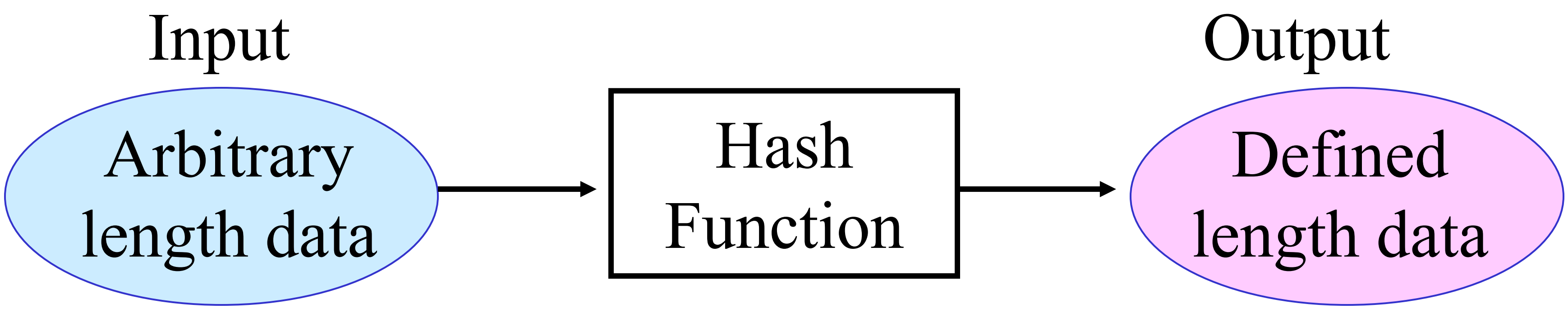
New Message Difference for MD4

Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro
The University of Electro-Communications
28/March/2007 @ FSE 2007

Introduction of MD4



- MD4 is a 128-bit hash function.
- Many hash functions such as MD5 and SHA-1, are designed based on MD4.
- Cryptanalysis of MD4 is important.

Collision Attack is Important !!

- Collision attack means finding (M, M') such that Hash(M)=Hash(M'), $M \neq M'$.

- Collision can threaten some applications.
  forging certificate, forging signature,
  key recovery on NMAC/HMAC
  password recovery on APOP, and so on.

Message Difference for Various Improved Collision Attack

- In 2005, Wang et al. proposed efficient collision attack. (less than 2^8 MD4)
- Naito et al. improved the complexity. (less than 3 MD4)
- Shulåffer and Oswald proposed automated sufficient condition search algorithm.

Common Fact

All previous known attacks use the same message difference as Wang et al.'s.

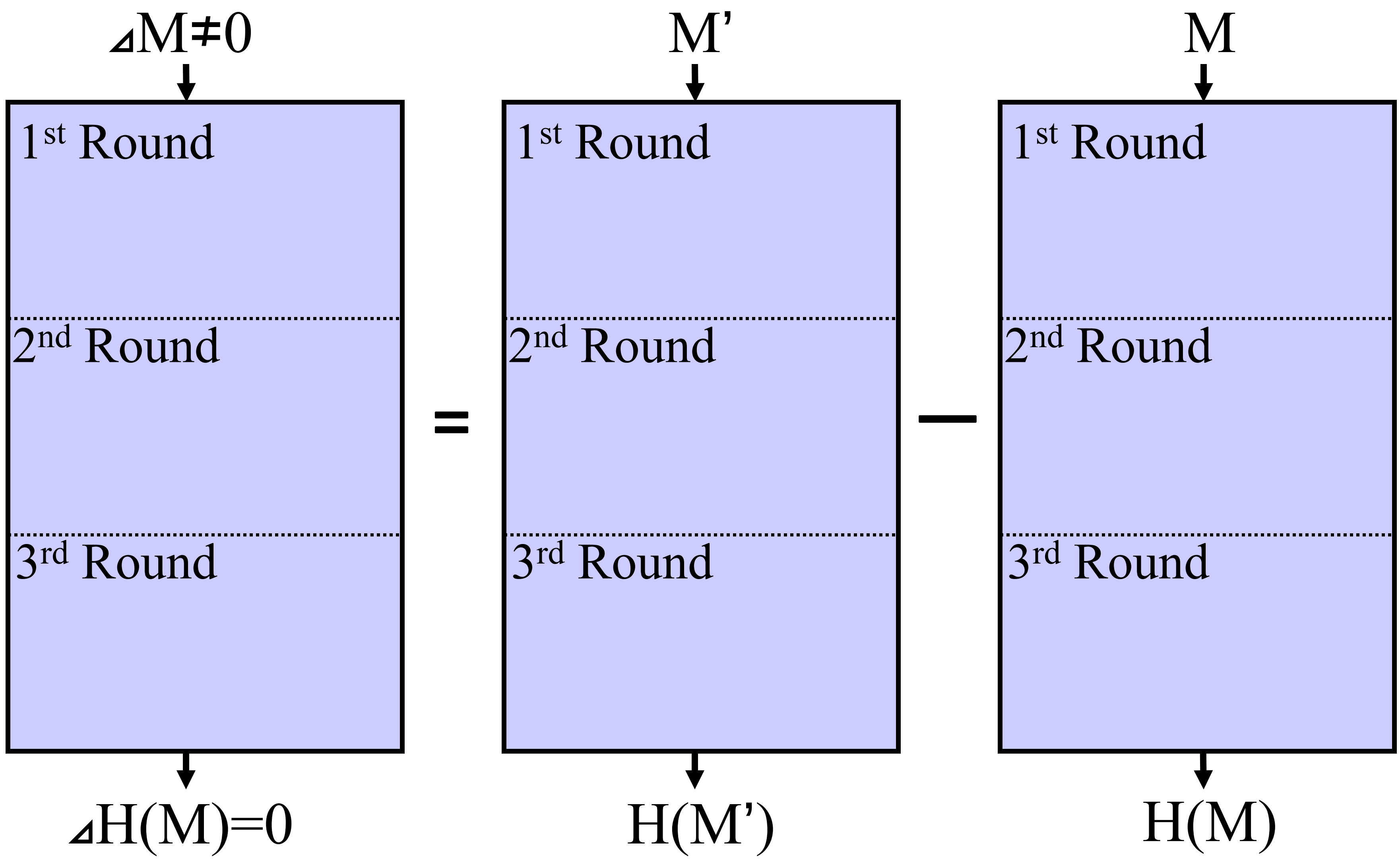
Our Result

- We propose new message difference and new local collision that are the best for collision attack on MD4.
- Our attack generates a collision with less than 2 MD4 computations.

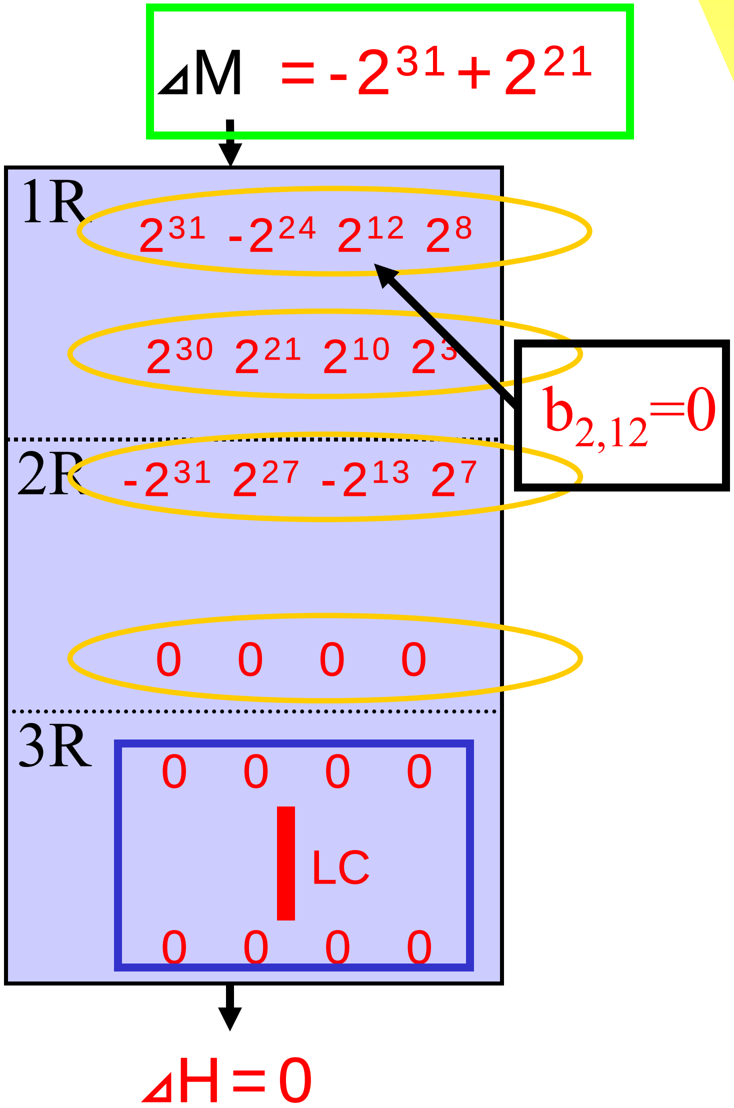
Generating collision is faster than checking collision!!

