九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Analysis of Security via Attacks on Reduced Versions of HAVAL

許, 容碩
九州大学大学院システム情報科学府

櫻井, 幸一
九州大学大学院システム情報科学研究院

http://hdl.handle.net/2324/6026

出版情報：Proc. of the 2003 Symposium on Cryptography and Information Security. 1, pp.551-556, 2003-01. 2003 Symposium on Cryptography and Information Security
バージョン：
権利関係：

KYUSHU UNIVERSITY

HAVAL 簡約版の衝突を通した安全性の分析
Analysis of Security via Attacks on Reduced Versions of HAVAL

許 容碩 *　　櫻井 幸一†
Yong-Sork HER　　Kouichi SAKURAI

あらまし HAVAL は Zheng らにより提案されたハッシュ関数であり, 128, 160, 192, 224 ビットといった可変長の出力が可能なハッシュ関数として, 3-pass, 4-pass, 5-pass で構成される．これらは段階の数, 置換の順序, ブール関数などが異なる．P.R.Kasselman や Park らは 3-pass の中の連続した 2-pass を利用することにより, 3-pass HAVAL の衝突を発見した．本論文では, HAVAL の安全性を検証するために, 3-pass の中の連続でない 2 つ (1-pass, 3-pass), また, 4-pass の中で連続した 2-pass を利用して HAVAL の衝突を発見することを試みた．これらの結果を通して HAVAL の安全性を分析する．この分析を通して, 置換の順序やブール関数が HAVAL の安全性に及ぼす影響について評価した．このために Park らの攻撃手法を導入した．

キーワード HAVAL, 暗号学的ハッシュ関数, 暗号化

1 はじめに

1.1 動機

暗号学的ハッシュ関数は出力の長さによって 2 つに分類される．出力の長さが固定されたハッシュ関数として, MD4, MD5, SHA-1 などが挙げられる．一方で, 出力の長さが可変であるようなハッシュ関数の 1 つに HAVAL が挙げられる [2, 4]．MD4 系列専用のハッシュ関数である HAVAL は Zheng らにより提案された [2]．HAVAL は 128, 160, 192, 224, 256 ビットと出力の長さが可変である初めてのハッシュ関数である [1, 5]．このハッシュ関数は 3-pass, 4-pass, 5-pass で構成される．HAVAL の 1 つの pass はブール関数を持ち, 32 個の定数 (最初の pass だけは定数は持たない), 1 つの置換を持つ．HAVAL の利点は, 3-pass, 4-pass, 5-pass によって 5 種類の長さの出力を生成することができることである．よって, HAVAL は 15 種類のの出力を表すことができる [5]．Kasselman らは 3-pass HAVAL の最後の連続する 2 つの pass の衝突を発見した [3]．また, Park らは pass HAVAL の最後の連続する 2 つの pass と最初の連続する 2 つの pass の衝突を発見した [4]．我々は, HAVAL を正確に解析するために 4-pass, 5-pass HAVAL の攻撃結果も必要であると考えている．本論文では, 3-pass HAVAL における連続でない 2 つの pass と 4-pass HAVAL における連続した 2 つの pass において衝突についての解析を行う．3-pass, 4-pass HAVAL の違いは段階の数, 置換の順序, そしてブール関数である．3-pass HAVAL の中から ⟨1,3⟩ を選び, 連続でない 2 つの pass という条件のもとで衝突があるかについて解析を行った．置換の順序, ブール関数が HAVAL の安全性と関係を把握するために 4-pass HAVAL を選んである．

1.2 関連研究

本論文において, 3-pass HAVAL の 1 番目と 3 番目の pass (⟨1,3⟩ と記述する．) について衝突の解析を行う．また, 4-pass HAVAL の削減された 2 つの pass の衝突を見つけるために連続する 2 つの pass ⟨1,2⟩, ⟨2,3⟩, ⟨3,4⟩ について, HAVAL の欠点を基にした Park らによる攻撃手法に似た方法によって衝突の解析を行う [4]．⟨ ⟩ は HAVAL を攻撃する際に用いる pass を意味している．例えば 3-pass HAVAL における ⟨1,2⟩ は 3 番目の pass を利用しないことを意味している．3-pass, 4-pass HAVAL の相違点は置換の順序や pass の数を含めたブール関数の数などがある．Park らの攻撃手法と我々の攻撃手法の相違点は, 用いられる方程式や変数などである [5]．削減された 2-pass HAVAL の衝突の解析のためには, 2 つのにおけるメッセージワードが同じかどうかを検証する必要がある．例えば, 3-pass HAVAL における ⟨1,2⟩ の攻撃において最初の pass は段階 29 において X_{28} を取る．

* 九州大学大学院システム情報科学府 〒 812-8581 福岡市東区箱崎 6-10-1, Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan
† 九州大学大学院システム情報科学研究院 〒 812-8581 福岡市東区箱崎 6-10-1, Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan

また, メッセージワード X_{28} の間隔は 10 段階で, 10 個の方程式を導くことができる．しかし, 4-pass HAVAL の ⟨3,4⟩ での攻撃では, 同じメッセージワード X_{23} の間隔が 12 段階であり, 12 個の方程式を得る．これは, 12 個の方程式は ⟨1,2⟩ の攻撃よりも複雑なものであることを意味している．また, 3-pass HAVAL の ⟨1,2⟩ での方程式は 64 回の排他論理演算を使用するが, 4-pass HAVAL の ⟨3,4⟩ での 12 個の方程式は 108 回の排他論理演算が必要となる．この原因は,HAVAL のブール関数によるものである．5 個のブール関数の間では, 4 番目のブール関数がブール関数の演算の観点から見て最も複雑なものである．よって, HAVAL の欠点を見つけるために 4-pass HAVAL の攻撃を行い, 3-pass HAVAL の攻撃との比較を行う.

1.3 研究の成果

我々は, 4-pass HAVAL の ⟨1,2⟩, ⟨2,3⟩, ⟨3,4⟩ と 3-pass HAVAL の ⟨1,3⟩ の衝突についての解析を行う． Park らは 3-pass HAVAL ⟨1,2⟩, ⟨2,3⟩ において衝突を発見している．本論文では 4-pass HAVAL の衝突を発見し, 3-pass HAVAL と 4-pass HAVAL に対する攻撃法の比較より HAVAL の欠点の解析を行う．今回の研究の大きな成果は 2 つである．1 つ目は 3-pass HAVAL の ⟨1,3⟩ への攻撃に成功したことである．前述の Kasselman, Park の攻撃方法では, 3-pass HAVAL において連続する 2 つの pass を利用していたが [3, 5], 我々は 3-pass HAVAL の連続ではない ⟨1,3⟩ への攻撃を行った．2 つ目は, 4-pass HAVAL の攻撃結果より HAVAL の欠点の解析を行ったことである．HAVAL の pass の削減における共通点は, 次の段階での変数の変化を基にして導出された方程式である．HAVAL には 3-pass, 4-pass, 5-pass により構成される 3 種類がある．各々の HAVAL の違いは置換の順序とブール関数の数である．我々は 4-pass HAVAL の衝突を発見することで HAVAL の攻撃に影響を与える要素を見つけることができた．もし 4-pass HAVAL に衝突が発見されたら 4 番目のブール関数が安全でないということも分かった．結論を言うと, 置換の順序は HAVAL の攻撃に影響を与えるものである．特に, 3-pass HAVAL の ⟨2,3⟩ と 4-pass HAVAL の ⟨2,3⟩ とを比較した時に衝突の数に違いが見られることが分かった．この結果は置換の順序によるものである．また, 3-pass HAVAL の ⟨1,2⟩ と 4-pass HAVAL の ⟨1,2⟩ の場合は衝突の数が同じになった．ブール関数の場合は, 3-pass HAVAL では 3 つのブール関数が用いられ 4-pass HAVAL ではそれに 1 つのブール関数が加えられる．ブール関数は HAVAL の安全性を維持するための重要な要素であるが, 4-pass HAVAL において衝突を発見することができた．HAVAL の安全性の検証の公正性, 効率性を向上させるために 3 つの種類の 4-pass HAVAL の攻撃を行った．その結果から, 4-pass HAVAL の ⟨1,2⟩ ⟨2,3⟩ ⟨3,4⟩ での衝突を見つけることで 5-pass HAVAL への攻撃の可能性を示すことができる．HAVAL では, 8 個の変数の中で唯 1 つだけが次の段階において変化する．これは HAVAL の欠点である.

表 1: HAVAL に対する攻撃

	Penzhorm	Park ら	我々の攻撃
3-pass HAVAL	⟨2,3⟩	⟨1,2⟩,⟨2,3⟩	⟨1,3⟩
4-pass HAVAL			⟨1,3⟩, ⟨2,3⟩, ⟨3,4⟩

2 HAVAL の原理と HAVAL の既存の攻撃

本章では, HAVAL のアルゴリズムと既存の攻撃に対して簡単に説明する.

2.1 HAVAL の原理

このハッシュ関数は 3-pass, 4-pass, 5-pass で構成される [1].

■ 単位演算

HAVAL の単位演算について述べる．i 段での段関数の入力を $T_{i,j}(j = 0, 1, \ldots, 7)$ とする.

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

$R = P^{>>7} + t_{i,7}^{>>11} + W_{\mathrm{ord}_r(i)} + K_i,$

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

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

r は pass 番号, $\mathrm{ord}_r(i)$ はワードプロセッシング順序を示している．K_i は, 32 ビット定数とする．2-pass から 5-pass の定数 K_i は $(i = 0, \ldots, 31)$ は省略され, 定数は各段階で違う.

