# Collision Search Attack for 53-Step HAS-160

Hong-Su Cho[1], Sangwoo Park[2],
Soo Hak Sung[3], and Aaram Yun[2]

[1] Grad. School of Information Security, Korea Univ.
[2] National Security Research Institute (NSRI), Korea
[3] Dept. of Computing Information & Mathematics, Paichai Univ.

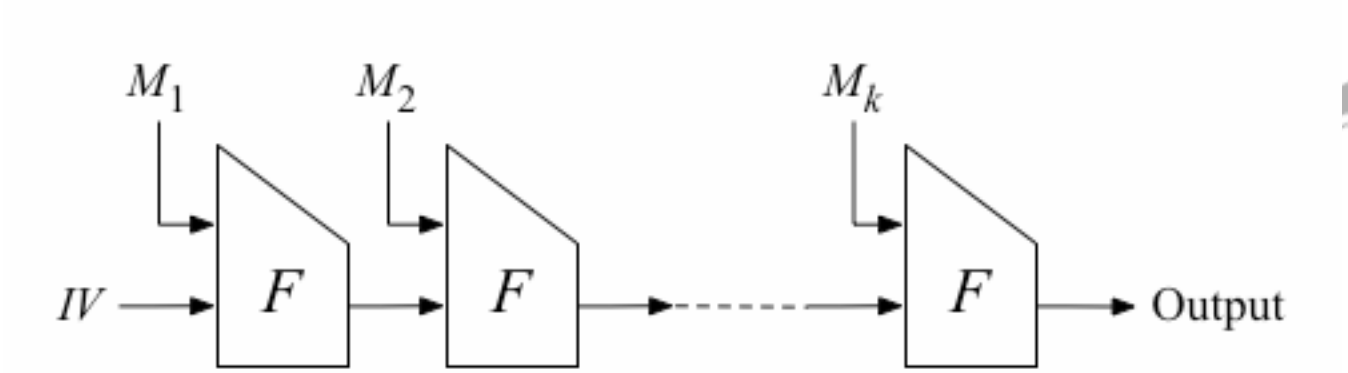
# Introduction

# HAS-160

- Cryptographic hash function widely in use in South Korea
  - Developed by Korean cryptographers (Chae Hoon Lim et al.)
  - Is a Korean industry standard
  - Is part of KCDSA signature scheme
    - Is being used daily by everybody in Korean internet commerce

# HAS-160

- Uses the Merkle-Damgård construction
  - First design a ‘composition function’, then iterate



# HAS-160

- Overall characteristics
  - Message block size: 512 bits
  - Internal state size: 160 bits
  - Compression function consists of 80 steps
  - 1 round = 20 steps
    - (4 rounds in total)
  - So far, essentially the same as SHA-1
    (We'll be back to the description soon)

# Previous attack on HAS-160

- Yun et al., *Finding Collision on 45-Step HAS-160*, ICISC 2005
  - Collision attack for the first 45-step version of HAS-160 (out of 80 steps in total)
  - Found collision pairs consisting of single message blocks (complexity: $2^{14}$)
  - An application of Xiaoyun Wang's techniques to HAS-160

# Our work

- Extends the 45-step result of ICISC 2005 to 53 steps
  - Similar techniques are used
  - The differential path is now more complicated due to more message differences to deal with
  - The complexity: $2^{55}$ hash computations
    - Could be feasible but still difficult to carry out the actual search

# Mendel's attack

- Florian Mendel, *Colliding Message Pair for 53-Step HAS-160*, ePrint archive, 2006
  - Found an actual collision pair!
  - The attack complexity: $2^{35}$
  - Uses the identical differential path found by us, but finds a two-block collision pair by clever search strategy