Procedure of Collision Attack

Differential Attack



Attack Procedure



1. Local Collision in 3rd round.

   Insert some difference in 3rd round and cancel it in few steps.

2. ⊿M **Core Technique**

   Insert message difference to realize local collision.

3. Differential Path

   Analyze how ⊿M propagates.

4. Chaining Variable Condition

   Make Conditions of chaining variables to hold differential path.

5. Collision Search

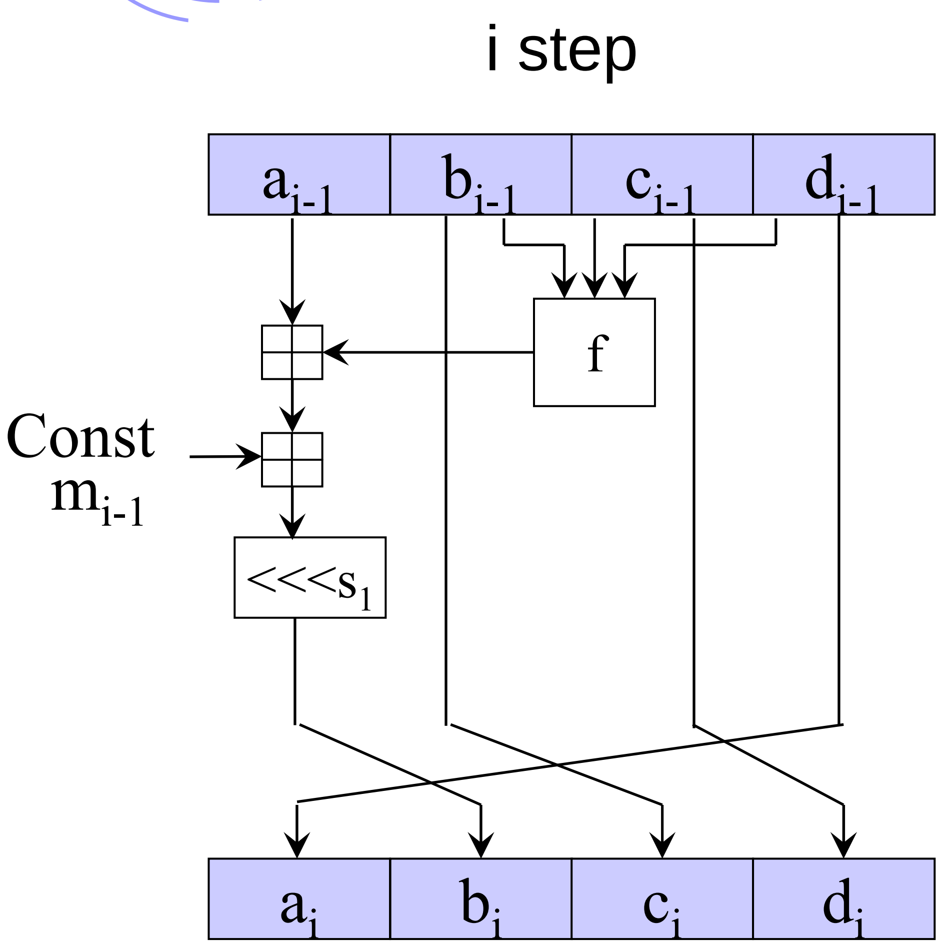
   By using message modification, search a message satisfying all conditions.

Constructing the Best Local Collision

1. Study of Wang et al.'s local collision
2. Analyze why it is not the best
3. Construct the best local collision

Structure of MD4

Structure of MD4

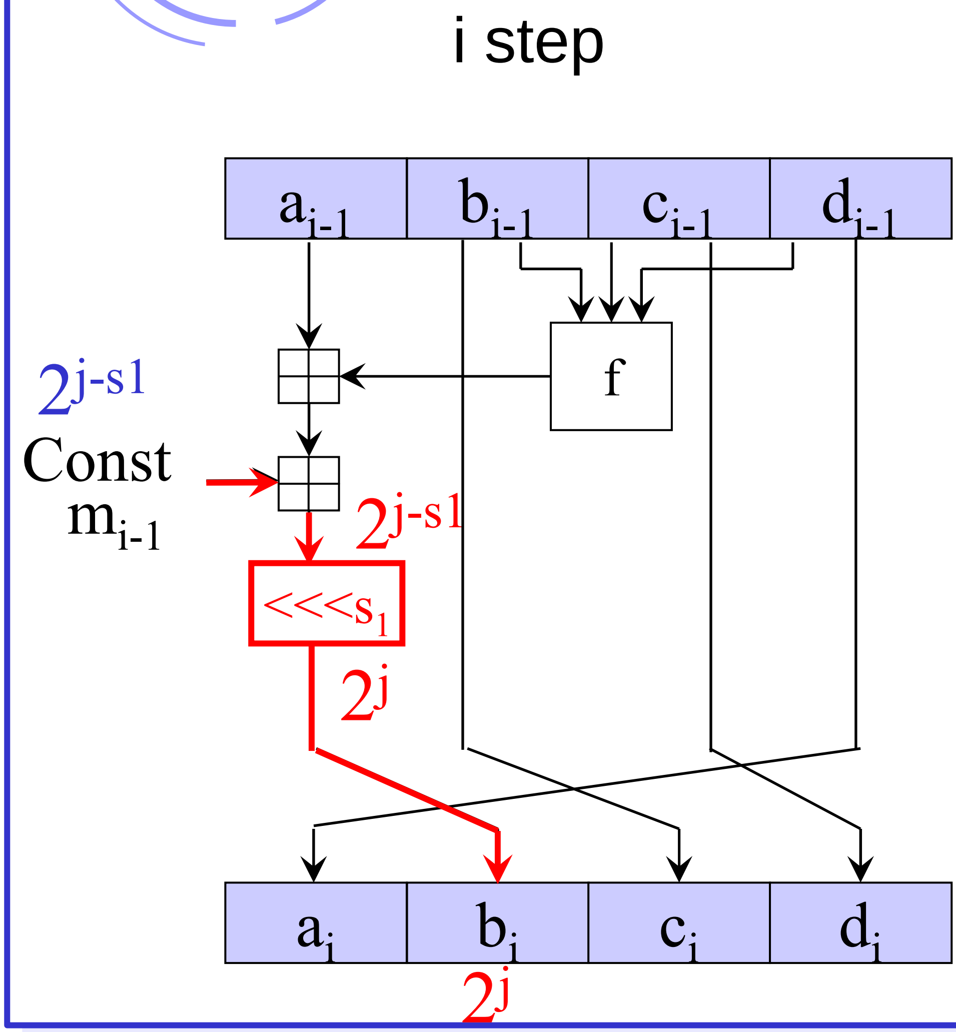


MD4 has 48 steps.

