Preimage Attacks on 5-Pass HAVAL Reduced to 158 steps and One-Block 3-Pass HAVAL

Yasuhide Sakai [1], **Yu Sasaki [2]**, Lei Wang [1],

Kazuo Ota [1], and Kazuo Sakiyama [1]

1: The University of Electro-Communications

2: NTT Corporation

07/June/2011 ACNS2011

Research Summary

Cryptanalysis on 256-bit hash function HAVAL

- Best preimage attack on 5-pass HAVAL

	#steps (total 160)	Time	Memory
Previous	151	2^{241}	2^{64}
Ours	**158**	2^{254}	2^{41}

- Short (1-block) preimages on 3-pass HAVAL

	#steps (total 96)	Time	Memory	Length of Preimages
Previous	96 (full)	2^{225}	2^{64}	2 blocks
Ours	96 (full)	2^{244}	2^{15}	**1 block**

Contents

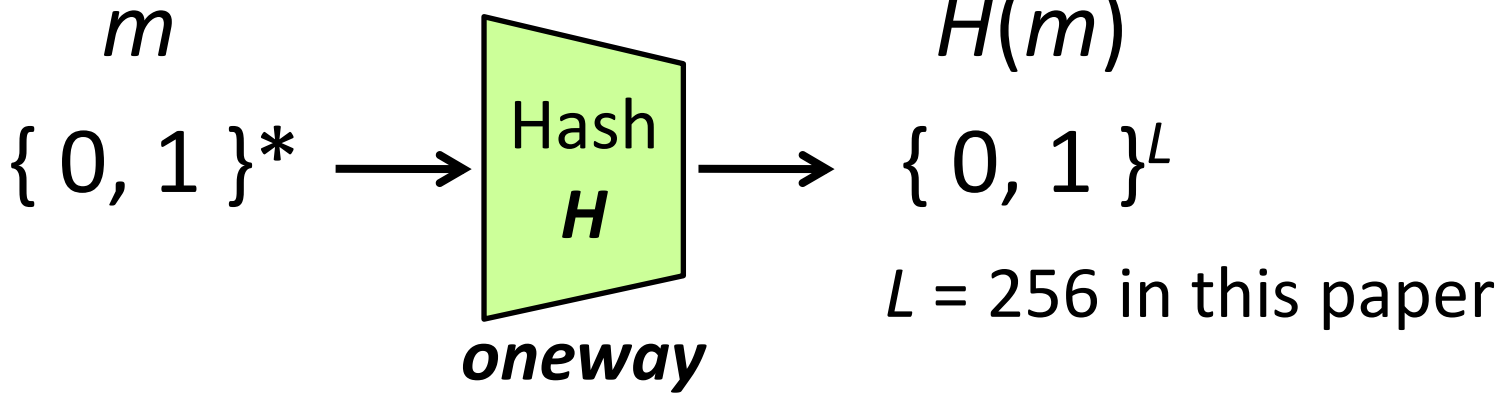
- Introduction
- Meet-in-the-middle preimage attack
- Attacks on HAVAL
- Conclusion

Contents

- Introduction
- Meet-in-the-middle preimage attack
- Attacks on HAVAL
- Conclusion

Hash Function

- Input: Messages of arbitrary length
- Output: Fixed size digest

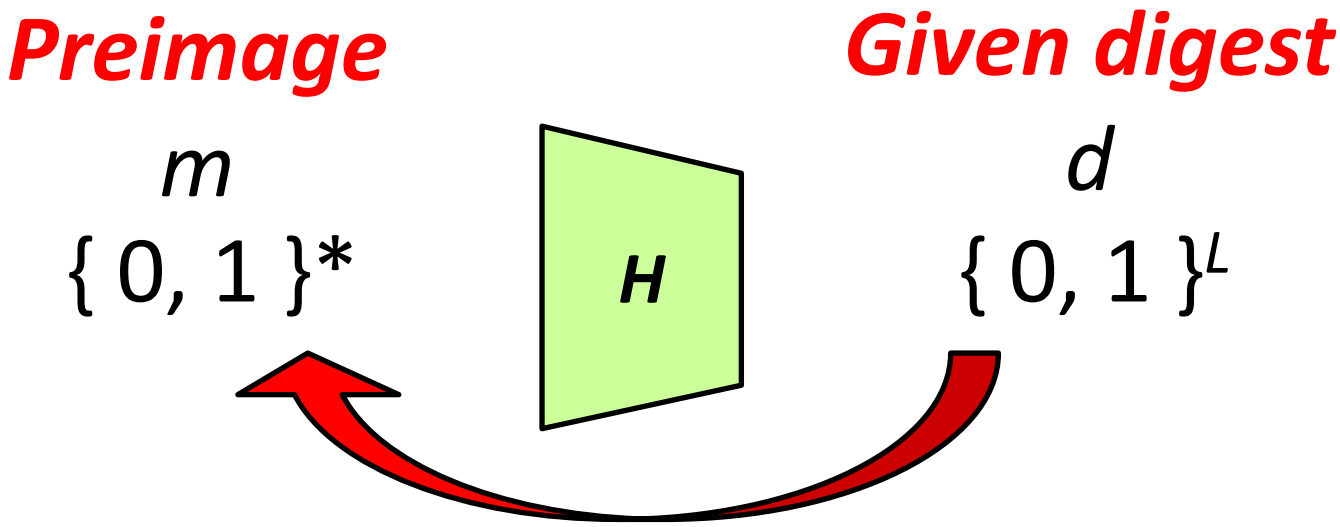


- Hash functions are oneway functions.

