Preimage attacks on 3-pass HAVAL and step-reduced MD5

Jean-Philippe Aumasson, Willi Meier, Florian Mendel

University of Applied Sciences Northwestern Switzerland
School of Engineering

TU Graz

Previous preimage attacks

Google(*collision attack*) $\approx$ 3 500 000

Google (*preimage attack*) $\approx$ 15 000

- MD2 (2004)
- Parallel FFT-Hashing (2007)
- Syndrome-based hash (2007)
- HAS-V (2007)
- Tiger (2007)
- MD4 (2008)
- GOST (2008)
- Snefru (2008)
- SHA-0/1 (2008)

The preimage problem

h is a function $\{0,1\}^\star \mapsto \{0,1\}^n$, specified as an algorithm

Problem: "Given y, find x such that $h(x) = y$"

Given what? either

1. a **random range** element
2. the image of a **random domain** element
3. **any fixed** value

Attacks here work for 1, 2, 3

Content of this talk

MD5: how to invert. . .

- 22 steps?
- 31 steps?
- 47 steps?

What about **HAVAL**?

How to turn random-IV attacks to fixed-IV attacks?

MD5

- 1991: publication (Rivest)
- 1993: **collision** attack (compression function)
- 2005: **collision** attack (hash function)
- 2005+: faster, chosen-prefix, meaningful **collisions**

Previous talk: preimage attacks on reduced-step MD5 with delayed start

MD5 compression function

Input

- chain value $H_0 H_1 H_2 H_3$
- message $M_0 M_1 \dots M_{15}$

Algorithm

- copy $H_0 H_1 H_2 H_3$ into $A_0 B_0 C_0 D_0$
- for $i = 1 \dots 64$

$$
\begin{array}{rcl}
A_i & = & D_{i-1} \\
B_i & = & f_i(A_{i-1}, B_{i-1}, C_{i-1}, D_{i-1}, M_{\sigma(i)}) \\
C_i & = & B_{i-1} \\
D_i & = & C_{i-1}
\end{array}
$$

- return $(A_0 + A_{64}) \| (B_0 + B_{64}) \| (C_0 + C_{64}) \| (D_0 + D_{64})$

Unrolling (**index**, function, message word)

1	$f_1(A_0, B_0, C_0, D_0, 0)$	**17**	$f_{17}(A_{16}, B_{16}, C_{16}, D_{16}, 1)$
2	$f_2(A_1, B_1, C_1, D_1, 1)$	**18**	$f_{18}(A_{17}, B_{17}, C_{17}, D_{17}, 6)$
3	$f_3(A_2, B_2, C_2, D_2, 2)$	**19**	$f_{19}(A_{18}, B_{18}, C_{18}, D_{18}, 11)$
4	$f_4(A_3, B_3, C_3, D_3, 3)$	**20**	$f_{20}(A_{19}, B_{19}, C_{19}, D_{19}, 0)$
5	$f_5(A_4, B_4, C_4, D_4, 4)$	**21**	$f_{21}(A_{20}, B_{20}, C_{20}, D_{20}, 5)$
6	$f_6(A_5, B_5, C_5, D_5, 5)$	**22**	$f_{22}(A_{21}, B_{21}, C_{21}, D_{21}, 10)$
7	$f_7(A_6, B_6, C_6, D_6, 6)$	**23**	$f_{23}(A_{22}, B_{22}, C_{22}, D_{22}, 15)$
8	$f_8(A_7, B_7, C_7, D_7, 7)$	**24**	$f_{24}(A_{23}, B_{23}, C_{23}, D_{23}, 4)$
9	$f_9(A_8, B_8, C_8, D_8, 8)$	**25**	$f_{25}(A_{24}, B_{24}, C_{24}, D_{24}, 9)$
10	$f_{10}(A_9, B_9, C_9, D_9, 9)$	**26**	$f_{26}(A_{25}, B_{25}, C_{25}, D_{25}, 14)$
11	$f_{11}(A_{10}, B_{10}, C_{10}, D_{10}, 10)$	**27**	$f_{27}(A_{26}, B_{26}, C_{26}, D_{26}, 3)$
12	$f_{12}(A_{11}, B_{11}, C_{11}, D_{11}, 11)$	**28**	$f_{28}(A_{27}, B_{27}, C_{27}, D_{27}, 8)$
13	$f_{13}(A_{12}, B_{12}, C_{12}, D_{12}, 12)$	**29**	$f_{29}(A_{28}, B_{28}, C_{28}, D_{28}, 13)$
14	$f_{14}(A_{13}, B_{13}, C_{13}, D_{13}, 13)$	**30**	$f_{30}(A_{29}, B_{29}, C_{29}, D_{29}, 2)$
15	$f_{15}(A_{14}, B_{14}, C_{14}, D_{14}, 14)$	**31**	$f_{31}(A_{30}, B_{30}, C_{30}, D_{30}, 7)$
16	$f_{16}(A_{15}, B_{15}, C_{15}, D_{15}, 15)$	**32**	$f_{32}(A_{31}, B_{31}, C_{31}, D_{31}, 12)$