$<<<s_i$: Left Rotation

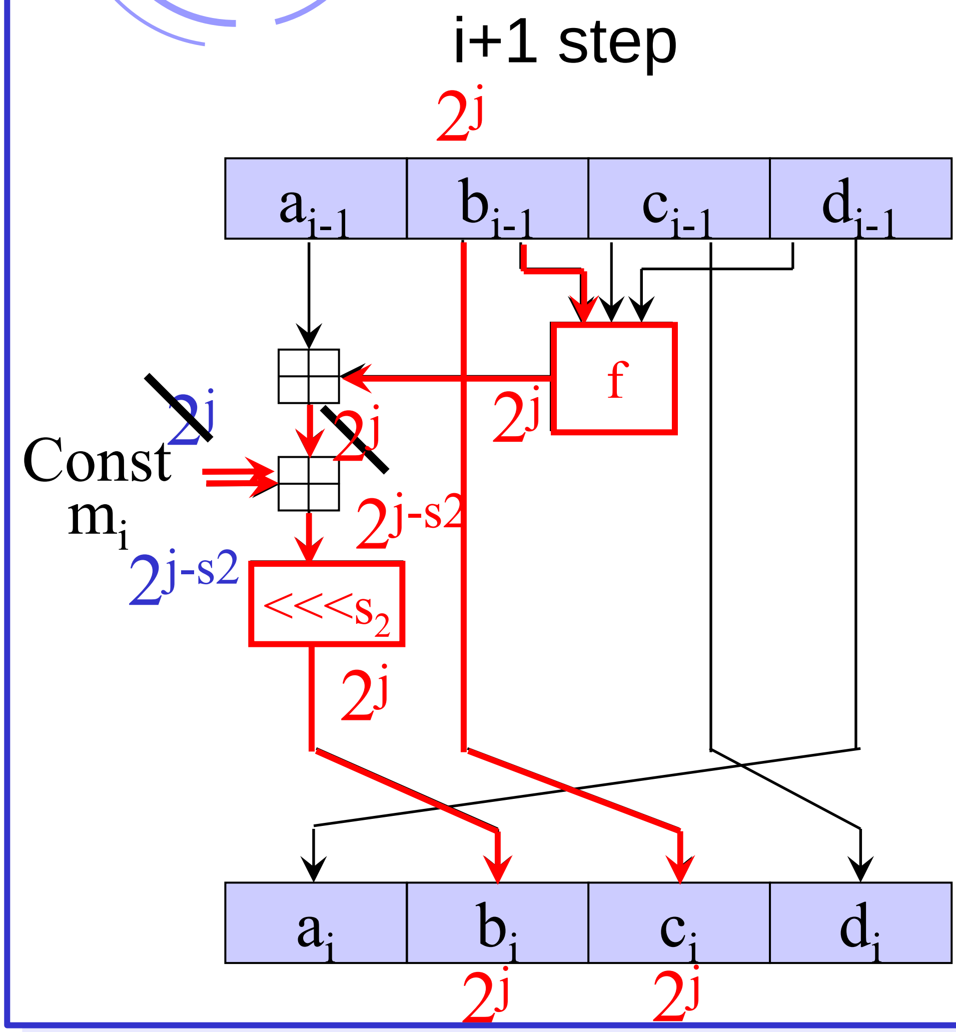
f: Boolean Function (XOR is considered for Local Collision)

Wang et al's Local Collision 1/6



1. Make diff with 2^{j-s1} of m_{i-1} .

Wang et al's Local Collision 2/6

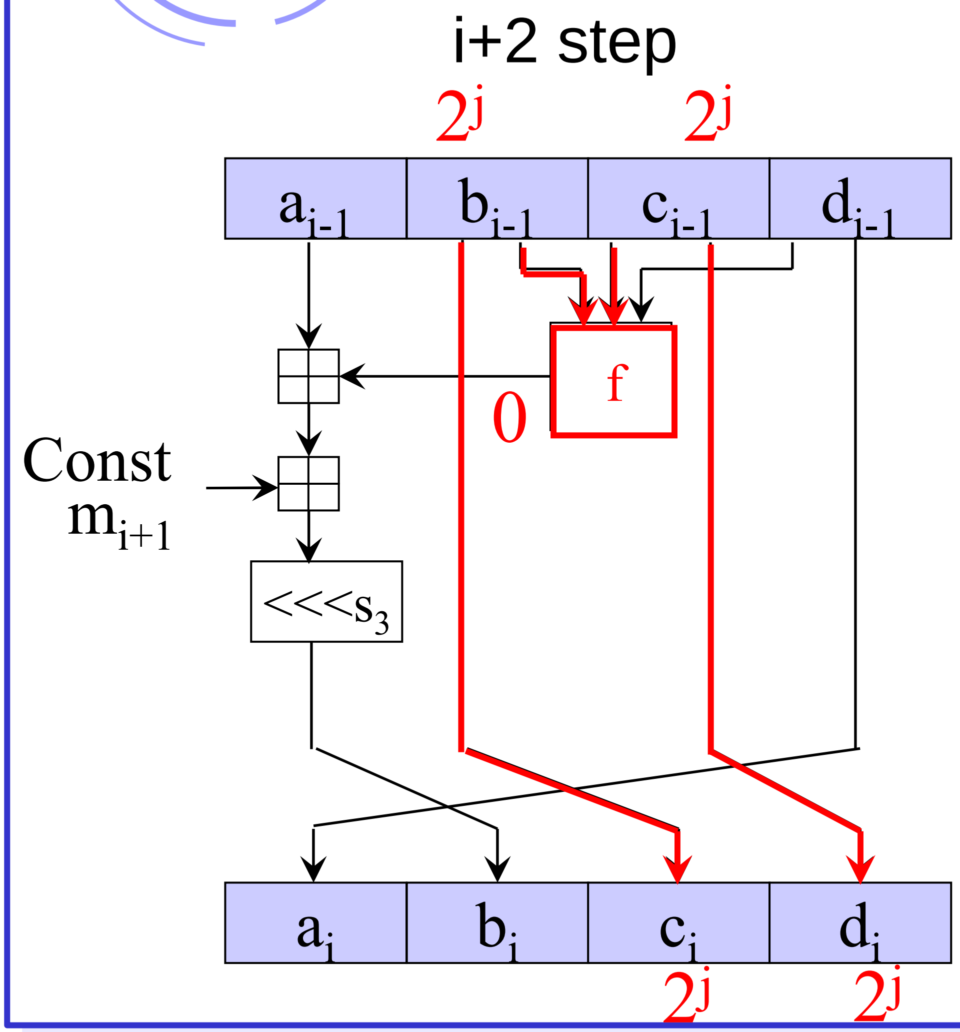


1. Make diff with 2^{j-s1} of m_{i-1} .

2. Cancel diff with 2^j of m_i .

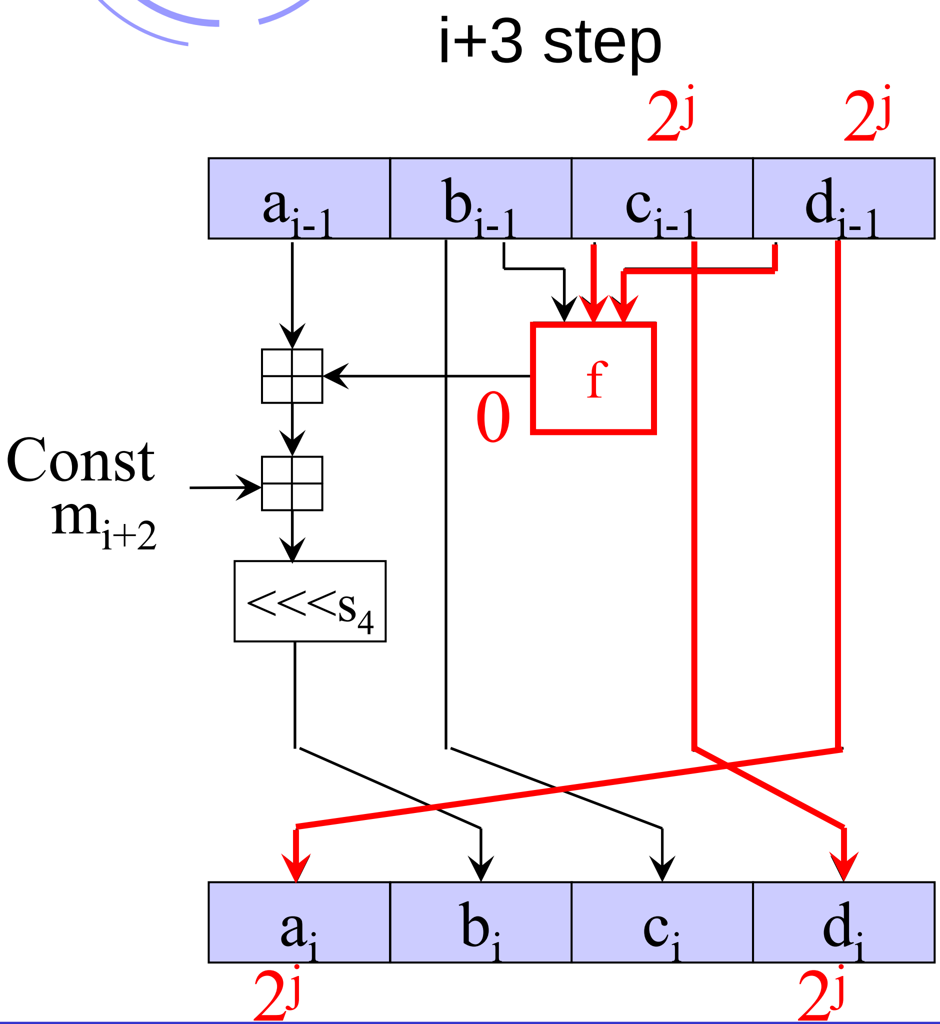
   Make diff with 2^{j-s2} of m_i .

