{31}, A_{32}, B_{33})^{>>7} + C_{26}{}^{>>11} + X_{26} + 0xBE5466CF$;

From Pass1 we can get X_{26}=0, R=0xbe5466cf, C_{26}=0, by absent bits computation, the 21th bit of

$$F_2 = D_{27}A_{32}B_{33} \oplus E_{28}H_{31}A_{32} \oplus D_{27}A_{32} \oplus D_{27}H_{31} \oplus G_{30}A_{32} \oplus E_{28}B_{33} \oplus E_{28}H_{31} \oplus F_{29}A_{32} \oplus F_{29}$$

is $A_{32}B_{33} \oplus A_{32} \oplus H_{31} \oplus G_{30}A_{32}$, remain bits of F_2 are $G_{30}A_{32}$.

Because $C_{26}{}^{>>11} + X_{26} + R$ =0xbe5466cf, using fixed carry method: if $G_{30,28}$=0, $G_{30,27}$=0, $G_{30,26}$=0, $G_{30,17}$=0, $G_{30,16}$=0, $G_{30,7}$=0, then $C_{34,21}$=0, $C_{34,10}$=1, $C_{34,0}$=1will always be hold.

Step35: $D_{35} = F_2 (E_{28}, F_{29}, G_{30}, H_{31}, A_{32}, B_{33}, C_{34})^{>>7} + D_{27}{}^{>>11} + X_{18} + 0x34E90C6C$;

From Pass1 we can get X_{18}=0xe3ffffef, R=0x34e90c6c, D_{27}=0x00000401, by absent bits computation,

$F_2 = E_{28}B_{33}C_{34} \oplus F_{29}A_{32}B_{33} \oplus E_{28}B_{33} \oplus E_{28}A_{32} \oplus H_{31}B_{33} \oplus F_{29}C_{34} \oplus F_{29}A_{32} \oplus G_{30}B_{33} \oplus G_{30}$ $= H_{31}B_{33} \oplus G_{30}B_{33} \oplus G_{30}$.

Because $D_{27}^{>>11} + X_{18} + R$ =0x18e9105c, using fixed carry method: if $H_{31,28}$=1, $G_{30,17}$=0, $G_{30,16}$=0, $G_{30,7}$=0, then $D_{35,21}$=0, $D_{35,10}$=0, $D_{35,0}$=0 will always be hold.

For step36 and step37, we can't perform absent bits computation determinately. But we can also use fixed carry method to fulfill $E_{36,21}$= 0 , $F_{37,21}$= 0, $E_{36,10}$= 1, $F_{37,10}$= 1 , $E_{36,0}$= 1 , $F_{37,0}$=1 with probability not less than 1/2. Then the remain 6 conditions in Pass2 are $H_{39,21}$=1, $B_{41,21}$=0, $C_{42,21}$=1, $D_{43,21}$=0, $E_{44,21}$=1, $F_{45,21}$=1. The computational complexity of the attack is reduced to 2^{30}-2^{32} for the first block and 2^{27}-2^{29} for the second block.

5.3 Fast Attack Algorithm (first block)

A fast attack algorithm for the first block near collision is given as follows, which can also be used to find second block collision with only slight modification on fixed value. We can use evolution computing or other heuristic algorithms to find such fixed value instead of manual calculation.

Algorithm: Finding first block near collision

S1. Choose registers with fixed value according Table3:

A_0=0x00000000	B_1=0x00000000	C_2=0x00000000	D_3=0x00000000
E_4=0x00000000	F_5=0x00000c00	G_6=0x00000000	H_7=0x00000010
A_8=0x00000410	B_9=0x00000000	C_{10}=0x000008e0	D_{11}=0x00200880
E_{12}=0x03c00801	F_{13}=0x00000080	G_{14}=0x20000001	F_{15}=0x02000001
A_{16}=0x02000000	B_{17}=0x00000000	C_{18}=0x00000000	D_{19}=0x00000000
E_{20}=0x00200801	F_{21}=0x02000000	G_{22}=0x00000000	H_{23}=0x00200800
A_{24}=0x00000000	B_{25}=0x00000000	C_{26}=0x00000000	D_{27}=0x00200800
E_{28}=0x00000000	F_{29}=0x00000000		

S2. Random choose $H_{31,(27,11)}$, $H_{31,(9,1)}$, $G_{30,(15,12)}$, $G_{30,(9,3)}$, and compute:

H_{31}=0xf0000401+ $H_{31,(27,11)}$ +$H_{31,(9,1)}$;

G_{30}=$G_{30,(15,12)}$+$G_{30,(9,3)}$;

S3. Compute X_0,X_1…X_{15} by A_0,B_1,…H_{31};

X_0 = A_0 - F_1 (IV-B, IV-C, IV-D, IV-E, IV-F, IV-G, IV-H) $^{>>7}$ - IV-A $^{>>11}$;

X_1 = B_1 - F_1 (IV-C, IV-D, IV-E, IV-F, IV-G, IV-H, A_0) $^{>>7}$ - IV-B $^{>>11}$;

…

X_{31} = H_{31} - F_1 (A_{24}, B_{25}, C_{26}, D_{27}, E_{28}, F_{29}, G_{30}) $^{>>7}$ - H_{23} $^{>>11}$;

S4. Continue compute remain step, if any condition is not satisfied, then jump to **S2** (early abort); else find collision.