First 2 rounds

1	$f(A_0, B_0, C_0, D_0, 0)$	**17**	$g(A_{16}, B_{16}, C_{16}, D_{16}, 1)$
2	$f(A_1, B_1, C_1, D_1, 1)$	**18**	$g(A_{17}, B_{17}, C_{17}, D_{17}, 6)$
3	$f(A_2, B_2, C_2, D_2, 2)$	**19**	$g(A_{18}, B_{18}, C_{18}, D_{18}, 11)$
4	$f(A_3, B_3, C_3, D_3, 3)$	**20**	$g(A_{19}, B_{19}, C_{19}, D_{19}, 0)$
5	$f(A_4, B_4, C_4, D_4, 4)$	**21**	$g(A_{20}, B_{20}, C_{20}, D_{20}, 5)$
6	$f(A_5, B_5, C_5, D_5, 5)$	**22**	$g(A_{21}, B_{21}, C_{21}, D_{21}, 10)$
7	$f(A_6, B_6, C_6, D_6, 6)$	**23**	$g(A_{22}, B_{22}, C_{22}, D_{22}, 15)$
8	$f(A_7, B_7, C_7, D_7, 7)$	**24**	$g(A_{23}, B_{23}, C_{23}, D_{23}, 4)$
9	$f(A_8, B_8, C_8, D_8, 8)$	**25**	$g(A_{24}, B_{24}, C_{24}, D_{24}, 9)$
10	$f(A_9, B_9, C_9, D_9, 9)$	**26**	$g(A_{25}, B_{25}, C_{25}, D_{25}, 14)$
11	$f(A_{10}, B_{10}, C_{10}, D_{10}, 10)$	**27**	$g(A_{26}, B_{26}, C_{26}, D_{26}, 3)$
12	$f(A_{11}, B_{11}, C_{11}, D_{11}, 11)$	**28**	$g(A_{27}, B_{27}, C_{27}, D_{27}, 8)$
13	$f(A_{12}, B_{12}, C_{12}, D_{12}, 12)$	**29**	$g(A_{28}, B_{28}, C_{28}, D_{28}, 13)$
14	$f(A_{13}, B_{13}, C_{13}, D_{13}, 13)$	**30**	$g(A_{29}, B_{29}, C_{29}, D_{29}, 2)$
15	$f(A_{14}, B_{14}, C_{14}, D_{14}, 14)$	**31**	$g(A_{30}, B_{30}, C_{30}, D_{30}, 7)$
16	$f(A_{15}, B_{15}, C_{15}, D_{15}, 15)$	**32**	$g(A_{31}, B_{31}, C_{31}, D_{31}, 12)$

Inverting 22 steps

1	$f(A_0, B_0, C_0, D_0, 0)$	**17**	$g(A_{16}, B_{16}, C_{16}, D_{16}, 1)$
2	$f(A_1, B_1, C_1, D_1, 1)$	**18**	$g(A_{17}, B_{17}, C_{17}, D_{17}, 6)$
3	$f(A_2, B_2, C_2, D_2, 2)$	**19**	$g(A_{18}, B_{18}, C_{18}, D_{18}, 11)$
4	$f(A_3, B_3, C_3, D_3, 3)$	**20**	$g(A_{19}, B_{19}, C_{19}, D_{19}, 0)$
5	$f(A_4, B_4, C_4, D_4, 4)$	**21**	$g(A_{20}, B_{20}, C_{20}, D_{20}, 5)$
6	$f(A_5, B_5, C_5, D_5, 5)$	**22**	$g(A_{21}, B_{21}, C_{21}, D_{21}, 10)$
7	$f(A_6, B_6, C_6, D_6, 6)$		
8	$f(A_7, B_7, C_7, D_7, 7)$		
9	$f(A_8, B_8, C_8, D_8, 8)$		
10	$f(A_9, B_9, C_9, D_9, 9)$		
11	$f(A_{10}, B_{10}, C_{10}, D_{10}, 10)$		
12	$f(A_{11}, B_{11}, C_{11}, D_{11}, 11)$		
13	$f(A_{12}, B_{12}, C_{12}, D_{12}, 12)$		
14	$f(A_{13}, B_{13}, C_{13}, D_{13}, 13)$		
15	$f(A_{14}, B_{14}, C_{14}, D_{14}, 14)$		
16	$f(A_{15}, B_{15}, C_{15}, D_{15}, 15)$		