Wang et al's Local Collision 3/6



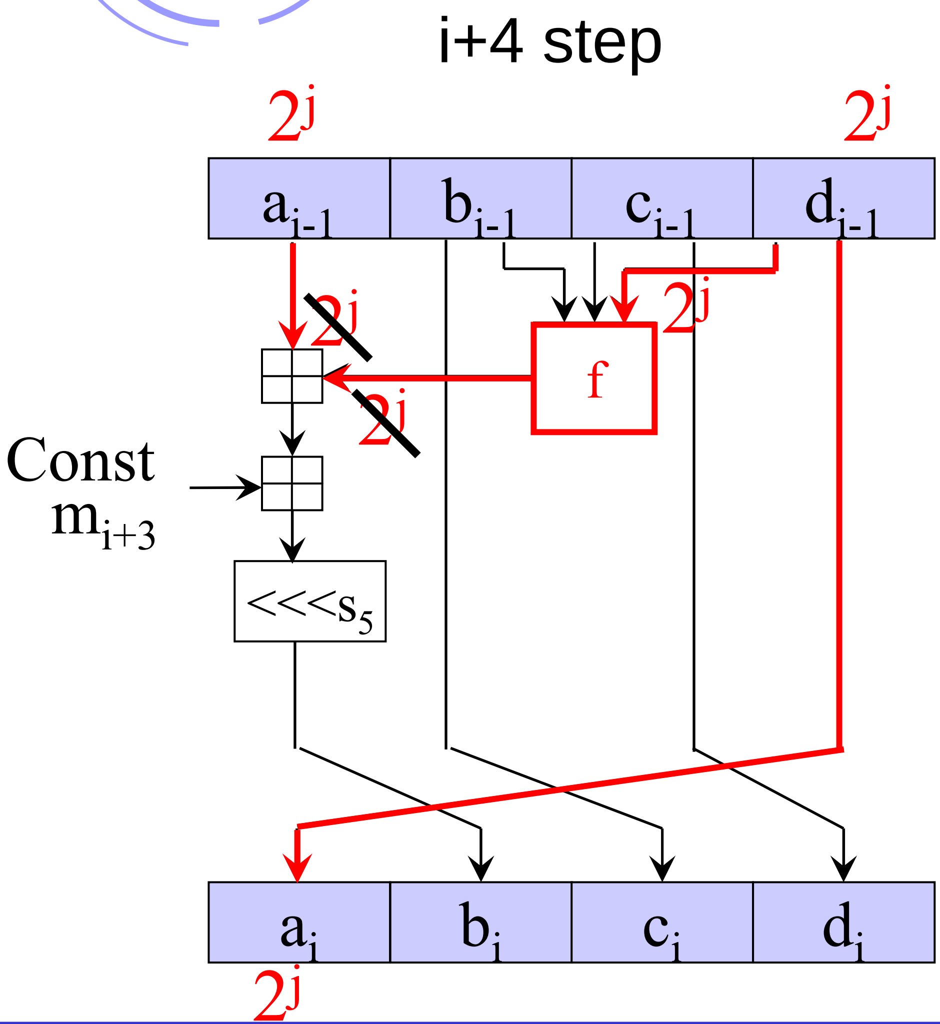
1. Make diff with 2^{j-s1} of m_{i-1} .
2. Cancel diff with 2^j of m_i .
   Make diff with 2^{j-s2} of m_i .
3. No difference

Wang et al's Local Collision 4/6



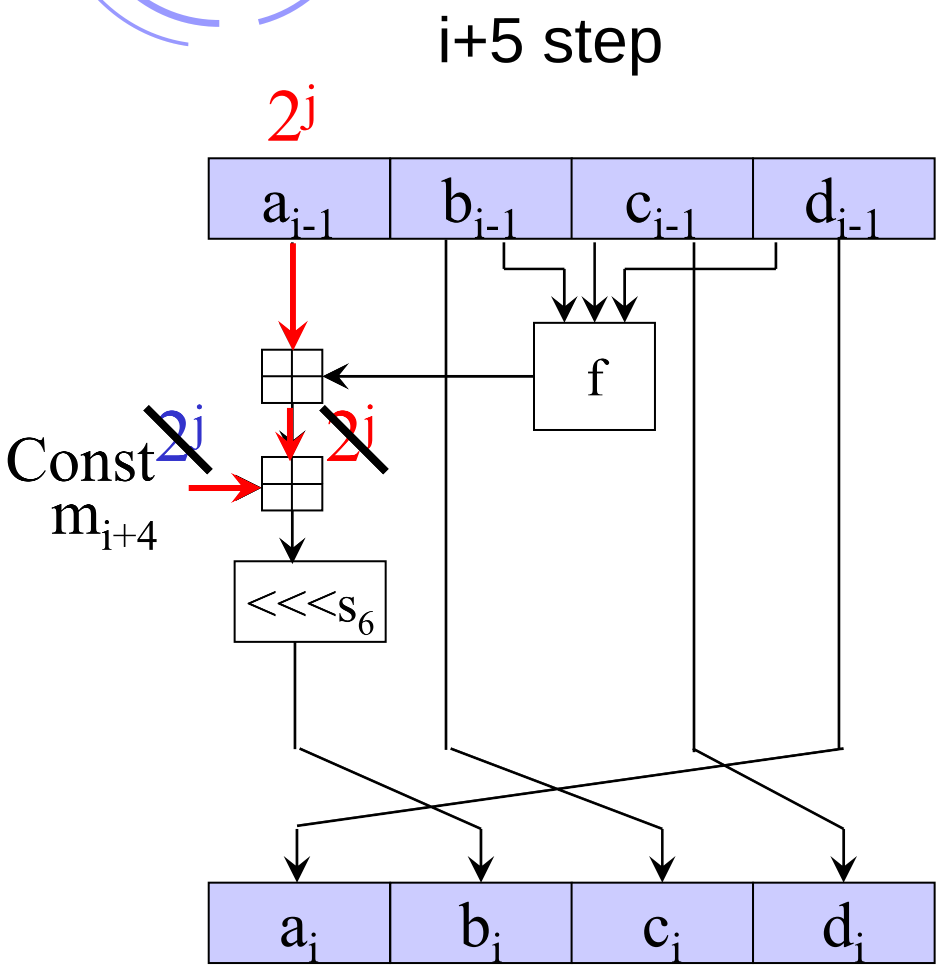
1. Make diff with 2^{j-s1} of m_{i-1} .
2. Cancel diff with 2^j of m_i .
   Make diff with 2^{j-s2} of m_i .
3. No difference
4. No difference

Wang et al's Local Collision 5/6



1. Make diff with 2^{j-s1} of m_{i-1} .
2. Cancel diff with 2^j of m_i .
   Make diff with 2^{j-s2} of m_i .
3. No difference
4. No difference
5. No difference

Wang et al's Local Collision 6/6



1. Make diff with 2^{j-s1} of m_{i-1} .
2. Cancel diff with 2^j of m_i .
   Make diff with 2^{j-s2} of m_i .
3. No difference
4. No difference
5. No difference
6. Cancel diff with 2^j of m_{i+4} .

All differences are cancelled !!

Summary of Wang et al.'s LC

1. Make diff with 2^{j-s1} of m_{i-1} .
2. Cancel diff with 2^j of m_i .

   Make diff with 2^{j-s2} of m_i .
3. No difference
4. No difference
5. No difference
6. Cancel diff with 2^j of m_{i+4} .

