情報保護學會論文誌
第12券 第4號, 2002. 8

3-pass HAVAL의 축소 라운드 안전성에 관한 연구

박 상 우*, 성 수 학**, 지 성 택*, 윤 이 중*, 임 종 인***

On the Security of reduced versions of 3-pass HAVAL

Sangwoo Park*, Soo Hak Sung**, Seongtaek Chee*, E-Joong Yoon*, Jong-In Lim***

요 약

HAVAL은 Zheng 등이 제안한 MD-계열의 해쉬 함수로서, 임의의 길이의 메시지를 입력으로 하며, 128, 160, 192, 224, 256 비트 길이의 해쉬값를 출력하는 해쉬 함수이다. HAVAL은 입력 메시지의 1024 비트 블록을 처리하는 회수에 따라 3-pass HAVAL, 4-pass HAVAL, 그리고, 5-pass HAVAL로 구분된다. 본 논문에서는 3-pass HAVAL의 축소 라운드의 충돌쌍을 찾는 방법을 제안한다. 본 논문에서 제안하는 방법에 의하여 3-pass HAVAL의 처음 두 라운드와 마지막 두 라운드에 대한 충돌쌍을 찾을 수 있다.

ABSTRACT

HAVAL is a dedicated hash function of the MD family which was proposed by Zheng et al.. HAVAL compresses a message of arbitrary length into a hash value of 128, 160, 192, 224, or 256 bits. HAVAL has a parameter that controls the number of passes a message block of 1024 bits is processed. A message block can be processed in 3,4, or 5 passes. When a message block is processed in three passes, we call such a case 3-pass HAVAL. So, there are three kinds of HAVAL: 3-pass HAVAL, 4-pass HAVAL, and 5-pass HAVAL.

In this paper, we study the security of reduced versions of 3-pass HAVAL. We propose a method for finding the collisions for the first two passes of 3-pass HAVAL and for the last two passes of 3-pass HAVAL. This approach of reducing the number of passes is similar to the initial attacks on MD4. We represent the first two passes of 3-pass HAVAL as HAVAL-12 and the last two passes of 3-pass HAVAL as HAVAL-23.

Keyword : *Hash function, Collision resistance, Collisions*

Ⅰ. 서 론

해쉬 함수(hash function)는 메시지 인증, 디지털 서명 등의 많은 암호 응용 서비스에 사용되는 대표적인 암호 논리이다. 해쉬 함수는 임의의 길이의 메시지를 입력으로 받아, 고정된 짧은 길이의 해쉬값을 출력하는 함수이며, 안전한 해쉬 함수는 충돌 회피성(collision resistance)을 만족하는 해쉬 함수이다. 충돌 회피성이란 동일한 해쉬값을 가지는 서로 다른 두 개의 메시지, 즉, 충돌쌍(collision)을 찾는 것이 계산상 불가능함을 의미한다.

R. Rivest가 해쉬 함수 MD4[1]를 제안한 이후로, MD4의 설계 원칙을 기반으로 하는 많은 전용 해쉬 함수(dedicated hash function)들이 제안되었다.

* 국가보안기술연구소({psw, chee, yej}@etri.re.kr)
** 배재대학교 전산정보수학과(sungsh@paichai.ac.kr)
*** 고려대학교 정보보호대학원(jilim@tiger.korea.ac.kr)

MD4의 설계 원칙을 기반으로 하는 전용 해쉬 함수들을 MD-계열 해쉬 함수라 하는데, 대표적인 MD-계열 전용 해쉬 함수로는 MD5[2], HAVAL[3], RIPEMD[4], RIPEMD-160[5], SHA-1[6] 등이 있다.

MD-계열 해쉬 함수의 안전성에 관한 연구도 계속되어 왔다. den Boer와 Bosselaers는 MD4의 마지막 두 라운드에 대한 공격 방법을 제안하였으며[7], Vaudenay는 MD4의 처음 두 라운드에 대한 공격 방법을 제안하였다[8]. 참고로, MD4는 3 라운드로 구성된다. Dobbertin은 MD4 전체 라운드에 대한 공격 방법을 제안하였으며[9], 결과적으로 MD4는 안전하지 않은 해쉬 함수임이 입증되었다. 또한, Dobbertin은 RIPEMD의 처음 두 라운드와 마지막 두 라운드의 충돌쌍을 찾는 공격 방법을 제안하였다[10]. Debaert와 Gilbert는 RIPEMD의 병렬 형태 각각의 충돌쌍을 찾는 방법을 제안하였다[11]. 그리고, den Boer와 Bosselaers는 MD5의 의사 충돌쌍을 찾는 방법을 제안하였다[12]. Chabaud와 Jaux는 SHA-0의 충돌쌍을 찾는 방법을 제안하였으며, 공격량은 약 2^{61} 정도이다. Kasselman과 Penzhorn은 3-pass HAVAL의 마지막 두 라운드에 대한 충돌쌍을 찾는 공격 방법을 제안하였다[13].

HAVAL은 Zheng 등이 제안한 MD-계열의 전용 해쉬 함수이다[3]. HAVAL은 임의의 길이의 메시지를 입력으로 하여, 128, 160, 192, 224, 256 비트의 모두 5 가지 종류의 길이의 해쉬값을 출력한다. HAVAL은 입력 메시지를 1,024 비트 단위로 구분하여 처리하는데, 1,024 비트 한 블록을 처리하는 회수에 따라 3-pass HAVAL, 4-pass HAVAL, 5-pass HAVAL로 구분된다. 여기서, 패스(pass)는 MD4나 MD5의 라운드에 해당한다.

본 논문에서는 3-pass HAVAL의 축소 라운드의 충돌쌍을 찾는 방법을 제안한다. 3-pass HAVAL의 처음 두 라운드와 마지막 두 라운드에 대한 충돌쌍을 찾는 공격 방법을 제안하는데, 이는 MD4에 대한 공격이 초기에는 MD4의 축소 라운드에 대하여 이루어진 것을 고려하면[7,8], 의미 있는 연구 분야가 된다. 본 논문에서는 3-pass HAVAL의 처음 두 라운드를 HAVAL-12, 마지막 두 라운드를 HAVAL-23으로 표시한다.

II. HAVAL의 구성 및 동작 방식

본 논문에서 +는 모듈러 2^{32} 덧셈을 표시한다. $X \oplus Y$, XY, $X \vee Y$는 각각 비트별 배타적 논리합(bitwise exclusive OR), 비트별 논리곱(bitwise AND), 그리고, 비트별 논리합(bitwise OR)을 표시한다. $\sim X$는 X의 비트별 보수(bitwise complement)를 그리고, $X^{\gg s}$는 X를 s 비트 우측 순환(right cyclic shift)함을 표시한다.

HAVAL의 압축 함수(compression function)는 8-워드(256-비트) 초기값 A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0와 32-워드 메시지 블록 $X=(X_0, X_1, \ldots, X_{31})$을 256-비트 출력값 ($AA$, BB, CC, DD, EE, FF, GG, HH)로 변환한다. 8-워드 초기값은 다음과 같다.

$A_0 = 0xec4e6c89$, $B_0 = 0x082efa98$,
$C_0 = 0x299f31d0$, $D_0 = 0xa4093822$,
$E_0 = 0x03707344$, $F_0 = 0x13198a2e$,
$G_0 = 0x85a308d3$, $H_0 = 0x243f6a88$.