  Easy to compute the output from an input, but hard to find an input from the output.

Resistance against Preimage Attacks

- For a given digest d, m s.t. $H(m) = d$ is called preimage.

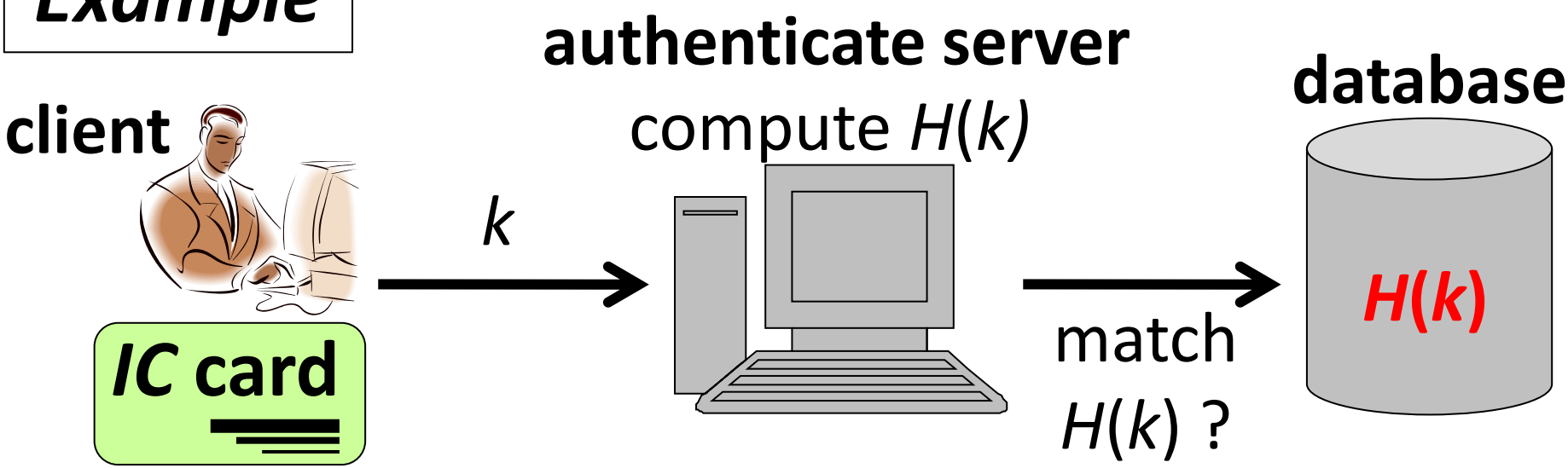


- Naïve search: randomly testing 2^L m.
- Securely designed hash functions must resist any preimage attack faster than 2^L comps.

Impact of Preimage Attacks (1/3)

- If preimage resistance is broken, almost all systems using hash functions become insecure.

Example

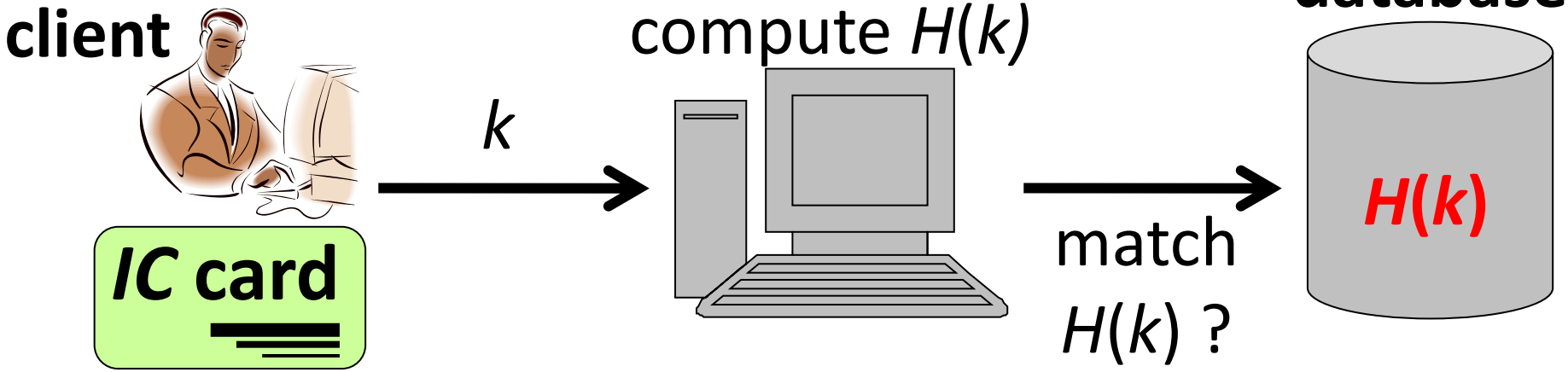


- $H(k)$ is stored to the database so that data leak of the database does not leak k.

