NTT

A Survey of Recent Cryptanalysis on Hash Functions

Yu Sasaki

NTT Corporation

30/Aug./2011 ASK 2011@NTU

NTT

Boomerang Distinguishers on MD4-Based Hash Functions: First Practical Results on Full 5-Pass HAVAL

Yu Sasaki

NTT Corporation

30/Aug./2011 ASK 2011@NTU

NTT

Summary

- Boomerang 4-sum distinguisher on the compression function of MD4-based structure.
- Point out previous boomerang attack on internal 5-pass HAVAL contains a critical flaw.
- First practical results on 5-pass HAVAL.

NTT

Comparison of Attack Results

Attack	Target	MD4	MD5	HAVAL 3-pass	HAVAL 4-pass	HAVAL 5-pass
Collision	Hash	2	2^{8}	2^{7}	2^{36}	2^{123}
Boomerang	BC	2^{6}	$2^{11.6}$	-	$2^{9.6}$	2^{61}
Boomerang	CF	-	**2^{10}**	**2^{4}**	**2^{11}**	**2^{11}**

NTT

Contents

- Introduction
- HAVAL specification
- Attack framework of boomerang 4-sum
- Application to 5-pass HAVAL
- Conclusion

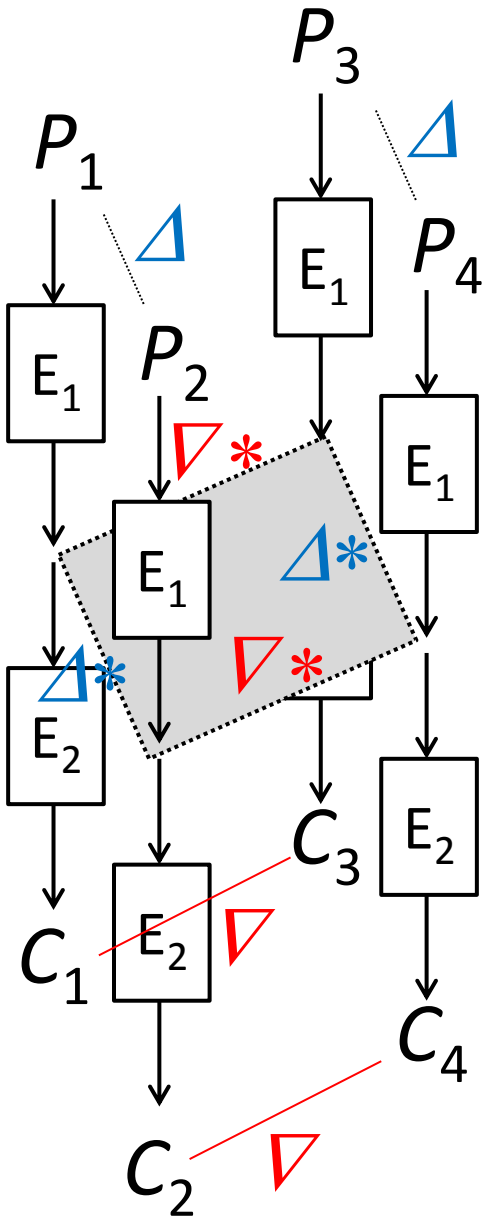
NTT

Motivation

- Recently, various cryptanalytic techniques have been developed on hash functions.
- Construction of the 4-sum distinguisher based on the boomerang attacks was proposed in 2011. [BNR11, LM11]
- Revisit the security of the MD4-based structure against these attacks.

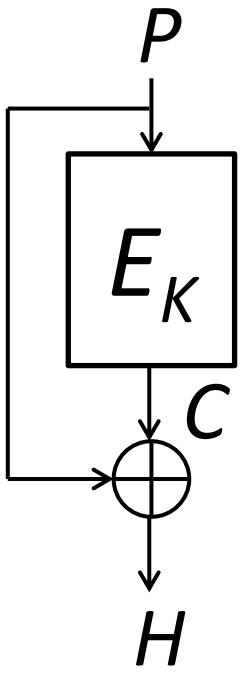
Boomerang Attack

- Proposed by Wagner.
- Assume
  - $\Pr[E_1(\Delta \rightarrow \Delta^*)] = p$
  - $\Pr[E_2(\nabla^* \rightarrow \nabla)] = q$
- Entire differential probability is p^2q^2.