6. Collision Example

Our attack can find many real collisions which are composed of two 2048-bit messages

(M_1,M_2) and (M_1',M_2') with the original initial value IV of HAVAL:

IV = 243f6a88 85a308d3 13198a2e 03707344 a4093822 299f31d0 082efa98 ec4e6c89

$H_1 = HAVAL(IV, M_1), H_2 = HAVAL(H_1, M_2)$;

$H'_1 = HAVAL(IV, M'_1), H'_2 = HAVAL(H'_1, M'_2)$

A collision example ($H_2 = H'_2$) for 4-Pass HAVAL is given in Table4.

Table 4. Collision example for 4-Pass HAVAL. H_2 is the hash value without message padding.

IV	243f6a88	85a308d3	13198a2e	03707344	a4093822	299f31d0	082efa98	ec4e6c89
M_1	7a6825d3	1cbc99ad	b5fa99a6	f3a55ed5	937d8fe2	ba3562be	e58f4b87	aefb7823
	e0000410	e0000000	000008e0	4020086f	03bfc7f0	7df8806f	fffffff1	fdbffff0
	7dffffff	fdfbffef	e3fffef	effffbff	ffff9000	f1ffbff0	ffdc0000	ffffc800
	ffffc000	00000000	00000000	00200800	ffdfbbef	ffffc000	00008010	d075e0b0
H_1	7368d98c	1f8df12d	515d3893	f63b2fae	10416272	7b8f0955	371830bc	8e92ec6c
M_2	1e062c01	efda9c87	90cddbaa	ad2dc583	080efe3b	d5719eb7	da5bea4a	ce7292f5
	e000fe10	e00ffc00	000006e0	4021066f	03bfbdf0	7df88031	fffffe01	fdbfffe0
	fdfffe0	fdfbfdef	e3ffffff	effffbdf	ffff9001	f1ffbff0	ffdc0000	ffffc800
	ffffc000	00000000	00000000	00200800	ffdfbbef	ffffc000	0000a000	fdab519a
H_2	94f2d340	e2c585eb	b30b13e4	64e6b980	1939508f	705f214b	e891d52e	09959923
M_1'	7a6825d3	1cbc99ad	b5fa99a6	f3a55ed5	937d8fe2	ba3562be	e58f4b87	aefb7823
	e0000810	e0000000	000008e0	4020086f	03bfc7f0	7df8806f	fffffff1	fdbffff0
	fdfffffff	fdfbffef	e3ffffef	effffbff	ffff9000	f1ffbff0	ffdc0000	ffffc800
	ffffc000	00000000	00000000	00200800	ffdfbbef	ffffc000	00008010	d075e0b0
H_1'	7368d98c	9f8df12d	515d3893	763b2fae	10416272	7b8f0955	371830bc	8e92ec6c
M_2'	1e062c01	efda9c87	90cddbaa	ad2dc583	080efe3b	d5719eb7	da5bea4a	ce7292f5
	e000fa10	e00ffc00	000006e0	4021066f	03bfbdf0	7df88031	fffffe01	fdbfffe0
	7dfffe0	fdfbfdef	e3ffffff	effffbdf	ffff9001	f1ffbff0	ffdc0000	ffffc800
	ffffc000	00000000	00000000	00200800	ffdfbbef	ffffc000	0000a000	fdab519a
H_2'	94f2d340	e2c585eb	b30b13e4	64e6b980	1939508f	705f214b	e891d52e	09959923

The computational complexity of the attack is about 2^{30}-2^{32} for the first block and 2^{27}-2^{29} for the second block. We use this attack to find 256-bit collisions of 4-Pass HAVAL in 3-4 hours for the first block and 1 hour for the second block on a common PC. The 256-bit collisions can be convert to 128,160,192,224 bits collisions easily according to original HAVAL algorithm.

7. Summary

In this paper we show an attack against full version of 4-Pass HAVAL, using the correct initial value as specified for the algorithm. This attack also works for all possible output lengths of the algorithm. The computational complexity of the attack is about 2^{30}-2^{32} for the first block and 2^{27}-2^{29} for the second block.

In this attack fixed carry digit method and early abort method are used to reduce the number of trials for finding collisions. Using these methods, the probability and the complexity to find a collision are greatly improved. These methods are especially suitable for hash functions such as HAVAL and SHA-2, which have a lot of registers.

References

1. E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
2. Y. Zheng, J. Pieprzyk, J. Seberry, *HAVAL* – A One-Way Hashing Algorithm with Variable Length of Output, *AUSCRYPT 1992, LNCS 718*, Springer-Verlag, 1992, 83–104.
3. H. Dobbertin, Cryptanalysis of MD4. *Journal of Cryptology*, **11**(4):253-271,1998.
4. Y.S. Her, K. Sakurai, S.H. Kim, Attacks for Finding Collision in Reduced Versions of 3-Pass and 4-Pass HAVAL, *Proceedings International Conference on Computers, Communications and Systems, CE-15*, 2003, 75–78.
5. P. Kasselman, W. Penzhorn, Cryptanalysis of Reduced Version of HAVAL, *Electronics letters*, Vol. 36, No. 1, January 2000, 30–31.
6. S. Park, S. H. Sung, S. Chee, J. Lim, On the Security of Reduced Versions of 3-Pass HAVAL, *ACISP 2002, LNCS 2384*, J. Seberry, L. Batten, Eds., 2002, 406–419.
7. H. Yoshida, A. Biryukov, C. De Canniere, *et al*, Non-Randomness of the Full 4 and 5-Pass HAVAL, *SCN 2004*, Springer-Verlag, *LNCS 3352*, 2005, 324–336.
8. B. Van Rompay, A. Biryukov, B. Preneel, J. Vandewalle. Cryptanalysis of 3-Pass HAVAL. Advances in Cryptology -*ASIACRYPTO'03*, Springer-Verlag, 2003, *LNCS, 2894*,228-245.
9. X. Y. Wang, D. G. Feng, Y. X. Yuan, An Attack on Hash Function HAVAL-128, *Chinese Science(E)*, 2005,35(3):1-12.
10. X. Y. Wang, H. B. Yu, How to break MD5 and other hash functions. *Advances in Cryptology-Eurocrypt'05*, Springer-Verlag, 2005, *LNCS, 3494*,19-35.
11. Zhangyi Wang, Huanguo Zhang, Zhongpin Qin, Qingshu Meng, A Fast Attack on the MD5 Hash Function, *Journal of Shanghai Jiaotong University (Science)*,Vol.E11,No.2,2006.

