Cryptanalysis of the Full HAVAL with 4 and 5 Passes

Hongbo Yu[1], Xiaoyun Wang[2⋆], Aaram Yun[3], and Sangwoo Park[3]

[1] Shandong University, Jinan 250100, China
yhb@mail.sdu.edu.cn
[2] Shandong University and Tsinghua University, China
xywang@sdu.edu.cn
[3] National Security Research Institute,
161 Gajeong-dong, Yuseong-gu, Daejeon 305-350, Korea
{aaram, psw}@etri.re.kr

Abstract. HAVAL is a cryptographic hash function with variable digest size proposed by Zheng, Pieprzyk and Seberry in 1992. It has three variants, 3-, 4-, and 5-pass HAVAL. Previous results on HAVAL suggested only practical collision attacks for 3-pass HAVAL. In this paper, we present collision attacks for 4 and 5 pass HAVAL. For 4-pass HAVAL, we describe two practical attacks for finding 2-block collisions, one with 2^{43} computations and the other with 2^{36} computations. In addition, we show that collisions for 5-pass HAVAL can be found with about 2^{123} computations, which is the first attack more efficient than the birthday attack.

Keywords: Hash function, collision, differential path, message modification

1 Introduction

The hash function HAVAL was proposed by Zheng, Pieprzyk and Seberry at Auscrypt '92 [11]. It has a similar structure as the well-known hash functions such as MD4 [3] and MD5 [4]. In Asiacrypt '03, Rompay et al. gave a collision attack for 3-pass HAVAL with complexity 2^{29} computations [1]. The fastest attack on 3-pass HAVAL was presented by X.Y.Wang et al. [5], and it can find a collision with time complexity less than 2^7 computations. In SCN 2004, Y.Yoshida et al. showed that the compression functions of full 4-pass and 5-pass HAVAL are not random and can be distinguished from a truly random function [2].

In this paper, we use the method of *modular differential* to analyze the full 4-pass and 5-pass HAVAL. This method was presented early in 1997 by X.Y.Wang [10], and formalized in Eurocrypt '05 [6, 7]. This type of cryptanalysis is powerful to break the most prevailing hash functions such as MD4 [6], MD5 [7], SHA-0 [8] and SHA-1 [9].

⋆ Supported by the National Natural Science Foundation of China (NSFC Grant No.90604036 and No.60525201) and 973 Project (No.2004CB318000)

In this paper, we provide two practical attacks for 4-pass HAVAL, with 2^{43} and 2^{36} HAVAL computations, respectively. In addition, we give the first theoretical attack for 5-pass HAVAL with a complexity less than 2^{123} computations.

The rest of the paper is organized as follows: in Section 2, we give a brief description of HAVAL algorithm. In section 3, we introduce some basic conclusions and notations used in our paper. The attack details are described in Sections 4, 5, and 6. Section 7 concludes the paper.

2 Description of HAVAL

In this section we provide a brief description of HAVAL. Since the structure of 4-pass and 5-pass version of HAVAL are essentially the same, here we only give the description of 4-pass HAVAL. We use modified and simplified notations than those in the original paper [11], and omit all non-relevant parts.

Although HAVAL supports digest sizes of 128, 160, 192, 224, and 256 bits, the main algorithm computes 256-bit digests and the other sizes are supported by post-processing the 256-bit hash value. Therefore for our purposes we may consider HAVAL as a hash function with output size of 256 bits.

HAVAL is a Merkle-Damgård hash function, which uses a compression function to digest messages. The compression function H of HAVAL takes a 1024-bit message and a 256-bit initial value as input, and produces 256-bit hash value as output. The message is represented as 32 message words, m_0, m_1, ..., m_{31}, each consisting of 32 bits. The 256-bit initial value (or chaining value) is represented as the following 8 words, a_0, b_0, ..., and h_0:

$a_0 = 0x243f6a88$, $b_0 = 0x85a308d3$, $c_0 = 0x13198a2e$, $d_0 = 0x03707344$,
$e_0 = 0xa4093822$, $f_0 = 0x299f31d0$, $g_0 = 0x082efa98$, $h_0 = 0xec4e6c89$.

4-pass HAVAL uses the following four boolean functions:

Pass	Function
1	$f_1(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_0 \oplus x_0x_3 \oplus x_1x_3 \oplus x_2x_4 \oplus x_5x_6$
2	$f_2(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_1x_3 \oplus x_4 \oplus x_1x_4 \oplus x_0x_5 \oplus x_2x_5 \oplus x_1x_2x_5 \oplus x_1x_6 \oplus x_0x_1x_6 \oplus x_2x_6$
3	$f_3(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_2x_3 \oplus x_0x_4 \oplus x_5 \oplus x_1x_6 \oplus x_0x_2x_6 \oplus x_5x_6$
4	$f_4(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = x_0x_1 \oplus x_3 \oplus x_0x_3 \oplus x_0x_4 \oplus x_0x_2x_4 \oplus x_0x_5 \oplus x_1x_2x_5 \oplus x_4x_5 \oplus x_0x_6 \oplus x_2x_6 \oplus x_5x_6 \oplus x_0x_5x_6$

In HAVAL, the boolean functions are applied bitwisely to 32-bit input variables to produce 32-bit output values.

4-Pass HAVAL Compression Function Given a 1024-bit message block $M = (m_0, m_1, ..., m_{31})$, the compressing process is as follows:

1. Let $(aa, bb, cc, dd, ee, ff, gg, hh)$ be the input of compressing process for M. Initialize chaining variables (a, b, c, d, e, f, g, h) as $(aa, bb, cc, dd, ee, ff, gg, hh)$.
2. Perform the following 128 steps:
   For j=1, 2, 3, and 4
   For $i = 0$ to 31
   $p := f_j(g, f, e, d, c, b, a)$
   $r := (p \gg 7) + (h \gg 11) + m_{ord(j,i)} + k_{j,i}$
   $h := g,\ g := f,\ f := e,\ e := d,\ d := c,\ c := b,\ b := a,\ a := r$
   The operation in each step employs a constant $k_{j,i}$(See ref.[11]). $\gg s$ represents the s bit rotation to the right. $+$ denotes addition modulo 2^{32}. The orders of message words in each pass can refer to [11].
3. Add a, b, c, d, e, f, g, h respectively to the input value, i.e.,
   $aa := a + aa$, $bb := b + bb$, ..., $hh := h + hh$
4. $H(M) = hh \| gg \| ff \| ee \| dd \| cc \| bb \| aa$, where $\|$ denotes the bit concatenation.

3 Some Basic Conclusions and Notations

In this section, we give several properties of the four boolean functions f_1, f_2, f_3, f_4.

Proposition Let $y_1 = f_1(x_6, x_5, x_4, x_3, x_2, x_1, x_0)$, and $y_{1,x_i} = f_1(x_6, ..., x_{i+1}, \neg x_i, ..., x_0)$, where $\neg x_i$ is the complement of the bit x_i. Then

1. $y_1 = y_{1,x_0} \iff x_3 = 1$.
   $y_1 = x_0$ and $y_{1,x_0} = \neg x_0 \iff x_3 = 0$ and $x_1x_3 \oplus x_5x_6 \oplus x_2x_4 = 0$.
   $y_1 = \neg x_0$ and $y_{1,x_0} = x_0 \iff x_3 = 0$ and $x_1x_3 \oplus x_5x_6 \oplus x_2x_4 = 1$.
2. $y_1 = y_{1,x_1} \iff x_3 = 0$.
   $y_1 = x_1$ and $y_{1,x_1} = \neg x_1 \iff x_3 = 1$ and $x_5x_6 \oplus x_2x_4 \oplus x_0x_3 \oplus x_0 = 0$.
   $y_1 = \neg x_1$ and $y_{1,x_1} = x_1 \iff x_3 = 1$ and $x_5x_6 \oplus x_2x_4 \oplus x_0x_3 \oplus x_0 = 1$.
3. $y_1 = y_{1,x_2} \iff x_4 = 0$.
   $y_1 = x_2$ and $y_{1,x_2} = \neg x_2 \iff x_4 = 1$ and $x_1x_3 \oplus x_5x_6 \oplus x_0x_3 \oplus x_0 = 0$.
   $y_1 = \neg x_2$ and $y_{1,x_2} = x_2 \iff x_4 = 1$ and $x_1x_3 \oplus x_5x_6 \oplus x_0x_3 \oplus x_0 = 1$.
4. $y_1 = y_{1,x_3} \iff x_0 \oplus x_1 = 0$.
   $y_1 = x_3$ and $y_{1,x_3} = \neg x_3 \iff x_0 \oplus x_1 = 1$ and $x_5x_6 \oplus x_2x_4 \oplus x_0 = 0$.
   $y_1 = \neg x_3$ and $y_{1,x_3} = x_3 \iff x_0 \oplus x_1 = 1$ and $x_5x_6 \oplus x_2x_4 \oplus x_0 = 1$.
5. $y_1 = y_{1,x_4} \iff x_2 = 0$.
   $y_1 = x_4$ and $y_{1,x_4} = \neg x_4 \iff x_2 = 1$ and $x_1x_3 \oplus x_5x_6 \oplus x_0x_3 \oplus x_0 = 0$.
   $y_1 = \neg x_4$ and $y_{1,x_4} = x_4 \iff x_2 = 1$ and $x_1x_3 \oplus x_5x_6 \oplus x_0x_3 \oplus x_0 = 1$.
6. $y_1 = y_{1,x_5} \iff x_6 = 0$.
   $y_1 = x_5$ and $y_1 = \neg y_{1,x_5} \iff x_6 = 1$ and $x_1x_3 \oplus x_2x_4 \oplus x_0x_3 \oplus x_0 = 0$.
   $y_1 = \neg x_5$ and $y_1 = y_{1,x_5} \iff x_6 = 1$ and $x_1x_3 \oplus x_2x_4 \oplus x_0x_3 \oplus x_0 = 1$.
7. $y_1 = y_{1,x_6} \iff x_5 = 0$.
   $y_1 = x_6$ and $y_1 = \neg y_{1,x_6} \iff x_5 = 1$ and $x_3x_1 \oplus x_2x_4 \oplus x_0x_3 \oplus x_0 = 0$.
   $y_1 = \neg x_6$ and $y_1 = y_{1,x_6} \iff x_5 = 1$ and $x_3x_1 \oplus x_2x_4 \oplus x_0x_3 \oplus x_0 = 1$.

Here, $x_i \in \{0, 1\}$ $(0 \le i \le 6)$.

It is easy to deduce the similar properties of the other three functions f_2, f_3 and f_4. We omit them because of the limited pages.

Notations In order to describe our attack conveniently, we define some notations.

1. $M = (m_i)_{i<32}$ and $M' = (m'_i)_{i<32}$ denote a collection of 32 words respectively.
2. $\Delta m_i = m'_i - m_i$, $\Delta a_i = a'_i - a_i$, ..., $\Delta h_i = h'_i - h_i$, $\Delta p_i = p'_i - p_i$ denote the modular differences of two variables.
3. a_i, b_i, c_i, d_i, e_i, f_i, g_i, h_i and a'_i, b'_i, c'_i, d'_i, e'_i, f'_i, g'_i, h'_i denote the chaining variables after the i-th step corresponding to the message blocks M and M' respectively. According to the HAVAL algorithm, we know that $b_i = a_{i-1}$, $c_i = a_{i-2}$, $d_i = a_{i-3}$, $e_i = a_{i-4}$, $f_i = a_{i-5}$, $g_i = a_{i-6}$, $h_i = a_{i-7}$.
4. $x_{i,j}$ denotes the j-th bit of 32-bit word x_i. For example, $a_{i,j}$ is the j-th bit of a_i.
5. $x_i[j]$ is the value obtained by modifying the jth bit of x_i from 0 to 1 (hence this notation implicitly states that $x_{i,j} = 0$. Similarly, $x_i[-j]$ is the value obtained by modifying the jth bit of x_i from 1 to 0.
6. $x_i[\pm j_1, \pm j_2, \ldots, \pm j_k]$ is shorthand for $x_i[\pm j_1][\pm j_2] \ldots [\pm j_k]$, i.e., modifying x_i at bit positions j_1, ..., j_k according to the $\pm$ signs.

4 The Attack against 4-Pass HAVAL with One Message Word Difference

Our collision attack can be divided into three phases: 1. Choose a appropriate message difference and deduce the differential path according to the specified message difference. 2. Determine the corresponding chaining variable conditions. 3. Fulfill the message modification to guarantee that a portion of the conditions hold.