Compression with Block-Ciphers

- Compression function can be constructed based on block-ciphers.
- E.g. 12 secure PGV construction
- Can we exploit boomerang differential paths for block-ciphers?



Boomerang Distinguisher on Hash

- 4-sum can be constructed against the compression function with a boomerang differential for the internal cipher.

Boomerang Attack:

$$P_1 \oplus P_2 = \Delta, P_3 \oplus P_4 = \Delta,$$
$$C_1 \oplus C_2 = \nabla, C_3 \oplus C_4 = \nabla.$$

4-sum on compression function :

$$H_1 \oplus H_2 \oplus H_3 \oplus H_4$$
$$= P_1 \oplus P_2 \oplus P_3 \oplus P_4 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4$$
$$= \Delta \oplus \Delta \oplus \nabla \oplus \nabla = 0$$

NTT

Boomerang Distinguisher on Hash

- k-sum problem:

  Finding k different inputs whose XOR-sum is 0.

- zero-sum problem:

  Finding a set of inputs which the XOR-sum is 0, and XOR-sum of the corresponding outputs is 0.

Boomerang Distinguisher on Hash

- 4-sum can be constructed against the compression function with a boomerang differential for the internal cipher.

Boomerang Attack:

$$P_1 \oplus P_2 = \Delta, P_3 \oplus P_4 = \Delta,$$
$$C_1 \oplus C_2 = \nabla, C_3 \oplus C_4 = \nabla.$$

4-sum on compression function :

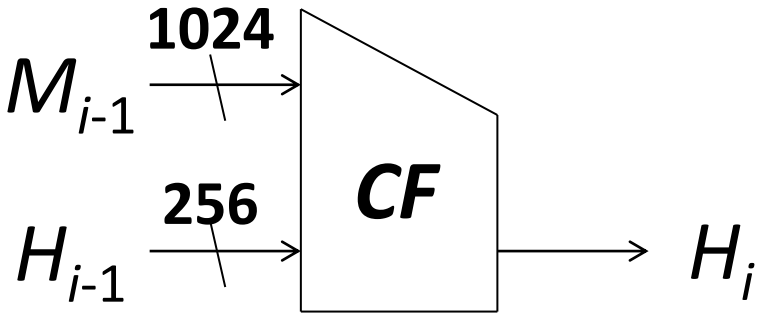
$$H_1 \oplus H_2 \oplus H_3 \oplus H_4$$
$$= P_1 \oplus P_2 \oplus P_3 \oplus P_4 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4$$
$$= \Delta \oplus \Delta \oplus \nabla \oplus \nabla = 0$$