Appendix

In this appendix we give a description of 4-Pass HAVAL that are discussed in this paper.

The initial value to be used in the first application of the compression function is specified as follows (hexadecimal notation):

```
IV-A = 0xEC4E6C89; IV-B = 0x082EFA98; IV-C = 0x299F31D0; IV-D = 0xA4093822;
IV-E = 0x03707344; IV-F = 0x13198A2E; IV-G = 0x85A308D3; IV-H = 0x243F6A88;
```

The compression function applies the following 128 steps (four passed of 32 steps each):

Pass1 $F_1(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_1x_3 \oplus x_5x_6 \oplus x_2x_4 \oplus x_0x_3 \oplus x_0$

Step0: $A_0 = F_1$ (IV-B, IV-C, IV-D, IV-E, IV-F, IV-G, IV-H) $^{>>7}$ + IV-A $^{>>11}$ +X_0 ;
Step1: $B_1 = F_1$ (IV-C, IV-D, IV-E, IV-F, IV-G, IV-H, A_0) $^{>>7}$ + IV-B $^{>>11}$ +X_1 ;
Step2: $C_2 = F_1$ (IV-D, IV-E, IV-F, IV-G, IV-H, A_0, B_1) $^{>>7}$ + IV-C $^{>>11}$ +X_2 ;
Step3: $D_3 = F_1$ (IV-E, IV-F, IV-G, IV-H, A_0, B_1, C_2) $^{>>7}$ + IV-D $^{>>11}$ +X_3 ;
Step4: $E_4 = F_1$ (IV-F, IV-G, IV-H, A_0, B_1, C_2, D_3) $^{>>7}$ + IV-E $^{>>11}$ +X_4 ;
Step5: $F_5 = F_1$ (IV-G, IV-H, A_0, B_1, C_2, D_3, E_4) $^{>>7}$ + IV-F $^{>>11}$ +X_5 ;
Step6: $G_6 = F_1$ (IV-H, A_0, B_1, C_2, D_3, E_4, F_5) $^{>>7}$ + IV-G $^{>>11}$ +X_6 ;
Step7: $H_7 = F_1$ (A_0, B_1, C_2, D_3, E_4, F_5, G_6) $^{>>7}$ + IV-H $^{>>11}$ +X_7 ;
Step8: $A_8 = F_1$ (B_1, C_2, D_3, E_4, F_5, G_6, H_7) $^{>>7}$ + A_0 $^{>>11}$ +X_8 ;
Step9: $B_9 = F_1$ (C_2, D_3, E_4, F_5, G_6, H_7, A_8) $^{>>7}$ + B_1 $^{>>11}$ +X_9 ;
Step10: $C_{10} = F_1$ (D_3, E_4, F_5, G_6, H_7, A_8, B_9) $^{>>7}$ + C_2 $^{>>11}$ +X_{10} ;
Step11: $D_{11} = F_1$ (E_4, F_5, G_6, H_7, A_8, B_9, C_{10}) $^{>>7}$ + D_3 $^{>>11}$ +X_{11} ;
Step12: $E_{12} = F_1$ (F_5, G_6, H_7, A_8, B_9, C_{10}, D_{11}) $^{>>7}$ + E_4 $^{>>11}$ +X_{12} ;
Step13: $F_{13} = F_1$ (G_6, H_7, A_8, B_9, C_{10}, D_{11}, E_{12}) $^{>>7}$ + F_5 $^{>>11}$ +X_{13} ;
Step14: $G_{14} = F_1$ (H_7, A_8, B_9, C_{10}, D_{11}, E_{12}, F_{13}) $^{>>7}$ + G_6 $^{>>11}$ +X_{14} ;
Step15: $H_{15} = F_1$ (A_8, B_9, C_{10}, D_{11}, E_{12}, F_{13}, G_{14}) $^{>>7}$ + H_7 $^{>>11}$ +X_{15} ;
Step16: $A_{16} = F_1$ (B_9, C_{10}, D_{11}, E_{12}, F_{13}, G_{14}, H_{15}) $^{>>7}$ + A_8 $^{>>11}$ +X_{16} ;
Step17: $B_{17} = F_1$ (C_{10}, D_{11}, E_{12}, F_{13}, G_{14}, H_{15}, A_{16}) $^{>>7}$ + B_9 $^{>>11}$ +X_{17} ;
Step18: $C_{18} = F_1$ (D_{11}, E_{12}, F_{13}, G_{14}, H_{15}, A_{16}, B_{17}) $^{>>7}$ + C_{10} $^{>>11}$ +X_{18} ;
Step19: $D_{19} = F_1$ (E_{12}, F_{13}, G_{14}, H_{15}, A_{16}, B_{17}, C_{18}) $^{>>7}$ + D_{11} $^{>>11}$ +X_{19} ;
Step20: $E_{20} = F_1$ (F_{13}, G_{14}, H_{15}, A_{16}, B_{17}, C_{18}, D_{19}) $^{>>7}$ + E_{12} $^{>>11}$ +X_{20} ;
Step21: $F_{21} = F_1$ (G_{14}, H_{15}, A_{16}, B_{17}, C_{18}, D_{19}, E_{20}) $^{>>7}$ + F_{13} $^{>>11}$ +X_{21} ;
Step22: $G_{22} = F_1$ (H_{15}, A_{16}, B_{17}, C_{18}, D_{19}, E_{20}, F_{21}) $^{>>7}$ + G_{14} $^{>>11}$ +X_{22} ;
Step23: $H_{23} = F_1$ (A_{16}, B_{17}, C_{18}, D_{19}, E_{20}, F_{21}, G_{22}) $^{>>7}$ + H_{15} $^{>>11}$ +X_{23} ;
Step24: $A_{24} = F_1$ (B_{17}, C_{18}, D_{19}, E_{20}, F_{21}, G_{22}, H_{23}) $^{>>7}$ + A_{16} $^{>>11}$ +X_{24} ;
Step25: $B_{25} = F_1$ (C_{18}, D_{19}, E_{20}, F_{21}, G_{22}, H_{23}, A_{24}) $^{>>7}$ + B_{17} $^{>>11}$ +X_{25} ;
Step26: $C_{26} = F_1$ (D_{19}, E_{20}, F_{21}, G_{22}, H_{23}, A_{24}, B_{25}) $^{>>7}$ + C_{18} $^{>>11}$ +X_{26} ;
Step27: $D_{27} = F_1$ (E_{20}, F_{21}, G_{22}, H_{23}, A_{24}, B_{25}, C_{26}) $^{>>7}$ + D_{19} $^{>>11}$ +X_{27} ;
Step28: $E_{28} = F_1$ (F_{21}, G_{22}, H_{23}, A_{24}, B_{25}, C_{26}, D_{27}) $^{>>7}$ + E_{20} $^{>>11}$ +X_{28} ;
Step29: $F_{29} = F_1$ (G_{22}, H_{23}, A_{24}, B_{25}, C_{26}, D_{27}, E_{28}) $^{>>7}$ + F_{21} $^{>>11}$ +X_{29} ;
Step30: $G_{30} = F_1$ (H_{23}, A_{24}, B_{25}, C_{26}, D_{27}, E_{28}, F_{29}) $^{>>7}$ + G_{22} $^{>>11}$ +X_{30} ;
Step31: $H_{31} = F_1$ (A_{24}, B_{25}, C_{26}, D_{27}, E_{28}, F_{29}, G_{30}) $^{>>7}$ + H_{23} $^{>>11}$ +X_{31} ;