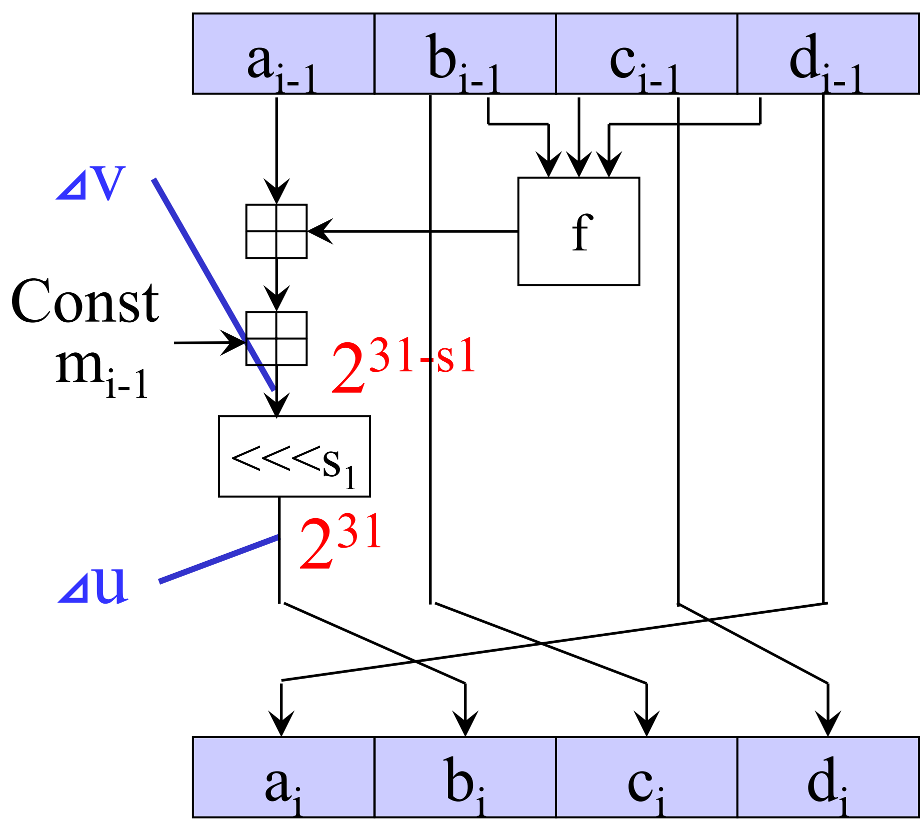
If j = MSB, cancellation succeeds with probability 1.

When we make diff at MSB, we will fail with 1/2.

Proof: next page

Therefore, total success probability is 1/4.

Proof: Difference in MSB



bit position (31-s1)

v: 000000001000000

+

⊿v: 000000001000000

||

v': 0000000100000000

After rotation by s1 bits.

u: 100000000000000

u': 000000000000001

⊿u≠2^{31}, not desired difference .

Prob of avoiding carry is 1/2 .

The Best Local Collision

- Wang et al.'s LC makes two differences in MSB.

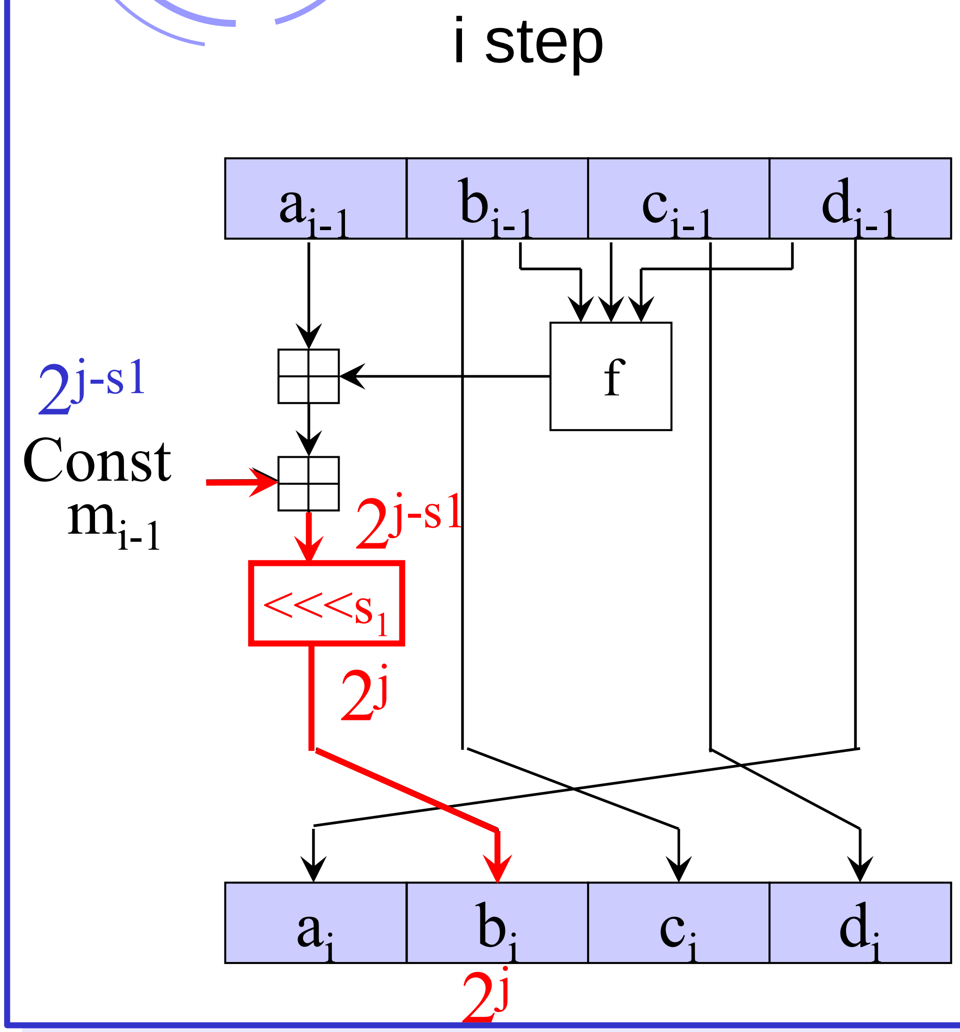
Success prob of LC :**1/4**

- At least 1 difference is necessary.

- If LC that consists of 1 difference in MSB exists, such LC is the best.