NTT

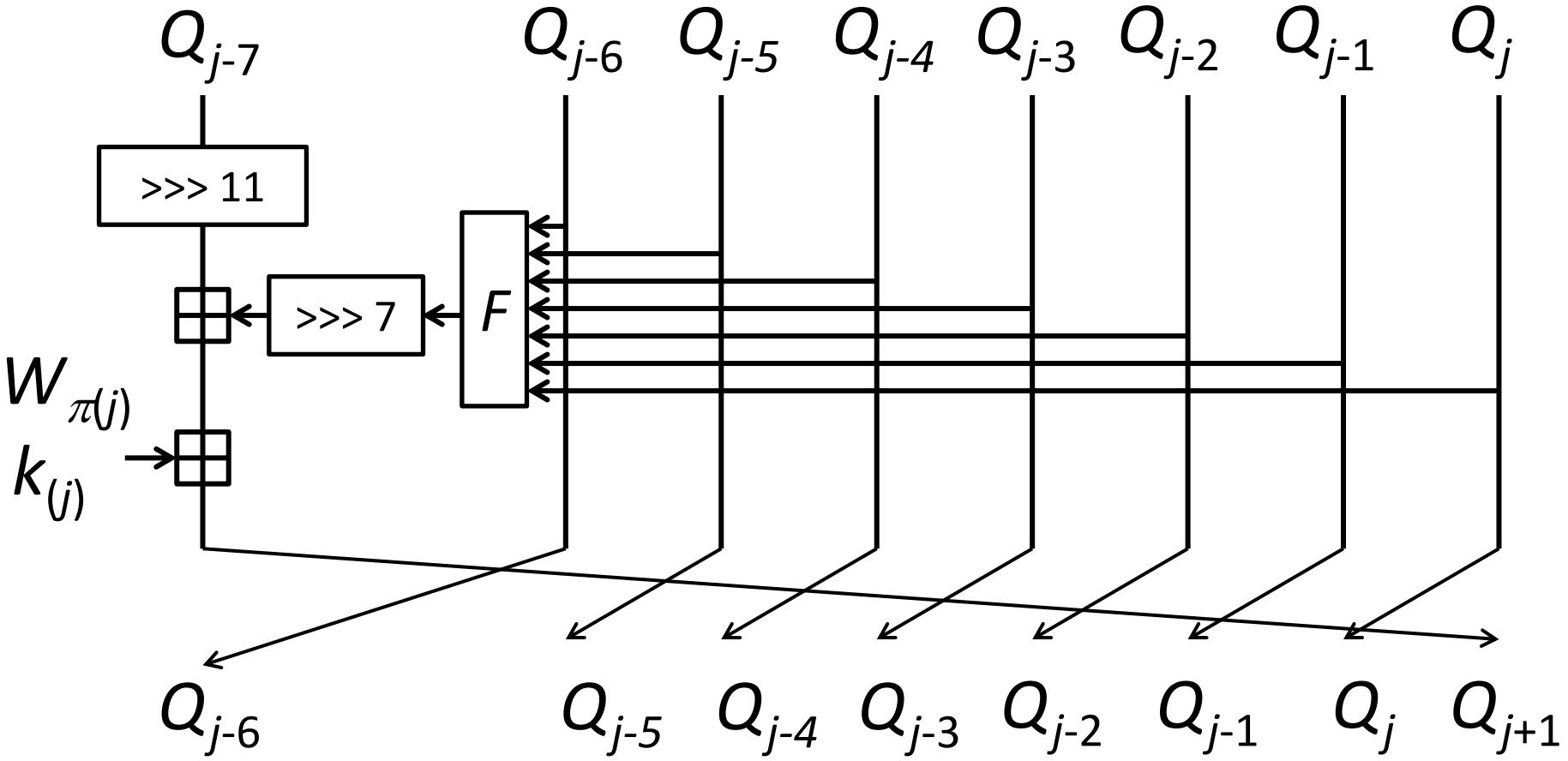
Introduction of HAVAL

Hash Function HAVAL

- Proposed by Zheng et al. in 1992.
- MD4-based structure
- 256-bit output
- 3 versions for different security level
  - 3-pass, 4-pass, 5-pass (160 steps for 5-pass)
- Number of steps: 32X steps for X-pass



HAVAL Step Function



HAVAL Message Schedule

- 32 message words in each round.
- Each word is used exactly once in each round.
- The order of message words changes in different rounds.

index for each round																															
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
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
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
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
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

Previous Analyses on 5-Pass HAVAL

- Theoretical collision attack was proposed at FSE2006 [YWY+06]: 2^{123}
- Preimage attack on 158 steps was proposed at ACNS2011 [SSW+11]: 2^{254}
- Related-key boomerang attack on internal cipher was proposed at ICICS2005 [KBP+05]: 2^{61}

➡ We show this includes a flaw.

No result within a practical complexity

Summary of Boomerang Distinguishers on Hash Function

Collection of the knowledge distributed in several papers.