Pass2

$F_2(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_0x_1x_6 \oplus x_1x_2x_5 \oplus x_1x_6 \oplus x_2x_6 \oplus x_1x_3 \oplus x_0x_5 \oplus x_2x_5 \oplus x_1x_4 \oplus x_4$

Step32: $A_{32} = F_2$ (B_{25}, C_{26}, D_{27}, E_{28}, F_{29}, G_{30}, H_{31}) $^{>>7}$ + A_{24} $^{>>11}$ +X_5 + 0x452821E6;
Step33: $B_{33} = F_2$ (C_{26}, D_{27}, E_{28}, F_{29}, G_{30}, H_{31}, A_{32}) $^{>>7}$ + B_{25} $^{>>11}$ +X_{14} + 0x38D01377;
Step34: $C_{34} = F_2$ (D_{27}, E_{28}, F_{29}, G_{30}, H_{31}, A_{32}, B_{33}) $^{>>7}$ + C_{26} $^{>>11}$ +X_{26} + 0xBE5466CF;
Step35: $D_{35} = F_2$ (E_{28}, F_{29}, G_{30}, H_{31}, A_{32}, B_{33}, C_{34}) $^{>>7}$ + D_{27} $^{>>11}$ +X_{18} + 0x34E90C6C;
Step36: $E_{36} = F_2$ (F_{29}, G_{30}, H_{31}, A_{32}, B_{33}, C_{34}, D_{35}) $^{>>7}$ + E_{28} $^{>>11}$ +X_{11} + 0xC0AC29B7;
Step37: $F_{37} = F_2$ (G_{30}, H_{31}, A_{32}, B_{33}, C_{34}, D_{35}, E_{36}) $^{>>7}$ + F_{29} $^{>>11}$ +X_{28} + 0xC97C50DD;
Step38: $G_{38} = F_2$ (H_{31}, A_{32}, B_{33}, C_{34}, D_{35}, E_{36}, F_{37}) $^{>>7}$ + G_{30} $^{>>11}$ +X_7 + 0x3F84D5B5;
Step39: $H_{39} = F_2$ (A_{32}, B_{33}, C_{34}, D_{35}, E_{36}, F_{37}, G_{38}) $^{>>7}$ + H_{31} $^{>>11}$ +X_{16} + 0xB5470917;
Step40: $A_{40} = F_2$ (B_{33}, C_{34}, D_{35}, E_{36}, F_{37}, G_{38}, H_{39}) $^{>>7}$ + A_{32} $^{>>11}$ +X_0 + 0x9216D5D9;
Step41: $B_{41} = F_2$ (C_{34}, D_{35}, E_{36}, F_{37}, G_{38}, H_{39}, A_{40}) $^{>>7}$ + B_{33} $^{>>11}$ +X_{23} + 0x8979FB1B;
Step42: $C_{42} = F_2$ (D_{35}, E_{36}, F_{37}, G_{38}, H_{39}, A_{40}, B_{41}) $^{>>7}$ + C_{34} $^{>>11}$ +X_{20} + 0xD1310BA6;
Step43: $D_{43} = F_2$ (E_{36}, F_{37}, G_{38}, H_{39}, A_{40}, B_{41}, C_{42}) $^{>>7}$ + D_{35} $^{>>11}$ +X_{22} + 0x98DFB5AC;
Step44: $E_{44} = F_2$ (F_{37}, G_{38}, H_{39}, A_{40}, B_{41}, C_{42}, D_{43}) $^{>>7}$ + E_{36} $^{>>11}$ +X_1 + 0x2FFD72DB;
Step45: $F_{45} = F_2$ (G_{38}, H_{39}, A_{40}, B_{41}, C_{42}, D_{43}, E_{44}) $^{>>7}$ + F_{37} $^{>>11}$ +X_{10} + 0xD01ADFB7;