We have obtained two collision attacks for 4-pass HAVAL. Both methods find two-block collisions, i.e., collision pairs consisting of two 2048-bit messages $M_0 \| M_1$ and $M'_0 \| M'_1$. Since both attacks use essentially the same methodology, we will briefly give an outline for the first attack in this section, and then give more detailed exposition for the second attack in the next section.

In the first method, message differences are given only on the message word m_5 with difference 2^{31}. That is, for both blocks M_0 and M_1, we have

$$\Delta m_i = m'_i - m_i = \begin{cases} 2^{31} & \text{if } i = 5, \\ 0 & \text{otherwise.} \end{cases}$$

In the first block, the difference introduced at step 6 by m_5 is propagated until step 33, where m_5 is again used and the first inner collision is produced. The message word m_5 is again used at step 95, near the end of the pass 3. From step 95 to step 122, the differences are propagated so that at each step only one chaining variable difference is active. At step 123, the message word m_5 is again used and from then two chaining variables are active at each step, ending up as a near-collision with two active variables.

In the second block, the initial differences produced by the first block, as well as the one introduced by m_5 at step 6 is again eliminated at step 33. From step 95 to the end of the second block, the differences propagate in a similar fashion as in the first block, except that all the signs are reversed. Therefore at the end of the second block the output differences cancel the input difference of the second block, producing a two-block collision. The differential paths are given in Table 4 and Table 5. Due to space constraint, we will omit the tables for sufficient conditions for the differential paths.

Using the message modification technique, explained in Section 5.3, we may satisfy all the conditions in the first pass with probability 1. Therefore the probability for the third and fourth passes is the success probability of the whole algorithm, which can be estimated to be greater than 2^{-43}. In Table 1 we provide an example of a collision pair we found.

Note that the message word m_5 appears at step 33, the beginning of the second pass, and it again appears at step 95, almost at the end of the third pass, which gives a long stretch of steps without differences.

Table 1. A collision pair for 4-pass HAVAL. H is the common hash value with little-endian and no message padding.

M_0	00000000	00000000	00000000	00000080	00000000	00000080	00000080	00000000
	00000000	00000000	00002000	0000e0ff	0000e0ff	00000000	0080f3ff	00c0ecff
	0040ecff	0040ffff	0080feff	0080feff	0080ffff	00fcffff	00000000	00fcffff
	00fcffff	00fcffff	00000000	00fcffff	00000000	00000000	40070000	d9dc1fdc
M_1	0000e87f	0000f8ff	0020f0ff	000100ff	00ff0174	000ff0f2	c001e484	00daf1fb
	c01706fa	80eff3f9	00d6f1ff	80f7ff1f	f7fffd40	00000000	00200028	0000003e
	00002088	000020a0	00007ef9	00000008	00c045ba	00003bc0	003cfcfc	007c1f03
	00bc81fe	00c4ddfb	003cfeff	00000000	00000000	00000200	3f000000	a095d965
M_0	00000000	00000000	00000000	00000080	00000000	00000000	00000080	00000000
	00000000	00000000	00002000	0000e0ff	0000e0ff	00000000	0080f3ff	00c0ecff
	0040ecff	0040ffff	0080feff	0080feff	0080ffff	00fcffff	00000000	00fcffff
	00fcffff	00fcffff	00000000	00fcffff	00000000	00000000	40070000	d9dc1fdc
M_1	0000e87f	0000f8ff	0020f0ff	000100ff	00ff0174	000ff072	c001e484	00daf1fb
	c01706fa	80eff3f9	00d6f1ff	80f7ff1f	f7fffd40	00000000	00200028	0000003e
	00002088	000020a0	00007ef9	00000008	00c045ba	00003bc0	003cfcfc	007c1f03
	00bc81fe	00c4ddfb	003cfeff	00000000	00000000	00000200	3f000000	a095d965
H	481a1bf8	04defc01	a62b7444	63979a59	93e9b12d	b20d82bd	7e626c25	22db74ca

5 The Attack against 4-Pass HAVAL with Two Message Word Differences

5.1 Choosing the Differential Path

For this second attack, we have found another differential path using differences at message words m_8 and m_{16}. In the first block, we will use $\Delta m_8 = 2^{13}$ and $\Delta m_{16} = -2^2$, and in the second block $\Delta m_8 = -2^{13}$ and $\Delta m_{16} = 2^2$.

The differential path for the first block consists of two inner collisions in steps 9–48 and steps 71–79, and a near-collision (steps 117–128). The path for the second block has similar structure.

The main difference between this attack and the attack described in Section 4 is that, in the current attack we also use the advanced message modification technique, which will be explained in Subsection 5.3. This enables us to correct more conditions in the second pass. Therefore here we can afford to have our first inner collision to stretch further into the second pass by using two message word differences. Hence we select ΔM_0 and ΔM_1 to ensure that in this path the differences of 3–4 rounds happen with high probability.

5.2 Deriving the Sufficient Conditions for Collision Path

In this section, we derive a set of sufficient conditions, summarized in Table 8, which ensures the collision path to hold. We give an example explaining how to deduce the set of sufficient conditions.

In step 9 of the differential path presented in Table 6, the message difference $\Delta m_8 = 2^{13}$ produces the changed variable $a_9[-14, 15]$. The difference $a_9[-14]$ doesn't produce any more bit differences between step 10 and step 16, and the difference $a_9[15]$ is used to produce the difference $a_{15}[-8, -9, -10, 11]$ in step 15.

1. In step 9, $a'_9 = a_9[-14, 15]$ iff $a_{9,14} = 1$ and $a_{9,15} = 0$.
2. In step 10, $(a_9[-14, 15], a_8, a_7, a_6, a_5, a_4, a_3, a_2)$
   $\rightarrow (a_{10}, a_9[-14, 15], a_8, a_7, a_6, a_5, a_4, a_3)$.
   From 1 of Proposition , $a'_{10} = a_{10}$ iff $a_{6,14} = 1$ and $a_{6,15} = 1$.
3. In step 11, $(a_{10}, a_9[-14, 15], a_8, a_7, a_6, a_5, a_4, a_3)$
   $\rightarrow (a_{11}, a_{10}, a_9[-14, 15], a_8, a_7, a_6, a_5, a_4)$.
   From 2 of Proposition , $a'_{11} = a_{11}$ iff $a_{7,14} = 0$ and $a_{7,15} = 0$.
4. In step 12, $(a_{11}, a_{10}, a_9[-14, 15], a_8, a_7, a_6, a_5, a_4)$
   $\rightarrow (a_{12}, a_{11}, a_{10}, a_9[-14, 15], a_8, a_7, a_6, a_5)$.
   From 3 of Proposition , $a'_{12} = a_{12}$ iff $a_{7,14} = 0$ and $a_{7,15} = 0$.
5. In step 13, $(a_{12}, a_{11}, a_{10}, a_9[-14, 15], a_8, a_7, a_6, a_5)$
   $\rightarrow (a_{13}, a_{12}, a_{11}, a_{10}, a_9[-14, 15], a_8, a_7, a_6)$.
   From 4 of Proposition , $a'_{13} = a_{13}$ iff $a_{12,14} \oplus a_{11,14} = 0$ and $a_{12,15} \oplus a_{11,15} = 0$.
6. In step 14, $(a_{13}, a_{12}, a_{11}, a_{10}, a_9[-14, 15], a_8, a_7, a_6)$
   $\rightarrow (a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, a_9[-14, 15], a_8, a_7)$.
   From 5 of Proposition , $a'_{14} = a_{14}$ iff $a_{11,14} = 0$ and $a_{11,15} = 0$.

7. In step 15, $(a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, a_9[-14, 15], a_8, a_7)$
$\to (a_{15}[-8, -9, -10, 11], a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, a_9[-14, 15], a_8)$.
From 6 of Proposition , $a'_{15} = a_{15}[-8, -9, -10, 11]$ iff
$a_{15,8} = 1$, $a_{15,9} = 1$, $a_{15,10} = 1$, $a_{15,11} = 0$, $a_{8,14} = 0$, $a_{8,15} = 1$ and
$a_{13,15}a_{11,15} \oplus a_{12,15}a_{10,15} \oplus a_{14,15}a_{11,15} \oplus a_{14,15} = 0$.
8. In step 16, $(a_{15}[-8, -9, -10, 11], a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, a_9[-14, 15], a_8)$
$\to (a_{16}[4], a_{15}[-8, -9, -10, 11], a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, a_9[-14, 15])$.
From 6 of Proposition , $a'_{16} = a_{16}[4]$ iff $a_{16,4} = 0$, $a_{10,14} = 0$, $a_{10,15} = 0$,
$a_{12,8} = 1$, $a_{12,9} = 1$, $a_{12,10} = 1$, $a_{12,11} = 0$ and
$a_{14,11}a_{12,11} \oplus a_{10,11}a_{9,11} \oplus a_{13,11}a_{11,11} = 0$.

There are 25 equations in steps 9–16. We can simplify the above 25 conditions and classify them into two types:

- Conditions with exact form
  After a little simplification, there are 24 conditions with exact form, i.e., of form $a_i = 0$ or $a_i = 1$:

  $$a_{16,4} = 0,\ a_{6,14} = 1,\ a_{6,15} = 1,\ a_{7,14} = 0,\ a_{7,15} = 0,\ a_{8,14} = 0,\ a_{8,15} = 1,$$
  $$a_{9,14} = 1,\ a_{9,15} = 0,\ a_{10,14} = 0,\ a_{10,15} = 0,\ a_{11,14} = 0,\ a_{11,15} = 0,\ a_{12,8} = 1,$$
  $$a_{12,9} = 1,\ a_{12,10} = 1,\ a_{12,11} = 0,\ a_{12,14} = 0,\ a_{12,15} = 0,\ a_{14,15} = 0,\ a_{15,8} = 1,$$
  $$a_{15,9} = 1,\ a_{15,10} = 1,\ a_{15,11} = 0$$

  $a_{12,14} = 0$ is derived from two equations: $a_{11,14} \oplus a_{12,14} = 0$ and $a_{11,14} = 0$.
  $a_{12,15} = 0$ is derived from two equations: $a_{11,15} \oplus a_{12,15} = 0$ and $a_{11,15} = 0$.
  $a_{14,15} = 0$ is deduced by the following three equations: $a_{13,15}a_{11,15} \oplus a_{12,15}a_{10,15} \oplus a_{14,15}a_{11,15} \oplus a_{14,15} = 0$, $a_{11,15} = 0$, and $a_{12,15} = 0$.

- Conditions expressed as multi-variable equations:
  There is only one condition which is expressed as a multi-variable equation:

  $$a_{10,11}a_{9,11} \oplus a_{13,11}a_{11,11} = 0 \qquad (1)$$

Each equation with the first form holds with probability $\frac{1}{2}$, and the equation (1) holds with probability $\frac{5}{8}$. So the total probability for the 9-16 step differential is $\frac{5}{2^{27}}$.

Similarly, we can determine all the other conditions which result in the differential paths in Table 6 and Table 7. Summing up all these sufficient conditions, we obtain Table 8 and Table 9.

5.3 Message Modification

We modify M_0 and M_1 so that almost all conditions in Table 8 and 9 hold. The modification include the basic modification and advanced modification techniques.

Basic modification The basic modification is a simple message modification used to ensure all the conditions in the first round (step 1-32) hold. For example, given a message $M_0 = (m_i)_{i<32}$, we compute a_6 and correct a_6 to satisfy the two conditions in Table 8 by setting $a_6 = a_6 \vee 0x6000$, then update m_5 as:

$$m_5 = a_6 - (f(b_0, a_0, a_1, a_2, a_3, a_4, a_5) \gg 7) - (c_0 \gg 11)$$

It is easy to correct all the conditions from step 1 to step 32 of the differential paths in Table 8 and Table 9.