Inverting 22 steps

Pick $M_0 \ldots M_{11}$

From **1** to **12**, compute $A_{12} B_{12} C_{12} D_{12}$

From **22** to **17**, compute $A_{16} B_{16} C_{16} D_{16}$

Choose M_{12} such that $B_{13} = A_{16}$
Choose M_{13} such that $B_{14} = D_{16}$
Choose M_{14} such that $B_{15} = C_{16}$
Choose M_{15} such that $B_{16} = B_{16}$

Cost: 22 steps

31 steps: same idea…

1	$f(A_0, B_0, C_0, D_0, 0)$	**17**	$g(A_{16}, B_{16}, C_{16}, D_{16}, 1)$
2	$f(A_1, B_1, C_1, D_1, 1)$	**18**	$g(A_{17}, B_{17}, C_{17}, D_{17}, 6)$
3	$f(A_2, B_2, C_2, D_2, 2)$	**19**	$g(A_{18}, B_{18}, C_{18}, D_{18}, 11)$
4	$f(A_3, B_3, C_3, D_3, 3)$	**20**	$g(A_{19}, B_{19}, C_{19}, D_{19}, 0)$
5	$f(A_4, B_4, C_4, D_4, 4)$	**21**	$g(A_{20}, B_{20}, C_{20}, D_{20}, 5)$
6	$f(A_5, B_5, C_5, D_5, 5)$	**22**	$g(A_{21}, B_{21}, C_{21}, D_{21}, 10)$
7	$f(A_6, B_6, C_6, D_6, 6)$	**23**	$g(A_{22}, B_{22}, C_{22}, D_{22}, 15)$
8	$f(A_7, B_7, C_7, D_7, 7)$	**24**	$g(A_{23}, B_{23}, C_{23}, D_{23}, 4)$
9	$f(A_8, B_8, C_8, D_8, 8)$	**25**	$g(A_{24}, B_{24}, C_{24}, D_{24}, 9)$
10	$f(A_9, B_9, C_9, D_9, 9)$	**26**	$g(A_{25}, B_{25}, C_{25}, D_{25}, 14)$
11	$f(A_{10}, B_{10}, C_{10}, D_{10}, 10)$	**27**	$g(A_{26}, B_{26}, C_{26}, D_{26}, 3)$
12	$f(A_{11}, B_{11}, C_{11}, D_{11}, 11)$	**28**	$g(A_{27}, B_{27}, C_{27}, D_{27}, 8)$
13	$f(A_{12}, B_{12}, C_{12}, D_{12}, 12)$	**29**	$g(A_{28}, B_{28}, C_{28}, D_{28}, 13)$
14	$f(A_{13}, B_{13}, C_{13}, D_{13}, 13)$	**30**	$g(A_{29}, B_{29}, C_{29}, D_{29}, 2)$
15	$f(A_{14}, B_{14}, C_{14}, D_{14}, 14)$	**31**	$g(A_{30}, B_{30}, C_{30}, D_{30}, 7)$
16	$f(A_{15}, B_{15}, C_{15}, D_{15}, 15)$		

M_{12} input only once...