Step46: $G_{46} = F_2(H_{39}, A_{40}, B_{41}, C_{42}, D_{43}, E_{44}, F_{45})^{\gg 7} + G_{38}^{\gg 11} + X_4 + 0xB8E1AFED;$

Step47: $H_{47} = F_2(A_{40}, B_{41}, C_{42}, D_{43}, E_{44}, F_{45}, G_{46})^{\gg 7} + H_{39}^{\gg 11} + X_8 + 0x6A267E96;$

Step48: $A_{48} = F_2(B_{41}, C_{42}, D_{43}, E_{44}, F_{45}, G_{46}, H_{47})^{\gg 7} + A_{40}^{\gg 11} + X_{30} + 0xBA7C9045;$

Step49: $B_{49} = F_2(C_{42}, D_{43}, E_{44}, F_{45}, G_{46}, H_{47}, A_{48})^{\gg 7} + B_{41}^{\gg 11} + X_3 + 0xF12C7F99;$

Step50: $C_{50} = F_2(D_{43}, E_{44}, F_{45}, G_{46}, H_{47}, A_{48}, B_{49})^{\gg 7} + C_{42}^{\gg 11} + X_{21} + 0x24A19947;$

Step51: $D_{51} = F_2(E_{44}, F_{45}, G_{46}, H_{47}, A_{48}, B_{49}, C_{50})^{\gg 7} + D_{43}^{\gg 11} + X_9 + 0xB3916CF7;$

Step52: $E_{52} = F_2(F_{45}, G_{46}, H_{47}, A_{48}, B_{49}, C_{50}, D_{51})^{\gg 7} + E_{44}^{\gg 11} + X_{17} + 0x0801F2E2;$

Step53: $F_{53} = F_2(G_{46}, H_{47}, A_{48}, B_{49}, C_{50}, D_{51}, E_{52})^{\gg 7} + F_{45}^{\gg 11} + X_{24} + 0x858EFC16;$

Step54: $G_{54} = F_2(H_{47}, A_{48}, B_{49}, C_{50}, D_{51}, E_{52}, F_{53})^{\gg 7} + G_{46}^{\gg 11} + X_{29} + 0x636920D8;$

Step55: $H_{55} = F_2(A_{48}, B_{49}, C_{50}, D_{51}, E_{52}, F_{53}, G_{54})^{\gg 7} + H_{47}^{\gg 11} + X_6 + 0x71574E69;$

Step56: $A_{56} = F_2(B_{49}, C_{50}, D_{51}, E_{52}, F_{53}, G_{54}, H_{55})^{\gg 7} + A_{48}^{\gg 11} + X_{19} + 0xA458FEA3;$

Step57: $B_{57} = F_2(C_{50}, D_{51}, E_{52}, F_{53}, G_{54}, H_{55}, A_{56})^{\gg 7} + B_{49}^{\gg 11} + X_{12} + 0xF4933D7E;$

Step58: $C_{58} = F_2(D_{51}, E_{52}, F_{53}, G_{54}, H_{55}, A_{56}, B_{57})^{\gg 7} + C_{50}^{\gg 11} + X_{15} + 0x0D95748F;$

Step59: $D_{59} = F_2(E_{52}, F_{53}, G_{54}, H_{55}, A_{56}, B_{57}, C_{58})^{\gg 7} + D_{51}^{\gg 11} + X_{13} + 0x728EB658;$

Step60: $E_{60} = F_2(F_{53}, G_{54}, H_{55}, A_{56}, B_{57}, C_{58}, D_{59})^{\gg 7} + E_{52}^{\gg 11} + X_2 + 0x718BCD58;$

Step61: $F_{61} = F_2(G_{54}, H_{55}, A_{56}, B_{57}, C_{58}, D_{59}, E_{60})^{\gg 7} + F_{53}^{\gg 11} + X_{25} + 0x82154AEE;$

Step62: $G_{62} = F_2(H_{55}, A_{56}, B_{57}, C_{58}, D_{59}, E_{60}, F_{61})^{\gg 7} + G_{54}^{\gg 11} + X_{31} + 0x7B54A41D;$

Step63: $H_{63} = F_2(A_{56}, B_{57}, C_{58}, D_{59}, E_{60}, F_{61}, G_{62})^{\gg 7} + H_{55}^{\gg 11} + X_{27} + 0xC25A59B5;$

Pass3 $F_3(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_0x_2x_6 \oplus x_2x_3 \oplus x_0x_4 \oplus x_1x_6 \oplus x_5x_6 \oplus x_5$

Step64: $A_{64} = F_3(B_{57}, C_{58}, D_{59}, E_{60}, F_{61}, G_{62}, H_{63})^{\gg 7} + A_{56}^{\gg 11} + X_{19} + 0x9C30D539;$