Impact of Preimage Attacks (2/3)

- If preimage resistance is broken, almost all systems using hash functions become insecure.

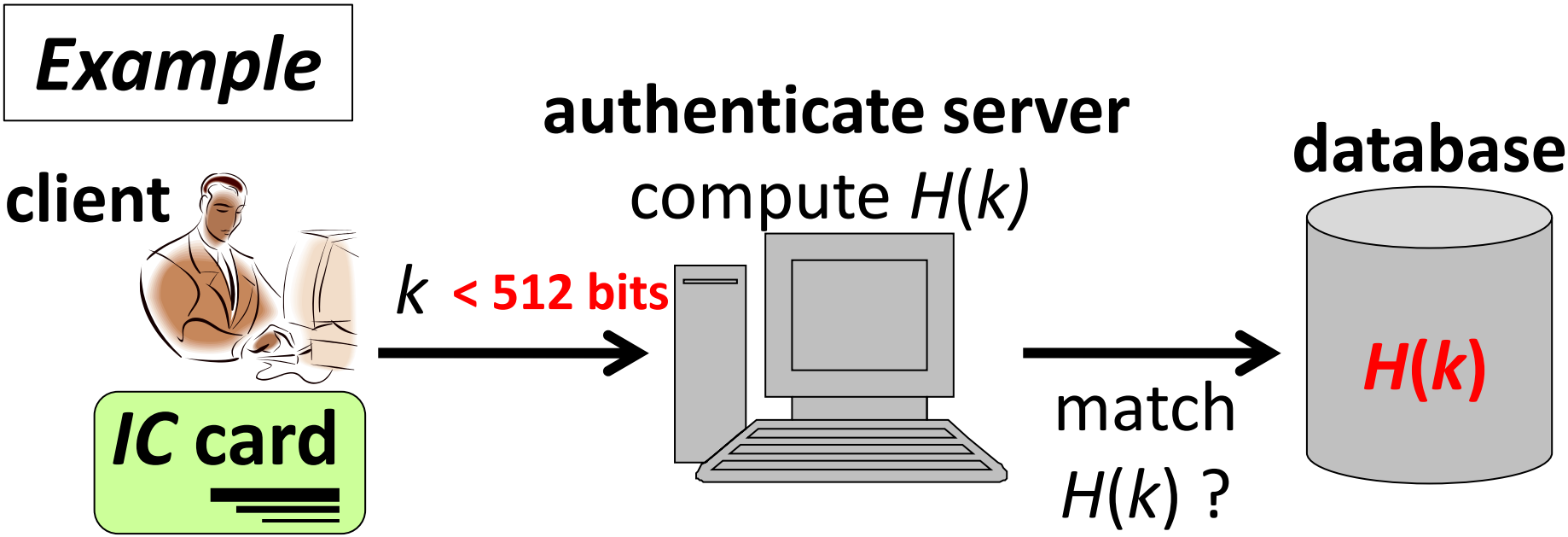
Example



- If H is not preimage resistance, k can be recovered from $H(k)$.

Impact of Preimage Attacks (3/3)

- In protocols in practice, the maximum bit length of k is often specified by the system, say 512 bits.



- Only if generated preimages are enough short (< 512 bits), the system gets influenced.

Research Summary (agein)

Cryptanalysis on 256-bit hash function HAVAL

- Best preimage attack on 5-pass HAVAL

	#steps (total 160)	Time	Memory
Previous	151	2^{241}	2^{64}
Ours	**158**	2^{254}	2^{41}

- Short (1-block) preimages on 3-pass HAVAL

	#steps (total 96)	Time	Memory	Length of Preimages
Previous	96 (full)	2^{225}	2^{64}	2 blocks
Ours	96 (full)	2^{244}	2^{15}	**1 block**

Motivation of Analyzing HAVAL

Give some feedback to the hash function design by studying existing hash functions more deeply.

	old design: MD4 based structure	new design (SHA-3): various types
Collision resistance		
Preimage resistance		

Motivation of Analyzing HAVAL

Give some feedback to the hash function design by studying existing hash functions more deeply.

	old design: MD4 based structure	new design (SHA-3): various types
Collision resistance	by Prof. Wang	under discussion in the SHA3 competition
Preimage resistance	**Our target** →	