■ブール関数

3-pass HAVAL は, ブール関数 f_1, f_2, f_3 を用いる．同様に, 4-pass HAVAL はブール関数 f_1, f_2, f_3, f_4 を, 5-pass HAVAL は, ブール関数 $f_1, f_2, \ldots, f_5$ を用いる．置換の順序は各 HAVAL によって違う (表 2 参照)．すなわち, 3-pass HAVAL は, 置換の順序 $\phi_{3,1}$, $\phi_{3,2}$, $\phi_{3,3}$ を用いる．同様に, 4-pass HAVAL は置換の順序 $\phi_{4,1}$, $\phi_{4,2}$, $\phi_{4,3}$, $\phi_{4,4}$ を, 5-pass HAVAL は置換の順序 $\phi_{5,1}, \phi_{5,2}, \ldots, \phi_{5,5}$ を用いる.

■ 初期値

HAVAL では, 以下のように各々が 32 ビットである 8 個の初期値により構成される．初期値は 3-pass, 4-pass, 5-pass ともに同じである.

$A_0 = Oxec4e6c89$, $B_0 = Ox082efa98$,

$C_0 = Ox299f31d0$, $D_0 = OxA4093822$,

表 2: 置換の順序

置換の順序,	x_6	x_5	x_4	x_3	x_2	x_1	x_0
$\phi_{3,1}$	x_1	x_0	x_3	x_5	x_6	x_2	x_4
$\phi_{3,2}$	x_4	x_2	x_1	x_0	x_5	x_3	x_6
$\phi_{3,3}$	x_6	x_1	x_2	x_3	x_4	x_5	x_0
$\phi_{4,1}$	x_2	x_6	x_1	x_4	x_5	x_3	x_0
$\phi_{4,2}$	x_3	x_5	x_2	x_0	x_1	x_6	x_4
$\phi_{4,3}$	x_1	x_4	x_3	x_6	x_0	x_2	x_5
$\phi_{4,4}$	x_6	x_4	x_0	x_5	x_2	x_1	x_3
$\phi_{5,1}$	x_3	x_4	x_1	x_0	x_5	x_2	x_6
$\phi_{5,2}$	x_6	x_2	x_1	x_0	x_3	x_4	x_5
$\phi_{5,3}$	x_2	x_6	x_0	x_4	x_3	x_1	x_5
$\phi_{5,4}$	x_1	x_5	x_3	x_2	x_0	x_4	x_6
$\phi_{5,5}$	x_2	x_5	x_0	x_6	x_4	x_3	x_1

$E_0 = Ox03707344$, $F_0 = Ox13198a2e$,
$G_0 = Ox85a308d3$, $H_0 = Ox243f6a88$

2.2 HAVAL に対する既存の攻撃

HAVAL への攻撃は最初に Kasselman らにより試みられた．出力長が 256 ビットである 3-pass HAVAL の 2, 3-pass で衝突を発見した．また, Park らは 3-pass の中の 1, 2-pass と 2, 3-pass で衝突を発見した．彼らは差分方程式を導入し, それを解く事で内部の衝突を発見した．はじめに 2 つのメッセージ (X, $\bar{X}$) を選択する． $\bar{X}$ は X の代わりのメッセージである．そのとき, 彼らは以下の方程式のように k 段と l 段の間で内部の衝突を発見した [5].

$$f_k^l(X_k, f_{k-1}) = f_k^l(\bar{X}_k, f_{k-1})$$

衝突を発見するために, 彼らは同じメッセージを発見しようとした．各々の pass において同じメッセージが現れる間隔は 8 段である．8 個の変数の中で次の段で変化するのは 1 つだけなので変化した 1 つの変数は次の 8 段まで値が変わらない．よってメッセージの間隔が 8 段に近いようなメッセージを決定する．3-pass HAVAL の ⟨1,2⟩ の場合,X_{28} での間隔は 10 段であり, 3-pass HAVAL の ⟨2,3⟩, における pass1 と pass2 では 9 段である．

3 HAVAL に対する我々の攻撃

本論文では 4-pass HAVAL の ⟨1,2⟩, ⟨2,3⟩, ⟨3,4⟩ に対して攻撃を行う．また, 3-pass HAVAL の非連続し pass⟨1,3⟩ に対しても攻撃を行う．本章では数式が複雑な 4-pass の ⟨3,4⟩ を中心に説明する．他の攻撃については結果のみ付録で紹介する．

3.1 4-pass Haval の ⟨3,4⟩ に対する攻撃

4-pass HAVAL⟨3,4⟩ における衝突を発見するために, メッセージブロックを選択する．このメッセージブロックは 3 番目の pass の 93 段階と 4 番目の pass の 104 段階に利用する．この違いを以下のように定義する．

$$\Delta x = x - \bar{x} \mod 2^{32}$$

$A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i$ と $\bar{A}_i, \bar{B}_i, \bar{C}_i, \bar{D}_i, \bar{E}_i, \bar{F}_i, \bar{G}_i, \bar{H}_i$ は段 i での変数で, $X = (X_0, X_1, \ldots, X_{31})$ と $\bar{X} = (\bar{X}_0, \bar{X}_1, \ldots, \bar{X}_{31})$ はメッセージブロックである．