Step65: $B_{65} = F_3(C_{58}, D_{59}, E_{60}, F_{61}, G_{62}, H_{63}, A_{64})^{\gg 7} + B_{57}^{\gg 11} + X_9 + 0x2AF26013;$

Step66: $C_{66} = F_3(D_{59}, E_{60}, F_{61}, G_{62}, H_{63}, A_{64}, B_{65})^{\gg 7} + C_{58}^{\gg 11} + X_4 + 0xC5D1B023;$

Step67: $D_{67} = F_3(E_{60}, F_{61}, G_{62}, H_{63}, A_{64}, B_{65}, C_{66})^{\gg 7} + D_{59}^{\gg 11} + X_{20} + 0x286085F0;$

Step68: $E_{68} = F_3(F_{61}, G_{62}, H_{63}, A_{64}, B_{65}, C_{66}, D_{67})^{\gg 7} + E_{60}^{\gg 11} + X_{28} + 0xCA417918;$

Step69: $F_{69} = F_3(G_{62}, H_{63}, A_{64}, B_{65}, C_{66}, D_{67}, E_{68})^{\gg 7} + F_{61}^{\gg 11} + X_{17} + 0xB8DB38EF;$

Step70: $G_{70} = F_3(H_{63}, A_{64}, B_{65}, C_{66}, D_{67}, E_{68}, F_{69})^{\gg 7} + G_{62}^{\gg 11} + X_8 + 0x8E79DCB0;$

Step71: $H_{71} = F_3(A_{64}, B_{65}, C_{66}, D_{67}, E_{68}, F_{69}, G_{70})^{\gg 7} + H_{63}^{\gg 11} + X_{22} + 0x603A180E;$

Step72: $A_{72} = F_3(B_{65}, C_{66}, D_{67}, E_{68}, F_{69}, G_{70}, H_{71})^{\gg 7} + A_{64}^{\gg 11} + X_{29} + 0x6C9E0E8B;$

Step73: $B_{73} = F_3(C_{66}, D_{67}, E_{68}, F_{69}, G_{70}, H_{71}, A_{72})^{\gg 7} + B_{65}^{\gg 11} + X_{14} + 0xB01E8A3E;$

Step74: $C_{74} = F_3(D_{67}, E_{68}, F_{69}, G_{70}, H_{71}, A_{72}, B_{73})^{\gg 7} + C_{66}^{\gg 11} + X_{25} + 0xD71577C1;$

Step75: $D_{75} = F_3(E_{68}, F_{69}, G_{70}, H_{71}, A_{72}, B_{73}, C_{74})^{\gg 7} + D_{67}^{\gg 11} + X_{12} + 0xBD314B27;$

Step76: $E_{76} = F_3(F_{69}, G_{70}, H_{71}, A_{72}, B_{73}, C_{74}, D_{75})^{\gg 7} + E_{68}^{\gg 11} + X_{24} + 0x78AF2FDA;$

Step77: $F_{77} = F_3(G_{70}, H_{71}, A_{72}, B_{73}, C_{74}, D_{75}, E_{76})^{\gg 7} + F_{69}^{\gg 11} + X_{30} + 0x55605C60;$

Step78: $G_{78} = F_3(H_{71}, A_{72}, B_{73}, C_{74}, D_{75}, E_{76}, F_{77})^{\gg 7} + G_{70}^{\gg 11} + X_{16} + 0xE65525F3;$

Step79: $H_{79} = F_3(A_{72}, B_{73}, C_{74}, D_{75}, E_{76}, F_{77}, G_{78})^{\gg 7} + H_{71}^{\gg 11} + X_{26} + 0xAA55AB94;$

Step80: $A_{80} = F_3(B_{73}, C_{74}, D_{75}, E_{76}, F_{77}, G_{78}, H_{79})^{\gg 7} + A_{72}^{\gg 11} + X_{31} + 0x57489862;$

Step81: $B_{81} = F_3(C_{74}, D_{75}, E_{76}, F_{77}, G_{78}, H_{79}, A_{80})^{\gg 7} + B_{73}^{\gg 11} + X_{15} + 0x63E81440;$

Step82: $C_{82} = F_3(D_{75}, E_{76}, F_{77}, G_{78}, H_{79}, A_{80}, B_{81})^{\gg 7} + C_{74}^{\gg 11} + X_7 + 0x55CA396A;$

Step83: $D_{83} = F_3(E_{76}, F_{77}, G_{78}, H_{79}, A_{80}, B_{81}, C_{82})^{\gg 7} + D_{75}^{\gg 11} + X_3 + 0x2AAB10B6;$

Step84: $E_{84} = F_3(F_{77}, G_{78}, H_{79}, A_{80}, B_{81}, C_{82}, D_{83})^{\gg 7} + E_{76}^{\gg 11} + X_1 + 0xB4CC5C34;$

Step85: $F_{85} = F_3(G_{78}, H_{79}, A_{80}, B_{81}, C_{82}, D_{83}, E_{84})^{\gg 7} + F_{77}^{\gg 11} + X_0 + 0x1141E8CE;$

Step86: $G_{86} = F_3(H_{79}, A_{80}, B_{81}, C_{82}, D_{83}, E_{84}, F_{85})^{\gg 7} + G_{78}^{\gg 11} + X_{18} + 0xA15486AF;$

Step87: $H_{87} = F_3(A_{80}, B_{81}, C_{82}, D_{83}, E_{84}, F_{85}, G_{86})^{\gg 7} + H_{79}^{\gg 11} + X_{27} + 0x7C72E993;$

Step88: $A_{88} = F_3(B_{81}, C_{82}, D_{83}, E_{84}, F_{85}, G_{86}, H_{87})^{\gg 7} + A_{80}^{\gg 11} + X_{13} + 0xB3EE1411;$