HAVAL 압축 함수의 각 패스는 32 단계로 구성되며, 각 단계는 서로 다른 워드들을 처리한다. 워드

〔표 1〕 워드 처리 순서

pass 1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
pass 2	5	14	26	18	11	28	7	16	0	23	20	22	1	10	4	8
	30	3	21	9	17	24	29	6	19	12	15	13	2	25	31	27
pass 3	19	9	4	20	28	17	8	22	29	14	25	12	24	30	16	26
	31	15	7	3	1	0	18	27	13	6	21	10	23	11	5	2
pass 4	24	4	0	14	2	7	28	23	26	6	30	20	18	25	19	3
	22	11	31	21	8	27	12	9	1	29	5	15	17	10	16	13
pass 5	27	3	21	26	17	11	20	29	19	0	12	7	13	8	31	10
	5	9	14	30	18	6	28	24	2	23	16	22	4	1	25	15

처리 순서는 패스마다 다르며, 구체적인 순서는 〔표 1〕과 같다.

각 패스는 서로 다른 부울 함수(Boolean function)를 사용한다. i번째 패스에 사용되는 부울 함수 f_i는 다음과 같다.

$$f_1(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_0x_1 \oplus x_0$$

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

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

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

$$f_5(x_6,x_5,x_4,x_3,x_2,x_1,x_0) = x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_0x_1x_2x_3 \oplus x_0x_5 \oplus x_0$$

다음으로, HAVAL의 단계 함수(step function)를 소개한다. $T_{i,j}(j=0,1,\ldots,7)$를 단계 i에서의 단계 함수의 입력으로 설정한다. 그리고, Q를 다음으로 설정한다.

- 3-pass HAVAL:
  $Q=f_r(P_{3,r}(T_{i,6},T_{i,5},T_{i,4},T_{i,3},T_{i,2},T_{i,1},T_{i,0}))$
- 4-pass HAVAL:
  $Q=f_r(P_{4,r}(T_{i,6},T_{i,5},T_{i,4},T_{i,3},T_{i,2},T_{i,1},T_{i,0}))$
- 5-pass HAVAL:
  $Q=f_r(P_{5,r}(T_{i,6},T_{i,5},T_{i,4},T_{i,3},T_{i,2},T_{i,1},T_{i,0}))$

HAVAL의 단계 함수는 다음 형태를 가진다.

$$R = Q^{\gg 7} + T_{i,7}^{\gg 11} + X_{ord_r(i)} + K_i,$$
$$T_{i+1,7} = T_{i,6};\ T_{i+1,6} = T_{i,5};$$
$$T_{i+1,5} = T_{i,4};\ T_{i+1,4} = T_{i,3};$$
$$T_{i+1,3} = T_{i,2};\ T_{i+1,2} = T_{i,1};$$
$$T_{i+1,1} = T_{i,0};\ T_{i+1,0} = R,$$

위 식에서 r은 패스 번호이며, $ord_r(i)$는 〔표 1〕의 워드 처리 순서이고, K_i는 32-비트 상수이다. 모든 상수는 π의 소수점 이하 값으로부터 결정된다. 패스 1에서 상수 $K_i(i=0,\ldots,31)$는 생략된다. 패스 2부터 패스 5에서는 상수는 각 단계마다 모두 서로 다르다. 단계 i의 입력 ($T_{i,6}$, $T_{i,5}$, $T_{i,4}$, $T_{i,3}$, $T_{i,2}$, $T_{i,1}$, $T_{i,0}$)는 3-pass HAVAL에서는 $P_{3,r}$로, 4-pass HAVAL에서는 $P_{4,r}$로, 5-pass HAVAL에서는 $P_{5,r}$로 순환되어 부울 함수 f_r로 처리된다. $P_{3,r}$, $P_{4,r}$, $P_{5,r}$은 〔표 2〕와 같다.

〔표 2〕 단계 입력 순환 방법

순환	x_6	x_5	x_4	x_3	x_2	x_1	x_0
$P_{3,1}$	x_1	x_0	x_3	x_5	x_6	x_2	x_4
$P_{3,2}$	x_4	x_2	x_1	x_0	x_5	x_3	x_6
$P_{3,3}$	x_6	x_1	x_2	x_3	x_4	x_5	x_0
$P_{4,1}$	x_2	x_6	x_1	x_4	x_5	x_3	x_0
$P_{4,2}$	x_3	x_5	x_2	x_0	x_1	x_6	x_4
$P_{4,3}$	x_1	x_4	x_3	x_6	x_0	x_2	x_5
$P_{4,4}$	x_6	x_3	x_0	x_5	x_2	x_1	x_4
$P_{5,1}$	x_3	x_4	x_1	x_0	x_5	x_2	x_6
$P_{5,2}$	x_6	x_2	x_1	x_0	x_3	x_4	x_5
$P_{5,3}$	x_2	x_6	x_0	x_4	x_3	x_1	x_5
$P_{5,4}$	x_1	x_5	x_3	x_2	x_0	x_4	x_6
$P_{5,5}$	x_2	x_5	x_0	x_6	x_4	x_3	x_1

Ⅲ. HAVAL-12에 대한 공격 방법

본 절에서는 3-pass HAVAL의 처음 두 라운드인 HAVAL-12의 충돌쌍을 찾는 공격 방법을 제안한다.

두 개의 32-비트 벡터 X와 $\hat{X}$에 대하여, X와 $\hat{X}$의 difference ΔX를 다음으로 정의한다.

$$\Delta X = X - \hat{X} (\mathrm{mod}\, 2^{32})$$

$A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i$를 입력 메시지 블록 $X=(X_0,\ldots,X_{31})$에 대한 단계 i이후의 연결 변수로 정의한다. 그리고, $\hat{A}_i$, $\hat{B}_i$, $\hat{C}_i$, $\hat{D}_i$, $\hat{E}_i$, $\hat{F}_i$, $\hat{G}_i$, $\hat{H}_i$를 입력 메시지 블록 $\hat{X}=(\hat{X}_0,\ldots,\hat{X}_{31})$에 대한 단계 i 이후의 연결 변수로 정의한다.

HAVAL-12의 충돌쌍을 찾는다는 것은 단계 64 이후의 연결 변수 값이 서로 동일하게 되는 서로 다른 두 개의 메시지 블록 X와 $\hat{X}$를 찾는 것이다.

HAVAL 압축 함수는 8개의 연결 변수들을 가지고 있으며, 각 단계에서 단지 한 개의 연결 변수만이 update된다. 따라서, 단계 i에서 X와 $\hat{X}$에 의해 update된 연결 변수에 0이 아닌 difference가 발

생하면, 단계 $i+8$ 까지는 그 difference를 제거할 기회가 없다.

HAVAL-12에서 메시지 워드 X_{28}은 단계 29와 단계 38에서 입력되며, 두 단계의 차이는 9가 된다. 그러므로, 본 절에서는 다음과 같은 두 개의 서로 다른 메시지 블록 X와 $\widehat{X}$를 고려하도록 한다.

$$X_{28} \neq \widehat{X}_{28}, \quad X_i = \widehat{X}_i (i \neq 28)$$

〔표 3〕은 단계 29부터 단계 38에서 적용되는 연결 변수와 메시지 워드를 나타낸다. 음영 있는 네모로 표시된 연결 변수는 각 단계에서 update되는 연결 변수이다.