1	$f(A_0, B_0, C_0, D_0, 0)$	**17**	$g(A_{16}, B_{16}, C_{16}, D_{16}, 1)$
2	$f(A_1, B_1, C_1, D_1, 1)$	**18**	$g(A_{17}, B_{17}, C_{17}, D_{17}, 6)$
3	$f(A_2, B_2, C_2, D_2, 2)$	**19**	$g(A_{18}, B_{18}, C_{18}, D_{18}, 11)$
4	$f(A_3, B_3, C_3, D_3, 3)$	**20**	$g(A_{19}, B_{19}, C_{19}, D_{19}, 0)$
5	$f(A_4, B_4, C_4, D_4, 4)$	**21**	$g(A_{20}, B_{20}, C_{20}, D_{20}, 5)$
6	$f(A_5, B_5, C_5, D_5, 5)$	**22**	$g(A_{21}, B_{21}, C_{21}, D_{21}, 10)$
7	$f(A_6, B_6, C_6, D_6, 6)$	**23**	$g(A_{22}, B_{22}, C_{22}, D_{22}, 15)$
8	$f(A_7, B_7, C_7, D_7, 7)$	**24**	$g(A_{23}, B_{23}, C_{23}, D_{23}, 4)$
9	$f(A_8, B_8, C_8, D_8, 8)$	**25**	$g(A_{24}, B_{24}, C_{24}, D_{24}, 9)$
10	$f(A_9, B_9, C_9, D_9, 9)$	**26**	$g(A_{25}, B_{25}, C_{25}, D_{25}, 14)$
11	$f(A_{10}, B_{10}, C_{10}, D_{10}, 10)$	**27**	$g(A_{26}, B_{26}, C_{26}, D_{26}, 3)$
12	$f(A_{11}, B_{11}, C_{11}, D_{11}, 11)$	**28**	$g(A_{27}, B_{27}, C_{27}, D_{27}, 8)$
13	$f(A_{12}, B_{12}, C_{12}, D_{12}, 12)$	**29**	$g(A_{28}, B_{28}, C_{28}, D_{28}, 13)$
14	$f(A_{13}, B_{13}, C_{13}, D_{13}, 13)$	**30**	$g(A_{29}, B_{29}, C_{29}, D_{29}, 2)$
15	$f(A_{14}, B_{14}, C_{14}, D_{14}, 14)$	**31**	$g(A_{30}, B_{30}, C_{30}, D_{30}, 7)$
16	$f(A_{15}, B_{15}, C_{15}, D_{15}, 15)$		

31 steps

Pick $M_0 \ldots M_{11}, M_{13}, M_{14}, M_{15}$

From **1** to **12**, compute $A_{12} B_{12} C_{12} D_{12}$

From **22** to **14**, compute $A_{13} B_{13} C_{13} D_{13}$

If $A_{13} = D_{12}$, $C_{13} = B_{12}$, and $D_{13} = C_{12}$:
then choose M_{12} such that $B_{13} = B_{13}$

Cost: $\approx 2^{96} \times 31$ steps

47 steps: M_2 input only twice...

1	$f(\ldots, 0)$	**17**	$g(\ldots, 1)$	**33**	$h(\ldots, 5)$
2	$f(\ldots, 1)$	**18**	$g(\ldots, 6)$	**34**	$h(\ldots, 8)$
3	$f(\ldots, 2)$	**19**	$g(\ldots, 11)$	**35**	$h(\ldots, 11)$
4	$f(\ldots, 3)$	**20**	$g(\ldots, 0)$	**36**	$h(\ldots, 14)$
5	$f(\ldots, 4)$	**21**	$g(\ldots, 5)$	**37**	$h(\ldots, 1)$
6	$f(\ldots, 5)$	**22**	$g(\ldots, 10)$	**38**	$h(\ldots, 4)$
7	$f(\ldots, 6)$	**23**	$g(\ldots, 15)$	**39**	$h(\ldots, 7)$
8	$f(\ldots, 7)$	**24**	$g(\ldots, 4)$	**40**	$h(\ldots, 10)$
9	$f(\ldots, 8)$	**25**	$g(\ldots, 9)$	**41**	$h(\ldots, 13)$
10	$f(\ldots, 9)$	**26**	$g(\ldots, 14)$	**42**	$h(\ldots, 0)$
11	$f(\ldots, 10)$	**27**	$g(\ldots, 3)$	**43**	$h(\ldots, 3)$
12	$f(\ldots, 11)$	**28**	$g(\ldots, 8)$	**44**	$h(\ldots, 6)$
13	$f(\ldots, 12)$	**29**	$g(\ldots, 13)$	**45**	$h(\ldots, 9)$
14	$f(\ldots, 13)$	**30**	$g(\ldots, 2)$	**46**	$h(\ldots, 12)$
15	$f(\ldots, 14)$	**31**	$g(\ldots, 7)$	**47**	$h(\ldots, 15)$
16	$f(\ldots, 15)$	**32**	$g(\ldots, 12)$		

Differences propagation, general case

Pick random A_0, B_0, C_0, D_0 and M

1	$f($	A_0,	B_0,	C_0,	D_0,	$0)$
2	$f($	A_1,	B_1,	C_1,	D_1,	$1)$
3	$f($	A_2,	B_2,	C_2,	D_2,	$2)$