■ 目標
4-pass HAVAL の 3 番目の pass と 4 番目の pass における衝突を見つけるために, 異なる 2 つのメッセージ x と $\bar{x}$ を見つけなければならない．x と $\bar{x}$ は 93 段と 104 段の間で連鎖変数が同じでなければならない．例えば,
$A_{128} = \bar{A}_{128}, B_{128} = \bar{B}_{128}, C_{128} = \bar{C}_{128}, D_{128} = \bar{D}_{128}$
$E_{128} = \bar{E}_{128}, F_{128} = \bar{F}_{128}, G_{128} = \bar{G}_{128}, H_{128} = \bar{H}_{128}$
3-pass と 4-pass における衝突を発見するためには以下の式を満たす必要がある．

$$\begin{aligned} &A_{104} = \bar{A}_{104}, B_{104} = \bar{B}_{104}, C_{104} = \bar{C}_{104}, D_{104} = \bar{D}_{104} \\ &E_{104} = \bar{E}_{104}, F_{104} = \bar{F}_{104}, G_{104} = \bar{G}_{104}, H_{104} = \bar{H}_{104} \end{aligned} \tag{1}$$

■ 条件
数式 (1) から, 下の式が得られる．
$\triangle B_{104} = \triangle B_{103}, \triangle C_{104} = \triangle C_{102}, \triangle D_{104} = \triangle D_{101},$
$\triangle E_{104} = \triangle E_{100} \triangle F_{104} = \triangle F_{99}, \triangle G_{104} = \triangle G_{98}$
$\triangle A_{96} = 0, \triangle B_{103} = 0, \triangle C_{102} = 0, \triangle D_{101} = 0,$
$\triangle E_{104} = 0, \triangle F_{100} = 0, \triangle G_{99} = 0, \triangle H_{98} = 0$ 標準のメッセージワードは段 93 と段 104 で利用される．下の数式が得られる．

$$x_{23} \neq \bar{x}_{23},\ X_i \neq \bar{X}_i (i \neq 23)$$

93 段階において

$D_{93} = (G_{92}E_{92}C_{92} \oplus G_{92}H_{92} \oplus E_{92}A_{92} \oplus C_{92}F_{92} \oplus B_{92}C_{92} \oplus B_{92})^{>>7} + D_{92}^{>>11} + X_{23}$
$\bar{D}_{93} = (\bar{G}_{92}\bar{E}_{92}\bar{C}_{92} \oplus \bar{G}_{92}\bar{H}_{92} \oplus \bar{E}_{92}\bar{A}_{92} \oplus \bar{C}_{92}\bar{F}_{92} \oplus \bar{B}_{92}\bar{C}_{92} \oplus \bar{B}_{92})^{>>7} + \bar{D}_{92}^{>>11} + \bar{X}_{23}$
ゆえに
$A_{92} = \bar{A}_{92}, B_{92} = \bar{B}_{92}, C_{92} = \bar{C}_{92}, D_{92} = \bar{D}_{92}, E_{92} = \bar{E}_{92}, F_{92} = \bar{F}_{92}, G_{92} = \bar{G}_{92}, H_{92} = \bar{H}_{92}$
したっがて, 以下の方程式が成り立つ．
$\triangle D_{93} = \triangle X_{23} \neq 0$

94 段階において

$C_{94} = (F_{93}D_{93}B_{93} \oplus F_{93}G_{93} \oplus D_{93}H_{93} \oplus B_{93}E_{93} \oplus A_{93}B_{93} \oplus A_{93})^{>>7} + C_{93}^{>>11} + X_{11}$
$\bar{C}_{94} = (\bar{F}_{93}\bar{D}_{93}\bar{B}_{93} \oplus \bar{F}_{93}\bar{G}_{93} \oplus \bar{D}_{93}\bar{H}_{93} \oplus \bar{B}_{93}\bar{E}_{93} \oplus$

$\bar{A}_{93}\bar{B}_{93} \oplus \bar{A}_{93})^{>>7} + \bar{C}_{93}^{>>11} + \bar{X}_{11}$
$\triangle A_{93} = \triangle B_{93} = \triangle D_{93} = \triangle E_{93} = \triangle F_{93} = \triangle G_{93} = \triangle H_{93} = \triangle X_{93} = 0$ を, 上の方程式らから以下の方程式を導くことができる.