〔표 3〕 단계 29~단계 38의 연결 변수

단계	연결 변수								메시지 워드
29	A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	X_{28}
30	A_{30}	B_{30}	C_{30}	D_{30}	E_{30}	F_{30}	G_{30}	H_{30}	X_{29}
31	A_{31}	B_{31}	C_{31}	D_{31}	E_{31}	F_{31}	G_{31}	H_{31}	X_{30}
32	A_{32}	B_{32}	C_{32}	D_{32}	E_{32}	F_{32}	G_{32}	H_{32}	X_{31}
33	A_{33}	B_{33}	C_{33}	D_{33}	E_{33}	F_{33}	G_{33}	H_{33}	X_5
34	A_{34}	B_{34}	C_{34}	D_{34}	E_{34}	F_{34}	G_{34}	H_{34}	X_{14}
35	A_{35}	B_{35}	C_{35}	D_{35}	E_{35}	F_{35}	G_{35}	H_{35}	X_{26}
36	A_{36}	B_{36}	C_{36}	D_{36}	E_{36}	F_{36}	G_{36}	H_{36}	X_{18}
37	A_{37}	B_{37}	C_{37}	D_{37}	E_{37}	F_{37}	G_{37}	H_{37}	X_{11}
38	A_{38}	B_{38}	C_{38}	D_{38}	E_{38}	F_{38}	G_{38}	H_{38}	X_{28}

$(X, \widehat{X})$가 HAVAL-12의 충돌쌍이 되려면 다음을 만족하여야 한다.

$$A_{38} = \widehat{A}_{38},\ B_{38} = \widehat{B}_{38},\ C_{38} = \widehat{C}_{38},$$
$$D_{38} = \widehat{D}_{38},\ E_{38} = \widehat{E}_{38},\ F_{38} = \widehat{F}_{38},$$
$$G_{38} = \widehat{G}_{38},\ H_{38} = \widehat{H}_{38}.$$

그런데, 우리는 다음 사실을 알고 있다.

$$\Delta A_{38} = \Delta A_{32}, \Delta B_{38} = \Delta B_{31}, \Delta D_{38} = \Delta D_{37},$$
$$\Delta E_{38} = \Delta E_{36}, \Delta F_{38} = \Delta F_{35}, \Delta G_{38} = \Delta G_{34},$$
$$\Delta H_{38} = \Delta H_{33}.$$

그러므로, $(X, \widehat{X})$이 HAVAL-12의 충돌쌍이 되기 위한 조건을 다음으로 수립할 수 있다.

$$\Delta A_{32} = 0,\ \Delta B_{31} = 0,\ \Delta C_{38} = 0,\ \Delta D_{37} = 0,$$
$$\Delta E_{36} = 0,\ \Delta F_{35} = 0,\ \Delta G_{34} = 0,\ \Delta H_{33} = 0.$$

이제, 단계 29부터 단계 38 까지의 각 단계를 분석하고, $(X, \widehat{X})$이 충돌쌍이 되는 조건을 만족하는 방정식들을 수립한다. 연결 변수 D_{29}와 $\widehat{D}_{29}$는 단계 29에서 다음으로 update된다.

$$D_{29} = (G_{28} H_{28} \oplus C_{28} E_{28} \oplus B_{28} F_{28} \oplus A_{28} G_{28} \oplus A_{28})^{\gg 7} + D_{28}^{\gg 11} + X_{28}$$
$$\widehat{D}_{29} = (\widehat{G}_{28} \widehat{H}_{28} \oplus \widehat{C}_{28} \widehat{E}_{28} \oplus \widehat{B}_{28} \widehat{F}_{28} \oplus \widehat{A}_{28} \widehat{G}_{28} \oplus \widehat{A}_{28})^{\gg 7} + \widehat{D}_{28}^{\gg 11} + \widehat{X}_{28}.$$

그런데,

$$A_{28} = \widehat{A}_{28},\ B_{28} = \widehat{B}_{28}, C_{28} = \widehat{C}_{28}, D_{28} = \widehat{D}_{28},$$
$$E_{28} = \widehat{E}_{28},\ F_{28} = \widehat{F}_{28}, G_{28} = \widehat{G}_{28}, H_{28} = \widehat{H}_{28}$$

이므로, 다음 방정식을 얻을 수 있다.

$$\Delta D_{29} = \Delta X_{28} \neq 0.$$

연결 변수 C_{30}과 $\widehat{C}_{30}$은 단계 30에서 다음으로 update된다.

$$C_{30} = (F_{29} G_{29} \oplus B_{29} D_{29} \oplus A_{29} E_{29} \oplus H_{29} F_{29} \oplus H_{29})^{\gg 7} + C_{29}^{\gg 11} + X_{29}$$
$$\widehat{C}_{30} = (\widehat{F}_{29} \widehat{G}_{29} \oplus \widehat{B}_{29} \widehat{D}_{29} \oplus \widehat{A}_{29} \widehat{E}_{29} \oplus \widehat{H}_{29} \widehat{F}_{29} \oplus \widehat{H}_{29})^{\gg 7} + \widehat{C}_{29}^{\gg 11} + \widehat{X}_{29}.$$

그런데,

$$\Delta A_{29} = \Delta B_{29} = \Delta C_{29} = \Delta E_{29} = 0$$
$$\Delta F_{29} = \Delta G_{29} = \Delta H_{29} = 0,$$
$$\Delta X_{29} = 0,$$

이므로, 다음 방정식을 얻을 수 있다.

$$C_{30} - \widehat{C}_{30} = (F_{29} G_{29} \oplus B_{29} D_{29} \oplus A_{29} E_{29} \oplus H_{29} F_{29} \oplus H_{29})^{\gg 7} - (F_{29} G_{29} \oplus B_{29} \widehat{D}_{29} \oplus A_{29} E_{29} \oplus H_{29} F_{29} \oplus H_{29})^{\gg 7}.$$

다음 단계에서 B_{31}과 $\widetilde{B_{31}}$은 다음으로 update 된다.

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

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

그런데,

$$\Delta A_{30} = \Delta B_{30} = \Delta E_{30} = 0$$
$$\Delta F_{30} = \Delta G_{30} = \Delta H_{30} = 0$$

이고, $\Delta X_{30} = 0$이므로, 다음 방정식을 얻을 수 있다.

$$\Delta B_{31} = 0$$
$$\Leftrightarrow E_{30}F_{30} \oplus A_{30}C_{30} \oplus H_{30}D_{30} \oplus G_{30}E_{30} \oplus G_{30} = E_{30}F_{30} \oplus A_{30}\widetilde{C_{30}} \oplus H_{30}\widetilde{D_{30}} \oplus G_{30}E_{30} \oplus G_{30}$$
$$\Leftrightarrow A_{30}C_{30} \oplus H_{30}D_{30} = A_{30}\widetilde{C_{30}} \oplus H_{30}\widetilde{D_{30}}$$
$$\Leftrightarrow H_{30} \cdot (D_{30} \oplus \widetilde{D_{30}}) = A_{30} \cdot (C_{30} \oplus \widetilde{C_{30}}).$$

유사한 방법으로 단계 32부터 단계 38을 분석하여, 다음의 10개 방정식을 얻을 수 있다.