Modify C_0 to $C_0^\star$

X	**1**	$f($	A_0,	B_0,	$C_0^\star$,	D_0,	$0)$
X	**2**	$f($	A_1,	B_1,	C_1,	$C_0^\star$,	$1)$
X	**3**	$f($	$C_0^\star$,	B_2,	C_2,	D_2,	$2)$

$\Rightarrow$ all first steps affected (X=state modified)

Difference in C_0 + chosen IV

Pick random A_0, C_0, D_0 and M **and set $\mathbf{B_0} = \mathbf{0}$**

$$\begin{array}{ll}
\mathbf{1} & f(A_0\ ,B_0\ ,C_0\ ,D_0\ ,\ \ 0) \\
\mathbf{2} & f(A_1\ ,B_1\ ,C_1\ ,D_1\ ,\ \ 1) \\
\mathbf{3} & f(A_2\ ,B_2\ ,C_2\ ,D_2\ ,\ \ 2)
\end{array}$$

Modify C_0 to $C_0^\star$

$$\begin{array}{lll}
\surd & \mathbf{1} & f(A_0\ ,\ 0, C_0^\star\ ,D_0\ ,\ \ 0) \\
\surd & \mathbf{2} & f(A_1\ ,B_1\ ,\ 0, C_0^\star\ ,\ \ 1) \\
X & \mathbf{3} & f(C_0^\star\ ,B_2\ ,C_2\ ,\ 0,\ \ 2)
\end{array}$$

$\Rightarrow$ only step 3 affected

Difference in M_2

Pick random A_0, B_0, C_0, D_0 and M

$$
\begin{array}{ll}
\mathbf{1} & f(A_0, B_0, C_0, D_0, 0) \\
\mathbf{2} & f(A_1, B_1, C_1, D_1, 1) \\
\mathbf{3} & f(A_2, B_2, C_2, D_2, 2)
\end{array}
$$

Modify M_2

$$
\begin{array}{lll}
\surd & \mathbf{1} & f(A_0, B_0, C_0, D_0, 0) \\
\surd & \mathbf{2} & f(A_1, B_1, C_1, C_0, 1) \\
X & \mathbf{3} & f(A_2, B_2, C_2, D_2, 2)
\end{array}
$$

$\Rightarrow$ only step 3 affected

Absorbing differences

Pick random A_0, C_0, D_0 and M **and set $\mathbf{B_0} = \mathbf{0}$**

$$
\begin{array}{ll}
\mathbf{1} & f(A_0\ , B_0\ , C_0\ , D_0\ ,\ \ 0) \\
\mathbf{2} & f(A_1\ , B_1\ , C_1\ , D_1\ ,\ \ 1) \\
\mathbf{3} & f(A_2\ , B_2\ , C_2\ , D_2\ ,\ \ 2)
\end{array}
$$

Modify C_0 to $C_0^\star$ **and** M_2

$$
\begin{array}{lll}
\surd & \mathbf{1} & f(A_0\ ,\ 0, C_0^\star\ , D_0\ ,\ \ 0) \\
\surd & \mathbf{2} & f(A_1\ , B_1\ ,\ 0, C_0^\star\ ,\ \ 1) \\
\surd & \mathbf{3} & f(C_0^\star\ , B_2\ , C_2\ ,\ 0,\ \ 2)
\end{array}
$$

$\Rightarrow$ nothing changes!

Application to 47-step MD5: key steps

1	$f(\ldots, 0)$	**17**	$g(\ldots, 1)$	**33**	$h(\ldots, 5)$
2	$f(\ldots, 1)$	**18**	$g(\ldots, 6)$	**34**	$h(\ldots, 8)$
3	$f(\ldots, 2)$	**19**	$g(\ldots, 11)$	**35**	$h(\ldots, 11)$
4	$f(\ldots, 3)$	**20**	$g(\ldots, 0)$	**36**	$h(\ldots, 14)$
5	$f(\ldots, 4)$	**21**	$g(\ldots, 5)$	**37**	$h(\ldots, 1)$
6	$f(\ldots, 5)$	**22**	$g(\ldots, 10)$	**38**	$h(\ldots, 4)$
7	$f(\ldots, 6)$	**23**	$g(\ldots, 15)$	**39**	$h(\ldots, 7)$
8	$f(\ldots, 7)$	**24**	$g(\ldots, 4)$	**40**	$h(\ldots, 10)$
9	$f(\ldots, 8)$	**25**	$g(\ldots, 9)$	**41**	$h(\ldots, 13)$
10	$f(\ldots, 9)$	**26**	$g(\ldots, 14)$	**42**	$h(\ldots, 0)$
11	$f(\ldots, 10)$	**27**	$g(\ldots, 3)$	**43**	$h(\ldots, 3)$
12	$f(\ldots, 11)$	**28**	$g(\ldots, 8)$	**44**	$h(\ldots, 6)$
13	$f(\ldots, 12)$	**29**	$g(\ldots, 13)$	**45**	$h(\ldots, 9)$
14	$f(\ldots, 13)$	**30**	$g(\ldots, 2)$	**46**	$h(\ldots, 12)$
15	$f(\ldots, 14)$	**31**	$g(\ldots, 7)$	**47**	$h(\ldots, 15)$
16	$f(\ldots, 15)$	**32**	$g(\ldots, 12)$		