$\triangle C_{94} = 0$
$\Leftrightarrow F_{93}D_{93}B_{93} \oplus F_{93}G_{93} \oplus D_{93}H_{93} \oplus B_{93}E_{93} \oplus A_{93}B_{93} \oplus A_{93}$
$= \bar{F}_{93}\bar{D}_{93}\bar{B}_{93} \oplus \bar{F}_{93}\bar{G}_{93} \oplus \bar{D}_{93}\bar{H}_{93} \oplus \bar{B}_{93}\bar{E}_{93} \oplus \bar{A}_{93}\bar{B}_{93} \oplus \bar{A}_{93}$
$\Leftrightarrow F_{91}D_{93}B_{87} \oplus D_{93}H_{89} \oplus A_{88}B_{87} \oplus A_{88} = F_{91}\bar{D}_{93}B_{87} \oplus \bar{D}_{93}H_{89} \oplus \bar{A}_{88}B_{87} \oplus \bar{A}_{88}$
$\Leftrightarrow (F_{91}B_{87} \oplus H_{89})(D_{93} \oplus \bar{D}_{93}) = B_{87} \cdot (A_{88} \oplus \bar{A}_{88})$
同様に段階 95 から段階 104 までの方程式が得られる.

$$D_{93} - \bar{D}_{93} = X_{23} - \bar{X}_{23} \quad (2)$$
$$(F_{91}B_{87} \oplus H_{89})(D_{93} \oplus \bar{D}_{93}) = B_{87} \cdot (A_{88} \oplus \bar{A}_{88}) \quad (3)$$
$$(E_{92}C_{94} \oplus H_{89})(A_{88} \oplus \bar{A}_{88}) = A_{88}D_{93} \oplus \bar{A}_{88}\bar{D}_{93} \quad (4)$$
$$(B_{95}H_{89} \oplus E_{92})(D_{93} \oplus \bar{D}_{93}) = 0 \quad (5)$$
$$(C_{94}E_{92} \oplus F_{91}G_{90} \oplus B_{95} \oplus F_{91} \oplus E_{92} \oplus G_{90}) \quad (6)$$
$$(A_{96} \oplus \bar{A}_{96}) = (D_{93}A_{96} \oplus \bar{D}_{93}\bar{A}_{96}) \oplus (D_{93} \oplus \bar{D}_{93})$$
$$(B_{95}E_{92} \oplus H_{97} \oplus E_{92})(A_{96} \oplus \bar{A}_{96}) \quad (7)$$
$$= (B_{95}H_{97} \oplus E_{92} \oplus H_{97})(D_{93} \oplus \bar{D}_{93})$$

$$H_{97} \cdot (A_{96}D_{93} \oplus \bar{A}_{96}\bar{D}_{93}) \oplus (G_{98}C_{94} \oplus E_{92}) \quad (8)$$
$$(A_{96} \oplus \bar{A}_{96}) = (G_{98}E_{92} \oplus G_{98} \oplus C_{94} \oplus E_{92})(D_{93} \oplus \bar{D}_{93})$$
$$(C_{94}F_{99} \oplus H_{97} \oplus C_{94} \oplus F_{99})(D_{93} \oplus \bar{D}_{93}) \quad (9)$$
$$= E_{99} \cdot (A_{96} \oplus \bar{A}_{96}) \oplus A_{96} \oplus \bar{A}_{96}$$
$$(F_{99}G_{98}B_{95} \oplus G_{98}E_{100}A_{96} \oplus B_{95}E_{100}C_{94} \quad (10)$$
$$\oplus F_{99}E_{100} \oplus G_{98}C_{94} \oplus B_{95}E_{100} \oplus B_{95}A_{96} \oplus B_{95}C_{94}$$
$$\oplus E_{100}A_{96} \oplus E_{100}C_{94} \oplus H_{97}E_{100} \oplus H_{97})^{>>7} + D_{100}^{>>11}$$
$$= (F_{99}G_{98}B_{95} \oplus G_{98}E_{100}\bar{A}_{96} \oplus B_{95}E_{100}C_{94}$$
$$\oplus F_{99}E_{100} \oplus G_{98}C_{94} \oplus B_{95}E_{100} \oplus B_{95}\bar{A}_{96} \oplus B_{95}C_{94}$$
$$\oplus E_{100}\bar{A}_{96} \oplus E_{100}C_{94} \oplus H_{97}E_{100} \oplus H_{97})^{>>7} + \bar{D}_{100}^{>>11}$$
$$A_{103}^{>>11} + X_{23} = \bar{A}_{103}^{>>11} + \bar{X}_{23} \quad (11)$$

数式 (2) から数式 (11) までに, 次の方程式を得られる.

$$A_{103}^{>>11} - \bar{A}_{103}^{>>11} + D_{93} - \bar{D}_{93} = 0 \quad (12)$$
$$A_{88}D_{93} \oplus \bar{A}_{88}\bar{D}_{93} = 0 \quad (13)$$
$$(D_{93}A_{96} \oplus \bar{D}_{93}\bar{A}_{96}) \oplus (D_{93} \oplus \bar{D}_{93}) = 0 \quad (14)$$
$$H_{97} \cdot (D_{93} \oplus \bar{D}_{93}) = H_{97} \cdot (A_{96} \oplus \bar{A}_{96}) \quad (15)$$
$$G_{98} \cdot (D_{93} \oplus \bar{D}_{93}) = H_{97} \cdot (A_{96}D_{93} \oplus \bar{A}_{96}\bar{D}_{93}) \quad (16)$$
$$(H_{97} \oplus F_{99})(D_{93} \oplus \bar{D}_{93}) = \quad (17)$$
$$E_{99} \cdot (A_{96} \oplus \bar{A}_{96}) \oplus (A_{96} \oplus \bar{A}_{96})$$
$$(G_{98}E_{100}A_{96} \oplus F_{99}E_{100} \oplus E_{100}A_{96} \oplus H_{97}E_{100} \quad (18)$$
$$\oplus H_{97})^{>>7} + D_{100}^{>>11} = (G_{98}E_{100}\bar{A}_{96} \oplus F_{99}E_{100}$$
$$\oplus E_{100}\bar{A}_{96} \oplus H_{97}E_{100} \oplus H_{97})^{>>7} + \bar{D}_{100}^{>>11}$$