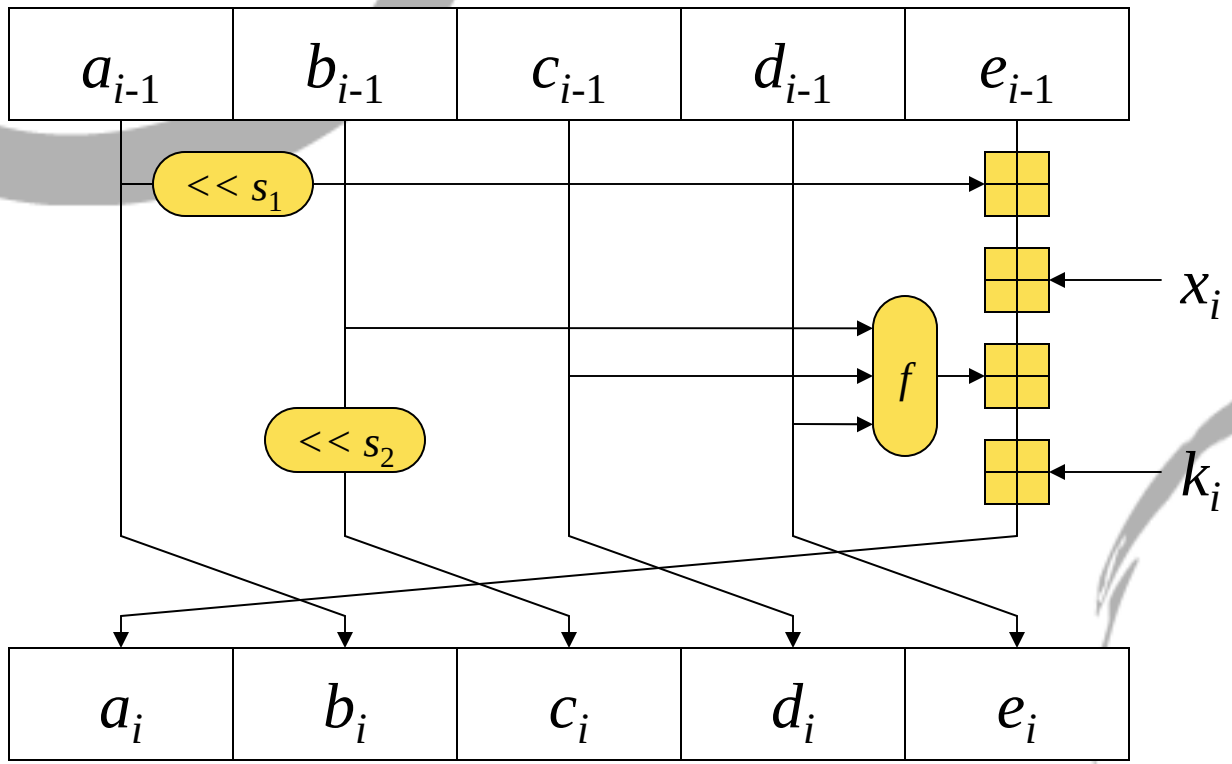
# Structure of HAS-160

# HAS-160

- Overall characteristics
  - Message block size: 512 bits
  - Internal state size: 160 bits
  - Compression function consists of 80 steps
  - 1 round = 20 steps
    - (4 rounds in total)
  - So far, essentially the same as SHA-1

# HAS-160

- State transformation (a step)



# HAS-160

- Boolean functions
  - Depends on the round, and same within each round

| Round | Boolean function |
|---|---|
| 1 | $(x \wedge y) \vee (\neg x \wedge z)$ |
| 2 | $x \oplus y \oplus z$ |
| 3 | $(x \vee \neg z) \oplus y$ |
| 4 | $x \oplus y \oplus z$ |

    - Same as the functions used in MD5
- Constants
  - Different for each step, not very important for us

# HAS-160

- Amounts of rotation
  - $s_1$ : different in each step, repeats at each round

| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $s_1$ | 5 | 11 | 7 | 15 | 6 | 13 | 8 | 14 | 7 | 12 | 9 | 11 | 8 | 15 | 6 | 12 | 9 | 14 | 5 | 13 |