Advanced message modification We correct some more conditions in round 2 by the advanced modification. If the condition on $a_{i,j}$ is wrong, we change the j-th bit of the corresponding message m and some other message words which produce a partial collision in the first round. A sample for correcting $a_{34,4}$ is given in Table 2. We define this kind of corrected condition as *rectifiable condition.*

Table 2. The message modification for correcting $a_{34,4}$

step	m_i	the modified m_i	new variable value	conditions
8	m_7	$m_7 \leftarrow m_7 + 2^{10}$	$a_8[11]$, a_7, a_6, a_5, a_4, a_3, a_2, a_1	$a_{8,11} = 0$
9	m_8		a_9, $a_8[11]$, a_7, a_6, a_5, a_4, a_3, a_2	$a_{5,11} = 1$
10	m_9		a_{10}, a_9, $a_8[11]$, a_7, a_6, a_5, a_4, a_3	$a_{6,11} = 0$
11	m_{10}		a_{11}, a_{10}, a_9, $a_8[11]$, a_7, a_6, a_5, a_4	$a_{6,11} = 0$
12	m_{11}		a_{12}, a_{11}, a_{10}, a_9, $a_8[11]$, a_7, a_6, a_5	$a_{11,11} \oplus a_{10,11} = 0$
13	m_{12}		a_{13}, a_{12}, a_{11}, a_{10}, a_9, $a_8[11]$, a_7, a_6	$a_{10,11} = 0$
14	m_{13}		a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, a_9, $a_8[11]$, a_7	$a_{7,11} = 0$
15	m_{14}	$m_{14} \leftarrow m_{14} - 2^3$	a_{15}, a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, a_9, $a_8[11]$	$a_{9,11} = 1$, $a_{13,11}a_{11,11} \oplus a_{12,11}a_{10,11}$ $\oplus a_{14,11}a_{11,11} \oplus a_{14,11} = 0$
16	m_{15}	$m_{15} \leftarrow m_{15} + 2^{31}$	a_{16}, a_{15}, a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, a_9	

In the first block, the rectifiable conditions are as follows:

$a_{34,4}$, $a_{34,14}$, $a_{35,4}$, $a_{35,14}$, $a_{35,25}$, $a_{36,14}$, $a_{36,25}$, $a_{37,25}$, $a_{37,14}$, $a_{37,4}$, $a_{38,25}$, $a_{39,25}$, $a_{40,25}$.

In the second block, the rectifiable conditions are as follows:

$a_{34,4}$, $a_{34,14}$, $a_{35,4}$, $a_{35,14}$, $a_{35,25}$, $a_{36,14}$, $a_{36,25}$, $a_{37,4}$, $a_{37,14}$, $a_{37,25}$, $a_{38,25}$, $a_{40,25}$.

By the two types of modification, there are 8 remaining conditions in Table 8, and 9 conditions in Table 9 that need to be satisfied.

5.4 Complexity Evaluation

In order to calculate the attack complexity, we need to estimate the probabilities of two truncated differentials, one is from step 1 to step 64, the other is from step 65 to step 128. After message modification, we know that the 1-64 step differential of the first block holds with probability 2^{-8} and that of the second block with probability 2^{-9}. What is left is to calculate the probability that all the equations in rounds 3-4 hold concurrently for both blocks.

Complexity Evaluation for the First Block

There are total 22 equations in rounds 3-4 for the first block. In order to deduce their probability, we divide these equations into three equation systems.

Equation System 1

$$\begin{cases} 0 = a_{71,14} \\ 0 = a_{69,14}a_{65,14} \oplus a_{67,14} \\ 0 = a_{66,14} \\ 0 = a_{73,14}a_{67,14} \oplus a_{70,14} \\ 0 = a_{72,14} \\ 0 = a_{75,14} \\ 1 = a_{70,14} \\ 0 = a_{77,14}a_{75,14} \oplus a_{76,14} \oplus a_{72,14} \end{cases}$$

The equation system 1 ensures the differential characteristics from step 71 to 79 in Table 6 hold.

There are two solutions for the 11 variables, so the equation system 1 holds with probability 2^{-10}.

Equation System 2

$$\begin{cases} 0 = a_{117,14} \\ 0 = a_{115,14}a_{113,14} \oplus a_{112,14}a_{111,14} \oplus a_{116,14} \oplus a_{112,14} \oplus a_{113,14} \\ \qquad \oplus a_{111,14} \oplus a_{114,14} \\ 0 = a_{116,14}a_{113,14} \oplus a_{118,14} \\ 0 = a_{118,14}a_{114,14} \oplus a_{119,14}a_{115,14} \oplus a_{113,14} \\ 1 = a_{120,14} \\ 0 = a_{121,14}a_{119,14} \oplus a_{116,14} \oplus a_{121,14} \\ 0 = a_{121,14}a_{120,14} \oplus a_{122,14}a_{116,14} \oplus a_{122,14} \oplus a_{118,14} \oplus a_{116,14} \\ \qquad a_{123,14}a_{118,14} \oplus a_{118,14} \oplus a_{123,14} \oplus a_{121,14} \end{cases}$$

The equation system 2 guarantees the differential characteristics from step 117 to 124 hold.

It is easy to show that there are 32 solutions for 13 variables which imply that the equation system 2 holds with probability 2^{-8}.

Equation System 3

$$\begin{cases} 0 = a_{125,3} \\ 0 = a_{123,3}a_{121,3} \oplus a_{120,3}a_{119,3} \oplus a_{124,3} \oplus a_{120,3} \oplus a_{121,3} \oplus a_{119,3} \oplus a_{122,3} \\ 0 = a_{124,3}a_{121,3} \oplus a_{126,3} \\ 1 = a_{127,3} \\ 0 = a_{126,3}a_{122,3} \oplus a_{121,3} \\ 0 = a_{122,3}a_{121,3} \oplus a_{126,3} \oplus a_{122,3} \oplus a_{123,3} \oplus a_{121,3} \oplus a_{124,3} \end{cases}$$

The equation system 3 ensures the differential characteristics in steps 125-128 hold.

Similarly, the equation system 3 has 7 solutions with 9 variables which the probability is $\frac{7}{2^9}$.

Additional Conditions for Near Collision

Our attack is to find collisions with two blocks, so the output difference for the first block should be $(0, -2^2, 0, 2^2, 0, 0, 0, 0)$ with no bit carries which results in two other conditions on outputs bb_0 and dd_0. For the second block, the differential path needs two conditions in IVs which come from two conditions on aa_0 and cc_0 in the first block. So the additional four conditions for the first block are as follows:

$$aa_{0,3} = 0, \ bb_{0,3} = 1, \ cc_{0,3} = 0, \ dd_{0,3} = 0$$

where

$$aa_0 = a_0 + a_{128}, \ bb_0 = b_0 + a_{127}, \ cc_0 = c_0 + a_{126}, \ dd_0 = d_0 + a_{125}$$

It is noted that the four input words in the second block aa_0, bb_0, cc_0, dd_0 are also the output words in the first block.

Considering 8 conditions left after the message modification, the probability for the differential path in the first block is about

$$\frac{1}{2^8} \cdot \frac{1}{2^{10}} \cdot \frac{1}{2^8} \cdot \frac{7}{2^9} \cdot \frac{1}{2^4} \approx \frac{1}{2^{36}}$$

Complexity Evaluation for the Second Block

For the second block, given a message M_1, after the modifications, M_1 and M_1' generate the differential in Table 7 with the probability

$$\frac{1}{2^9} \cdot \frac{1}{2^{10}} \cdot \frac{1}{2^8} \cdot \frac{7}{2^9} \approx \frac{1}{2^{33}}$$

The two differential paths corresponding to two blocks consist of a collision for 4 pass HAVAL, and the time complexity for the attack is about 2^{36} HAVAL computations.

5.5 Collision Search Algorithm

Summarizing the above technique details, we give an overview of the collision search algorithm.

1. Searching the first block M_0.
   (a) Choose a 1024-bit message $M_0 = (x_i)_{i<31}$ randomly and modify its first 30 words by the basic modification technique such that the conditions in steps 6-30 of Table 8 are satisfied.
   (b) Modify x_{30} and x_{31} to correct the conditions in steps 31-32 of Table 8 by the basic modification technique.
   (c) Apply the advanced modification to make the 13 rectifiable conditions to hold in round 2.
   (d) Compute $H(M_0) = (aa_0, bb_0, cc_0, dd_0, ee_0, ff_0, gg_0, hh_0)$ and $H(M_0') = (aa_0', bb_0', cc_0', dd_0', ee_0', ff_0', gg_0', hh_0')$.
   If $H(M_0') - H(M_0) = \varDelta H_1$, $aa_{0,3} = 0$, $bb_{0,3} = 1$, $cc_{0,3} = 0$ and $dd_{0,3} = 0$ hold , output M_0 and M_0'. Otherwise, select another x_{30} and x_{31} randomly and go to step (b).
2. Searching the second block M_1 by the similar method as M_0.

Using our search algorithm, it takes roughly 8 hours to find a 4-pass collision on a standard notebook PC, and we give a collision example in Table 3.

Table 3. A collision for 4-pass HAVAL. H is the common hash value with little-endian and no message padding.

M_0	1c6574fd	b56fff65	0feff335	d7404793	095e0c30	dcc386ab	86e85ecd	eb730b21
	0ba01f27	8e3e84e2	39e35d80	afdf0ea8	23a57ffb	903fbb44	24e03671	d63ffe68
	375e43b1	2dd81090	f408a2c5	ecc32b28	43f17d20	062e68d3	b9d1bd80	f0572c76
	e3d648b1	184ebe01	92def272	f43fe3d4	6bde4810	fc5666f3	17eec0a9	24b1dda8
M_1	7a329389	28a58673	3b7f4890	6cbb79b7	c33fac13	65ad0193	60d345c4	fa126a11
	476dcbe0	5d582432	6f782165	e8875939	dc262382	ea5d1608	23893c79	d396a5c5
	ff8d6cfb	73d43ab1	ac0b2882	a4642004	69ac7042	1cec975e	a0c5a43a	f7fa309a
	661e6061	aad0c8f0	684e80da	d8540f60	960f8720	257a61c5	87eb3f8c	98c490a3
M_0'	1c6574fd	b56fff65	0feff335	d7404793	095e0c30	dcc386ab	86e85ecd	eb730b21
	0ba03f27	8e3e84e2	39e35d80	afdf0ea8	23a57ffb	903fbb44	24e03671	d63ffe68
	375e43ad	2dd81090	f408a2c5	ecc32b28	43f17d20	062e68d3	b9d1bd80	f0572c76
	e3d648b1	184ebe01	92def272	f43fe3d4	6bde4810	fc5666f3	17eec0a9	24b1dda8
M_1'	7a329389	28a58673	3b7f4890	6cbb79b7	c33fac13	65ad0193	60d345c4	fa126a11
	476dabe0	5d582432	6f782165	e8875939	dc262382	ea5d1608	23893c79	d396a5c5
	ff8d6cff	73d43ab1	ac0b2882	a4642004	69ac7042	1cec975e	a0c5a43a	f7fa309a
	661e6061	aad0c8f0	684e80da	d8540f60	960f8720	257a61c5	87eb3f8c	98c490a3
H	9dcc0bd8	009a1246	4e0b128c	1193ec10	86ddc85e	a90ea714	8c95871c	946cabf1

6 The Attack against 5-Pass HAVAL

We adopt the similar notations for the description of 5-pass HAVAL and its details can refer to [11].

A one-block collision for 5-pass HAVAL is found with probability higher than the birthday attack. Similar to section 3, it's easy to deduce the properties of the five round functions. We choose a message difference $\Delta M = (\Delta m_i)_{i<32}$ with $\Delta m_i = 0, i \neq 8$ and $\Delta m_8 = -1$.

The collision differential path is given in Table 10 and 11. A set of sufficient conditions for the collision path are listed in Table 12 and 13. Given any 1024-bit message M, after the message modification, M and M' produce a partial collision from step 9 to step 71 with probability higher than 2^{-40}. Utilizing the same method as in Section 5.4, it is easy to prove that the second partial collision from step 117 to step 142 holds with probability 2^{-83}. So M and M' consist of a collision with probability about 2^{-123}, and the resulting attack is faster than the birthday attack.

7 Conclusion

In this paper, we describe two practical attacks on 4-pass HAVAL with probability 2^{-43} and 2^{-36} respectively, and also give a theoretical attack on 5-pass HAVAL which is faster than birthday attack.

Acknowledgement We would like to thank Orr Dunkelman for his valuable comments and suggestions for this paper.