$$D_{29} - \widetilde{D_{29}} = X_{28} - \widetilde{X_{28}} \quad (1)$$

$$C_{30} - \widetilde{C_{30}} = (F_{27}G_{26} \oplus B_{23}D_{29} \oplus A_{24}E_{28} \oplus H_{25})^{\gg 7} - (F_{27}G_{26} \oplus B_{23}\widetilde{D_{29}} \oplus A_{24}E_{28} \oplus H_{25})^{\gg 7} \quad (2)$$

$$(C_{30} \oplus \widetilde{C_{30}})A_{24} = (D_{29} \oplus \widetilde{D_{29}})H_{25} \quad (3)$$

$$(D_{29} \oplus \widetilde{D_{29}})(E_{28} \oplus F_{27}) = (C_{30} \oplus \widetilde{C_{30}})G_{26} \quad (4)$$

$$(C_{30} \oplus \widetilde{C_{30}})(F_{27}B_{31} \oplus A_{32} \oplus B_{31}) = (D_{29} \oplus \widetilde{D_{29}})(F_{27}A_{32} \oplus F_{27} \oplus B_{31}) \quad (5)$$

$$(C_{30} \oplus \widetilde{C_{30}})(E_{28}H_{33} \oplus E_{28} \oplus A_{32}) = (D_{29} \oplus \widetilde{D_{29}})E_{28} \quad (6)$$

$$(D_{29} \oplus \widetilde{D_{29}})(B_{31}G_{34} \oplus H_{33}A_{32} \oplus B_{31} \oplus E_{28}) = D_{29}C_{30} \oplus \widetilde{D_{29}}\,\widetilde{C_{30}} \quad (7)$$

$$(C_{30} \oplus \widetilde{C_{30}})(A_{32}F_{35} \oplus G_{34}H_{33} \oplus A_{32} \oplus B_{31}) = D_{29}C_{30} \oplus \widetilde{D_{29}}\,\widetilde{D_{30}} \oplus D_{29} \oplus \widetilde{D_{29}} \quad (8)$$

$$(H_{33}B_{31}E_{36} \oplus B_{31}F_{35}G_{34} \oplus H_{33}B_{31} \oplus H_{33}F_{35} \oplus B_{31}A_{32} \oplus E_{36}G_{34} \oplus F_{35}G_{34} \oplus C_{30}B_{31} \oplus C_{30})^{\gg 7} + D_{29}^{\gg 11} = (H_{33}B_{31}E_{36} \oplus B_{31}F_{35}G_{34} \oplus H_{33}B_{31} \oplus H_{33}F_{35} \oplus B_{31}A_{32} \oplus E_{36}G_{34} \oplus F_{35}G_{34} \oplus C_{30}B_{31} \oplus C_{30})^{\gg 7} + \widetilde{D_{29}^{\gg 11}} \quad (9)$$

$$C_{30}^{\gg 11} + X_{28} = \widetilde{C_{30}^{\gg 11}} + \widetilde{X_{28}} \quad (10)$$

상기의 10개 방정식에서, $i = 1, 2, \ldots, 7$에 대하여,

$$A_{24} = A_{24+i},\ A_{32} = A_{32+i},\ B_{23} = B_{23+i},$$
$$B_{31} = B_{31+i},\ C_{30} = C_{30+i},\ D_{29} = D_{29+i},$$
$$E_{28} = E_{28+i},\ E_{36} = E_{36+i},\ F_{27} = F_{27+i},$$
$$F_{35} = F_{35+i},\ G_{26} = G_{26+i},\ G_{34} = G_{34+i},$$
$$H_{25} = H_{25+i},\ H_{33} = H_{33+i}.$$

이다. 이제, (1)부터 (10)의 방정식의 해를 구하고, $(X, \widetilde{X})$가 충돌쌍이 되는 연결 변수의 값을 결정한다. 우선, 다음을 설정한다.

$$A_{24} = H_{25} = G_{26} = F_{27} = E_{28} = B_{31} = A_{32} = 0.$$

그러면, 방정식 (3), (4), (5), (6)이 만족된다. 방정식 (1)과 (10)에 의해 다음 방정식을 얻는다.

$$C_{30}^{\gg 11} - \widetilde{C_{30}^{\gg 11}} + D_{29} - \widetilde{D_{29}} = 0.$$

결과적으로, 충돌쌍을 찾기 위해서는 다음의 5개 방정식의 해를 구하여야 한다.

$$C_{30} - \widetilde{C_{30}} = (B_{23}D_{29})^{\gg 7} - (B_{23}\widetilde{D_{29}})^{\gg 7} \quad (11)$$

$$D_{29}C_{30} \oplus \widetilde{D_{29}}\,\widetilde{C_{30}} = 0 \quad (12)$$

$$(C_{30} \oplus \widetilde{C_{30}})G_{34}F_{35} = D_{29}C_{30} \oplus \widetilde{D_{29}}\,\widetilde{C_{30}} \oplus D_{29} \oplus \widetilde{D_{29}} \quad (13)$$

$$(H_{33}F_{35}\oplus E_{36}G_{34}\oplus F_{35}G_{34}\oplus C_{30})^{\gg 7} + D_{29}^{\gg 11} = (H_{33}F_{35}\oplus E_{36}G_{34}\oplus F_{35}G_{34} \oplus \widehat{C_{30}})^{\gg 7} + \widehat{D_{29}^{\gg 11}} \quad (14)$$

$$C_{30}^{\gg 11} - \widehat{C_{30}^{\gg 11}} + D_{29} - \widehat{D_{29}} = 0 \quad (15)$$

다음은 방정식 (11), (12), (13), (14), (15)의 해들이다.

$$B_{23} = 2^7 = 0x80$$
$$D_{29} = -1 = 0xffffffff, \quad \widehat{D_{29}} = 0$$
$$C_{30} = 0, \quad \widehat{C_{30}} = -1 = 0xffffffff$$
$$H_{33} = G_{34} = -1 = 0xffffffff$$
$$E_{36} = 0$$

여기서, 우리는 F_{35}의 구체적인 값을 설정할 수 없다. 왜냐하면, 단계 27에서 X_{26}에 의해 F_{27}이 update 되고, 단계 35에서도 X_{26}에 의해 F_{35}가 update되기 때문이다. 그리고, $F_{27}=0$임을 이미 알고 있다.

〔표 4〕 방정식 (1)~(10)의 해

B_{23}	0x80		
A_{24}	0		
H_{25}	0		
G_{26}	0		
F_{27}	0		
E_{28}	0		
D_{29}	0xffffffff	$\widehat{D_{29}}$	0
C_{30}	0	$\widehat{C_{30}}$	0xffffffff
B_{31}	0		
A_{32}	0		
H_{33}	0xffffffff		
G_{34}	0xffffffff		
F_{35}	임의의 값		
E_{36}	0		

이제 충돌쌍 $(X, \widehat{X})$를 결정한다. $X_i(22 \le i \le 25, 27 \le i \le 31)$의 값을 쉽게 결정할 수 있다. 단계 33에서

$$H_{33} = (D_{32}F_{32}A_{32}\oplus F_{32}B_{32}C_{32} \oplus D_{32}F_{32}\oplus D_{32}B_{32}\oplus F_{32}E_{32}\oplus A_{32}C_{32}\oplus B_{32}C_{32} \oplus G_{32}F_{32}\oplus G_{32})^{\gg 7} + H_{32}^{\gg 11} + X_5 + 0x452821e6.$$

임을 알고 있다. 〔표 4〕의 해들을 사용해서, 다음을 계산할 수 있다.

$$X_5 = 0xffffffff - 0x452821e6.$$

유사한 방법으로, 단계 34에서, 다음을 얻을 수 있다.

$$X_{14} = 0xffffffff - 0x38d01377.$$

다음으로, X_{18}과 X_{26}의 값을 결정한다. F_{35}는 임의의 값을 가질 수 있으므로, 단계 27에서 얻은 X_{26}의 값을 활용할 수 있다. 단계 35에서

$$F_{35} = (B_{34}D_{34}G_{34}\oplus D_{34}H_{34}A_{34}\oplus B_{34}D_{34} \oplus B_{34}H_{34}\oplus D_{34}C_{34}\oplus G_{34}A_{34}\oplus H_{34}A_{34} \oplus E_{34}D_{34}\oplus E_{34})^{\gg 7} + F_{34}^{\gg 11} + X_{26} + 0xbe5466cf$$