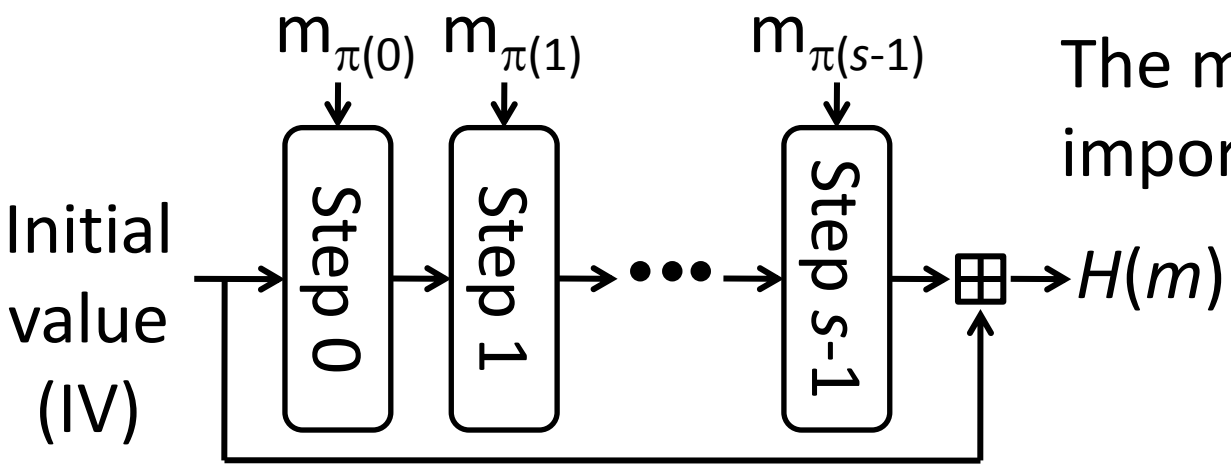
Contents

- Introduction
- Meet-in-the-middle preimage attack
- Attacks on HAVAL
- Conclusion

Meet-in-the-Middle (MitM) Preimage Attack

- The framework of the MitM preimage attack was proposed by Aoki and Sasaki at SAC08.
- It works well for a class of hash functions (MD4 based structure).

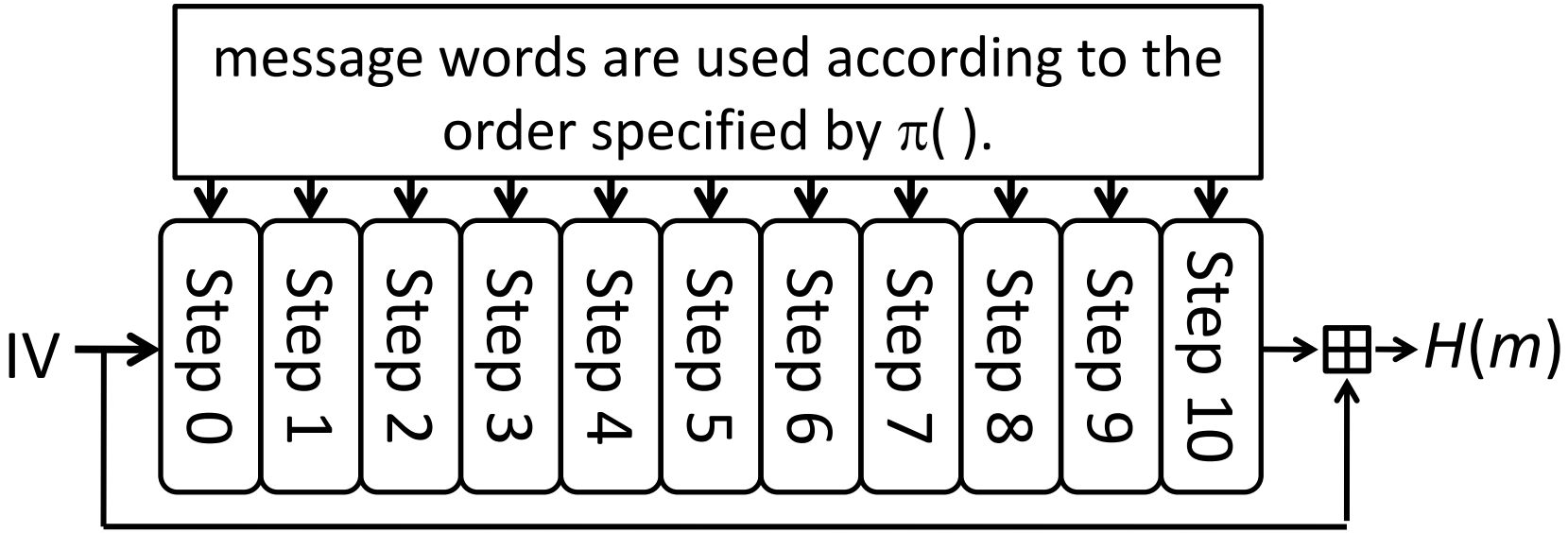
Input message: $m = (m_0||m_1|| \ldots m_{w-2}||m_{w-1})$



The message order $\pi(\ )$ is important for this attack.