数式 (2) から数式 (18) までに方程式の結果を表 3 で示す.
段階 97 の演算は

$$H_{97} = (B_{96}C_{96}F_{96} \oplus C_{96}A_{96}E_{96} \oplus F_{96}A_{96}G_{96} \quad (19)$$
$$\oplus B_{96}A_{96} \oplus C_{96}G_{96} \oplus F_{96}A_{96} \oplus F_{96}E_{96}$$
$$\oplus F_{96}G_{96} \oplus A_{96}E_{96} \oplus A_{96}G_{96} \oplus D_{96}A_{96}$$
$$\oplus D_{96})^{>>7} + H_{96}^{>>11} + X_{24}$$

表 3 の結果より, 以下の方程式が得られる.

表 3: 数式の結果

A_{88}	Oxffffffff	$\bar{A}_{88}$	
H_{89}	0	$\bar{H}_{89}$	0
G_{90}	0	$\bar{G}_{90}$	
F_{91}	0	$\bar{F}_{91}$	
E_{92}	0	$\bar{E}_{92}$	
D_{93}	0	$\bar{D}_{93}$	Oxffffffff
C_{94}	0	$\bar{C}_{94}$	
B_{95}	0	$\bar{B}_{95}$	
A_{96}	Oxffffffff	$\bar{A}_{96}$	0
H_{97}	0	$\bar{H}_{97}$	
G_{98}	0	$\bar{G}_{98}$	
F_{99}	0	$\bar{F}_{99}$	
E_{100}	0	$\bar{E}_{100}$	

$X_{24} = H_{97} - Ox7a325381 = Oxffffffff - Ox7a325381 = Ox85cdac7e$
同様に, 表 4 に示される結果が得られる.

3.2 Haval の他の攻撃の結果

HAVAL の他の pass に対する攻撃結果は付録で紹介する.

4 HAVAL の攻撃に対する安全性分析

我々Park らの HAVAL に対する攻撃手法を拡張した. 我々の目的は HAVAL の安全性に対する正確な分析にある. 5 個のブール関数の中で, 4 番目のブール関数は, 演算が最も複雑である. それで, われらは 5-passHAVAL より 4-pass HAVAL の攻撃を選択した. 3-pass と 4-pass の相違点は置換の順序とブール関数である. 本章では, 4-pass HAVAL の攻撃方法ら仲では, われらは 3, 4-pass の攻撃方法を強調する. 我々は 2pass 簡約した 4-pass の

表 4: 4-pass HAVAL ⟨3,4⟩ の攻撃結果

$X_i(\bar{X}_i)$	Values	$X_i(\bar{X}_i)$	Values
$X_0(\bar{X}_0)$	Oxc470b767	$X_{16}(\bar{X}_{16})$	
$X_1(\bar{X}_1)$		$X_{17}(\bar{X}_{17})$	
$X_2(\bar{X}_2)$	Ox93db30a3	$X_{18}(\bar{X}_{18})$	
$X_3(\bar{X}_3)$		$X_{19}(\bar{X}_{19})$	
$X_4(\bar{X}_4)$	Oxd76a7988	$X_{20}(\bar{X}_{20})$	
$X_5(\bar{X}_5)$	Ox502945cd	$X_{21}(\bar{X}_{21})$	Oxd4563aa3
$X_6(\bar{X}_6)$	Ox9c9043d6	$X_{22}(\bar{X}_{22})$	
$X_7(\bar{X}_7)$		$X_{23}(\bar{X}_{23})$	Ox31a3c1ea
$X_8(\bar{X}_8)$		$X_{24}(\bar{X}_{24})$	Ox85cdac7e
$X_9(\bar{X}_9)$		$X_{25}(\bar{X}_{25})$	
$X_{10}(\bar{X}_{10})$	Ox8be7ce0a	$X_{26}(\bar{X}_{26})$	
$X_{11}(\bar{X}_{11})$	Ox64786ce2	$X_{27}(\bar{X}_{27})$	Ox838d166c
$X_{12}(\bar{X}_{12})$		$X_{28}(\bar{X}_{28})$	
$X_{13}(\bar{X}_{13})$	Ox4c11ebef	$X_{29}(\bar{X}_{29})$	
$X_{14}(\bar{X}_{14})$	Ox94b44651	$X_{30}(\bar{X}_{30})$	
$X_{15}(\bar{X}_{15})$		$X_{31}(\bar{X}_{31})$	