이므로,

$$F_{35} = X_{26} + 0xbe5466cf$$

를 얻을 수 있다. 또한, 단계 36에서

$$E_{36} = (A_{35}C_{35}F_{35}\oplus C_{35}G_{35}H_{35}\oplus A_{35}C_{35} \oplus A_{35}G_{35}\oplus C_{35}B_{35}\oplus F_{35}H_{35}\oplus G_{35}H_{35} \oplus D_{35}C_{35}\oplus D_{35})^{\gg 7} + E_{35}^{\gg 11} + X_{18} + 0x34e90c6c,$$

이므로,

$$X_{18} = -(F_{35}^{\gg 7} + 0x34e90c6c)$$

임을 알 수 있다. 그러므로, 다음을 얻는다.

$$X_{26} = -0xbe5466cf + (-0x34e90c6c - X_{18})^{\gg 25}$$

그리고, 단계 27로부터 $X_{26} = -(C_{22}^{\gg 7} + F_{19}^{\gg 11})$ 이므로, X_{18}에 대한 다음 조건을 얻을 수 있다.

$$-(C_{22}^{\gg 7} + F_{19}^{\gg 11}) = -0xb5466cf + (-0x34e90c6c - X_{19})^{\gg 25}$$

위 방정식을 해결하기 위하여, X_{18}을 임의의 값으로

놓고 C_{22}를 계산한다.

$$C_{22}=(F_{19}^{\gg 11}+0xbe5466cf - (-0x34e90c6c-X_{18})^{\gg 25})^{\gg 25}$$

단계 22로부터,

$$C_{22}=(F_{21}G_{21}\oplus B_{21}D_{21}\oplus A_{21}E_{21}\oplus H_{21}F_{21}\oplus H_{21})^{\gg 7} + C_{21}^{\gg 11}+X_{21}$$

이므로, X_{21}에 대한 다음 방정식을 얻는다.

$$X_{21}=(F_{19}^{\gg 11}+0xbe5466cf-(-0x34e90c6c - X_{18})^{\gg 25})^{\gg 25}-(F_{21}G_{21}\oplus B_{21}D_{21} \oplus A_{21}E_{21}\oplus H_{21}F_{21}\oplus H_{21})^{\gg 7}+C_{21}^{\gg 11}.$$

결과적으로 우리는 충돌쌍에 대한 다음 조건을 얻게 된다.

$$X_5=0xffffffff-0x452821e6$$
$$X_{14}=0xffffffff-0x38d01377$$
$$X_{21}=(F_{19}^{\gg 11}+0xbe5466cf-(-0x34e90c6c - X_{18})^{\gg 25})^{\gg 25}-(F_{21}G_{21}\oplus B_{21}D_{21} \oplus A_{21}E_{21}\oplus H_{21}F_{21}\oplus H_{21})^{\gg 7}+C_{21}^{\gg 11}.$$

$X_i(22\le i\le 31)$는 단계 함수로부터 결정되며, $X_j(j\neq 5,14,21\le i\le 31)$는 임의의 값을 가질 수 있다. 따라서, HAVAL-12에 대한 많은 충돌쌍이 존재한다. [표 5]에 충돌쌍 중에 한 개을 제시하며, [표 5]의 충돌쌍은 다음을 해쉬값으로 가진다.

0xa273fd7f, 0x483d4aa4, 0xab5eafc5, 0x2e8b8ef9, 0xe1d63dc2, 0xa2c51648, 0xdbf75650, 0x13548df.

HAVAL-12에서 메시지 워드 X_{26}은 단계 26과 단계 34에서 입력되며, 두 단계의 차이는 8이다. 따라서, X_{26}과 $\widehat{X_{26}}$을 이용한 HAVAL-12 공격을 고려할 수 있다. 그러나, X_{26}과 $\widehat{X_{26}}$을 이용해서는 HAVAL-12의 충돌쌍을 찾을 수 없다. 지금부터, 다음 메시지 블록 X와 $\widehat{X}$를 고려하면, HAVAL-12의 충돌쌍을 찾을 수 없음을 보인다.

$$X_{26}\neq \widehat{X_{26}},\quad X_i=\widehat{X_i}(i\neq 26).$$

[표 5] HAVAL-12의 충돌쌍 (X, $\widehat{X}$)

$X_0(\widehat{X_0})$	0	$X_{16}(\widehat{X_{16}})$	0
$X_1(\widehat{X_1})$	0	$X_{17}(\widehat{X_{17}})$	0
$X_2(\widehat{X_2})$	0	$X_{18}(\widehat{X_{18}})$	0
$X_3(\widehat{X_3})$	0	$X_{19}(\widehat{X_{18}})$	0
$X_4(\widehat{X_4})$	0	$X_{20}(\widehat{X_{20}})$	0
$X_5(\widehat{X_5})$	0xbad7de19	$X_{21}(\widehat{X_{21}})$	0xeccfd659
$X_6(\widehat{X_6})$	0	$X_{22}(\widehat{X_{22}})$	0xb593ece4
$X_7(\widehat{X_7})$	0	$X_{23}(\widehat{X_{23}})$	0x2d8e2ef4
$X_8(\widehat{X_8})$	0	$X_{24}(\widehat{X_{24}})$	0xcd6f4a4a
$X_9(\widehat{X_9})$	0	$X_{25}(\widehat{X_{25}})$	0x4a45d2f3
$X_{10}(\widehat{X_{10}})$	0	$X_{26}(\widehat{X_{26}})$	0xcd256396
$X_{11}(\widehat{X_{11}})$	0	$X_{27}(\widehat{X_{27}})$	0xb9107999
$X_{12}(\widehat{X_{12}})$	0	$X_{28}(\widehat{X_{28}})$	0x260791c2 (0x260791c3)
$X_{13}(\widehat{X_{13}})$	0	$X_{29}(\widehat{X_{29}})$	0x92102afd
$X_{14}(\widehat{X_{14}})$	0xc72fec88	$X_{30}(\widehat{X_{30}})$	0xf0000000
$X_{15}(\widehat{X_{15}})$	0	$X_{31}(\widehat{X_{31}})$	0

HAVAL-12에서 메시지 워드 X_{26}은 단계 26과 단계 34에서 입력되며, 두 단계의 차이는 8이다. HAVAL-23에 적용한 공격과 유사한 방법으로 단계 26부터 단계 34를 분석하면 충돌쌍을 찾기 위한 다음의 방정식을 구할 수 있다.

$$F_{27}-\widehat{F_{27}}=X_{26}-\widehat{X_{26}} \quad (29)$$

$$(F_{27}\oplus\widehat{F_{27}})D_{21}=0 \quad (30)$$

$$(F_{27}\oplus\widehat{F_{27}})B_{23}=0 \quad (31)$$

$$(F_{27}\oplus\widehat{F_{27}})(G_{26}\oplus H_{25})=0 \quad (32)$$

$$(F_{27}\oplus\widehat{F_{27}})E_{28}=0 \quad (33)$$

$$(F_{27}\oplus\widehat{F_{27}})(E_{28}\oplus 0xffffffff)=0 \quad (34)$$

$$(F_{27}\oplus\widehat{F_{27}})(D_{29}A_{32}\oplus B_{31}C_{30}\oplus C_{29}\oplus E_{28}\oplus G_{26})=0 \quad (35)$$

$$(F_{27}\oplus\widehat{F_{27}})(E_{28}\oplus 0xffffffff)=0 \quad (36)$$

$$F_{27}^{\gg 11}-\widehat{F_{27}^{\gg 11}}=-(X_{26}-\widehat{X_{26}}) \quad (37)$$

식 (29)부터 식 (37)을 만족하는 해를 찾아보자. $X_{26} \neq \widehat{X_{26}}$이므로 식 (10)에서 $F_{27} - \widehat{F_{27}}$임을 알 수 있다. 그리고, $F_{27} \oplus \widehat{F_{27}} \neq 0$이므로, 적당한 k에 대해 k번째 성분이 '1'인 것이 존재한다. 즉, $(F_{27} \oplus \widehat{F_{27}})(k)$를 $F_{27} \oplus \widehat{F_{27}}$의 k번째 성분이라고 하면, $(F_{27} \oplus \widehat{F_{27}})(k) = 1$인 k가 존재한다. 식 (33)으로부터 $E_{28}(k) = 0$이다. 그런데, 식 (36)으로부터 $E_{28}(k) = 0$이 되어 모순이 발생한다. 따라서, 식 (29)부터 식 (37)을 만족하는 해는 존재하지 않으며, 결과적으로 X_{26}과 $\widehat{X_{26}}$을 이용한 HAVAL-12의 충돌쌍을 찾을 수 없다.