Step89: $B_{89} = F_3(C_{82}, D_{83}, E_{84}, F_{85}, G_{86}, H_{87}, A_{88})^{\gg 7} + B_{81}^{\gg 11} + X_6 + 0x636FBC2A;$

Step90: $C_{90} = F_3(D_{83}, E_{84}, F_{85}, G_{86}, H_{87}, A_{88}, B_{89})^{\gg 7} + C_{82}^{\gg 11} + X_{21} + 0x2BA9C55D;$

Step91: $D_{91} = F_3(E_{84}, F_{85}, G_{86}, H_{87}, A_{88}, B_{89}, C_{90})^{\gg 7} + D_{83}^{\gg 11} + X_{10} + 0x741831F6;$

Step92: $E_{92} = F_3(F_{85}, G_{86}, H_{87}, A_{88}, B_{89}, C_{90}, D_{91})^{\gg 7} + E_{84}^{\gg 11} + X_{23} + 0xCE5C3E16;$

Step93: $F_{93} = F_3(G_{86}, H_{87}, A_{88}, B_{89}, C_{90}, D_{91}, E_{92})^{\gg 7} + F_{85}^{\gg 11} + X_{11} + 0x9B87931E;$

Step94: $G_{94} = F_3\ (H_{87},\ A_{88},\ B_{89},\ C_{90},\ D_{91},\ E_{92},\ F_{93})^{\gg 7} + G_{86}^{\gg 11} + X_5 + 0xAFD6BA33;$

Step95: $H_{95} = F_3\ (A_{88},\ B_{89},\ C_{90},\ D_{91},\ E_{92},\ F_{93},\ G_{94})^{\gg 7} + H_{87}^{\gg 11} + X_2 + 0x6C24CF5C;$

Pass4

$$F_4(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_1x_2x_5 \oplus x_0x_2x_4 \oplus x_0x_5x_6 \oplus x_0x_1 \oplus x_2x_6 \oplus x_0x_5 \oplus x_4x_5 \oplus x_5x_6 \oplus x_0x_4 \oplus x_0x_6 \oplus x_0x_3 \oplus x_3$$

Step96: $A_{96} = F_4\ (B_{89},\ C_{90},\ D_{91},\ E_{92},\ F_{93},\ G_{94},\ H_{95})^{\gg 7} + A_{88}^{\gg 11} + X_{24} + 0x7A325381;$

Step97: $B_{97} = F_4\ (C_{90},\ D_{91},\ E_{92},\ F_{93},\ G_{94},\ H_{95},\ A_{96})^{\gg 7} + B_{89}^{\gg 11} + X_4 + 0x28958677;$

Step98: $C_{98} = F_4\ (D_{91},\ E_{92},\ F_{93},\ G_{94},\ H_{95},\ A_{96},\ B_{97})^{\gg 7} + C_{90}^{\gg 11} + X_0 + 0x3B8F4898;$

Step99: $D_{99} = F_4\ (E_{92},\ F_{93},\ G_{94},\ H_{95},\ A_{96},\ B_{97},\ C_{98})^{\gg 7} + D_{91}^{\gg 11} + X_{14} + 0x6B4BB9AF;$

Step100: $E_{100} = F_4\ (F_{93},\ G_{94},\ H_{95},\ A_{96},\ B_{97},\ C_{98},\ D_{99})^{\gg 7} + E_{92}^{\gg 11} + X_2 + 0xC4BFE81B;$

Step101: $F_{101} = F_4\ (G_{94},\ H_{95},\ A_{96},\ B_{97},\ C_{98},\ D_{99},\ E_{100})^{\gg 7} + F_{93}^{\gg 11} + X_7 + 0x66282193;$

Step102: $G_{102} = F_4\ (H_{95},\ A_{96},\ B_{97},\ C_{98},\ D_{99},\ E_{100},\ F_{101})^{\gg 7} + G_{94}^{\gg 11} + X_{28} + 0x61D809CC;$

Step103: $H_{103} = F_4\ (A_{96},\ B_{97},\ C_{98},\ D_{99},\ E_{100},\ F_{101},\ G_{102})^{\gg 7} + H_{95}^{\gg 11} + X_{23} + 0xFB21A991;$

Step104: $A_{104} = F_4\ (B_{97},\ C_{98},\ D_{99},\ E_{100},\ F_{101},\ G_{102},\ H_{103})^{\gg 7} + A_{96}^{\gg 11} + X_{26} + 0x487CAC60;$

Step105: $B_{105} = F_4\ (C_{98},\ D_{99},\ E_{100},\ F_{101},\ G_{102},\ H_{103},\ A_{104})^{\gg 7} + B_{97}^{\gg 11} + X_6 + 0x5DEC8032;$

Step106: $C_{106} = F_4\ (D_{99},\ E_{100},\ F_{101},\ G_{102},\ H_{103},\ A_{104},\ B_{105})^{\gg 7} + C_{98}^{\gg 11} + X_{30} + 0xEF845D5D;$

Step107: $D_{107} = F_4\ (E_{100},\ F_{101},\ G_{102},\ H_{103},\ A_{104},\ B_{105},\ C_{106})^{\gg 7} + D_{99}^{\gg 11} + X_{20} + 0xE98575B1;$

Step108: $E_{108} = F_4\ (F_{101},\ G_{102},\ H_{103},\ A_{104},\ B_{105},\ C_{106},\ D_{107})^{\gg 7} + E_{100}^{\gg 11} + X_{18} + 0xDC262302;$