  - $s_2$ : same within a round

| i | 1R | 2R | 3R | 4R |
|---|---|---|---|---|
| $s_2$ | 10 | 17 | 25 | 30 |

# HAS-160

- Message scheduling
  - 1 message block = 512 bits
    = sixteen 32-bit words $m_0$, $m_1$, …, $m_{15}$
  - HAS-160 = 4 rounds
  - 1 round = 20 steps
  - 1 step uses 1 message word
    - 4 more message words are needed
    - In each round, $m_{16}$, $m_{17}$, $m_{18}$, $m_{19}$ are defined as XOR of 4 other words

# HAS-160

- Message scheduling

| | $m_{16}$ | | | | | $m_{17}$ | | | | | $m_{18}$ | | | | | $m_{19}$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 1R | 18 | 0 | 1 | 2 | 3 | 19 | 4 | 5 | 6 | 7 | 16 | 8 | 9 | 10 | 11 | 17 | 12 | 13 | 14 | 15 |
| 2R | 18 | 3 | 6 | 9 | 12 | 19 | 15 | 2 | 5 | 8 | 16 | 11 | 14 | 1 | 4 | 17 | 7 | 10 | 13 | 0 |
| 3R | 18 | 12 | 5 | 14 | 7 | 19 | 0 | 9 | 2 | 11 | 16 | 4 | 13 | 6 | 15 | 17 | 8 | 1 | 10 | 3 |
| 4R | 18 | 7 | 2 | 13 | 8 | 19 | 3 | 14 | 9 | 4 | 16 | 15 | 10 | 5 | 0 | 17 | 11 | 6 | 1 | 12 |

- In 1st Round, $m_{16} = m_0 \oplus m_1 \oplus m_2 \oplus m_3$, …
- In 2nd Round, $m_{16} = m_3 \oplus m_6 \oplus m_9 \oplus m_{12}$, …

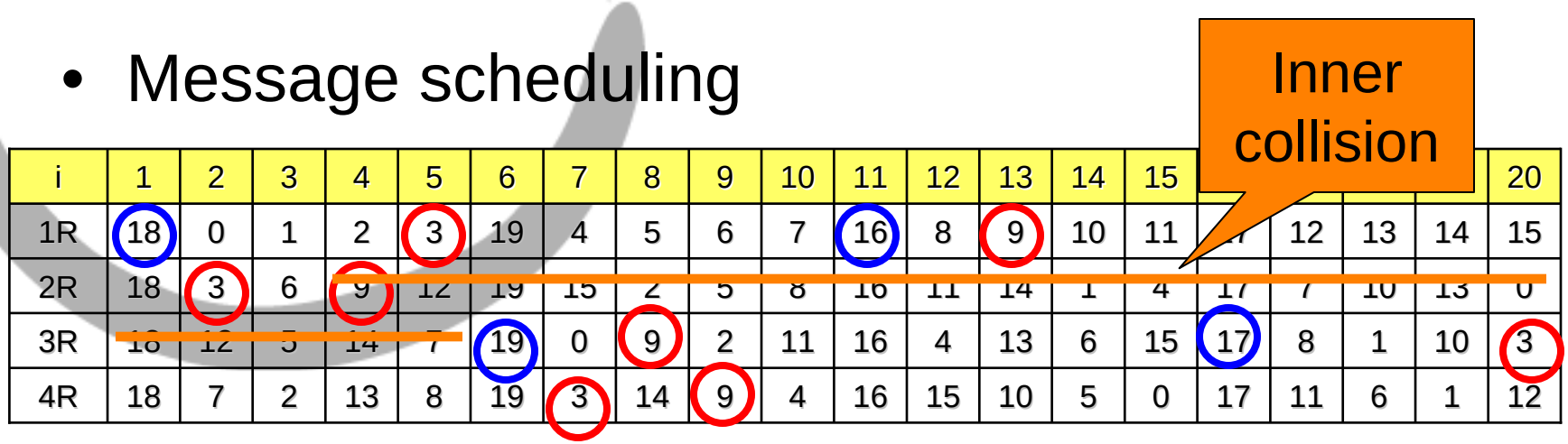
# Finding Differential Path

# Ideas

- Give message words $2^{31}$ differences (i.e., at the MSB)
  - Modular addition and XOR will behave identically
- Put message differences so that early inner collision is possible