Ⅳ. HAVAL-23에 대한 공격 방법

Kasselman과 Penzhorn 이미 HAVAL-23의 충돌쌍을 찾는 공격 방법을 제안한 바 있다.[13] 본 절에서는 Kasselman과 Penzhorn의 방법(KP 공격)과 유사한 방법으로 HAVAL-23의 충돌쌍을 찾고자 한다.

HAVAL-23의 충돌쌍을 찾는 다는 것은 단계 96이후에 다음을 만족하는 두 개의 서로 다른 메시지 블록 X와 $\widehat{X}$를 찾는 것이다.

$$A_{96} = \widehat{A_{96}},\ B_{96} = \widehat{B_{96}},\ C_{96} = \widehat{C_{96}},\ D_{96} = \widehat{D_{96}},$$
$$E_{96} = \widehat{E_{96}},\ F_{96} = \widehat{F_{96}},\ G_{96} = \widehat{G_{96}},\ H_{96} = \widehat{H_{96}}.$$

충돌쌍을 찾기 위하여 다음을 만족하는 메시지 블록 X와 $\widehat{X}$를 고려한다.

$$X_{19} \neq \widehat{X_{19}}, \quad X_i = \widehat{X_i} (i \neq 19).$$

HAVAL-23에서 메시지 워드 X_{19}은 단계 57과 단계 65에서 입력되며, 두 단계의 차이는 8이다. [표 6]은 단계 57부터 단계 65에서 적용되는 연결 변수와 메시지 워드를 나타낸다. 음영 있는 네모안에 있는 연결 변수는 각 단계에서 update되는 연결 변수를 표시한다.

$(X, \widehat{X})$가 HAVAL-23의 충돌쌍이 되기 위해서는 다음을 만족하여야 한다.

$$A_{65} = \widehat{A_{65}},\ B_{65} = \widehat{B_{65}},\ C_{65} = \widehat{C_{65}},\ D_{65} = \widehat{D_{65}},$$
$$E_{65} = \widehat{E_{65}},\ F_{65} = \widehat{F_{65}},\ G_{65} = \widehat{G_{65}},\ H_{65} = \widehat{H_{65}}.$$

[표 6] 단계 57~단계 65의 연결 변수

단계	연결 변수								메시지 워드
57	A_{57}	B_{57}	C_{57}	D_{57}	E_{57}	F_{57}	G_{57}	H_{57}	X_{19}
58	A_{58}	B_{58}	C_{58}	D_{58}	E_{58}	F_{58}	G_{58}	H_{58}	X_{12}
59	A_{59}	B_{59}	C_{59}	D_{59}	E_{59}	F_{59}	G_{59}	H_{59}	X_{15}
60	A_{60}	B_{60}	C_{60}	D_{60}	E_{60}	F_{60}	G_{60}	H_{60}	X_{13}
61	A_{61}	B_{61}	C_{61}	D_{61}	E_{61}	F_{61}	G_{61}	H_{61}	X_2
62	A_{62}	B_{62}	C_{62}	D_{62}	E_{62}	F_{62}	G_{62}	H_{62}	X_{25}
63	A_{63}	B_{63}	C_{63}	D_{63}	E_{63}	F_{63}	G_{63}	H_{63}	X_{31}
64	A_{64}	B_{64}	C_{64}	D_{64}	E_{64}	F_{64}	G_{64}	H_{64}	X_{27}
65	A_{65}	B_{65}	C_{65}	D_{65}	E_{65}	F_{65}	G_{65}	H_{65}	X_{19}

그런데,

$\Delta A_{65} = \Delta A_{64}$, $\Delta B_{65} = \Delta B_{63}$, $\Delta C_{65} = \Delta C_{62}$, $\Delta D_{65} = \Delta D_{61}$, $\Delta E_{65} = \Delta E_{60}$, $\Delta F_{65} = \Delta F_{59}$, $\Delta G_{65} = \Delta G_{58}$,

이므로, $(X, \widehat{X})$이 HAVAL-23의 충돌쌍이 되는 조건을 다음으로 수립할 수 있다.

$$\Delta A_{64} = 0,\ \Delta B_{63} = 0,\ \Delta C_{62} = 0,\ \Delta D_{61} = 0,$$
$$\Delta E_{60} = 0,\ \Delta F_{59} = 0,\ \Delta G_{58} = 0,\ \Delta H_{65} = 0.$$

단계 57부터 단계 65를 분석하여 다음의 9개 방정식을 수립할 수 있다.

$$H_{57} - \widehat{H_{57}} = X_{19} - \widehat{X_{19}} \tag{16}$$

$$(H_{57} \oplus \widehat{H_{57}})(C_{54} E_{52} \oplus B_{55}) = 0 \tag{17}$$

$$(H_{57} \oplus \widehat{H_{57}})(D_{53} A_{56} \oplus B_{55} \oplus A_{56}) = 0 \tag{18}$$

$$(H_{57} \oplus \widehat{H_{57}})(C_{54} G_{58} \oplus F_{59} \oplus G_{58}) = 0 \tag{19}$$

$$(H_{57} \oplus \widehat{H_{57}})(B_{55} E_{60} \oplus B_{55} \oplus F_{59}) = 0 \tag{20}$$

$$(H_{57} \oplus \widehat{H_{57}}) A_{56} = 0 \tag{21}$$

$$(H_{57} \oplus \widehat{H_{57}})(F_{59} C_{62} \oplus D_{61} E_{60} \oplus F_{59} \oplus G_{38} \oplus A_{56}) = 0 \tag{22}$$

$$(H_{57} \oplus \widehat{H_{57}})(G_{58} \oplus 0xffffffff) = 0 \tag{23}$$

$$H_{57}^{\gg 11} - \widehat{H_{57}}^{\gg 11} = -(X_{19} - \widehat{X_{19}}) \quad (24)$$

가장 먼저, H_{57}과 $\widehat{H_{57}}$의 값을 결정한다. 식 (16)으로부터, 다음 식을 얻을 수 있다.

$$H_{57}^{\gg 11} - \widehat{H_{57}}^{\gg 11} + H_{57} - \widehat{H_{57}} = 0. \quad (25)$$

Eurocrypt'92에서 Berson은 n-비트 X와 Y와 주어지면, $(X-Y)^{\gg k} - (X^{\gg k} - Y^{\gg k})$의 값은 0, $2^{n-k}-1$, 2^{n-k}, 2^n-1 중에 하나임을 증명하였다.[14] 그러므로, 식 (25)의 해는 다음 식들의 해를 결정하는 방법으로 찾을 수 있다.