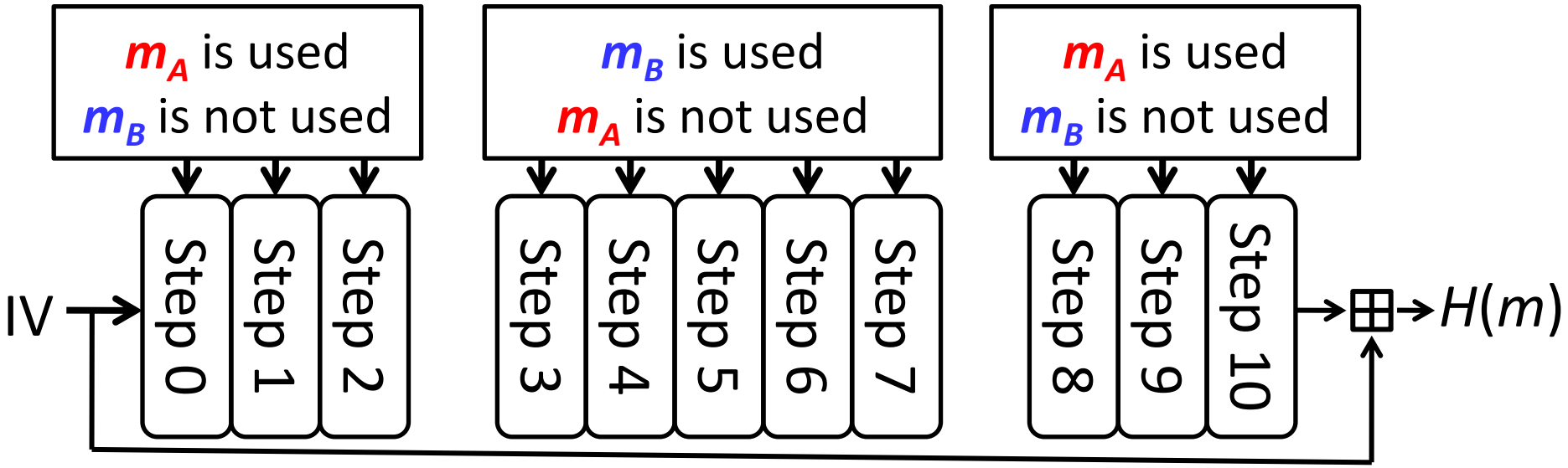
Basic Attack Framework

- Separate the target into inner part and outer part so that both parts can be computed independently.