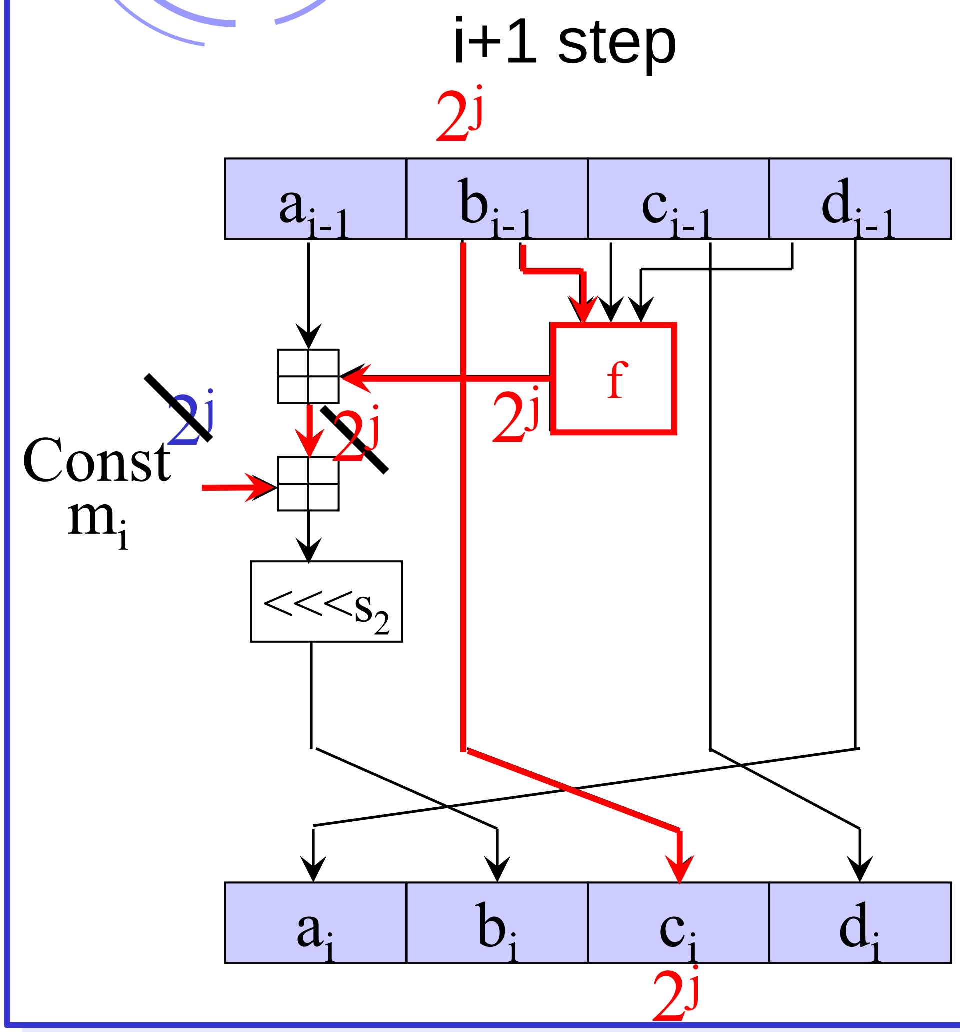
Success prob is **1/2**

New Local Collision 1/5



1. Make diff with 2^{j-s1} of m_{i-1}.

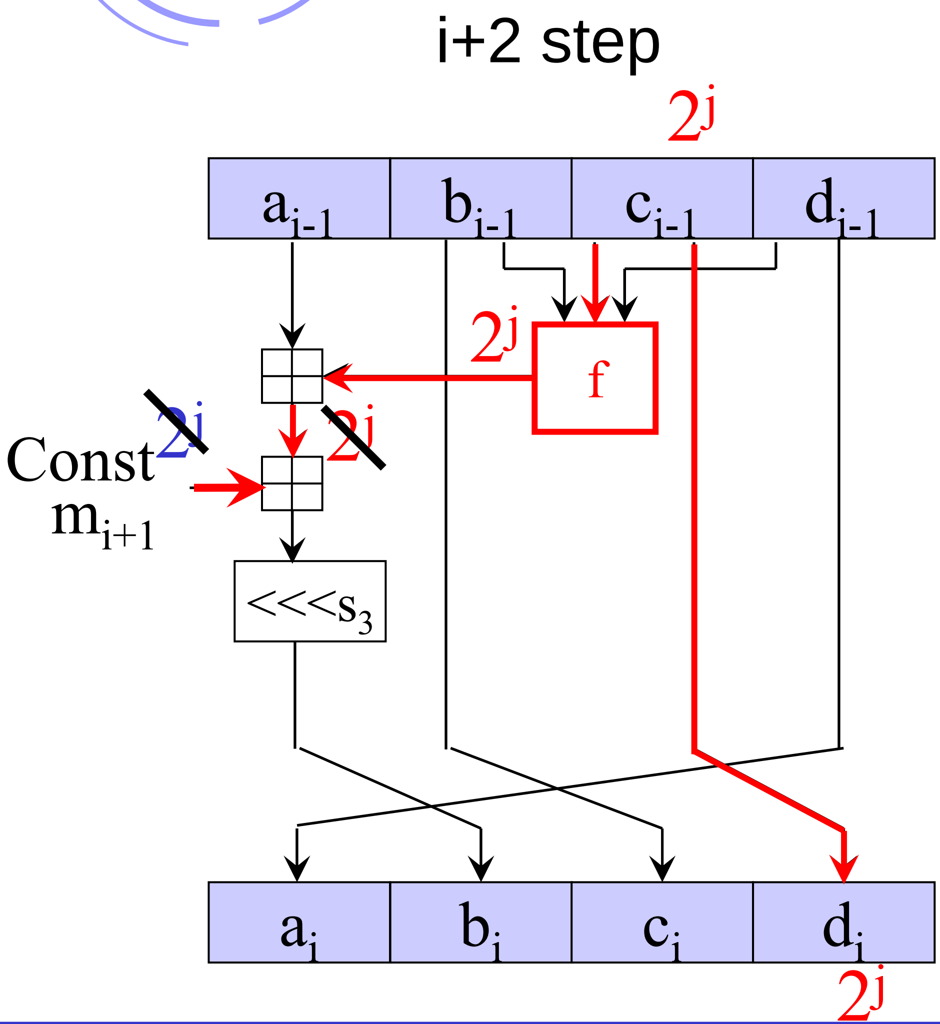
New Local Collision 2/5



1. Make diff with 2^{j-s1} of m_{i-1}.

2. Cancel diff with 2^j of m_i.

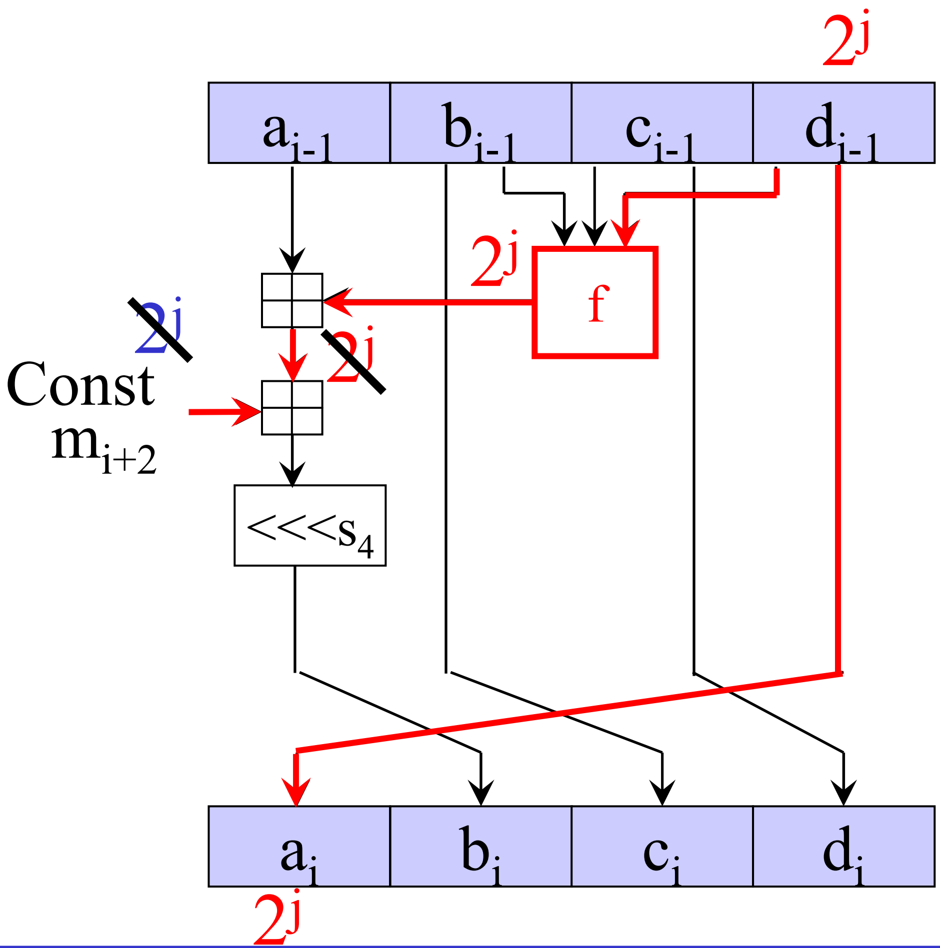
New Local Collision 3/5



1. Make diff with 2^{j-s1} of m_{i-1}.
2. Cancel diff with 2^j of m_i.
3. Cancel diff with 2^j of m_{i+1}.

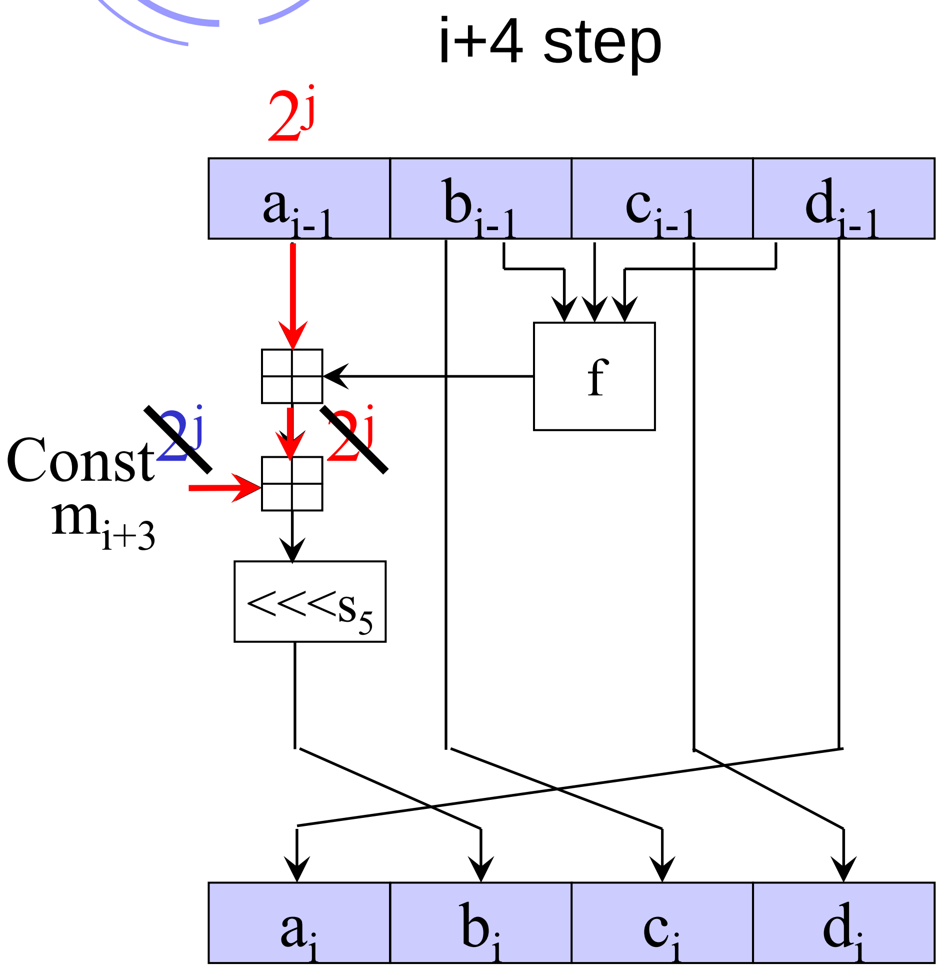
New Local Collision 4/5

i+3 step



1. Make diff with 2^{j-s1} of m_{i-1}.
2. Cancel diff with 2^j of m_i.
3. Cancel diff with 2^j of m_{i+1}.
4. Cancel diff with 2^j of m_{i+2}.