# For 45-step collision path…

- Message scheduling

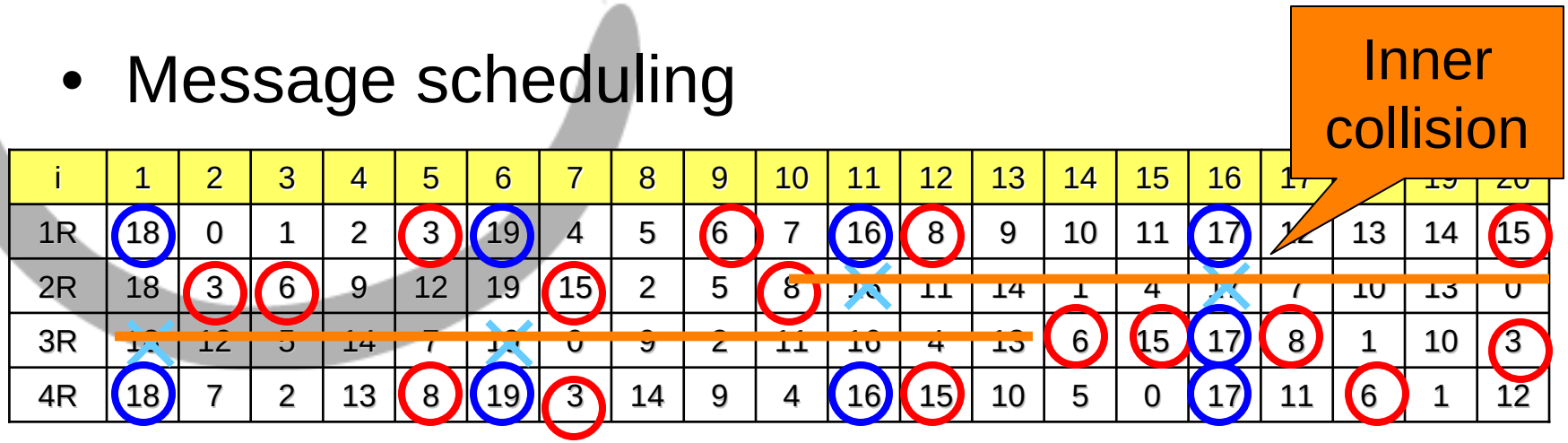



| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1R | 18 | 0 | 1 | 2 | 3 | 19 | 4 | 5 | 6 | 7 | 16 | 8 | 9 | 10 | 11 | [illegible] | 12 | 13 | 14 | 15 |
| 2R | 18 | 3 | 6 | 9 | 12 | 19 | 15 | 2 | 5 | 8 | 16 | 11 | 14 | 1 | 4 | 17 | 7 | 10 | 13 | 0 |
| 3R | 18 | 12 | 5 | 14 | 7 | 19 | 0 | 9 | 2 | 11 | 16 | 4 | 13 | 6 | 15 | 17 | 8 | 1 | 10 | 3 |
| 4R | 18 | 7 | 2 | 13 | 8 | 19 | 3 | 14 | 9 | 4 | 16 | 15 | 10 | 5 | 0 | 17 | 11 | 6 | 1 | 12 |

  - Give differences at $m_3$ and $m_9$
  - This could produce an inner collision at step 25 which extends to step 45.
  - $m_3$ and $m_9$ are chosen so that at Round 2 the difference for $m_{16}$ is cancelled

# For 53-step collision path…

- Message scheduling




| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1R | 18 | 0 | 1 | 2 | 3 | 19 | 4 | 5 | 6 | 7 | 16 | 8 | 9 | 10 | 11 | 17 | 12 | 13 | 14 | 15 |
| 2R | 18 | 3 | 6 | 9 | 12 | 19 | 15 | 2 | 5 | 8 | 1 | 11 | 14 | 1 | 4 | 7 | 7 | 10 | 13 | 0 |
| 3R | 12 | 12 | 5 | 14 | 7 | 16 | 0 | 9 | 2 | 11 | 10 | 4 | 13 | 6 | 15 | 17 | 8 | 1 | 10 | 3 |
| 4R | 18 | 7 | 2 | 13 | 8 | 19 | 3 | 14 | 9 | 4 | 16 | 15 | 10 | 5 | 0 | 17 | 11 | 6 | 1 | 12 |

- Give differences at $m_3$, $m_6$, $m_8$, and $m_{15}$
- This could produce an inner collision at step 30 which extends to step 53.