$$(H_{57} - \widehat{H_{57}})^{\gg 11} + (H_{57} - \widehat{H_{57}}) = 0 \quad (26)$$

$$(H_{57} - \widehat{H_{57}})^{\gg 11} + (H_{57} - \widehat{H_{57}}) = 2^{21} - 1 \quad (27)$$

$$(H_{57} - \widehat{H_{57}})^{\gg 11} + (H_{57} - \widehat{H_{57}}) = 2^{21} \quad (28)$$

$$(H_{57} - \widehat{H_{57}})^{\gg 11} + (H_{57} - \widehat{H_{57}}) = 2^{32} - 1 \quad (29)$$

$t = H_{57} - \widehat{H_{57}}$로 설정한다. 그러면, 식 (26)에 대해서는 $t=0$이며, 식 (28)에 대해서는 $t=0x5555555b$과 $t=0xaaaaaaab$이고, 식 (29)에 대해서는 $t=0x55555555$이고 $t=0xaaaaaaaa$이다. 그리고, 식 (27)에 대한 해는 존재하지 않는다. 그러므로, H_{57}과 $\widehat{H_{57}}$의 값을 결정하기 위해서는 $H_{57} - \widehat{H_{57}}$이 $0x55555555$, $0x5555555b$, $0xaaaaaaaa$, 그리고, $0xaaaaaaab$이 되는 H_{57}과 $\widehat{H_{57}}$을 찾고, 이들이 식 (25)를 만족하는지 여부를 확인하여야 한다.

$(H_{57} \oplus \widehat{H_{57}})(k)$를 $H_{57} \oplus \widehat{H_{57}}$의 k번째 비트라고 하자. $(H_{57} \oplus \widehat{H_{57}})(k) = 1$이면, 식 (17)부터 식 (25)로부터 다음을 얻는다.

$$C_{54}(k)E_{52}(k) \oplus B_{55}(k) = 0$$
$$D_{53}(k)A_{56}(k) \oplus B_{55}(k) \oplus A_{56}(k) = 0$$
$$C_{54}(k)G_{58}(k) \oplus F_{59}(k) \oplus G_{58}(k) = 0$$
$$B_{55}(k)E_{60}(k) \oplus B_{55}(k) \oplus F_{59}(k) = 0$$
$$A_{56}(k) = 0$$
$$F_{59}(k)C_{62}(k) \oplus D_{61}(k)E_{60}(k) \oplus F_{59}(k) \oplus G_{38}(k) \oplus A_{56}(k) = 0$$
$$G_{58}(k) \oplus 1 = 0$$

상기 식들의 해는 다음과 같다.

$$E_{52}(k) = 0,\ C_{54}(k) = 1,\ B_{55}(k) = 0,$$
$$A_{56}(k) = 0,\ G_{58}(k) = 1,\ F_{59}(k) = 0,$$
$$E_{60}(k) = 1,\ D_{61}(k) = 1.$$

그리고, $D_{53}(k)$와 $C_{62}(k)$는 임의의 값을 가질 수 있다. 식 (16)부터 식 (24)의 해는 다음과 같다. $S = H_{57} \oplus \widehat{H_{57}}$이고 R은 32-비트 랜덤수이다.

$$E_{52} = (\sim S)R,\ G_{58} = S \vee R,$$
$$D_{53} = \text{임의의 값},\ F_{59} = (\sim S)R,$$
$$C_{54} = S \vee R,\ E_{60} = S \vee R,$$
$$B_{55} = (\sim S)R,\ D_{61} = S \vee R,$$
$$A_{56} = (\sim S)R,\ C_{62} = \text{임의의값}$$

이제 HAVAL-23의 충돌쌍 $(X, \widehat{X})$을 결정하는 알고리즘을 제안한다.

〔단계 1〕 $i \neq 2, 6, 9, 12, 13, 15, 19, 24, 29$에 대한 X_i의 값을 임의의 값으로 설정한다.

〔단계 2〕 X_9를 다음으로 결정한다.

$$X_9 = E_{52} - (A_{51}C_{51}F_{51} \oplus C_{51}G_{51}H_{51} \oplus A_{51}C_{51} \oplus A_{51}G_{51} \oplus C_{51}B_{51} \oplus F_{51}H_{51} \oplus G_{51}H_{51} \oplus D_{51}C_{51} \oplus D_{51})^{\gg 7} - E_{51}^{\gg 11} - 0x83916cf1$$

〔단계 3〕 D_{53}을 다음으로 설정한다.

$$D_{53} = (H_{52}B_{52}E_{52} \oplus B_{52}F_{52}G_{52} \oplus H_{52}B_{52} \oplus H_{52}F_{52} \oplus B_{52}A_{52} \oplus E_{52}G_{52} \oplus F_{52}G_{52} \oplus C_{52}B_{52} \oplus C_{52})^{\gg 7} + D_{52}^{\gg 11} + X_{17} + 0x0801f2e2$$

〔단계 4〕 X_{24}, X_{29}, X_6을 계산한다.

$$X_{24} = C_{54} - (G_{53}A_{53}D_{53} \oplus A_{53}E_{53}F_{53} \oplus G_{53}A_{53} \oplus G_{53}E_{53} \oplus A_{53}H_{53} \oplus D_{53}F_{53} \oplus E_{53}F_{53} \oplus B_{53}A_{53} \oplus B_{53})^{\gg 7} - C_{53}^{\gg 11} - 0x858efc16$$

$$X_{29} = B_{55} - (F_{54}H_{54}C_{54} \oplus H_{54}D_{54}E_{54} \oplus F_{54}H_{54} \oplus F_{54}D_{54} \oplus H_{54}G_{54} \oplus C_{54}E_{54} \oplus D_{54}E_{54} \oplus A_{54}H_{54} \oplus A_{54})^{\gg 7} - B_{54}^{\gg 11} - 0x636920d8$$

$$X_6 = A_{56} - (E_{55}G_{55}B_{55} \oplus G_{55}C_{55}D_{55} \oplus E_{55}G_{55} \oplus E_{55}C_{55} \oplus G_{55}F_{55} \oplus B_{55}D_{55} \oplus C_{55}D_{55} \oplus H_{55}G_{55} \oplus H_{55})^{\gg 7} - A_{55}^{\gg 11} - 0x71574e69$$

〔단계 5〕 X_{19}와 $\overline{X}_{19}$를 계산한다.

$$X_{19} = H_{57} - (D_{56}F_{56}A_{56} \oplus F_{56}B_{56}C_{56} \oplus D_{56}F_{56} \oplus D_{56}B_{56} \oplus F_{56}E_{56} \oplus A_{56}C_{56} \oplus B_{56}C_{56} \oplus G_{56}F_{56} \oplus G_{56})^{\gg 7} - H_{56}^{\gg 11} - 0xa458fea3$$

$$\overline{X}_{19} = \overline{H}_{57} - (D_{56}F_{56}A_{56} \oplus F_{56}B_{56}C_{56} \oplus D_{56}F_{56} \oplus D_{56}B_{56} \oplus F_{56}E_{56} \oplus A_{56}C_{56} \oplus B_{56}C_{56} \oplus G_{56}F_{56} \oplus G_{56})^{\gg 7} - H_{56}^{\gg 11} - 0xa458fea3$$

〔단계 6〕 유사한 방법으로 $X_{12}, X_{15}, X_{13}, X_2$을 결정한다.

$H_{57} = 0xaaaab004$, $\overline{H}_{57} = 0x0000055a$, 그리고, $S = H_{57} \oplus \overline{H}_{57} = 0xaaaaab55e$로 설정한다. 〔표 7〕은 다음을 해쉬값으로 가지는 HAVAL-23의 충돌쌍이다.

0xa3ad3176, 0x40e4b13c, 0x374e6bde, 0xcda35c41, 0x83b2496d, 0xb4931a23, 0xa08a1d28, 0x5b8ef68c.