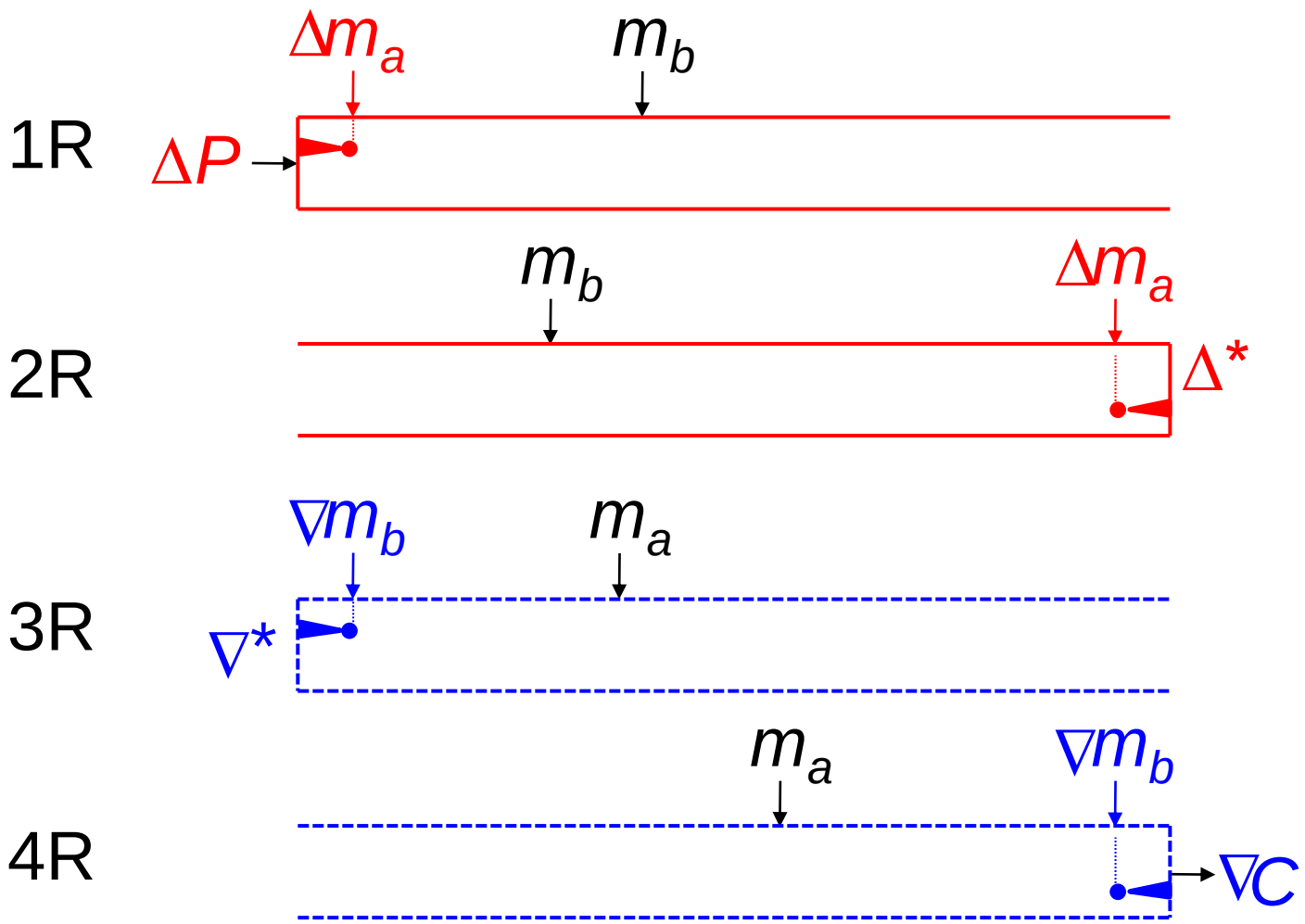
mainly from [BNR11, KBP+05, LM11]