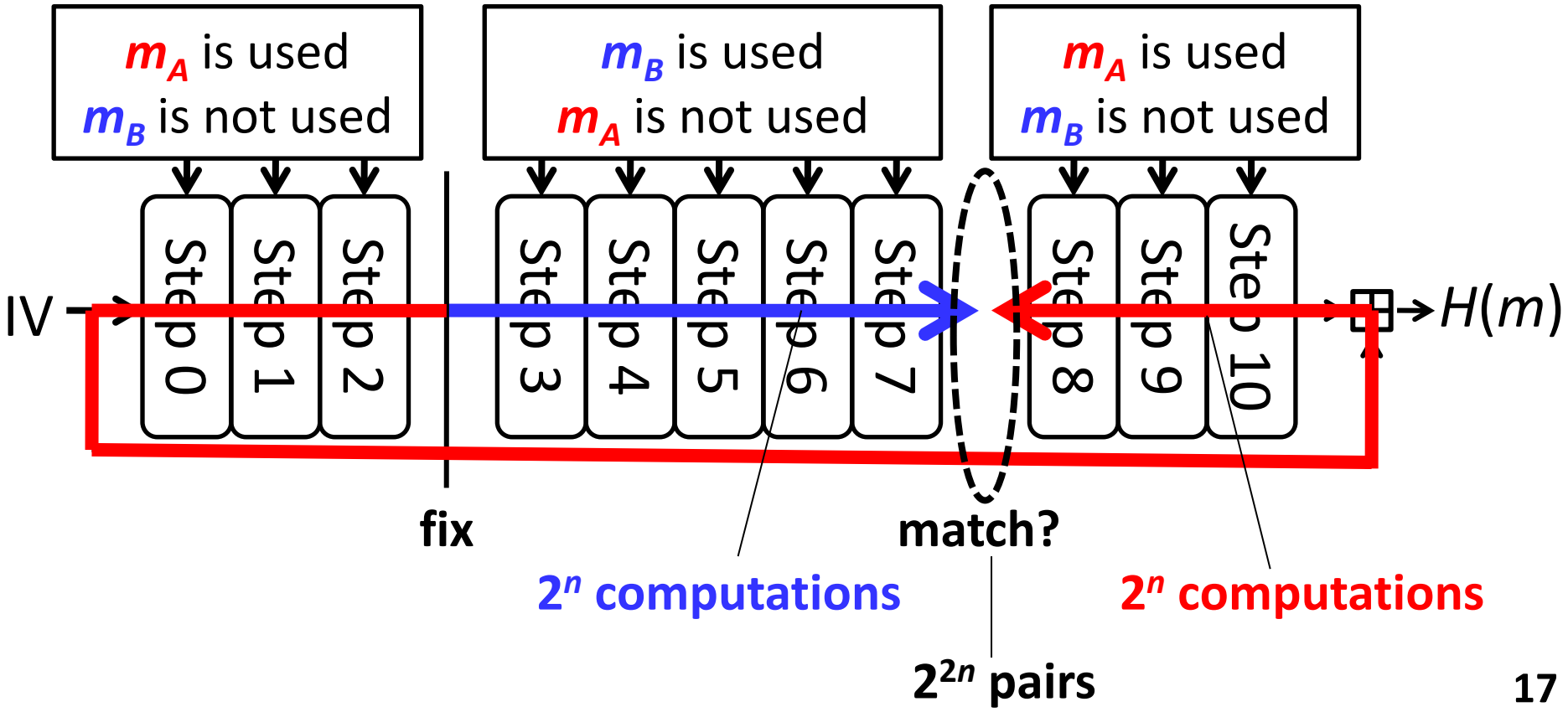
Basic Attack Framework

- Separate the target into inner part and outer part so that both parts can be computed independently.



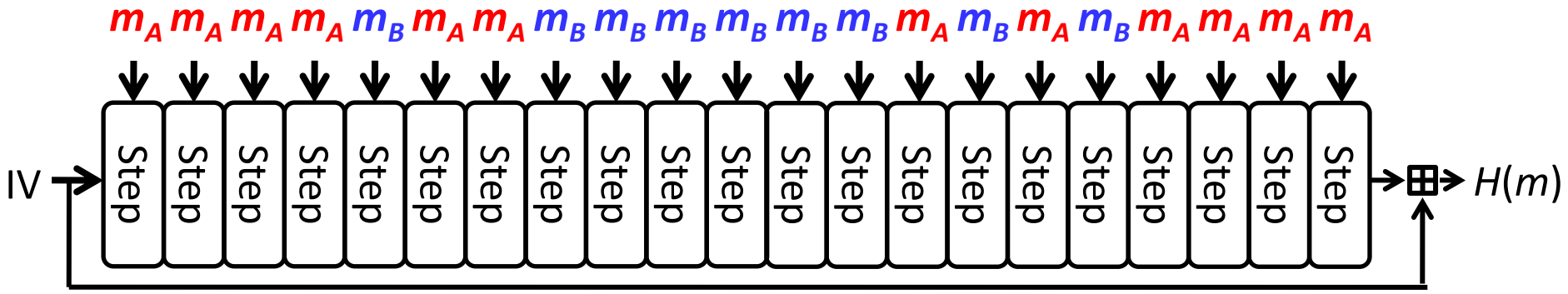
Basic Attack Framework

- Separate the target into inner part and outer part so that both parts can be computed independently.
- Assume the size of m_w is n bits.



Attack Extension

- Several improved techniques were proposed.



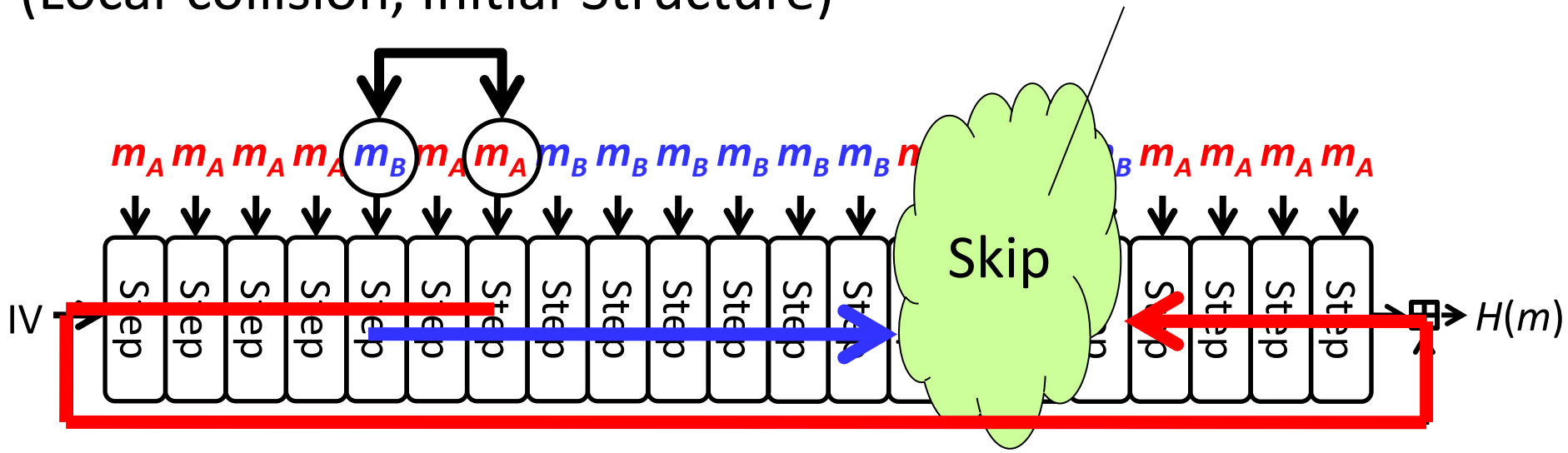
Attack Extension

- Several improved techniques were proposed.