HAVAL で衝突を発見した． 衝突の理由は次に段階で 8 個の連鎖変数中から但し 1 個の連鎖変数だけ変わる．4-pass HAVAL の ⟨1,2⟩ への攻撃方法は 4-pass HAVAL の ⟨1,2⟩ きて似ている．4-pass の ⟨2,3⟩ 攻撃方法は他の方程式へ誘導になる．例を上げれば, 57 段階と 65 段階までの X_{19} の 連鎖変数は同じあるために, 我々は $t = H_{57} - \bar{H}_{57}$ でついて 4 つの値を得ることができる．4 つの値を考慮しなければならない．それため, 4-pass HAVAL の 4-pass HAVAL ⟨2,3⟩ の攻撃は困難である．3-pass HAVAL の場合に, われらは ⟨1,3⟩ への攻撃を試みた．Kasselman らと Park らなどは 3-pass HAVAL 中から連続した 2 つの pass に対する攻撃を試みたが, 非連続 pass の攻撃を試みたのである．これは 3-pass HAVAL の安全性に問題性が あったということを見せたのである．結論的に, HAVAL は 8 個のブール変数を使用しながらも, 単位演算の単純性で安全性に問題が発生したのである．表 5 は HAVAL の衝突結果を示す． 4-pass HAVAL の ⟨3,4⟩ が一番脆弱なことが示された．

表 5: 衝突の結果

3-pass	⟨1,2⟩	⟨2,3⟩	⟨1,3⟩
衝突	12-pair	9-pair	6-pair
確率	0.375	0.28	0.186
4-pass	⟨1,2⟩	⟨2,3⟩	⟨3,4⟩
衝突	12-pair	5-pair	13-pair
確率	0.375	0.156	0.406

5 ハッシュ関数に対する攻撃の分析

暗号学的ハッシュ関数に対する攻撃方法は 2 種類で分類できる．最初は, ブール関数の弱点を攻撃することで, 他のひとつは単位演算に対する攻撃方法である．ブール関数の弱点を利用した攻撃は MD4 に対する桑門と田中の攻撃方法である [7]．例えば, MD4 に 2 番目のブール関数は次のような 特徴を 持っている．
$G(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$ ($\wedge$: bitwiseAND, $\vee$: bitwiseOR) 2 番目ブール関数の 3 個の変数の中で 2 ケが同じならば, 残り 1 つの変数と関係なく, 結果は同じである．結局, 桑門と田中はこのようなブール関数の弱点を利用した MD4 に対する衝突を発見した．単位演算に対する攻撃は本論文で導入になった方法である．MD4 は 3 個の変数にしかならないけれど, HAVAL は 8 個の変数の利用した．しかし, 次に段階で 8 個の連鎖変数中から 1 個の連鎖変数だけ変わる．

6 まとめ

本論文で, 我々が 3-pass HAVAL の ⟨1,3⟩ に対する攻撃方法を試みた．また, 4 -pass HAVAL の ⟨1,2⟩ と ⟨2,3⟩ と ⟨3,4⟩ について攻撃を試みた．HAVAL は最初の可変出力値を持つ暗号学的ハッシュ関数であった．しかし, 他の ハッシュ関数に比べて, 多くのブール変数を使用するにも次に段階で 1 つのブール変数だけ異なる, 単位演算の単純性よって安全性に問題が発見された．今後の課題はそれぞれの攻撃らに対して実際の具現を通し速度と衝突に対する分析を実施にならなければならない．また, 3-pass HAVAL に対する全体 pass 対する攻撃と 5-pass HAVAL に対する衝突に対する研究が必要とする．

謝辞

本研究は一部，21 世紀 COE プログラム「システム情報科学での社会基盤システム形成」の支援と文部科学省科学研究費補助金学術創成研究課題番号 14GS0218「社会基盤を構築するためのシステム LSI 設計手法の研究」(研究代表安浦寛人九州大学システム LSI 研究センター長) の支援を受けている．

参考文献

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

[2] Ronald L.Rivest *"The message digest algorithm"* Crypto'90 LNCS 537, pp303-311, Springe-Verlag, 1991

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

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

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

[6] B.Preneel *"Analysis and design of cryptographic hash functions"* PhD thesis, Katholieke Universiteit Leuven, 1993