NTT

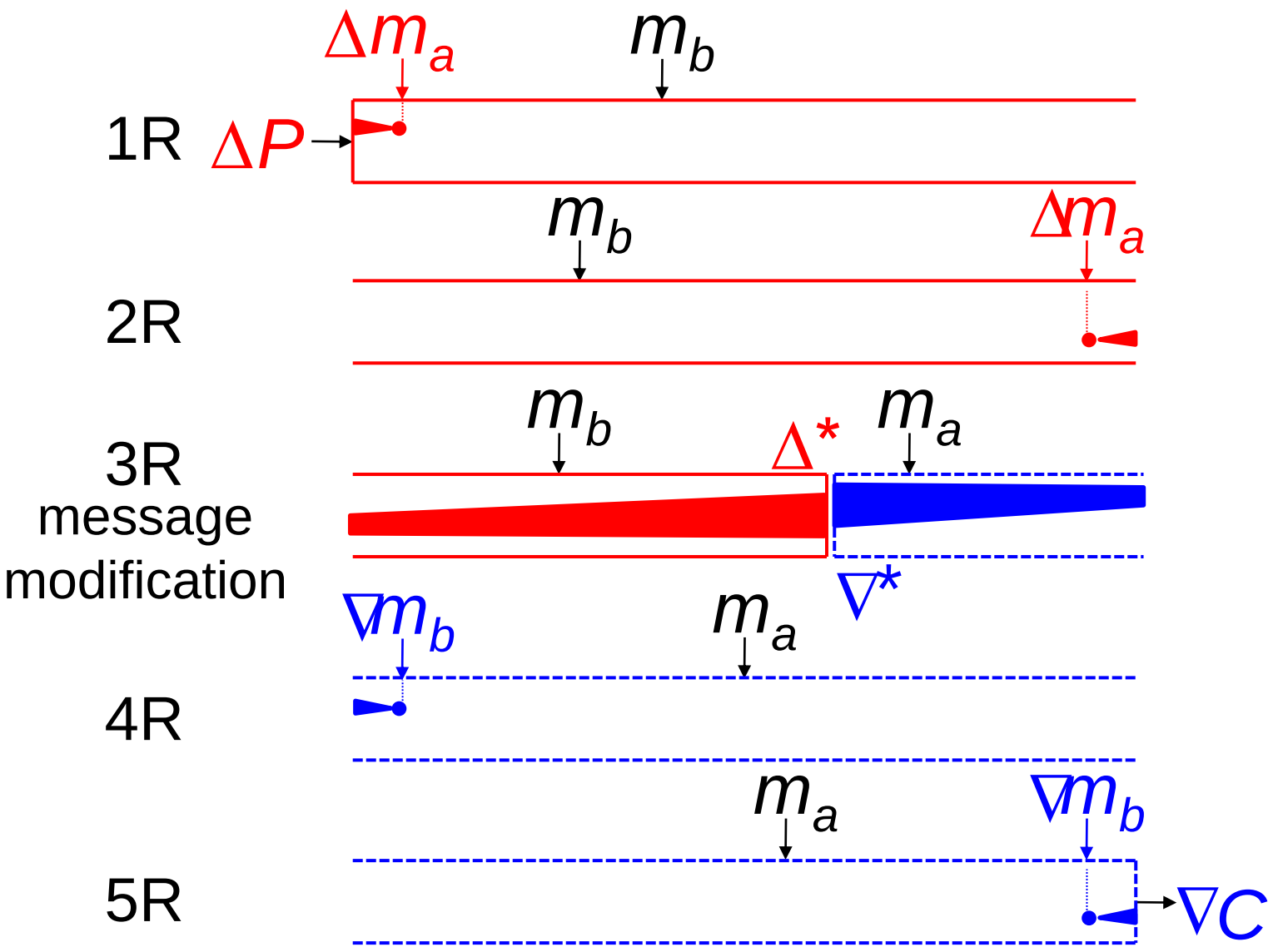
Procedure of Boomerang Distinguisher

1. Message Differences (ΔM)
2. Differential Paths and Sufficient Conditions (*DP*)
3. Contradiction between Two Paths (*CP*)
4. Message Modification (*MM*)
5. Amplified Probability (*AP*)

ΔM for 4-Round (MD5, 4-HAVAL)



ΔM for 5-Round (5-HAVAL)



Contradiction of Two Paths

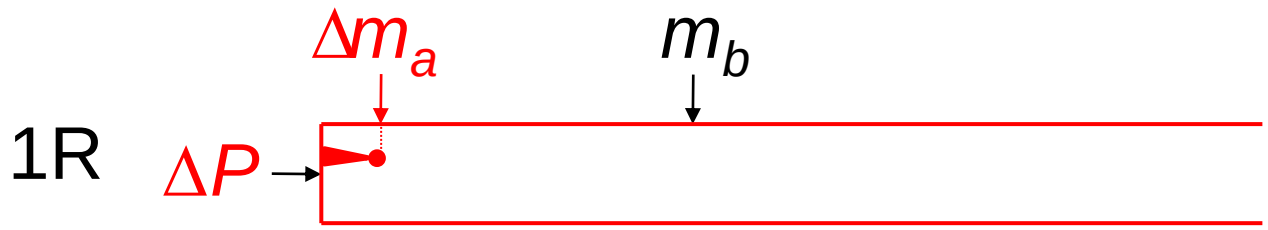
- In 2009, Murphy showed that two differential paths for E_1 and E_2 cannot be independent.

Condition 1. E_1 and E_2 do not require to fix the same bit to different value.