References

1. B. V. Rompay, A. Biryukov, B. Preneel, and J. Vandewalle. Cryptanalysis of 3-Pass HAVAL, Asiacrypt 2003, LNCS 2894, pp. 228–245, 2003.
2. H. Yoshida, A. Biryukov, C. D. Canniere, J. Lano, and B. Preneel. Non-randomness of the Full 4 and 5-Pass HAVAL, SCN 2004, LNCS 3352, pp. 324–336, 2005.
3. R. L. Rivest. The MD4 Message Digest Algorithm, Crypto '90, LNCS 537, pp. 303–311, 1991.
4. R. L. Rivest. The MD5 Message-Digest Algorithm, Request for Comments(RFC 1320), Internet Activities Board, Internet Privacy Task Force, 1992.
5. X. Y. Wang, D. Feng, and X. Yu. An attack on Hash Function HAVAL-128. Science in China Ser. F Information Sciences, Vol. 48, No. 5, pp. 545–556, 2005.
6. X. Y. Wang, X. J. Lai, D. Feng, H. Chen, and X. Yu. Cryptanalysis for Hash Functions MD4 and RIPEMD, Eurocrypt '05, LNCS 3494, pp. 1–18, 2005.
7. X. Y. Wang and H. B. Yu. How to Break MD5 and Other Hash Functions, Eurocrypt '05, LNCS 3494, pp. 19–35, 2005.
8. X. Y. Wang, H. B. Yu, and Y. L. Yin. Efficient Collision Search Attacks on SHA-0, Crypto '05, LNCS 3621, pp. 1–16, 2005.
9. X. Y. Wang, Y. L. Yin, and H. B. Yu. Finding collisions on the Full SHA-1, Crypto '05, LNCS 3621, pp. 17–36, 2005.

10. X. Y. Wang. The Collision attack on SHA-0, in Chinese, to appear on `www.infosec.sdu.edu.cn`, 1997.
11. Y. Zheng, J. Pieprzyk and J. Seberry. HAVAL — A One-way Hashing Algorithm with Variable Length of Output, Auscrypt '92, LNCS 718, pp. 83–104, 1993.

Appendix: Tables

Table 4. A differential path for the first block of 4-pass HAVAL, for 2^{43} attack. Here $m_5' = m_5 + 2^{31}$.

Step i	m'_{i-1}	Δa_i	Outputs for M_0'
6	m_5'	2^{31}	$a_6[32]$, a_5, a_4, a_3, a_2, a_1, a_0, a_{-1}
7	m_6		a_7, $a_6[32]$, a_5, a_4, a_3, a_2, a_1, a_0
...	...	...	...
13	m_{12}		a_{13}, a_{12}, a_{11}, a_{10}, a_9, a_8, a_7, $a_6[32]$
14	m_{13}	2^{20}	$a_{14}[-21, 22]$, a_{13}, a_{12}, a_{11}, a_{10}, a_9, a_8, a_7
15	m_{14}		a_{15}, $a_{14}[-21, 22]$, a_{13}, a_{12}, a_{11}, a_{10}, a_9, a_8
16	m_{15}		a_{16}, a_{15}, $a_{14}[-21, 22]$, a_{13}, a_{12}, a_{11}, a_{10}, a_9
17	m_{16}		a_{17}, a_{16}, a_{15}, $a_{14}[-21, 22]$, a_{13}, a_{12}, a_{11}, a_{10}
18	m_{17}	-2^{14}	$a_{18}[15, 16, 17, -18]$, a_{17}, a_{16}, a_{15}, $a_{14}[-21, 22]$, a_{13}, a_{12}, a_{11}
19	m_{18}		a_{19}, $a_{18}[15, 16, 17, -18]$, a_{17}, a_{16}, a_{15}, $a_{14}[-21, 22]$, a_{13}, a_{12}
...	...	...	...
24	m_{23}		a_{24}, a_{23}, a_{22}, a_{21}, a_{20}, a_{19}, $a_{18}[15, 16, 17, -18]$, a_{17}
25	m_{24}	2^{10}	$a_{25}[11]$, a_{24}, a_{23}, a_{22}, a_{21}, a_{20}, a_{19}, $a_{18}[15, 16, 17, -18]$
...	...	...	...
32	m_{31}		a_{32}, a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}, $a_{25}[11]$
33	m_5'		a_{33}, a_{32}, a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}
...	...	...	...
95	m_5'	2^{31}	$a_{95}[-32]$, a_{94}, a_{93}, a_{92}, a_{91}, a_{90}, a_{89}, a_{88}
...	...	...	...
102	m_7		a_{102}, a_{101}, a_{100}, a_{99}, a_{98}, a_{97}, a_{96}, $a_{95}[-32]$
103	m_{28}	-2^{20}	$a_{103}[-21]$, a_{102}, a_{101}, a_{100}, a_{99}, a_{98}, a_{97}, a_{96}
...	...	...	...
110	m_{25}		a_{110}, a_{109}, a_{108}, a_{107}, a_{106}, a_{105}, a_{104}, $a_{103}[-21]$
111	m_{19}	-2^9	$a_{111}[-10]$, a_{110}, a_{109}, a_{108}, a_{107}, a_{106}, a_{105}, a_{104}
...	...	...	...
118	m_{27}		a_{118}, a_{117}, a_{116}, a_{115}, a_{114}, a_{113}, a_{112}, $a_{111}[-10]$
119	m_{12}	-2^{30}	$a_{119}[-31]$, a_{118}, a_{117}, a_{116}, a_{115}, a_{114}, a_{113}, a_{112}
120	m_9		a_{120}, $a_{119}[-31]$, a_{118}, a_{117}, a_{116}, a_{115}, a_{114}, a_{113}
121	m_1		a_{121}, a_{120}, $a_{119}[-31]$, a_{118}, a_{117}, a_{116}, a_{115}, a_{114}
122	m_{29}		a_{122}, a_{121}, a_{120}, $a_{119}[-31]$, a_{118}, a_{117}, a_{116}, a_{115}
123	m_5'	2^{31}	$a_{123}[32]$, a_{122}, a_{121}, a_{120}, $a_{119}[-31]$, a_{118}, a_{117}, a_{116}
124	m_{15}		a_{124}, $a_{123}[32]$, a_{122}, a_{121}, a_{120}, $a_{119}[-31]$, a_{118}, a_{117}
125	m_{17}		a_{125}, a_{124}, $a_{123}[32]$, a_{122}, a_{121}, a_{120}, $a_{119}[-31]$, a_{118}
126	m_{10}		a_{126}, a_{125}, a_{124}, $a_{123}[32]$, a_{122}, a_{121}, a_{120}, $a_{119}[-31]$
127	m_{16}	-2^{19}	$a_{127}[-20]$, a_{126}, a_{125}, a_{124}, $a_{123}[32]$, a_{122}, a_{121}, a_{120}
128	m_{13}		a_{128}, $a_{127}[-20]$, a_{126}, a_{125}, a_{124}, $a_{123}[32]$, a_{122}, a_{121}

Table 5. A differential path for the second block of 4-pass HAVAL, up to step 95, for 2^{43} attack. From step 95, the path is the same as in the Table 4 except the signs.

Step	m'_{i-1}	Δa_i	Outputs for M'_1
0			aa_0, $bb_0[-20]$, cc_0, dd_0, ee_0, $ff_0[32]$, gg_0, hh_0
1	m_0		a_1, aa_0, $bb_0[-20]$, cc_0, dd_0, ee_0, $ff_0[32]$, gg_0
2	m_1		a_2, a_1, aa_0, $bb_0[-20]$, cc_0, dd_0, ee_0, $ff_0[32]$
3	m_2	2^{20}	$a_3[21]$, a_2, a_1, aa_0, $bb_0[-20]$, cc_0, dd_0, ee_0
4	m_3		a_4, $a_3[21]$, a_2, a_1, aa_0, $bb_0[-20]$, cc_0, dd_0
5	m_4		a_5, a_4, $a_3[21]$, a_2, a_1, aa_0, $bb_0[-20]$, cc_0
6	m'_5	2^{31}	$a_6[32]$, a_5, a_4, $a_3[21]$, a_2, a_1, aa_0, $bb_0[-20]$
7	m_6	-2^8-2^{24}	$a_7[-9,25,26,27,-28]$, $a_6[32]$, a_5, a_4, $a_3[21]$, a_2, a_1, aa_0
8	m_7	-2^{17}	$a_8[18,19,20,-21]$, $a_7[-9,25,...,-28]$, $a_6[32]$, a_5, a_4, $a_3[21]$, a_2, a_1
9	m_8	-2^{11}	$a_9[12,13,-14]$, $a_8[18,...,-21]$, $a_7[-9,25,...,-28]$, $a_6[32]$, a_5, a_4, $a_3[21]$, a_2
10	m_9	2^6	$a_{10}[-7,8]$, $a_9[12,13,-14]$, $a_8[18,...,-21]$, $a_7[-9,25,...,-28]$, $a_6[32]$, a_5, a_4, $a_3[21]$
11	m_{10}	2^9	$a_{11}[10]$, $a_{10}[-7,8]$, $a_9[12,13,-14]$, $a_8[18,...,-21]$, $a_7[-9,25,...,-28]$, $a_6[32]$, a_5, a_4
12	m_{11}		a_{12}, $a_{11}[10]$, $a_{10}[-7,8]$, $a_9[12,13,-14]$, $a_8[18,...,-21]$, $a_7[-9,25,...,-28]$, $a_6[32]$, a_5
13	m_{12}		a_{13}, a_{12}, $a_{11}[10]$, $a_{10}[-7,8]$, $a_9[12,13,-14]$, $a_8[18,...,-21]$, $a_7[-9,25,...,-28]$, $a_6[32]$
14	m_{13}		a_{14}, a_{13}, a_{12}, $a_{11}[10]$, $a_{10}[-7,8]$, $a_9[12,13,-14]$, $a_8[18,...,-21]$, $a_7[-9,25,...,-28]$
15	m_{14}	-2^{29}	$a_{15}[-30]$, a_{14}, a_{13}, a_{12}, $a_{11}[10]$, $a_{10}[-7,8]$, $a_9[12,13,-14]$, $a_8[18,...,-21]$
16	m_{15}		a_{16}, $a_{15}[-30]$, a_{14}, a_{13}, a_{12}, $a_{11}[10]$, $a_{10}[-7,8]$, $a_9[12,13,-14]$
17	m_{16}		a_{17}, a_{16}, $a_{15}[-30]$, a_{14}, a_{13}, a_{12}, $a_{11}[10]$, $a_{10}[-7,8]$
18	m_{17}	2^{27}	$a_{18}[-28,29]$, a_{17}, a_{16}, $a_{15}[-30]$, a_{14}, a_{13}, a_{12}, $a_{11}[10]$
19	m_{18}	2^{30}	$a_{19}[31]$, $a_{18}[-28,29]$, a_{17}, a_{16}, $a_{15}[-30]$, a_{14}, a_{13}, a_{12}
20	m_{19}		a_{20}, $a_{19}[31]$, $a_{18}[-28,29]$, a_{17}, a_{16}, $a_{15}[-30]$, a_{14}, a_{13}
21	m_{20}		a_{21}, a_{20}, $a_{19}[31]$, $a_{18}[-28,29]$, a_{17}, a_{16}, $a_{15}[-30]$, a_{14}
22	m_{21}	-2^{22}	$a_{22}[23,...,26,-27]$, a_{21}, a_{20}, $a_{19}[31]$, $a_{18}[-28,29]$, a_{17}, a_{16}, $a_{15}[-30]$
23	m_{22}	2^{21}	$a_{23}[22]$, $a_{22}[23,...,-27]$, a_{21}, a_{20}, $a_{19}[31]$, $a_{18}[-28,29]$, a_{17}, a_{16}
24	m_{23}	-2^{14}	$a_{24}[15,...,18,-19]$, $a_{23}[22]$, $a_{22}[23,...,-27]$, a_{21}, a_{20}, $a_{19}[31]$, $a_{18}[-28,29]$, a_{17}
25	m_{24}	2^{10}	$a_{25}[11]$, $a_{24}[15,...,-19]$, $a_{23}[22]$, $a_{22}[23,...,-27]$, a_{21}, a_{20}, $a_{19}[31]$, $a_{18}[-28,29]$
26	m_{25}		a_{26}, $a_{25}[11]$, $a_{24}[15,...,-19]$, $a_{23}[22]$, $a_{22}[23,...,-27]$, a_{21}, a_{20}, $a_{19}[31]$
...	...	...	...
31	m_{30}		a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}, $a_{25}[11]$, $a_{24}[15,...,-19]$
32	m_{31}		a_{32}, a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}, $a_{25}[11]$
33	m'_5		a_{33}, a_{32}, a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}
...	...	...	...
95	m'_5	2^{31}	$a_{95}[32]$, a_{94}, a_{93}, a_{92}, a_{91}, a_{90}, a_{89}, a_{88}