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

付録

表 6: 4-pass HAVAL⟨1,2⟩ の攻撃結果

$X_i(\bar{X}_i)$	Values	$X_i(\bar{X}_i)$	Values
$X_0(\bar{X}_0)$		$X_{16}(\bar{X}_{16})$	
$X_1(\bar{X}_1)$		$X_{17}(\bar{X}_{17})$	
$X_2(\bar{X}_2)$		$X_{18}(\bar{X}_{18})$	Oxcb16f394
$X_3(\bar{X}_3)$		$X_{19}(\bar{X}_{19})$	
$X_4(\bar{X}_4)$		$X_{20}(\bar{X}_{20})$	
$X_5(\bar{X}_5)$	Oxbad7de19	$X_{21}(\bar{X}_{21})$	
$X_6(\bar{X}_6)$		$X_{22}(\bar{X}_{22})$	
$X_7(\bar{X}_7)$		$X_{23}(\bar{X}_{23})$	Ox2d8e2ef4
$X_8(\bar{X}_8)$		$X_{24}(\bar{X}_{24})$	Oxcd6f4a4a
$X_9(\bar{X}_9)$		$X_{25}(\bar{X}_{25})$	Ox4a45d2f3
$X_{10}(\bar{X}_{10})$		$X_{26}(\bar{X}_{26})$	Ox41ab9930
$X_{11}(\bar{X}_{11})$		$X_{27}(\bar{X}_{27})$	Oxb9107999
$X_{12}(\bar{X}_{12})$		$X_{28}(\bar{X}_{28})$	Ox260791c2 (Ox260791c3)
$X_{13}(\bar{X}_{13})$		$X_{29}(\bar{X}_{29})$	Ox92102afd
$X_{14}(\bar{X}_{14})$	Oxc72fec89	$X_{30}(\bar{X}_{30})$	Oxf0000000
$X_{15}(\bar{X}_{15})$		$X_{31}(\bar{X}_{31})$	0

表 7: 4-pass HAVAL⟨2,3⟩ の攻撃結果

$X_i(\bar{X}_i)$	Values	$X_i(\bar{X}_i)$	Values
$X_0(\bar{X}_0)$		$X_{16}(\bar{X}_{16})$	
$X_1(\bar{X}_1)$		$X_{17}(\bar{X}_{17})$	
$X_2(\bar{X}_2)$		$X_{18}(\bar{X}_{18})$	
$X_3(\bar{X}_3)$		$X_{19}(\bar{X}_{19})$	
$X_4(\bar{X}_4)$		$X_{20}(\bar{X}_{20})$	
$X_5(\bar{X}_5)$		$X_{21}(\bar{X}_{21})$	
$X_6(\bar{X}_6)$	Oxa7891c3e	$X_{22}(\bar{X}_{22})$	
$X_7(\bar{X}_7)$		$X_{23}(\bar{X}_{23})$	
$X_8(\bar{X}_8)$		$X_{24}(\bar{X}_{24})$	Ox73e6fac2
$X_9(\bar{X}_9)$	Oxbe38682c	$X_{25}(\bar{X}_{25})$	
$X_{10}(\bar{X}_{10})$		$X_{26}(\bar{X}_{26})$	
$X_{11}(\bar{X}_{11})$		$X_{27}(\bar{X}_{27})$	
$X_{12}(\bar{X}_{12})$		$X_{28}(\bar{X}_{28})$	
$X_{13}(\bar{X}_{13})$	Oxe34933c9	$X_{29}(\bar{X}_{29})$	
$X_{14}(\bar{X}_{14})$		$X_{30}(\bar{X}_{30})$	
$X_{15}(\bar{X}_{15})$	Ox9a31cbb1	$X_{31}(\bar{X}_{31})$	

表 8: 3-pass HAVAL⟨1,3⟩ の攻撃結果

$X_i(\bar{X}_i)$	Values	$X_i(\bar{X}_i)$	Values
$X_0(\bar{X}_0)$		$X_{16}(\bar{X}_{16})$	
$X_1(\bar{X}_1)$		$X_{17}(\bar{X}_{17})$	Ox4724c7df
$X_2(\bar{X}_2)$		$X_{18}(\bar{X}_{18})$	
$X_3(\bar{X}_3)$		$X_{19}(\bar{X}_{19})$	Ox63cf2ac7
$X_4(\bar{X}_4)$	Ox3a2e4fdd	$X_{20}(\bar{X}_{20})$	Oxd79f7a10
$X_5(\bar{X}_5)$		$X_{21}(\bar{X}_{21})$	
$X_6(\bar{X}_6)$		$X_{22}(\bar{X}_{22})$	
$X_7(\bar{X}_7)$		$X_{23}(\bar{X}_{23})$	
$X_8(\bar{X}_8)$		$X_{24}(\bar{X}_{24})$	
$X_9(\bar{X}_9)$	Oxd50d9fed	$X_{25}(\bar{X}_{25})$	
$X_{10}(\bar{X}_{10})$		$X_{26}(\bar{X}_{26})$	
$X_{11}(\bar{X}_{11})$		$X_{27}(\bar{X}_{27})$	
$X_{12}(\bar{X}_{12})$		$X_{28}(\bar{X}_{28})$	Ox35be86e8
$X_{13}(\bar{X}_{13})$		$X_{29}(\bar{X}_{29})$	
$X_{14}(\bar{X}_{14})$		$X_{30}(\bar{X}_{30})$	
$X_{15}(\bar{X}_{15})$		$X_{31}(\bar{X}_{31})$	