Our Focus

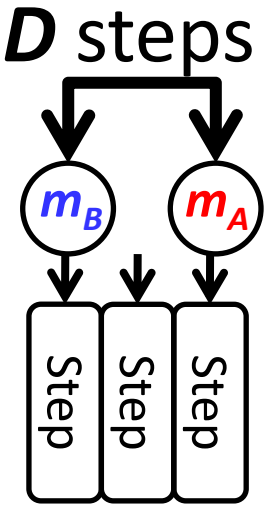
Exchange message positions
(Local-collision, Initial-Structure)

Ignore message words
for several steps.
(Partial-match *etc*.)



Local-Collision v.s. Initial-Structure

Both are techniques for exchanging message words *D* steps away



- Local-collision (previously used)
  - Advantage: *D* can be big
  - Disadvantage: possible values of *D* is limited
- Initial-Structure
  - Advantage: *D* can be any within a range
  - Disadvantage: the maximum *D* is limited

Contents

- Introduction
- Meet-in-the-middle preimage attack
- Attacks on HAVAL
- Conclusion

HAVAL

- HAVAL was proposed by Zheng *et al*. in 1992.
- 7 options for digest size. (We attack 256 bits.)
- 3 oprions for the number of rounds
  - 3-pass HAVAL: 3 rounds, 96 steps
  - 4-pass HAVAL: 4 rounds, 128 steps
  - 5-pass HAVAL: 5 rounds, 160 steps
- Input message: $m_0||m_1||,\ldots,m_{31}$
- The message order $\pi(\ )$ is defined in the specification.