Condition 2. E_1 (resp. E_2) do not require to fix the active bit for E_2 (resp. E_1).

- Be careful on using diff. on MSB in two paths.
- If contradict, rotate one of paths will help.

Amplified Probability



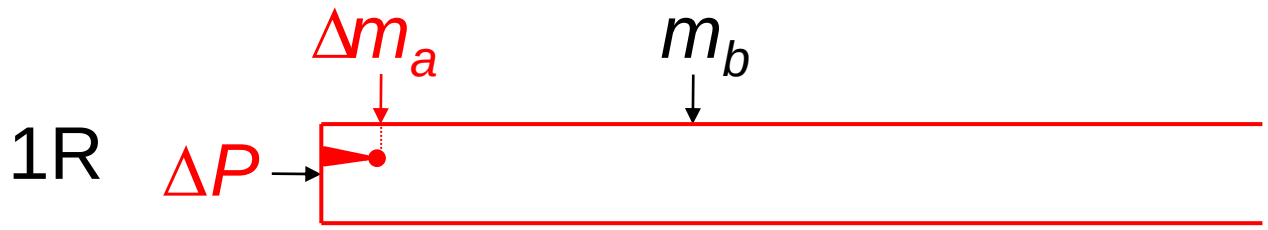
- Consider the differential (all possible differential paths) for the randomly satisfied part.
- Diff. probability is computed by experiment.

1. Randomly choose internal state and message value.

2. Make a message quartet with pre-determined ΔM.

3. Iterate sufficiently to compute the probability.

Amplified Probability



- Consider the differential (all possible differential paths) for the randomly satisfied part.
- Diff. probability is computed by experiment.

1. Randomly choose internal state and message value.

2. Make a message quartet with pre-determined ΔM.

3. Iterate sufficiently to compute the probability.

NTT

Quiz

- A differential
- Differentials
- Differential characteristic
- Differential characteristics
- Differential path
- Differential trail
- Multi-paths

Quiz

- A differential
- Differentials
- Differential characteristic
- Differential characteristics
- Differential path
- Differential trail
- Multi-paths

- 差分特性
- 差分特性
- 差分パス
- 多重パス

NTT

Practical Attack on 5-Pass HAVAL

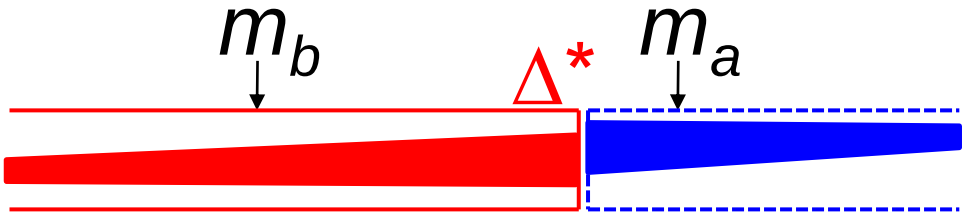
1. Proving a flaw of previous work
2. New attack on 5-pass HAVAL

ΔM for 5-Pass HAVAL

- First observed by [KBP+05]

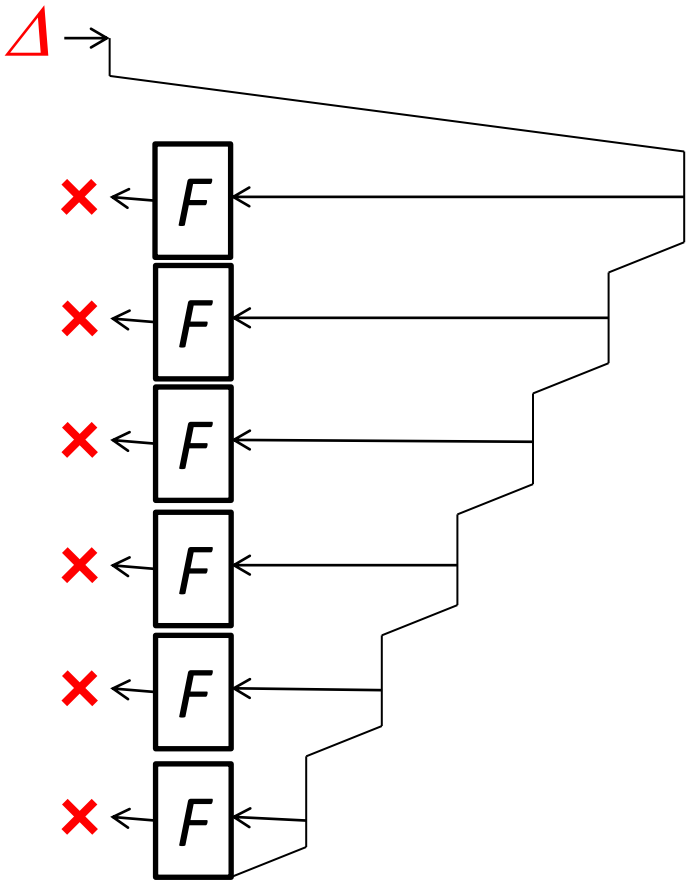
0	1	②	3	④	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
←	Δ															constant															
5	14	26	18	11	28	7	16	0	23	20	22	1	10	④	8	30	3	21	9	17	24	29	6	19	12	15	13	②	25	31	27
														constant														Δ	→		
19	9	④	20	28	17	8	22	29	14	25	12	24	30	16	26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