Table 6. A differential path for the first block of 4-pass HAVAL, for 2^{36} attack. Here $m'_8 = m_8 + 2^{13}$, $m'_{16} = m_{16} - 2^2$.

step i	m'_{i-1}	Δa_i	Outputs for M'_0
9	m'_8	2^{13}	$a_9[-14, 15]$, a_8, a_7, a_6, a_5, a_4, a_3, a_2
10	m_9		a_{10}, $a_9[-14, 15]$, a_8, a_7, a_6, a_5, a_4, a_3
11	m_{10}		a_{11}, a_{10}, $a_9[-14, 15]$, a_8, a_7, a_6, a_5, a_4
12	m_{11}		a_{12}, a_{11}, a_{10}, $a_9[-14, 15]$, a_8, a_7, a_6, a_5
13	m_{12}		a_{13}, a_{12}, a_{11}, a_{10}, $a_9[-14, 15]$, a_8, a_7, a_6
14	m_{13}		a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, $a_9[-14, 15]$, a_8, a_7
15	m_{14}	2^7	$a_{15}[-8, -9, -10, 11]$, a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, $a_9[-14, 15]$, a_8
16	m_{15}	2^3	$a_{16}[4]$, $a_{15}[-8, -9, -10, 11]$, a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, $a_9[-14, 15]$
17	m'_{16}	2^{28}	$a_{17}[29]$, $a_{16}[4]$, $a_{15}[-8, -9, -10, 11]$, a_{14}, a_{13}, a_{12}, a_{11}, a_{10}
18	m_{17}		a_{18}, $a_{17}[29]$, $a_{16}[4]$, $a_{15}[-8, -9, -10, 11]$, a_{14}, a_{13}, a_{12}, a_{11}
19	m_{18}		a_{19}, a_{18}, $a_{17}[29]$, $a_{16}[4]$, $a_{15}[-8, -9, -10, 11]$, a_{14}, a_{13}, a_{12}
20	m_{19}		a_{20}, a_{19}, a_{18}, $a_{17}[29]$, $a_{16}[4]$, $a_{15}[-8, -9, -10, 11]$, a_{14}, a_{13}
21	m_{20}		a_{21}, a_{20}, a_{19}, a_{18}, $a_{17}[29]$, $a_{16}[4]$, $a_{15}[-8, -9, -10, 11]$, a_{14}
22	m_{21}		a_{22}, a_{21}, a_{20}, a_{19}, a_{18}, $a_{17}[29]$, $a_{16}[4]$, $a_{15}[-8, -9, -10, 11]$
23	m_{22}	2^{21}	$a_{23}[22]$, a_{22}, a_{21}, a_{20}, a_{19}, a_{18}, $a_{17}[29]$, $a_{16}[4]$
24	m_{23}	$-2^{14} + 2^{24}$	$a_{24}[15, 16, 17, -18, 25]$, $a_{23}[22]$, a_{22}, a_{21}, a_{20}, a_{19}, a_{18}, $a_{17}[29]$
25	m_{24}		a_{25}, $a_{24}[15, 16, 17, -18, 25]$, $a_{23}[22]$, a_{22}, a_{21}, a_{20}, a_{19}, a_{18}
26	m_{25}		a_{26}, a_{25}, $a_{24}[15, 16, 17, -18, 25]$, $a_{23}[22]$, a_{22}, a_{21}, a_{20}, a_{19}
27	m_{26}		a_{27}, a_{26}, a_{25}, $a_{24}[15, 16, 17, -18, 25]$, $a_{23}[22]$, a_{22}, a_{21}, a_{20}
28	m_{27}		a_{28}, a_{27}, a_{26}, a_{25}, $a_{24}[15, 16, 17, -18, 25]$, $a_{23}[22]$, a_{22}, a_{21}
29	m_{28}		a_{29}, a_{28}, a_{27}, a_{26}, a_{25}, $a_{24}[15, 16, 17, -18, 25]$, $a_{23}[22]$, a_{22}
30	m_{29}		a_{30}, a_{29}, a_{28}, a_{27}, a_{26}, a_{25}, $a_{24}[15, 16, 17, -18, 25]$, $a_{23}[22]$
31	m_{30}		a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}, a_{25}, $a_{24}[15, 16, 17, -18, 25]$
32	m_{31}	$-2^3 + 2^{13}$	$a_{32}[-4, 14]$, a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}, a_{25}
...	...	...	...
39	m_7		a_{39}, a_{38}, a_{37}, a_{36}, a_{35}, a_{34}, a_{33}, $a_{32}[-4, 14]$
40	m'_{16}	-2^{24}	$a_{40}[-25]$, a_{39}, a_{38}, a_{37}, a_{36}, a_{35}, a_{34}, a_{33}
...	...	...	...
47	m_4		a_{47}, a_{46}, a_{45}, a_{44}, a_{43}, a_{42}, a_{41}, $a_{40}[-25]$
48	m'_8		a_{48}, a_{47}, a_{46}, a_{45}, a_{44}, a_{43}, a_{42}, a_{41}
...	...	...	...
71	m'_8	2^{13}	$a_{71}[14]$, a_{70}, a_{69}, a_{68}, a_{67}, a_{66}, a_{65}, a_{64}
...	...	...	...
78	m_{30}		a_{78}, a_{77}, a_{76}, a_{75}, a_{74}, a_{73}, a_{72}, $a_{71}[14]$
79	m'_{16}		a_{79}, a_{78}, a_{77}, a_{76}, a_{75}, a_{74}, a_{73}, a_{72}
...	...	...	...
117	m'_8	2^{13}	$a_{117}[14]$, a_{116}, a_{115}, a_{114}, a_{113}, a_{112}, a_{111}, a_{110}
...	...	...	...
124	m_{15}		a_{124}, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}, a_{118}, $a_{117}[14]$
125	m_{17}	2^2	$a_{125}[3]$, a_{124}, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}, a_{118}
126	m_{10}		a_{126}, $a_{125}[3]$, a_{124}, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}
127	m'_{16}	-2^2	$a_{127}[-3]$, a_{126}, $a_{125}[3]$, a_{124}, a_{123}, a_{122}, a_{121}, a_{120}
128	m_{13}		a_{128}, $a_{127}[-3]$, a_{126}, $a_{125}[3]$, a_{124}, a_{123}, a_{122}, a_{121}

Table 7. A differential path for the second block of 4-pass HAVAL, for 2^{36} attack. Here, $m'_8 = m_8 - 2^{13}$, $m'_{16} = m_{16} + 2^2$.

Step	m'_{i-1}	Δa_i	Output for M'_1
0			aa_0, $bb_0[-3]$, cc_0, $dd_0[3]$, ee_0, ff_0, gg_0, hh_0
1	m_0		a_1, aa_0, $bb_0[-3]$, cc_0, $dd_0[3]$, ee_0, ff_0, gg_0
2	m_1		a_2, a_1, aa_0, $bb_0[-3]$, cc_0, $dd_0[3]$, ee_0, ff_0
3	m_2		a_3, a_2, a_1, aa_0, $bb_0[-3]$, cc_0, $dd_0[3]$, ee_0
4	m_3		a_4, a_3, a_2, a_1, aa_0, $bb_0[-3]$, cc_0, $dd_0[3]$
5	m_4	2^{23}	$a_5[24]$, a_4, a_3, a_2, a_1, aa_0, $bb_0[-3]$, cc_0
6	m_5		a_6, $a_5[24]$, a_4, a_3, a_2, a_1, aa_0, $bb_0[-3]$
7	m_6	-2^{23}	$a_7[-24]$, a_6, $a_5[24]$, a_4, a_3, a_2, a_1, aa_0
8	m_7		a_8, $a_7[-24]$, a_6, $a_5[24]$, a_4, a_3, a_2, a_1
9	m'_8	-2^{13}	$a_9[14,15,16,17,18,19,20,-21]$, a_8, $a_7[-24]$, a_6, $a_5[24]$, a_4, a_3, a_2
10	m_9		a_{10}, $a_9[14,15,16,17,18,19,20,-21]$, a_8, $a_7[-24]$, a_6, $a_5[24]$, a_4, a_3
11	m_{10}		a_{11}, a_{10}, $a_9[14,15,16,17,18,19,20,-21]$, a_8, $a_7[-24]$, a_6, $a_5[24]$, a_4
12	m_{11}		a_{12}, a_{11}, a_{10}, $a_9[14,15,16,17,18,19,20,-21]$, a_8, $a_7[-24]$, a_6, $a_5[24]$
13	m_{12}		a_{13}, a_{12}, a_{11}, a_{10}, $a_9[14,15,16,17,18,19,20,-21]$, a_8, $a_7[-24]$, a_6
14	m_{13}		a_{14}, a_{13}, a_{12}, a_{11}, a_{10}, $a_9[14,15,16,17,18,19,20,-21]$, a_8, $a_7[-24]$
15	m_{14}	2^7	$a_{15}[-8,-9,-10,11]$, a_{14},..., $a_9[14,15,16,17,18,19,20,-21]$, a_8
16	m_{15}	-2^3	$a_{16}[-4]$, $a_{15}[-8,-9,-10,11]$,..., a_{10}, $a_9[14,15,16,17,18,19,20,-21]$
17	m'_{16}	2^{28}	$a_{17}[29]$, $a_{16}[-4]$, $a_{15}[-8,-9,-10,11]$, a_{14}, a_{13}, a_{12}, a_{11}, a_{10}
...	...	...	...
22	m_{21}		a_{22}, a_{21}, a_{20}, a_{19}, a_{18}, $a_{17}[29]$, $a_{16}[-4]$, $a_{15}[-8,-9,-10,11]$
23	m_{22}	2^{21}	$a_{23}[22]$, a_{22}, a_{21}, a_{20}, a_{19}, a_{18}, $a_{17}[29]$, $a_{16}[-4]$
24	m_{23}	2^{14}-2^{24}	$a_{24}[-15,-16,-17,18,-25]$, $a_{23}[22]$, a_{22}, a_{21}, a_{20}, a_{19}, a_{18}, $a_{17}[29]$
...	...	...	...
31	m_{30}		a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}, a_{25}, $a_{24}[-15,-16,-17,18,-25]$
32	m_{31}	2^3-2^{13}	$a_{32}[4,-14]$, a_{31}, a_{30}, a_{29}, a_{28}, a_{27}, a_{26}, a_{25}
...	...	...	...
39	m_7		a_{39}, a_{38}, a_{37}, a_{36}, a_{35}, a_{34}, a_{33}, $a_{32}[4,-14]$
40	m'_{16}	2^{24}	$a_{40}[25]$, a_{39}, a_{38}, a_{37}, a_{36}, a_{35}, a_{34}, a_{33}
...	...	...	...
47	m_4		a_{47}, a_{46}, a_{45}, a_{44}, a_{43}, a_{42}, a_{41}, $a_{40}[25]$
48	m'_8		a_{48}, a_{47}, a_{46}, a_{45}, a_{44}, a_{43}, a_{42}, a_{41}
...	...	...	...
71	m'_8	-2^{13}	$a_{71}[-14]$, a_{70}, a_{69}, a_{68}, a_{67}, a_{66}, a_{65}, a_{64}
...	...	...	...
78	m_{30}		a_{78}, a_{77}, a_{76}, a_{75}, a_{74}, a_{73}, a_{72}, $a_{71}[-14]$
79	m'_{16}		a_{79}, a_{78}, a_{77}, a_{76}, a_{75}, a_{74}, a_{73}, a_{72}
...	...	...	...
117	m'_8	-2^{13}	$a_{117}[-14]$, a_{116}, a_{115}, a_{114}, a_{113}, a_{112}, a_{111}, a_{110}
...	...	...	...
124	m_{15}		a_{124}, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}, a_{118}, $a_{117}[-14]$
125	m_{17}	-2^2	$a_{125}[-3]$, a_{124}, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}, a_{118}
126	m_{10}		a_{126}, $a_{125}[-3]$, a_{124}, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}
127	m'_{16}	2^2	$a_{127}[3]$, a_{126}, $a_{125}[-3]$, a_{124}, a_{123}, a_{122}, a_{121}, a_{120}
128	m_{13}		a_{128}, $a_{127}[3]$, a_{126}, $a_{125}[-3]$, a_{124}, a_{123}, a_{122}, a_{121}

Table 8. A set of sufficient conditions on a_i for the differential path given in Table 6

.