The attack

Stage 1: MITM

Pick M and IV with $B_0 = 0$,

1. store $(A_{29}, B_{29}, C_{29}, D_{29})$ for all 2^{32} C_0's (forward)
2. store $(A_{30}, B_{30}, C_{30}, D_{30})$ for all 2^{32} c C_{47}'s (backward)

Find entries such that

$$\begin{aligned} A_{30} &= D_{29} \\ D_{30} &= C_{29} \\ C_{30} &= B_{29} \end{aligned}$$

$\equiv$ 96-bit equality; 2^{64} choices $\Rightarrow$ repeat 2^{32} times

The attack

Stage 2: correction

Modify M_2 such that

$$B_{30} = g(A_{29}, B_{29}, C_{29}, D_{29}, \quad 2)$$

Modify C_0 accordingly

$\Rightarrow$ 96-bit preimage ($C_0 + C_{47}$ is random) with prob. 2^{-32}

Total cost: 2^{96} trials for a 128-bit preimage

Summary for MD5

Preimages for the compression function with

- chosen message except M_1 and M_2
- IV with $B_0 = 0$ and random C_0
- storage for 2^{36} bytes (64 Gb)
- $\mathbf{2^{96}}$ compressions

In comparison, bruteforce has

- random message
- chosen IV
- negligible memory
- $\mathbf{2^{128}}$ compressions

HAVAL

- 1992: publication (Zheng, Pieprzyk, Seberry)
- 2003: **collision** attack (3-pass)
- 2006: **collision** attack (4- and 5-pass)
- 2008: (partial) **second-preimage** attack (3-pass)

Similar to MD5 with

- 256-bit chain values
- 1024-bit blocks
- 3, 4, or 5 rounds

Preimages for 3-pass HAVAL

Same strategy as for MD5

- identify **absorption** properties in the initial steps
- MITM
- modify a M_i to complete the MITM
- correct initial steps

$\Rightarrow$ 2 attacks in $\mathbf{2^{224}}$ and storage of $\mathbf{2^{69}}$ bytes

(vs. 2^{256} and negligible memory)

Extension to the iterated hash

Attacks presented for the compression function
(with IV partially random, no padding)

Restrictions for the hash function:

- **padding**: not a problem, because message chosen
- **fixed IV**: makes direct application impossible

Iterated hash: basic MITM

Given image **H**:

1. compute a **list of images** from the fixed IV

$$(M_i, \text{compress}(\text{IV}, M_i))_i$$

2. compute a **list of preimages**

$$(H_i, M_i')_i,\ \text{compress}(H_i, M_i') = \mathbf{H}$$

Find entries such that

$$\text{compress}(\text{IV}, M_i)) = H_j$$

Cost: 2^{113} trials + 2^{36} bytes for MD5, 2^{241} + 2^{69} for HAVAL

Iterated hash: tree technique

Mendel & Rijmen (ICISC'07), Leurent (FSE'08)

Build a tree using **multi-target preimages**

Cost: 2^{102} trials + 2^{39} bytes for MD5, 2^{230} + 2^{71} for HAVAL

Conclusion

	trials	bytes
47-step MD5	2^{102}	2^{39}
3-pass HAVAL	2^{230}	2^{71}

First preimage attack for **original** reduced MD5

First preimage attacks for the HAVAL family

Questions?

Are the attacks effectively faster than bruteforce?
$\rightarrow$ Arguably yes (but not 2^{26} times faster)

Same strategy applies to MD4?
$\rightarrow$ No (because no M_i at very start and very end)

Same strategy applies to SHA-0/1/2?
$\rightarrow$ No (nontrivial message expansion)