3R message modification



Flaw of Previous Work

- Previous work assumed that 1-bit local collision can be constructed in the 3rd round.



Conditions for the path

$$Q_{69} = 0$$
$$Q_{67}Q_{68} \oplus Q_{71} = 0 \leftarrow$$
$$Q_{68} = 0 \leftarrow$$
$$Q_{72}Q_{69} \oplus Q_{67} = 0$$
$$Q_{73} \oplus Q_{71} \oplus Q_{72}Q_{69} = 0$$
$$Q_{71} = 1 \leftarrow$$
$$Q_{73} = 0$$

Contradiction !!

NTT

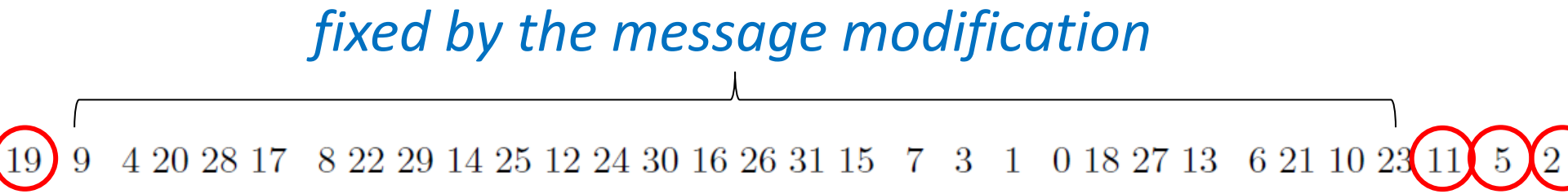
New Differential Path Construction

- Automated search for the differential propagation
  - Minimizing the total Hamming weight of chaining variables.

- By hand analysis for sufficient conditions and contradiction of two paths.

Message Modification

- Find a message quartet satisfying all conditions for the 3rd round.



- Still have message freedom in 4 words.
- Once you satisfy the 3rd round, you can iterate the remaining search $2^{32*4}=2^{128}$ times.
- Complexity for MM is free!

NTT

Experiments for Amplified Probability

- Carry out the random test to satisfy the differential path for the beginning and end.

Direction	Number of trials	Number of obtained 4-sums	Amplified probability
Back	1,000,000	53,065	$2^{-4.24}$
For	1,000,000	37,623	$2^{-4.73}$
Total	1,000,000	1,975	$2^{-8.98}$

- For the backward path, the best differential path has the success probability of 2^{-6}.
- $2^{1.76}$ improvement by the amplified probability.