New Local Collision 5/5

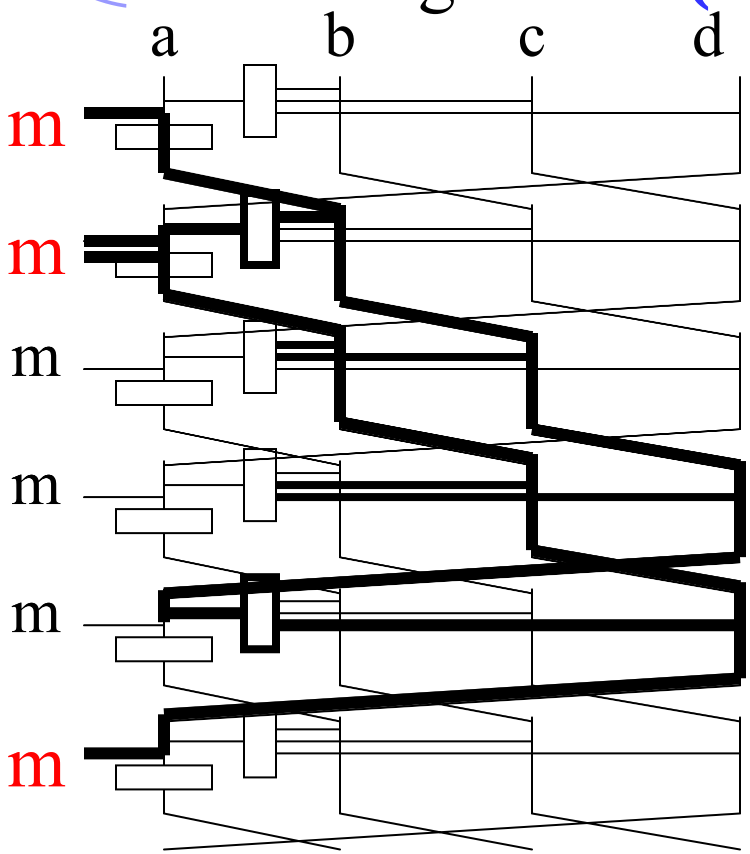


1. Make diff with 2^{j-s1} of m_{i-1}.
2. Cancel diff with 2^j of m_i.
3. Cancel diff with 2^j of m_{i+1}.
4. Cancel diff with 2^j of m_{i+2}.
5. Cancel diff with 2^j of m_{i+3}.

All differences are cancelled !!

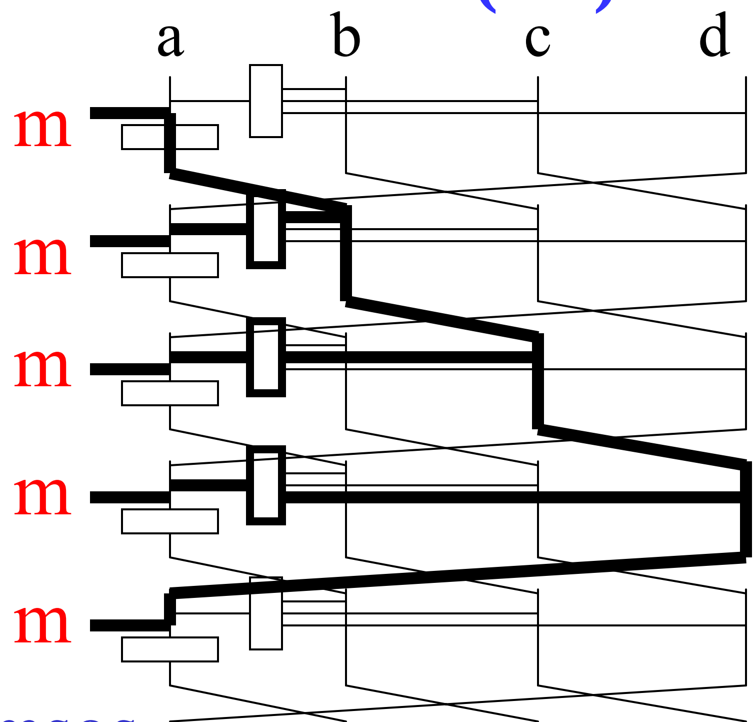
Comparison of Both Local Collisions

Wang et al.'s **(1/4)**



3 msgs are involved

Ours **(1/2)**



5 msgs

Msg expansion should be evaluated.

Analysis of Message Expansion

Which step we apply LC ?

New local collision

1. Make diff with 2^{j-s1} of m_{i-1}.
2. Cancel diff with 2^j of m_i.
3. Cancel diff with 2^j of m_{i+1}.
4. Cancel diff with 2^j of m_{i+2}.
5. Cancel diff with 2^j of m_{i+3}.

step	Index of message
33	0
34	8
35	4
36	12
37	2
38	10
39	6
40	14
41	1
42	9
43	5
44	13
45	3
46	11
47	7
48	15

There are 12 patterns.

Criteria for Good Msg Expansion

Criteria

Last difference in 2R round should be as early as possible.

In this example: 25

Some diff

No diff

2R

step	message
17	0
18	4
19	8
20	12
21	1
22	5
23	9
24	13
25	2
26	6
27	10
28	14
29	3
30	7
31	11
32	15

3R

step	message
33	0
34	8
35	4
36	12
37	2
38	10
39	6
40	14
41	1
42	9
43	5
44	13
45	3
46	11
47	7
48	15

Msg Expansion: New LC

Last step of diff in 2R

Case 1	25
Case 2	
Case 3	
Case 4	
Case 5	
Case 6	
Case 7	
Case 8	
Case 9	
Case 10	
Case 11	
Case 12	

2R

step	message
17	0
18	4
19	8
20	12
21	1
22	5
23	9
24	13
25	2
26	6
27	10
28	14
29	3
30	7
31	11
32	15

3R

step	message
33	0
34	8
35	4
36	12
37	2
38	10
39	6
40	14
41	1
42	9
43	5
44	13
45	3
46	11
47	7
48	15

Msg Expansion: New LC

Last step of diff in 2R

Case 1	25
Case 2	27
Case 3	
Case 4	
Case 5	
Case 6	
Case 7	
Case 8	
Case 9	
Case 10	
Case 11	
Case 12	

2R

step	message
17	0
18	4
19	8
20	12
21	1
22	5
23	9
24	13
25	2
26	6
27	10
28	14
29	3
30	7
31	11
32	15

3R

step	message
33	0
34	8
35	4
36	12
37	2
38	10
39	6
40	14
41	1
42	9
43	5
44	13
45	3
46	11
47	7
48	15

Msg Expansion: New LC

Last step of diff in 2R

Case 1	25
Case 2	27
Case 3	27
Case 4	
Case 5	
Case 6	
Case 7	
Case 8	
Case 9	
Case 10	
Case 11	
Case 12	

2R

step	message
17	0
18	4
19	8
20	12
21	1
22	5
23	9
24	13
25	2
26	6
27	10
28	14
29	3
30	7
31	11
32	15

3R

step	message
33	0
34	8
35	4
36	12
37	2
38	10
39	6
40	14
41	1
42	9
43	5
44	13
45	3
46	11
47	7
48	15

Result: Good msg Difference of our LC

Case 1	25
Case 2	27
Case 3	27
Case 4	28
Case 5	28
Case 6	28
Case 7	28
Case 8	28
Case 9	29
Case 10	31
Case 11	31
Case 12	32

As a result, Case 1 is the best.

$$\Delta M = \begin{cases} m_0: 2^{28} & m_{12}: 2^{31} \\ m_8: 2^{31} & m_2: 2^{31} \\ m_4: 2^{31} & \end{cases}$$

We also evaluated Wang et al.'s LC by using the same criteria. Then, the best value was the same.