Step109: $F_{109} = F_4\ (G_{102},\ H_{103},\ A_{104},\ B_{105},\ C_{106},\ D_{107},\ E_{108})^{\gg 7} + F_{101}^{\gg 11} + X_{25} + 0xEB651B88;$

Step110: $G_{110} = F_4\ (H_{103},\ A_{104},\ B_{105},\ C_{106},\ D_{107},\ E_{108},\ F_{109})^{\gg 7} + G_{102}^{\gg 11} + X_{19} + 0x23893E81;$

Step111: $H_{111} = F_4\ (A_{104},\ B_{105},\ C_{106},\ D_{107},\ E_{108},\ F_{109},\ G_{110})^{\gg 7} + H_{103}^{\gg 11} + X_3 + 0xD396ACC5;$

Step112: $A_{112} = F_4\ (B_{105},\ C_{106},\ D_{107},\ E_{108},\ F_{109},\ G_{110},\ H_{111})^{\gg 7} + A_{104}^{\gg 11} + X_{22} + 0x0F6D6FF3;$

Step113: $B_{113} = F_4\ (C_{106},\ D_{107},\ E_{108},\ F_{109},\ G_{110},\ H_{111},\ A_{112})^{\gg 7} + B_{105}^{\gg 11} + X_{11} + 0x83F44239;$

Step114: $C_{114} = F_4\ (D_{107},\ E_{108},\ F_{109},\ G_{110},\ H_{111},\ A_{112},\ B_{113})^{\gg 7} + C_{106}^{\gg 11} + X_{31} + 0x2E0B4482;$

Step115: $D_{115} = F_4\ (E_{108},\ F_{109},\ G_{110},\ H_{111},\ A_{112},\ B_{113},\ C_{114})^{\gg 7} + D_{107}^{\gg 11} + X_{21} + 0xA4842004;$

Step116: $E_{116} = F_4\ (F_{109},\ G_{110},\ H_{111},\ A_{112},\ B_{113},\ C_{114},\ D_{115})^{\gg 7} + E_{108}^{\gg 11} + X_8 + 0x69C8F04A;$

Step117: $F_{117} = F_4\ (G_{110},\ H_{111},\ A_{112},\ B_{113},\ C_{114},\ D_{115},\ E_{116})^{\gg 7} + F_{109}^{\gg 11} + X_{27} + 0x9E1F9B5E;$

Step118: $G_{118} = F_4\ (H_{111},\ A_{112},\ B_{113},\ C_{114},\ D_{115},\ E_{116},\ F_{117})^{\gg 7} + G_{110}^{\gg 11} + X_{12} + 0x21C66842;$

Step119: $H_{119} = F_4\ (A_{112},\ B_{113},\ C_{114},\ D_{115},\ E_{116},\ F_{117},\ G_{118})^{\gg 7} + H_{111}^{\gg 11} + X_9 + 0xF6E96C9A;$

Step120: $A_{120} = F_4\ (B_{113},\ C_{114},\ D_{115},\ E_{116},\ F_{117},\ G_{118},\ H_{119})^{\gg 7} + A_{112}^{\gg 11} + X_1 + 0x670C9C61;$

Step121: $B_{121} = F_4\ (C_{114},\ D_{115},\ E_{116},\ F_{117},\ G_{118},\ H_{119},\ A_{120})^{\gg 7} + B_{113}^{\gg 11} + X_{29} + 0xABD388F0;$

Step122: $C_{122} = F_4\ (D_{115},\ E_{116},\ F_{117},\ G_{118},\ H_{119},\ A_{120},\ B_{121})^{\gg 7} + C_{114}^{\gg 11} + X_5 + 0x6A51A0D2;$

Step123: $D_{123} = F_4\ (E_{116},\ F_{117},\ G_{118},\ H_{119},\ A_{120},\ B_{121},\ C_{122})^{\gg 7} + D_{115}^{\gg 11} + X_{15} + 0xD8542F68;$

Step124: $E_{124} = F_4\ (F_{117},\ G_{118},\ H_{119},\ A_{120},\ B_{121},\ C_{122},\ D_{123})^{\gg 7} + E_{116}^{\gg 11} + X_{17} + 0x960FA728;$

Step125: $F_{125} = F_4\ (G_{118},\ H_{119},\ A_{120},\ B_{121},\ C_{122},\ D_{123},\ E_{124})^{\gg 7} + F_{117}^{\gg 11} + X_{10} + 0xAB5133A3;$

Step126: $G_{126} = F_4\ (H_{119},\ A_{120},\ B_{121},\ C_{122},\ D_{123},\ E_{124},\ F_{125})^{\gg 7} + G_{118}^{\gg 11} + X_{16} + 0x6EEF0B6C;$

Step127: $H_{127} = F_4\ (A_{120},\ B_{121},\ C_{122},\ D_{123},\ E_{124},\ F_{125},\ G_{126})^{\gg 7} + H_{119}^{\gg 11} + X_{13} + 0x137A3BE4;$

Finally, the eight-word output of the compression function is computed with a feed-forward of the initial value:

$A=IV-A+A_{120}$ $B=IV-B+B_{121}$ $C=IV-C+C_{122}$ $D=IV-D+D_{123}$

$E=IV-E+E_{124}$ $F=IV-F+F_{125}$ $G=IV-G+G_{126}$ $H=IV-H+H_{127}$

The obtained words (A, B, C, D, E, F, G, H) serve as initial value for the next application of the compression function. In the end, the concatenated 256-bit value H||G||F||E||D||C||B||A serves as hash value of message. There is an optional output transformation, which allows reducing the length of this hash value to 128,160,192 or 224 bits.