Step i	a_i	Conditions of the chaining variable in each step
6	a_6	$a_{6,14}=1$, $a_{6,15}=1$
7	a_7	$a_{7,14}=0$, $a_{7,15}=0$
8	a_8	$a_{8,14}=0$, $a_{8,15}=1$
9	a_9	$a_{9,14}=1$, $a_{9,15}=0$
10	a_{10}	$a_{10,11}=0$, $a_{10,14}=0$, $a_{10,15}=0$
11	a_{11}	$a_{11,4}=0$, $a_{11,14}=0$, $a_{11,15}=0$
12	a_{12}	$a_{12,8}=1$, $a_{12,9}=1$, $a_{12,10}=1$, $a_{12,11}=0$, $a_{12,14}=0$, $a_{12,15}=0$,
13	a_{13}	$a_{13,4}=0$, $a_{13,8}=0$, $a_{13,9}=0$, $a_{13,10}=0$, $a_{13,11}=0$
14	a_{14}	$a_{14,4}=0$, $a_{14,8}=0$, $a_{14,9}=0$, $a_{14,10}=0$, $a_{14,11}=0$, $a_{14,15}=0$, $a_{14,29}=1$
15	a_{15}	$a_{15,4}=0$, $a_{15,8}=1$, $a_{15,9}=1$, $a_{15,10}=1$, $a_{15,11}=0$, $a_{15,29}=0$
16	a_{16}	$a_{16,4}=0$, $a_{16,8}=0$, $a_{16,9}=0$, $a_{16,10}=0$, $a_{16,11}=0$, $a_{16,29}=1$
17	a_{17}	$a_{17,4}=1$, $a_{17,8}=0$, $a_{17,9}=0$, $a_{17,10}=0$, $a_{17,11}=0$, $a_{17,22}=1$, $a_{17,29}=0$
18	a_{18}	$a_{18,4}=0$, $a_{18,8}=0$, $a_{18,9}=0$, $a_{18,10}=0$, $a_{18,11}=0$, $a_{18,22}=1$, $a_{18,25}=1$, $a_{18,29}=0$
19	a_{19}	$a_{19,4}=0$, $a_{19,25}=1$, $a_{19,29}=0$
20	a_{20}	$a_{20,22}=0$, $a_{20,29}=0$
21	a_{21}	$a_{21,15}=1$, $a_{21,16}=1$, $a_{21,17}=1$, $a_{21,18}=1$, $a_{21,22}=0$, $a_{21,25}=0$
22	a_{22}	$a_{22,4}=1$, $a_{22,15}=0$, $a_{22,16}=0$, $a_{22,17}=0$, $a_{22,18}=0$, $a_{22,22}=0$, $a_{22,25}=0$, $a_{22,29}=0$
23	a_{23}	$a_{23,15}=0$, $a_{23,16}=0$, $a_{23,17}=0$, $a_{23,18}=0$, $a_{23,22}=0$, $a_{23,25}=0$
24	a_{24}	$a_{24,15}=0$, $a_{24,16}=0$, $a_{24,17}=0$, $a_{24,18}=1$, $a_{24,22}=0$, $a_{24,25}=0$
25	a_{25}	$a_{25,15}=0$, $a_{25,16}=0$, $a_{25,17}=0$, $a_{25,18}=1$, $a_{25,22}=0$, $a_{25,25}=0$
26	a_{26}	$a_{26,15}=0$, $a_{26,16}=0$, $a_{26,17}=0$, $a_{26,18}=0$, $a_{26,22}=0$, $a_{26,25}=0$
27	a_{27}	$a_{27,4}=0$, $a_{27,14}=0$, $a_{27,15}=0$, $a_{27,16}=0$, $a_{27,17}=0$, $a_{27,18}=0$, $a_{27,25}=0$
28	a_{28}	$a_{28,4}=0$, $a_{28,14}=0$
29	a_{29}	$a_{29,4}=0$, $a_{29,14}=0$
30	a_{30}	$a_{30,4}=0$, $a_{30,14}=0$, $a_{30,18}=0$
31	a_{31}	$a_{31,4}=0$, $a_{31,14}=0$
32	a_{32}	$a_{32,4}=1$, $a_{32,14}=0$
34	a_{34}	$a_{34,4}=0$, $a_{34,14}=0$
35	a_{35}	$a_{35,4}=1$, $a_{35,14}=1$ $a_{35,25}=0$
36	a_{36}	$a_{36,4}=0$, $a_{36,14}=0$, $a_{36,25}=0$
37	a_{37}	$a_{37,4}=1$, $a_{37,14}=1$, $a_{37,25}=0$
38	a_{38}	$a_{38,4}=1$, $a_{38,14}=1$, $a_{38,25}=0$
39	a_{39}	$a_{39,25}=0$
40	a_{40}	$a_{40,25}=1$
42	a_{42}	$a_{42,25}=0$
43	a_{43}	$a_{43,25}=1$
44	a_{44}	$a_{44,25}=0$
45	a_{45}	$a_{45,25}=1$
46	a_{46}	$a_{46,25}=1$

Table 9. A set of sufficient conditions on a_i for the differential path given in Table 7

Step		Conditions of the chaining variable in each step
0	IVs	$aa_{0,3}=0,\ bb_{0,3}=1,\ cc_{0,3}=0,\ dd_{0,3}=0$
1	a_1	$a_{1,3}=0$
2	a_2	$a_{2,3}=ee_{0,3},\ a_{2,24}=1$
3-5	a_3	$a_{3,24}=0,\ a_{4,24}=1,\ a_{5,24}=0$
6	a_6	$a_{6,14}=1,\ a_{6,15}=1,\ a_{6,16}=1,\ a_{6,17}=1,\ a_{6,18}=1,\ a_{6,19}=1,\ a_{6,20}=1,$ $a_{6,21}=1,\ a_{6,24}=0$
7	a_7	$a_{7,14}=0,\ a_{7,15}=0,\ a_{7,16}=0,\ a_{7,17}=0,\ a_{7,18}=0,\ a_{7,19}=0,\ a_{7,20}=0,$ $a_{7,21}=0,\ a_{7,24}=1$
8	a_8	$a_{8,14}=0,\ a_{8,15}=1,\ a_{8,16}=0,\ a_{8,17}=0,\ a_{8,18}=0,\ a_{8,19}=0,\ a_{8,20}=1,$ $a_{8,21}=0,\ a_{8,24}=0$
9	a_9	$a_{9,11}=1,\ a_{9,14}=0,\ a_{9,15}=0,\ a_{9,16}=0,\ a_{9,17}=0,\ a_{9,18}=0,\ a_{9,19}=0,$ $a_{9,20}=0,\ a_{9,21}=1,\ a_{9,24}=0$
10	a_{10}	$a_{10,4}=1,\ a_{10,11}=1,\ a_{10,14}=0,\ a_{10,15}=0,\ a_{10,16}=0,\ a_{10,17}=0,\ a_{10,18}=0,$ $a_{10,19}=0,\ a_{10,20}=0,\ a_{10,21}=0,\ a_{10,24}=1$
11	a_{11}	$a_{11,4}=1,\ a_{11,14}=0,\ a_{11,15}=0,\ a_{11,16}=0,\ a_{11,17}=0,\ a_{11,18}=0,\ a_{11,19}=0,$ $a_{11,20}=0,\ a_{11,21}=0$
12	a_{12}	$a_{12,8}=1,\ a_{12,9}=1,\ a_{12,10}=1,\ a_{12,14}=0,\ a_{12,15}=0,\ a_{12,16}=0,\ a_{12,17}=0,$ $a_{12,18}=0,\ a_{12,19}=0,\ a_{12,20}=1,\ a_{12,21}=0$
13	a_{13}	$a_{13,4}=0,\ a_{13,8}=0,\ a_{13,9}=0,\ a_{13,10}=0,\ a_{13,11}=0$
14	a_{14}	$a_{14,4}=0,\ a_{14,8}=0,\ a_{14,9}=0,\ a_{14,10}=0,\ a_{14,11}=0,\ a_{14,15}=0,\ a_{14,20}=0,$ $a_{14,29}=1$
15	a_{15}	$a_{15,4}=0,\ a_{15,8}=1,\ a_{15,9}=1,\ a_{15,10}=1,\ a_{15,11}=0,\ a_{15,29}=0$
16	a_{16}	$a_{16,4}=1,\ a_{16,8}=0,\ a_{16,9}=0,\ a_{16,10}=0,\ a_{16,11}=0,\ a_{16,29}=1$
17	a_{17}	$a_{17,4}=1,\ a_{17,8}=0,\ a_{17,9}=0,\ a_{17,10}=0,\ a_{17,11}=0,\ a_{17,29}=0$
18	a_{18}	$a_{18,4}=0,\ a_{18,8}=0,\ a_{18,9}=0,\ a_{18,10}=0,\ a_{18,11}=0,\ a_{18,22}=0,\ a_{18,29}=0$
19	a_{19}	$a_{19,4}=0,\ a_{19,25}=0,\ a_{19,29}=0$
20	a_{20}	$a_{20,22}=0,\ a_{20,29}=0$
21	a_{21}	$a_{21,15}=1,\ a_{21,16}=1,\ a_{21,17}=1,\ a_{21,18}=1,\ a_{21,22}=0,\ a_{21,25}=0$
22	a_{22}	$a_{22,4}=0,\ a_{22,15}=0,\ a_{22,16}=0,\ a_{22,17}=0,\ a_{22,18}=0,\ a_{22,22}=0,\ a_{22,25}=0,$ $a_{22,29}=0$
23	a_{23}	$a_{23,15}=0,\ a_{23,16}=0,\ a_{23,17}=0,\ a_{23,18}=0,\ a_{23,22}=0,\ a_{23,25}=0$
24	a_{24}	$a_{24,15}=1,\ a_{24,16}=1,\ a_{24,17}=1,\ a_{24,18}=0,\ a_{24,22}=0,\ a_{24,25}=1$
25	a_{25}	$a_{25,15}=0,\ a_{25,16}=0,\ a_{25,17}=0,\ a_{25,18}=1,\ a_{25,22}=0,\ a_{25,25}=0$
26	a_{26}	$a_{26,15}=0,\ a_{26,16}=0,\ a_{26,17}=0,\ a_{26,18}=0,\ a_{26,22}=0,\ a_{26,25}=0$
27	a_{27}	$a_{27,4}=0,\ a_{27,14}=0,\ a_{27,15}=0,\ a_{27,16}=0,\ a_{27,17}=0,\ a_{27,18}=0,\ a_{27,25}=0$
28-29	a_{28}	$a_{28,4}=0,\ a_{28,14}=0,\ a_{29,4}=0,\ a_{29,14}=0$
30	a_{30}	$a_{30,4}=0,\ a_{30,14}=0,\ a_{30,18}=1$
31-32	a_{31}	$a_{31,4}=0,\ a_{31,14}=0,\ a_{32,4}=0,\ a_{32,14}=1$
34-35	a_{34}	$a_{34,4}=0,\ a_{34,14}=0,\ a_{35,4}=1,\ a_{35,14}=1,\ a_{35,25}=0$
36	a_{36}	$a_{36,4}=0,\ a_{36,14}=0,\ a_{36,25}=0$
37	a_{37}	$a_{37,4}=1,\ a_{37,14}=1,\ a_{37,25}=0$
38-39	a_{38}	$a_{38,4}=1,\ a_{38,14}=1,\ a_{38,25}=0,\ a_{39,25}=0$
40-46	a_{40}	$a_{40,25}=0,\ a_{42,25}=0,\ a_{43,25}=1,\ a_{44,25}=0,\ a_{45,25}=1,\ a_{46,25}=1$

Table 10. A differential path for the 5-pass HAVAL. Here $m'_8 = m_8 - 1$.