Confirmed that the best LC is really the best.

Comparison of #CVC in each method

We made differential path in 2R to minimize conditions.

Comparison of #non-negligible conditions

	Wang	Schläffer	Leurent	New LC
Round 1	96	122	70	???
Round 2	25	22	16	**9**
Round 3	2	2	2	**1**

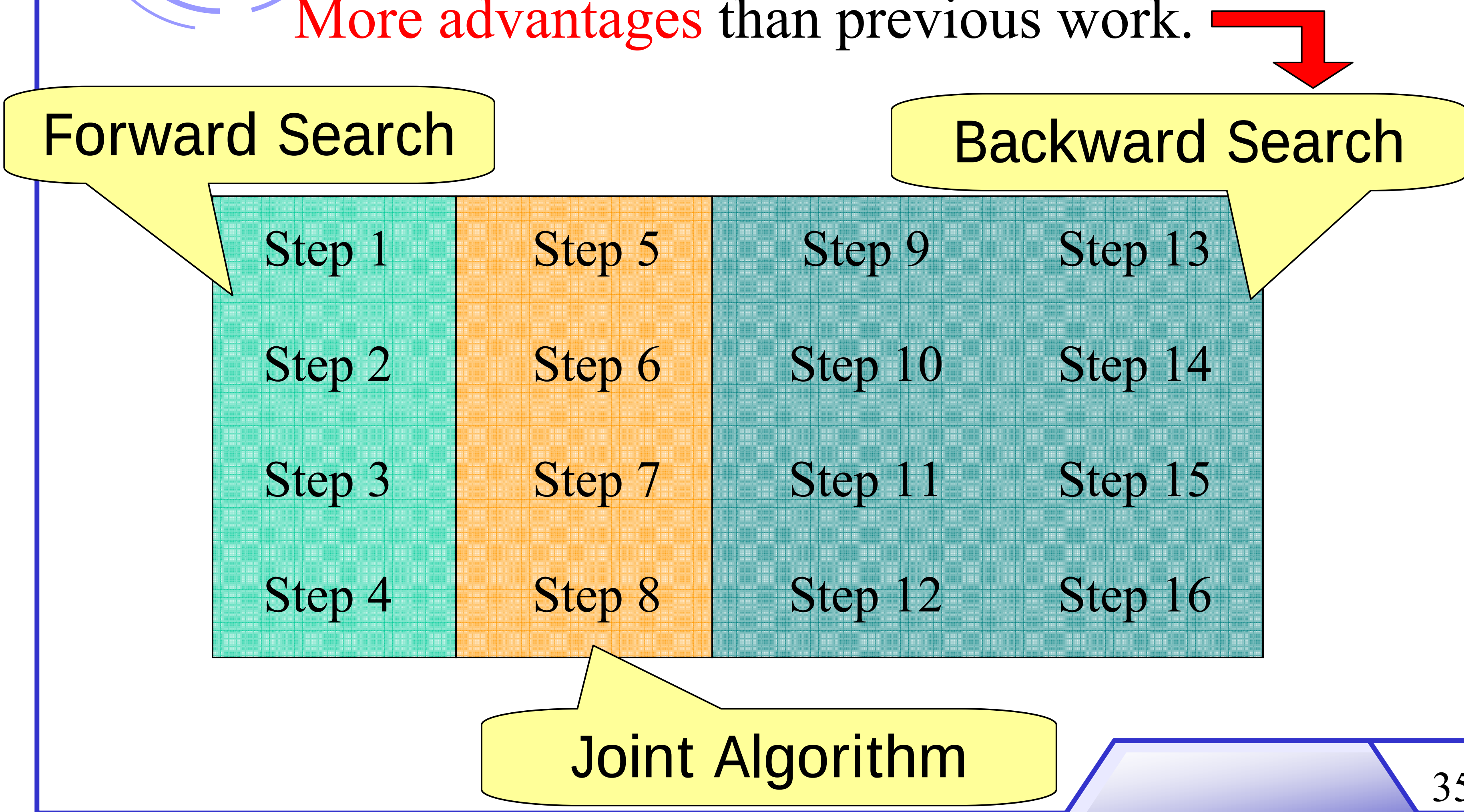
Remaining work is construction of path in the 1R.

5

Differential Path Construction Algorithm for the 1^{st} round

Differential Path Search Algorithm

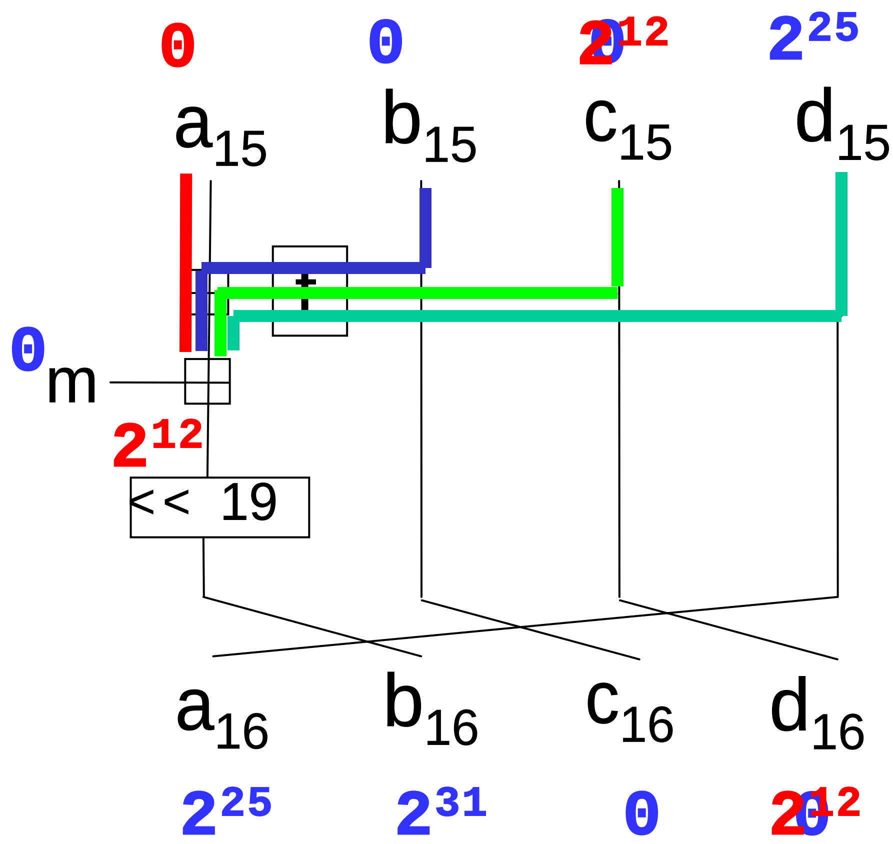
More advantages than previous work.



Backward Search

1. Calculate the difference before rotation.

2. There are 4 candidates to produce this diff.



Previous work [SO06] did not consider path through *f*.

We enlarged search space!!

#CVC: Final Result

Table: Comparison of #CVC in each method

	Wang	Schlåffer	Leurent	New LC
Round 1	96	122	70	167
Round 2	25	22	16	**9**
Round 3	2	2	2	**1**

Note: All CVCs in 1R are satisfied with probability 1.

Attack Complexity

- We also proposed message modification for out attack.

- Complexity of our attack
  → Less than 2 MD4 computations

New Record !!

Conclusion

- We proposed the best local collision and message difference for MD4 collision attack.
- We proposed algorithm for constructing differential path for 1R of MD4.
- By combining message modification, our attack generates a collision with complexity less than 2 MD4 computations, which is the fastest of all previous known works.

$$\Delta M = \begin{cases} \Delta m_0 = 2^{28} \quad \Delta m_2 = 2^{31} \quad \Delta m_4 = 2^{31} \quad \Delta m_8 = 2^{31} \quad \Delta m_{12} = 2^{31} \\ \Delta m_i = 0 \text{ (for other } i \text{)} \end{cases}$$

M	**b**cdd2674	53fce1ed	**2**5d202ce	e87d102e
	f45be728	acc992cc	6acfb3ea	7dbb29d4
	ed03bf75	c6aedc45	d442b710	fca27d99
	a5f5eff1	fb2ee79b	0f590d68	4989f380
M'	**c**cdd2674	53fce1ed	**a**5d202ce	e87d102e
	745be728	acc992cc	6acfb3ea	7dbb29d4
	6d03bf75	c6aedc45	d442b710	fca27d99
	25f5eff1	fb2ee79b	0f590d68	4989f380
hash	c257b7be	324f26ef	69d3d290	b01be001

Thank you for your Attention !!!