# Path for the whole HAS-160?

- Message scheduling

| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1R | 18 | 0 | 1 | 2 | 3 | 19 | 4 | 5 | 6 | 7 | 16 | 8 | 9 | 10 | 11 | 17 | 12 | 13 | 14 | 15 |
| 2R | 18 | 3 | 6 | 9 | 12 | 19 | 15 | 2 | 5 | 8 | 16 | 11 | 14 | 1 | 4 | 17 | 7 | 10 | 13 | 0 |
| 3R | 18 | 12 | 5 | 14 | 7 | 19 | 0 | 9 | 2 | 11 | 16 | 4 | 13 | 6 | 15 | 17 | 8 | 1 | 10 | 3 |
| 4R | 18 | 7 | 2 | 13 | 8 | 19 | 3 | 14 | 9 | 4 | 16 | 15 | 10 | 5 | 0 | 17 | 11 | 6 | 1 | 12 |

- So far, used only a few message word differences
- Tried to find an inner collision
- For the whole 80 steps, we will have to abandon this approach
- Some new ideas will be needed

# Our 53-step path

- We actually found such a differential path for the 53-step collision
- Uses 434 equations in total. Satisfaction probability: $2^{-434}$
- But we may use the message modification technique at Round 1 to enhance the probability

# Message modification

- Use the degree of freedom for the message to control the internal state of the hash function
- Slight problem: not all message words are independent

Dependent words

| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 1 | | | | | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1R | 18 | 0 | 1 | 2 | 3 | 19 | 4 | 5 | 6 | 7 | 1 | | | | | 17 | 12 | 13 | 14 | 15 |
| 2R | 18 | 3 | 6 | 9 | 12 | 19 | 15 | 2 | 5 | 8 | 16 | 11 | 14 | 1 | 4 | 17 | 7 | 10 | 13 | 0 |
| 3R | 18 | 12 | 5 | 14 | 7 | 19 | 0 | 9 | 2 | 11 | 16 | 4 | 13 | 6 | 15 | 17 | 8 | 1 | 10 | 3 |
| 4R | 18 | 7 | 2 | 13 | 8 | 19 | 3 | 14 | 9 | 4 | 16 | 15 | 10 | 5 | 0 | 17 | 11 | 6 | 1 | 12 |

# Redefine independent words

| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1R | 18 | 0 | 1 | 2 | 3 | 19 | 4 | 5 | 6 | 7 | 16 | 8 | 9 | 10 | 11 | 17 | 12 | 13 | 14 | 15 |
| 2R | 18 | 3 | 6 | 9 | 12 | 19 | 15 | 2 | 5 | 8 | 16 | 11 | 14 | 1 | 4 | 17 | 7 | 10 | 13 | 0 |
| 3R | 18 | 12 | 5 | 14 | 7 | 19 | 0 | 9 | 2 | 11 | 16 | 4 | 13 | 6 | 15 | 17 | 8 | 1 | 10 | 3 |
| 4R | 18 | 7 | 2 | 13 | 8 | 19 | 3 | 14 | 9 | 4 | 16 | 15 | 10 | 5 | 0 | 17 | 11 | 6 | 1 | 12 |

- In Round 1, $m_{18} = m_8 \oplus m_9 \oplus m_{10} \oplus m_{11}$
- Rewrite this as $m_{11} = m_{18} \oplus m_8 \oplus m_9 \oplus m_{10}$
- In Round 1, delay the appearance of dependent words as late as possible
- For independent words, use message modification. For dependent words, use probability

# Our collision search algorithm

- Using the differential path, and the message modification technique adapted to HAS-160, we found a collision search algorithm of complexity $2^{55}$
- Probably feasible by supercomputers?
- We haven’t found an actual collision pair