Comparison of Previous Attacks and Ours

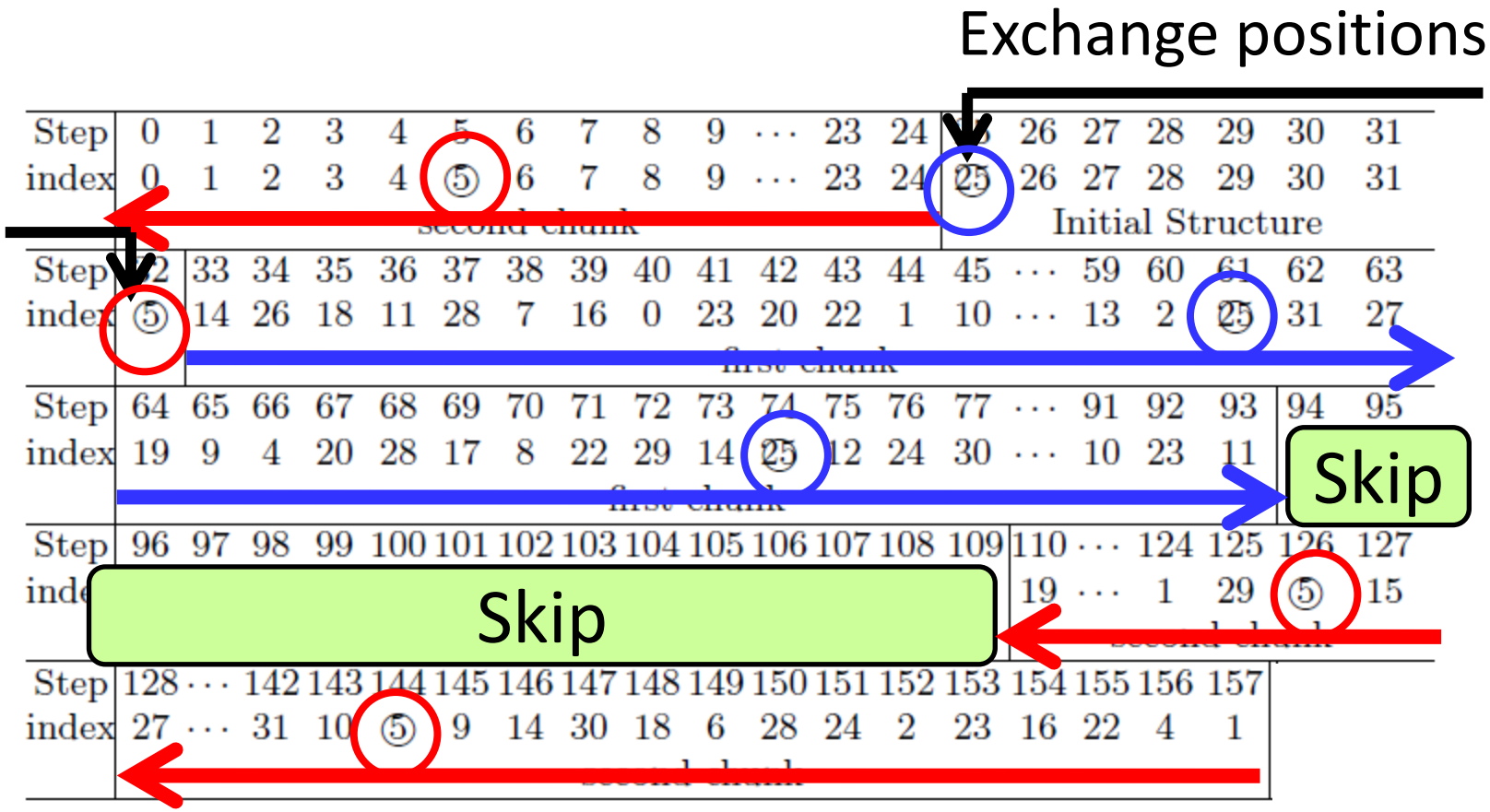
5-Pass HAVAL

	#steps (total 160)	Length of Preimages	Approach
Previous	151	2-blocks	Local-collision
Ours	**158**	2-blocks	Initial-structure

3-Pass HAVAL

	#steps (total 96)	Length of Preimages	Approach
Previous	96	2-blocks	Standard MitM
Ours	96	**1-block**	Based on [SAC08]

158-Step Attack on 5-Pass HAVAL

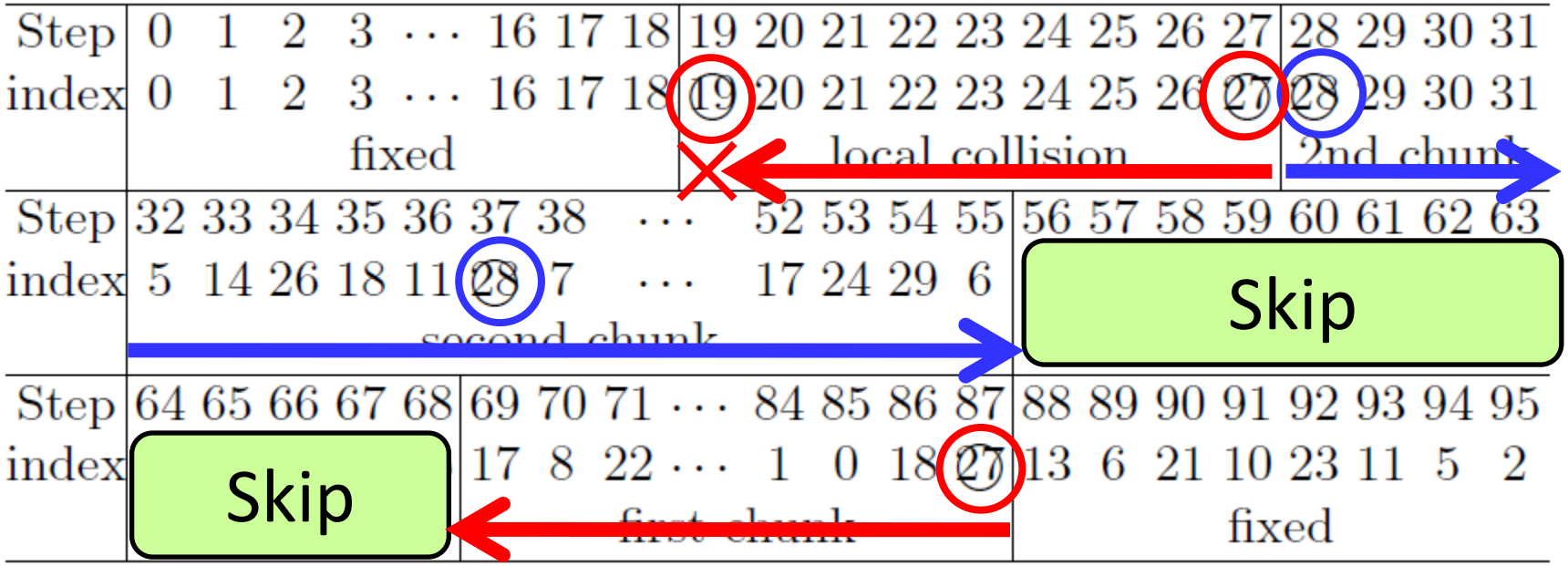


Refer to the paper for the construction of initial-structure.

Time complexity: 2^{254} Memory complexity: 2^{41}

1-Block Preimages for 3-Pass HAVAL

- Applied the technique against MD4 proposed by Aoki and Sasaki. (Refer to the paper for details.)



Time complexity: 2^{244}

Memory complexity: 2^{15}

Generated preimages:

Only 1-block

Contents

- Introduction
- Meet-in-the-middle preimage attack
- Attacks on HAVAL
- Conclusion

Conclusions

- Improved preimage attacks on HAVAL were presented.
- 5-Pass HAVAL
  - We used initial-structure instead of local-collision.
  - The number of attacked steps: 151 → 158
- 3-Pass HAVAL
  - Shorter preimages came to be generated.

Thank you for your attention !!