4-Sum Example of 5-Pass HAVAL

H_i^1	0x6ad6913b 0x52831497 0x42e2afea 0x042171e8 0x05c66540 0xf6308a5d 0x69b242bb 0xfeadf2df
M_i^1	0x55f408ea 0xade29473 0x5cd48f01 0x862fac29 0xb59b9103 0xdfe1dff3 0x44aaff68 0xa5716cc8
	0xd9b3c72a 0x9d9907bb 0x263e9a6f 0x0d81dbdd 0x1a1d1f69 0x35a88db0 0xb50f50b3 0xcb85d403
	0xe2898bd5 0x3dc4e64c 0x48a696ae 0x1568e06b 0x286a00c5 0x236529bd 0x8bb673fd 0x481411ed
	0xb2117cb1 0xe6911e8d 0x5816e997 0x1a8fc1d3 0xc5dda128 0x43e5f428 0xcf1e861f 0xf5258b98
H_{i+1}^1	0x50b484bf 0x9d28c720 0xc2a5ab4d 0x5aec2d4b 0x63659cae 0x0023f316 0xa02276be 0xeab5fb84
H_i^2	0x6ad6913b 0x52831497 0x42e2afea 0x042171e8 0x05c66540 0xf6308e5d 0x69b242bb 0xfeae32df
M_i^2	0x55f408ea 0xade29473 0xdcd48f01 0x862fac29 0xb59b9103 0xdfe1dff3 0x44aaff68 0xa5716cc8
	0xd9b3c72a 0x9d9907bb 0x263e9a6f 0x0d81dbdd 0x1a1d1f69 0x35a88db0 0xb50f50b3 0xcb85d403
	0xe2898bd5 0x3dc4e64c 0x48a696ae 0x1568e06b 0x286a00c5 0x236529bd 0x8bb673fd 0x481411ed
	0xb2117cb1 0xe6911e8d 0x5816e997 0x1a8fc1d3 0xc5dda128 0x43e5f428 0xcf1e861f 0xf5258b98
H_{i+1}^2	0xfa15769c 0x6ed1b19a 0x405b263b 0x57cd6359 0xd8688750 0xcdc3c9d3 0xa3dc7fd8 0x2e59f283
H_i^3	0xb70b5251 0x851d041a 0x7a5f5fad 0x98626bb1 0x9d739cbc 0x67bc3181 0xe48e4cac 0xeeb57f26
M_i^3	0x55f408ea 0xade29473 0x5cd48f01 0x862fac29 0x359b9103 0xdfe1dff3 0x44aaff68 0xa5716cc8
	0xd9b3c72a 0x9d9907bb 0x263e9a6f 0x0d81dbdd 0x1a1d1f69 0x35a88db0 0xb50f50b3 0xcb85d403
	0xe2898bd5 0x3dc4e64c 0x48a696ae 0x1568e06b 0x286a00c5 0x236529bd 0x8bb673fd 0x481411ed
	0xb2117cb1 0xe6911e8d 0x5816e997 0x1a8fc1d3 0xc5dda128 0x43e5f428 0xcf1e861f 0xf5258b98
H_{i+1}^3	0x9ce945d5 0xcfc2b6a3 0xfa225b10 0xef2d2714 0x7b12d42a 0x71af9a3a 0x1afe80af 0xdbbd87cb
H_i^4	0xb70b5251 0x851d041a 0x7a5f5fad 0x98626bb1 0x9d739cbc 0x67bc3581 0xe48e4cac 0xeeb5bf26
M_i^4	0x55f408ea 0xade29473 0xdcd48f01 0x862fac29 0x359b9103 0xdfe1dff3 0x44aaff68 0xa5716cc8
	0xd9b3c72a 0x9d9907bb 0x263e9a6f 0x0d81dbdd 0x1a1d1f69 0x35a88db0 0xb50f50b3 0xcb85d403
	0xe2898bd5 0x3dc4e64c 0x48a696ae 0x1568e06b 0x286a00c5 0x236529bd 0x8bb673fd 0x481411ed
	0xb2117cb1 0xe6911e8d 0x5816e997 0x1a8fc1d3 0xc5dda128 0x43e5f428 0xcf1e861f 0xf5258b98
H_{i+1}^4	0x464a37b2 0xa16ba11d 0x77d7d5fe 0xec0e5d22 0xf015becc 0x3f4f70f7 0x1eb889c9 0x1f617eca
4-sum	0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

NTT

Conclusion

- Applied the boomerang 4-sum for the MD4-based compression function.
- Point out the flaw of previous boomerang attack on 5-pass HAVAL.
- First results on full 5-pass HAVAL with a practical complexity.

Target:	MD5	3-HAVAL	4-HAVAL	5-HAVAL
Comp:	$\mathbf{2^{10}}$	$\mathbf{2^{4}}$	$\mathbf{2^{11}}$	$\mathbf{2^{11}}$

NTT

Thank you for your attention !!