Step	m'_{i-1}	Δa_i	Outputs for M'
9	m'_8	-1	$a_9[1,2,3,4,-5]$, a_8, a_7, a_6, a_5, a_4, a_3, a_2
10	m_9		a_{10}, $a_9[1,2,3,4,-5]$, a_8, a_7, a_6, a_5, a_4, a_3
11	m_{10}	-2^{28}	$a_{11}[29,-30]$, a_{10}, $a_9[1,2,3,4,-5]$, a_8, a_7, a_6, a_5, a_4
12	m_{11}		a_{12}, $a_{11}[29,-30]$, a_{10}, $a_9[1,2,3,4,-5]$, a_8, a_7, a_6, a_5
13	m_{12}		a_{13}, a_{12}, $a_{11}[29,-30]$, a_{10}, $a_9[1,2,3,4,-5]$, a_8, a_7, a_6
14	m_{13}	2^{21}	$a_{14}[22]$, a_{13}, a_{12}, $a_{11}[29,-30]$, a_{10}, $a_9[1,2,3,4,-5]$, a_8, a_7
15	m_{14}		a_{15}, $a_{14}[22]$, a_{13}, a_{12}, $a_{11}[29,-30]$, a_{10}, $a_9[1,2,3,4,-5]$, a_8
16	m_{15}		a_{16}, a_{15}, $a_{14}[22]$, a_{13}, a_{12}, $a_{11}[29,-30]$, a_{10}, $a_9[1,2,3,4,-5]$
17	m_{16}	-2^{14}	$a_{17}[15,-16]$, a_{16}, a_{15}, $a_{14}[22]$, a_{13}, a_{12}, $a_{11}[29,-30]$, a_{10}
18	m_{17}		a_{18}, $a_{17}[15,-16]$, a_{16}, a_{15}, $a_{14}[22]$, a_{13}, a_{12}, $a_{11}[29,-30]$
19	m_{18}		a_{19}, a_{18}, $a_{17}[15,-16]$, a_{16}, a_{15}, $a_{14}[22]$, a_{13}, a_{12}
20	m_{19}	-2^7-2^{17}	$a_{20}[8,9,-10,-18]$, a_{19}, a_{18}, $a_{17}[15,-16]$, a_{16}, a_{15}, $a_{14}[22]$, a_{13}
21	m_{20}		a_{21}, $a_{20}[8,9,-10,-18]$, a_{19}, a_{18}, $a_{17}[15,-16]$, a_{16}, a_{15}, $a_{14}[22]$
22	m_{21}	2^{10}	$a_{22}[11]$, a_{21}, $a_{20}[8,9,-10,-18]$, a_{19}, a_{18}, $a_{17}[15,-16]$, a_{16}, a_{15}
23	m_{22}	2^2	$a_{23}[3]$, $a_{22}[11]$, a_{21}, $a_{20}[8,9,-10,-18]$, a_{19}, a_{18}, $a_{17}[15,-16]$, a_{16}
24	m_{23}	2	$a_{24}[2]$, $a_{23}[3]$, $a_{22}[11]$, a_{21}, $a_{20}[8,9,-10,-18]$, a_{19}, a_{18}, $a_{17}[15,-16]$
25	m_{24}	-2^3-2^{26}	$a_{25}[-4,-27]$, $a_{24}[2]$, $a_{23}[3]$, $a_{22}[11]$, a_{21}, $a_{20}[8,9,-10,-18]$, a_{19}, a_{18}
26	m_{25}		a_{26}, $a_{25}[-4,-27]$, $a_{24}[2]$, $a_{23}[3]$, $a_{22}[11]$, a_{21}, $a_{20}[8,9,-10,-18]$, a_{19}
27	m_{26}		a_{27}, a_{26}, $a_{25}[-4,-27]$, $a_{24}[2]$, $a_{23}[3]$, $a_{22}[11]$, a_{21}, $a_{20}[8,9,-10,-18]$
28	m_{27}	-2^6+2^{19}	$a_{28}[-7,20]$, a_{27}, a_{26}, $a_{25}[-4,-27]$, $a_{24}[2]$, $a_{23}[3]$, $a_{22}[11]$, a_{21}
29	m_{28}		a_{29}, $a_{28}[-7,20]$, a_{27}, a_{26}, $a_{25}[-4,-27]$, $a_{24}[2]$, $a_{23}[3]$, $a_{22}[11]$
30	m_{29}	2^{31}	$a_{30}[32]$, a_{29}, $a_{28}[-7,20]$, a_{27}, a_{26}, $a_{25}[-4,-27]$, $a_{24}[2]$, $a_{23}[3]$
31	m_{30}	2^{23}	$a_{31}[24]$, $a_{30}[32]$, a_{29}, $a_{28}[-7,20]$, a_{27}, a_{26}, $a_{25}[-4,-27]$, $a_{24}[2]$
32	m_{31}	2^{22}	$a_{32}[23]$, $a_{31}[24]$, $a_{30}[32]$, a_{29}, $a_{28}[-7,20]$, a_{27}, a_{26}, $a_{25}[-4,-27]$
33	m_5		a_{33}, $a_{32}[23]$, $a_{31}[24]$, $a_{30}[32]$, a_{29}, $a_{28}[-7,20]$, a_{27}, a_{26}
34	m_{14}	-2^{15}	$a_{34}[-16]$, a_{33}, $a_{32}[23]$, $a_{31}[24]$, $a_{30}[32]$, a_{29}, $a_{28}[-7,20]$, a_{27}
35	m_{26}		a_{35}, $a_{34}[-16]$, a_{33}, $a_{32}[23]$, $a_{31}[24]$, $a_{30}[32]$, a_{29}, $a_{28}[-7,20]$
36	m_{18}	-2^{27}	$a_{36}[-28]$, a_{35}, $a_{34}[-16]$, a_{33}, $a_{32}[23]$, $a_{31}[24]$, $a_{30}[32]$, a_{29}
37	m_{11}		a_{37}, $a_{36}[-28]$, a_{35}, $a_{34}[-16]$, a_{33}, $a_{32}[23]$, $a_{31}[24]$, $a_{30}[32]$
38	m_{28}		a_{38}, a_{37}, $a_{36}[-28]$, a_{35}, $a_{34}[-16]$, a_{33}, $a_{32}[23]$, $a_{31}[24]$
39	m_7	2^{12}	$a_{39}[13]$, a_{38}, a_{37}, $a_{36}[-28]$, a_{35}, $a_{34}[-16]$, a_{33}, $a_{32}[23]$
40	m_{16}	2^5+2^{11}	$a_{40}[6,12]$, $a_{39}[13]$, a_{38}, a_{37}, $a_{36}[-28]$, a_{35}, $a_{34}[-16]$, a_{33}
41	m_0		a_{41}, $a_{40}[6,12]$, $a_{39}[13]$, a_{38}, a_{37}, $a_{36}[-28]$, a_{35}, $a_{34}[-16]$
42	m_{23}	2^{30}	$a_{42}[31]$, a_{41}, $a_{40}[6,12]$, $a_{39}[13]$, a_{38}, a_{37}, $a_{36}[-28]$, a_{35}
43	m_{20}	2^{23}	$a_{43}[24]$, $a_{42}[31]$, a_{41}, $a_{40}[6,12]$, $a_{39}[13]$, a_{38}, a_{37}, $a_{36}[-28]$
44	m_{22}		a_{44}, $a_{43}[24]$, $a_{42}[31]$, a_{41}, $a_{40}[6,12]$, $a_{39}[13]$, a_{38}, a_{37}
45	m_1		a_{45}, a_{44}, $a_{43}[24]$, $a_{42}[31]$, a_{41}, $a_{40}[6,12]$, $a_{39}[13]$, a_{38}
46	m_{10}		a_{46}, a_{45}, a_{44}, $a_{43}[24]$, $a_{42}[31]$, a_{41}, $a_{40}[6,12]$, $a_{39}[13]$
47	m_4	2	$a_{47}[2]$, a_{46}, a_{45}, a_{44}, $a_{43}[24]$, $a_{42}[31]$, a_{41}, $a_{40}[6,12]$
48	m'_8		a_{48}, $a_{47}[2]$, a_{46}, a_{45}, a_{44}, $a_{43}[24]$, $a_{42}[31]$, a_{41}
49	m_{30}		a_{49}, a_{48}, $a_{47}[2]$, a_{46}, a_{45}, a_{44}, $a_{43}[24]$, $a_{42}[31]$
50	m_3	2^{19}	$a_{50}[20]$, a_{49}, a_{48}, $a_{47}[2]$, a_{46}, a_{45}, a_{44}, $a_{43}[24]$
51	m_{21}		a_{51}, $a_{50}[20]$, a_{49}, a_{48}, $a_{47}[2]$, a_{46}, a_{45}, a_{44}
52	m_9		a_{52}, a_{51}, $a_{50}[20]$, a_{49}, a_{48}, $a_{47}[2]$, a_{46}, a_{45}

Table 11. A differential path for the 5-pass HAVAL(continued from Table 10)

53	m_{17}		a_{53}, a_{52}, a_{51}, $a_{50}[20]$, a_{49}, a_{48}, $a_{47}[2]$, a_{46}
54	m_{24}		a_{54}, a_{53}, a_{52}, a_{51}, $a_{50}[20]$, a_{49}, a_{48}, $a_{47}[2]$
55	m_{29}	2^{22}	$a_{55}[23]$, a_{54}, a_{53}, a_{52}, a_{51}, $a_{50}[20]$, a_{49}, a_{48}
56	m_6		a_{56}, $a_{55}[23]$, a_{54}, a_{53}, a_{52}, a_{51}, $a_{50}[20]$, a_{49}
57	m_{19}	2^{15}	$a_{57}[16]$, a_{56}, $a_{55}[23]$, a_{54}, a_{53}, a_{52}, a_{51}, $a_{50}[20]$
58	m_{12}		a_{58}, $a_{57}[16]$, a_{56}, $a_{55}[23]$, a_{54}, a_{53}, a_{52}, a_{51}
59	m_{15}		a_{59}, a_{58}, $a_{57}[16]$, a_{56}, $a_{55}[23]$, a_{54}, a_{53}, a_{52}
60	m_{13}		a_{60}, a_{59}, a_{58}, $a_{57}[16]$, a_{56}, $a_{55}[23]$, a_{54}, a_{53}
61	m_2		a_{61}, a_{60}, a_{59}, a_{58}, $a_{57}[16]$, a_{56}, $a_{55}[23]$, a_{54}
62	m_{25}		a_{62}, a_{61}, a_{60}, a_{59}, a_{58}, $a_{57}[16]$, a_{56}, $a_{55}[23]$
63	m_{31}	2^{11}	$a_{63}[12]$, a_{62}, a_{61}, a_{60}, a_{59}, a_{58}, $a_{57}[16]$, a_{56}
64	m_{27}		a_{64}, $a_{63}[12]$, a_{62}, a_{61}, a_{60}, a_{59}, a_{58}, $a_{57}[16]$
65	m_{19}		a_{65}, a_{64}, $a_{63}[12]$, a_{62}, a_{61}, a_{60}, a_{59}, a_{58}
66	m_9		a_{66}, a_{65}, a_{64}, $a_{63}[12]$, a_{62}, a_{61}, a_{60}, a_{59}
67	m_4		a_{67}, a_{66}, a_{65}, a_{64}, $a_{63}[12]$, a_{62}, a_{61}, a_{60}
68	m_{20}		a_{68}, a_{67}, a_{66}, a_{65}, a_{64}, $a_{63}[12]$, a_{62}, a_{61}
69	m_{28}		a_{69}, a_{68}, a_{67}, a_{66}, a_{65}, a_{64}, $a_{63}[12]$, a_{62}
70	m_{17}		a_{70}, a_{69}, a_{68}, a_{67}, a_{66}, a_{65}, a_{64}, $a_{63}[12]$
71	m'_8		a_{71}, a_{70}, a_{69}, a_{68}, a_{67}, a_{66}, a_{65}, a_{64}
...	...		...
117	m'_8	-1	$a_{117}[1,-2]$, a_{116}, a_{115}, a_{114}, a_{113}, a_{112}, a_{111}, a_{110}
118	m_{27}		a_{118}, $a_{117}[1,-2]$, a_{116}, a_{115}, a_{114}, a_{113}, a_{112}, a_{111}
119	m_{12}		a_{119}, a_{118}, $a_{117}[1,-2]$, a_{116}, a_{115}, a_{114}, a_{113}, a_{112}
120	m_9		a_{120}, a_{119}, a_{118}, $a_{117}[1,-2]$, a_{116}, a_{115}, a_{114}, a_{113}
121	m_1		a_{121}, a_{120}, a_{119}, a_{118}, $a_{117}[1,-2]$, a_{116}, a_{115}, a_{114}
122	m_{29}		a_{122}, a_{121}, a_{120}, a_{119}, a_{118}, $a_{117}[1,-2]$, a_{116}, a_{115}
123	m_5		a_{123}, a_{122}, a_{121}, a_{120}, a_{119}, a_{118}, $a_{117}[1,-2]$, a_{116}
124	m_{15}	-2^{26}	$a_{124}[27,28,29,-30]$, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}, a_{118}, $a_{117}[1,-2]$
125	m_{17}		a_{125}, $a_{124}[27,28,29,-30]$, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}, a_{118}
126	m_{10}	2^{22}	$a_{126}[23]$, a_{125}, $a_{124}[27,28,29,-30]$, a_{123}, a_{122}, a_{121}, a_{120}, a_{119}
127	m_{16}	-2^{15}	$a_{127}[-16]$, $a_{126}[23]$, a_{125}, $a_{124}[27,28,29,-30]$, a_{123}, a_{122}, a_{121}, a_{120}
128	m_{13}		a_{128}, $a_{127}[-16]$, $a_{126}[23]$, a_{125}, $a_{124}[27,28,29,-30]$, a_{123}, a_{122}, a_{121}
129	m_{27}		a_{129}, a_{128}, $a_{127}[-16]$, $a_{126}[23]$, a_{125}, $a_{124}[27,28,29,-30]$, a_{123}, a_{122}
130	m_3		a_{130}, a_{129}, a_{128}, $a_{127}[-16]$, $a_{126}[23]$, a_{125}, $a_{124}[27,28,29,-30]$, a_{123}
131	m_{21}		a_{131}, a_{130}, a_{129}, a_{128}, $a_{127}[-16]$, $a_{126}[23]$, a_{125}, $a_{124}[27,28,29,-30]$
132	m_{26}		a_{132}, a_{131}, a_{130}, a_{129}, a_{128}, $a_{127}[-16]$, $a_{126}[23]$, a_{125}
133	m_{17}		a_{133}, a_{132}, a_{131}, a_{130}, a_{129}, a_{128}, $a_{127}[-16]$, $a_{126}[23]$
134	m_{11}	2^{11}	$a_{134}[12]$, a_{133}, a_{132}, a_{131}, a_{130}, a_{129}, a_{128}, $a_{127}[-16]$
135	m_{20}		a_{135}, $a_{134}[12]$, a_{133}, a_{132}, a_{131}, a_{130}, a_{129}, a_{128}
136	m_{29}		a_{136}, a_{135}, $a_{134}[12]$, a_{133}, a_{132}, a_{131}, a_{130}, a_{129}
137	m_{19}		a_{137}, a_{136}, a_{135}, $a_{134}[12]$, a_{133}, a_{132}, a_{131}, a_{130}
138	m_0		a_{138}, a_{137}, a_{136}, a_{135}, $a_{134}[12]$, a_{133}, a_{132}, a_{131}
139	m_{12}		a_{139}, a_{138}, a_{137}, a_{136}, a_{135}, $a_{134}[12]$, a_{133}, a_{132}
140	m_7		a_{140}, a_{139}, a_{138}, a_{137}, a_{136}, a_{135}, $a_{134}[12]$, a_{133}
141	m_{13}		a_{141}, a_{140}, a_{139}, a_{138}, a_{137}, a_{136}, a_{135}, $a_{134}[12]$
142	m'_8		a_{142}, a_{141}, a_{140}, a_{139}, a_{138}, a_{137}, a_{136}, a_{135}