〔표 7〕 HAVAL-23의 충돌쌍 (X, $\overline{X}$)

$X_0(\overline{X}_0)$	0	$X_{16}(\overline{X}_{16})$	0
$X_1(\overline{X}_1)$	0	$X_{17}(\overline{X}_{17})$	0
$X_2(\overline{X}_2)$	0xd58a764	$X_{18}(\overline{X}_{18})$	0
$X_3(\overline{X}_3)$	0	$X_{19}(\overline{X}_{19})$	0xe65c265f (0x3bb17bb5)
$X_4(\overline{X}_4)$	0	$X_{20}(\overline{X}_{20})$	0
$X_5(\overline{X}_5)$	0	$X_{21}(\overline{X}_{21})$	0
$X_6(\overline{X}_6)$	0xa7891c3e	$X_{22}(\overline{X}_{22})$	0
$X_7(\overline{X}_7)$	0	$X_{23}(\overline{X}_{23})$	0
$X_8(\overline{X}_8)$	0	$X_{24}(\overline{X}_{24})$	0x73e6fac2
$X_9(\overline{X}_9)$	0xb38682c	$X_{25}(\overline{X}_{25})$	0
$X_{10}(\overline{X}_{10})$	0	$X_{26}(\overline{X}_{26})$	0
$X_{11}(\overline{X}_{11})$	0	$X_{27}(\overline{X}_{27})$	0
$X_{12}(\overline{X}_{12})$	0x4dcf6368	$X_{28}(\overline{X}_{28})$	0
$X_{13}(\overline{X}_{13})$	0xe34933c9	$X_{29}(\overline{X}_{29})$	0x6ea73074
$X_{14}(\overline{X}_{14})$	0	$X_{30}(\overline{X}_{30})$	0
$X_{15}(\overline{X}_{15})$	0x9a31cbb	$X_{31}(\overline{X}_{31})$	0

V. 결 론

본 논문에서는 3-pass HAVAL의 축소 라운드의 안전성을 분석하였다. 3-pass HAVAL의 처음 두 라운드인 HAVAL-12와 마지막 두 라운드인 HAVAL-23 각각에 대해서, 충돌쌍이 존재하는 조건을 수립하고, 조건을 만족하는 식을 분석하여, 결과적으로 충돌쌍을 결정할 수 있었다. 본 논문에서 제안하는 공격 방법이 3-pass HAVAL의 전체 라운드에 대한 것이 아니나, 3-pass HAVAL은 암호적으로 취약함을 가지고 있는 것으로 판단할 수 있다.

참 고 문 헌

〔1〕 Ronald L. Rivest, "The MD4 message digest algorithm", In Alfred J. Menezes and Scott~A. Vanstone, editors, *Advances in Cryptology ~ Crypto'90*, Volume 537 of *Lecture Notes in Computer Science*, pp. 303~311. Springer-Verlag, 1991.

〔2〕 Ronald L. Rivest, "The MD5 message digest algorithm", In Request for Comments (RFC) 1321, April. Internet Activities Board, Internet Privacy Task Force, 1992.

〔3〕 Yuliang Zheng, Josef Pieprzyk, and Jennifer Seberry. "HAVAL-A One-Way Hashing Algorithm with Variable Length of Output", In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology ~ Auscrypt'92, volume 718 of Lecture Notes in Computer Science*, pp. 83~104. Springer, 1992.

〔4〕 Research and Development in Advanced Communications Technologies in Europe, "RIPE: Integrity primitives for secure information systems", Final Report of RACE Integrity Primitives Evaluation (R1040), RACE, 1995.

〔5〕 Hans Dobbertin, Antoon Bosselaers, and Bart Preneel, "RIPEMD-160: A strengthened version of RIPEMD", *ftp.esat.kuleuven.ac.be/pub/COSIC/bossselae/ripemd*, April 1996.

〔6〕 National Institute of Standards and

Technology, "FIPS PUB 180-1: Secure Hash Standard", April 1995.

[7] Bert den Boer and Antoon Bosselaers. "An attack on the last two rounds of MD4", In Joan Feigenbaum, editor, *Advances in Cryptology - Crypto'91*, Volume 576 of *Lecture Notes in Computer Science*, pp. 194~203. Springer-Verlag, Berlin, 1992.

[8] Serge Vaudenay. "On the need for multi-permutations: Cryptanalysis of MD4 and SAFER", In Bart Preneel, editor, *Fast Software Encryption, Second International Workshop*, Volume 1008 of *Lecture Notes in Computer Science*, pp. 286~297, Leuven, Belgium, December 1995. Springer-Verlag, Berlin.

[9] Hans Dobbertin. "Cryptanalysis of MD4", Journal of Cryptology, Volume 11, number 4, pp. 253~271, 1998.

[10] Hans Dobbertin, "RIPEMD with two rounds compress function is not collision-free", *Journal of Cryptology*, Volume 10, number 1, pp. 51~69, 1997.

[11] Christophe Debaert and Henri Gilbert, "The RIPEMD^{L} and RIPEMD^{R} improved variants of MD4 are not collision free", In *Preproceegins of FSE* 2001, 8th Fast Software Encryption Workshop, pp. 54~69, Yokohama, Japan, April 2001.

[12] Bert den Boer and Antoon Bosselaers. "Collisions for the compression function of MD5", In Tor Helleseth, editor, *Advances in Cryptology - Eurocrypt'93*, Volume 765 of *Lecture Notes in Computer Science*, pp. 293~304. Springer-Verlag, Berlin, 1993.

[13] P.R. Kasselman and W.T. Penzhorn. "Cryptanalysis of reduced version of HAVAL", *Electronics Letters*, Volume 36, number 1, pp. 30~31, January 2000.

[14] Thomas A. Berson, "Differential cryptanalysis mod 2^{32} with applications to MD5", In Rainer A. Rueppel, editor, *Advances in Cryptology - Eurocrypt'92*, Volume 658 of *Lecture Notes in Computer Science*, pp. 71~80. Springer-Verlag, Berlin, 1992.

〈著者紹介〉

박 상 우(Sangwoo Park) 정회원
1989년 2월 : 고려대학교 수학교육과 졸업
1991년 8월 : 고려대학교 수학과 석사
1991년 8월~1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월~현재 : 국가보안기술연구소 선임연구원

성 수 학(Soo Hak Sung) 정회원
1982년 2월 : 경북대학교 수학과(학사)
1985년 2월 : KAIST 응용수학과(석사)
1988년 2월 : KAIST 응용수학과(박사)
1988년~1991년 : 한국전자통신연구원 선임연구원
1991년~현재 : 배재대학교 전산정보수학과 교수

지 성 택(Seongtaek Chee) 정회원
1985년 2월 : 서강대학교 수학과 졸업
1987년 2월 : 서강대학교 수학과 석사
1999년 2월 : 고려대학교 수학과 박사
1989년~1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월~현재 : 국가보안기술연구소 책임연구원

윤 이 중(E-Joong Yoon) 정회원
1990년 2월 : 인하대학교 전사과 석사
2002년 2월 : 충남대학교 컴퓨터과학과 박사
1990년 2월~2001년 2월 : 한국전자통신연구원 정보보호시스템연구부장
2001년 2월~현재 : 국가보안기술연구소 기반기술연구부장

임 종 인(Jong-In Lim) 정회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사(대수학 전공)
1986년 2월 : 고려대학교 수학과 박사(대수학 전공)
1986년 2월~현재 : 고려대학교 수학과 정교수
2000년 10월~현재 : 고려대학교 정보보호 대학원 원장
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계, 암호프로토콜, 공개키 암호 알고리즘의 분석