# Mendel’s attack

# Mendel's 2-block attack

- Florian Mendel found an actual collision pair for 53-step HAS-160
  - Only about a week after he read our paper!
  - Uses the same differential path we found
  - Instead of 1-block collision, he modified the attack to find 2-block collision pairs

# Mendel's 2-block attack

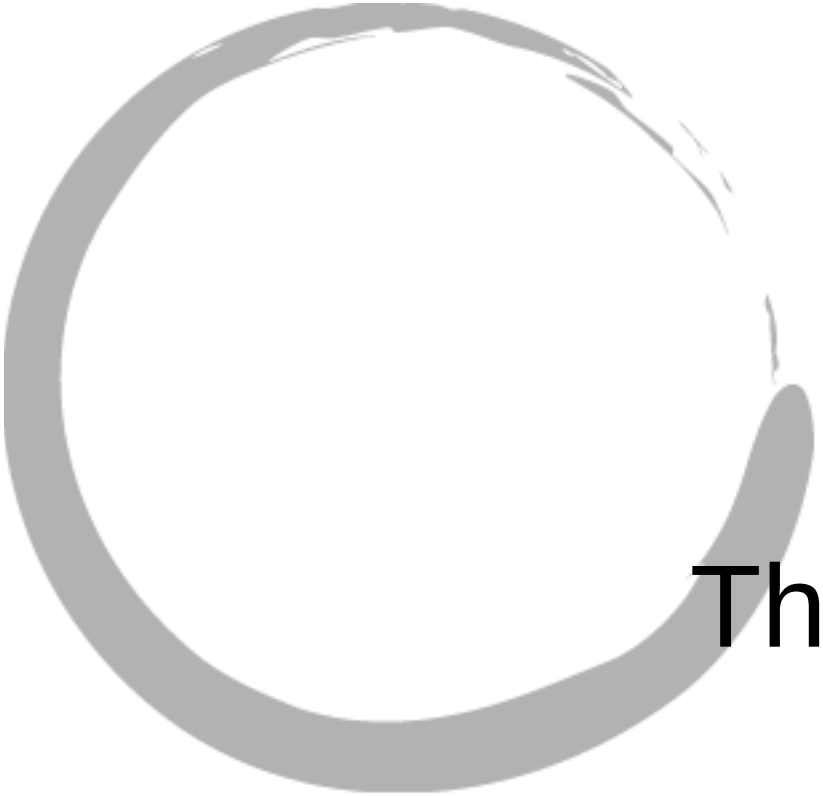
- (Very brief) outline of the attack
  - Modified the search strategy to enhance the probability for steps 1 to 16 (which was our bottleneck)
  - Had to randomize the IV
  - Therefore prepended an arbitrary message block to randomize the IV of the second block ➔ two-block collision pair
  - Complexity: Only $2^{35}$

# An actual collision pair

| | |
|---|---|
| $M_0$ | 34338ECF ED111A03 EB2EE891 763594E3 96080160 4558A929 EC731044 B7BADD0B<br>BC637C76 B21FA220 47493D4D B2AEAB79 A68354CF 5833D227 46DE18D7 F9FF5F3B |
| $M_1$ | 4E8F4717 D8E79F84 89D8FE81 **0**4B34CA7 01EA3C40 A364A502 **0**59F6AB9 22774031<br>**9**F3E80CE D647A926 1F61242A A1E224AB 901A5AEE 1BCEEEB1 EDEAA891 **3**1BDFF9A |
| $M'_1$ | 4E8F4717 D8E79F84 89D8FE81 **8**4B34CA7 01EA3C40 A364A502 **8**59F6AB9 22774031<br>**1**F3E80CE D647A926 1F61242A A1E224AB 901A5AEE 1BCEEEB1 EDEAA891 **B**1BDFF9A |
| H | 96D30020 DA815BDF DF265AB5 5B887F3E |

# Mendel's paper

- Florian Mendel, *Colliding Message Pair for 53-Step HAS-160*, Cryptology ePrint Archive, Report 2006/334, available at `http://eprint.iacr.org/2006/334`



Thank you