Table 12. A set of sufficient conditions on a_i for the differential path given in Table 10 and 11, up to the first inner collision

Step	Conditions of the chaining variable in each step
5	$a_{5,1}=0$, $a_{5,2}=0$, $a_{5,3}=0$, $a_{5,4}=1$, $a_{5,5}=0$
6	$a_{6,1}=0$, $a_{6,2}=0$, $a_{6,3}=0$, $a_{6,4}=0$, $a_{6,5}=0$
7	
8	$a_{8,1}=0$, $a_{8,2}=0$, $a_{8,3}=0$, $a_{8,4}=0$, $a_{8,5}=0$, $a_{8,29}=0$, $a_{8,30}=0$
9	$a_{9,1}=0$, $a_{9,2}=0$, $a_{9,3}=0$, $a_{9,4}=1$, $a_{9,5}=0$, $a_{9,29}=0$, $a_{9,30}=0$
10	$a_{10,1}=0$, $a_{10,2}=0$, $a_{10,3}=0$, $a_{10,4}=0$, $a_{10,5}=0$, $a_{10,22}=0$, $a_{10,29}=0$
11	$a_{11,22}=0$, $a_{11,29}=1$, $a_{11,30}=0$
12	$a_{12,1}=0$, $a_{12,2}=0$, $a_{12,3}=0$, $a_{12,4}=0$, $a_{12,5}=0$, $a_{12,29}=0$, $a_{12,30}=1$
13	$a_{13,1}=1$, $a_{13,2}=1$, $a_{13,3}=1$, $a_{13,4}=1$, $a_{13,5}=1$, $a_{13,15}=1$, $a_{13,16}=0$, $a_{13,22}=0$, $a_{13,29}=0$, $a_{13,30}=0$
14	$a_{14,15}=0$, $a_{14,16}=0$, $a_{14,22}=0$
15	$a_{15,22}=0$, $a_{15,29}=0$, $a_{15,30}=0$
16	$a_{16,8}=0$, $a_{16,9}=0$, $a_{16,10}=1$, $a_{16,15}=0$, $a_{16,16}=0$, $a_{16,18}=0$, $a_{16,29}=1$, $a_{16,30}=1$
17	$a_{17,8}=0$, $a_{17,9}=0$, $a_{17,10}=0$, $a_{17,15}=0$, $a_{17,16}=1$, $a_{17,18}=0$, $a_{17,22}=0$
18	$a_{18,2}=1$,$a_{18,11}=0$, $a_{18,15}=0$, $a_{18,16}=0$, $a_{18,22}=1$
19	$a_{19,3}=0$,$a_{19,8}=0$, $a_{19,9}=0$, $a_{19,10}=0$, $a_{19,11}=0$, $a_{19,18}=0$
20	$a_{20,2}=0$, $a_{20,3}=0$, $a_{20,8}=0$, $a_{20,9}=0$, $a_{20,10}=0$, $a_{20,15}=0$, $a_{20,16}=0$, $a_{20,18}=0$
21	$a_{21,2}=1$, $a_{21,8}=0$, $a_{21,9}=0$, $a_{21,10}=0$, $a_{21,11}=0$, $a_{21,15}=1$, $a_{21,16}=1$, $a_{21,18}=0$
22	$a_{22,2}=0$, $a_{22,3}=0$, $a_{22,4}=0$, $a_{22,11}=0$, $a_{22,27}=0$
23	$a_{23,2}=0$, $a_{23,3}=0$, $a_{23,4}=1$, $a_{23,8}=0$, $a_{23,9}=1$, $a_{23,10}=0$, $a_{23,11}=0$, $a_{23,18}=0$, $a_{23,27}=1$
24	$a_{24,2}=0$, $a_{24,3}=0$, $a_{24,4}=0$, $a_{24,7}=0$, $a_{24,8}=1$, $a_{24,9}=1$, $a_{24,10}=1$, $a_{24,18}=1$, $a_{24,20}=0$,$a_{24,27}=0$
25	$a_{25,2}=0$, $a_{25,4}=1$, $a_{25,7}=0$, $a_{25,11}=0$, $a_{25,20}=0$, $a_{25,27}=1$
26	$a_{26,3}=0$, $a_{26,4}=0$, $a_{26,11}=1$, $a_{26,23}=1$, $a_{26,27}=0$
27	$a_{27,2}=0$, $a_{27,3}=1$, $a_{27,7}=0$, $a_{27,20}=0$, $a_{27,32}=0$
28	$a_{28,2}=1$, $a_{28,4}=0$, $a_{28,7}=1$, $a_{28,20}=0$, $a_{28,23}=1$, $a_{28,24}=0$,$a_{28,27}=0$, $a_{28,32}=0$
29	$a_{29,4}=1$, $a_{29,7}=0$, $a_{29,20}=0$, $a_{29,23}=1$, $a_{29,24}=1$, $a_{29,27}=1$, $a_{29,32}=0$
30	$a_{30,7}=0$, $a_{30,16}=0$, $a_{30,20}=0$, $a_{30,23}=1$, $a_{30,24}=0$, $a_{30,32}=0$
31	$a_{31,7}=0$, $a_{31,16}=1$, $a_{31,20}=0$, $a_{31,23}=0$, $a_{31,23}=0$, $a_{31,24}=0$, $a_{31,32}=0$
32	$a_{32,16}=0$, $a_{32,23}=0$, $a_{32,24}=1$, $a_{32,28}=0$, $a_{32,32}=1$
33	$a_{33,16}=0$, $a_{33,23}=1$, $a_{33,24}=1$, $a_{33,28}=1$, $a_{33,32}=0$
34	$a_{34,13}=0$, $a_{34,16}=1$, $a_{34,24}=0$, $a_{34,28}=0$
35	$a_{35,16}=1$, $a_{35,23}=0$, $a_{35,24}=1$, $a_{35,28}=0$

Table 13. (Continued from Table 12)

Step	Conditions of the chaining variable in each step
36	$a_{36,12} = 0$, $a_{36,13} = 0$, $a_{36,16} = 1$, $a_{36,23} = 1$, $a_{36,28} = 1$, $a_{36,32} = 1$
37	$a_{37,6} = 1$, $a_{37,12} = 1$, $a_{37,13} = 1$, $a_{37,16} = 0$, $a_{37,28} = 1$, $a_{37,31} = 0$
38	$a_{38,6} = 0$, $a_{38,12} = 0$, $a_{38,13} = 0$, $a_{38,16} = 1$, $a_{38,24} = 0$, $a_{38,28} = 1$
39	$a_{39,6} = 0$, $a_{39,12} = 0$, $a_{39,13} = 0$, $a_{39,28} = 0$, $a_{39,31} = 0$
40	$a_{40,6} = 0$, $a_{40,12} = 0$, $a_{40,13} = 1$, $a_{40,24} = 0$, $a_{40,28} = 1$, $a_{40,31} = 1$
41	$a_{41,6} = 1$, $a_{41,12} = 1$, $a_{41,13} = 1$, $a_{41,24} = 1$, $a_{41,31} = 0$
42	$a_{42,2} = 1$, $a_{42,6} = 1$, $a_{42,12} = 1$, $a_{42,13} = 0$, $a_{42,24} = 0$, $a_{42,31} = 0$
43	$a_{43,6} = 0$, $a_{43,12} = 1$, $a_{43,13} = 1$, $a_{43,24} = 0$,$a_{43,31} = 1$
44	$a_{44,2} = 0$, $a_{44,6} = 1$, $a_{44,12} = 1$, $a_{44,24} = 1$, $a_{44,31} = 1$
45	$a_{45,2} = 1$, $a_{45,20} = 1$, $a_{45,24} = 1$, $a_{45,31} = 0$
46	$a_{46,2} = 0$, $a_{46,24} = 0$, $a_{46,31} = 1$
47	$a_{47,2} = 0$, $a_{47,20} = 0$, $a_{47,24} = 1$
48	$a_{48,2} = 1$, $a_{48,20} = 0$
49	$a_{49,2} = 1$, $a_{49,20} = 0$
50	$a_{50,2} = 0$, $a_{50,20} = 0$
51	$a_{51,2} = 1$, $a_{51,20} = 1$, $a_{51,23} = 0$
52	$a_{52,16} = 1$,$a_{52,20} = 1$, $a_{52,23} = 0$
53	$a_{53,20} = 0$, $a_{53,23} = 0$
54	$a_{54,20} = 1$, $a_{54,16} = 0$, $a_{54,23} = 0$
55	$a_{55,16} = 1$, $a_{55,23} = 0$
56	$a_{56,16} = 0$, $a_{56,23} = 1$
57	$a_{57,16} = 0$, $a_{57,23} = 1$
58	$a_{58,16} = 1$, $a_{58,23} = 0$
59	$a_{59,12} = 1$, $a_{59,16} = 1$, $a_{59,23} = 1$
60	$a_{60,12} = 0$, $a_{60,16} = 0$
61	$a_{61,12} = 0$, $a_{61,16} = 1$
62	$a_{62,12} = 0$
63	$a_{63,12} = 0$
64	$a_{64,12} = 1$
65	$a_{65,12} = 0$