Improved Cryptanalysis of Reduced RIPEMD-160

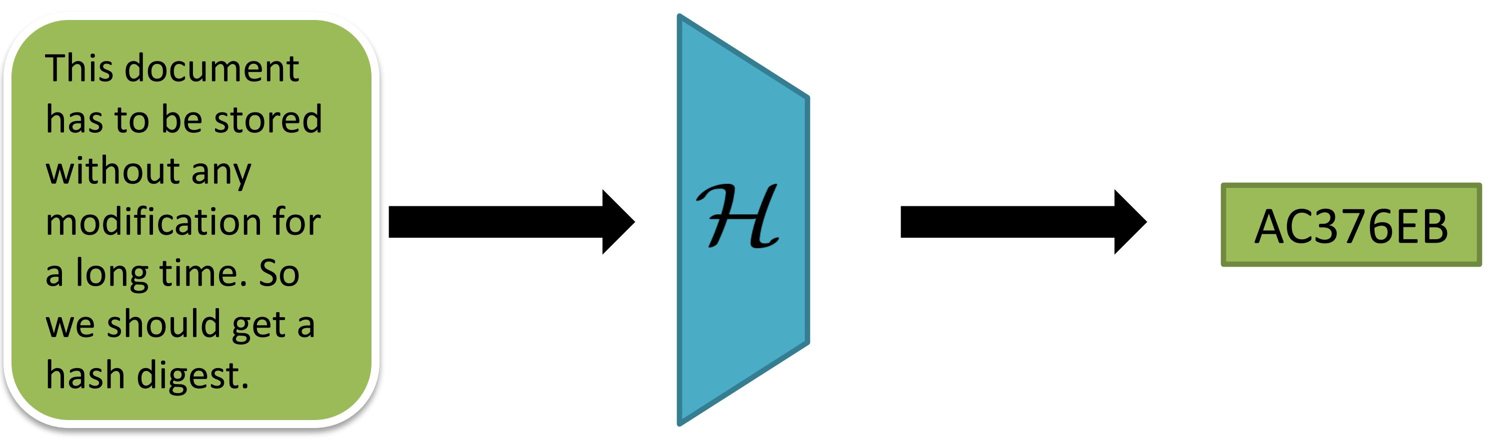
Florian Mendel, Thomas Peyrin, Martin Schläffer,
Lei Wang, and Shuang Wu

ASIACRYPT 2013

Cryptographic Hash Function

- **Public** function
  - Input: **arbitrary long** messages
  - Output: **short random** digests

- A **fundamental primitive** in cryptography



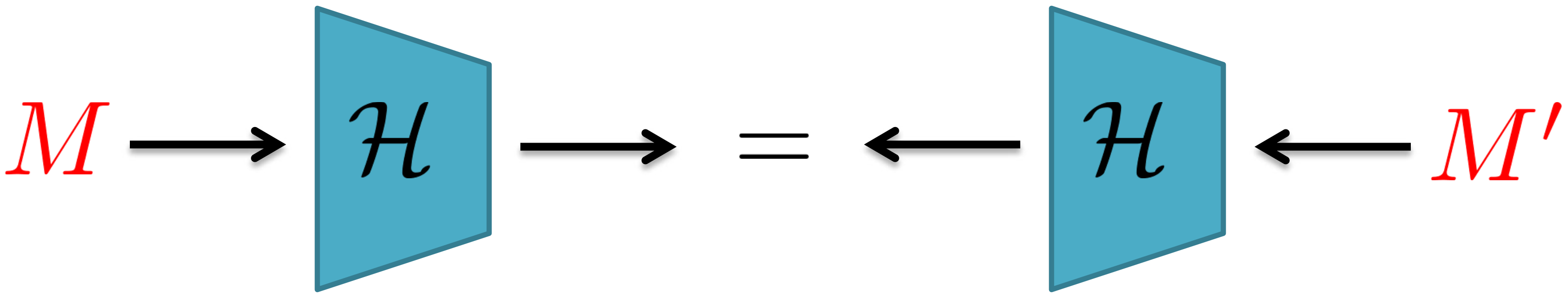
Security Notions

- **Collision** attack

  Find M and M' such that $M \neq M'$ and
  $$\mathcal{H}(M) = \mathcal{H}(M')$$

- Collision **resistance**

  Finding a collision takes **no less than $2^{n/2}$** computations (n is digest bit size).



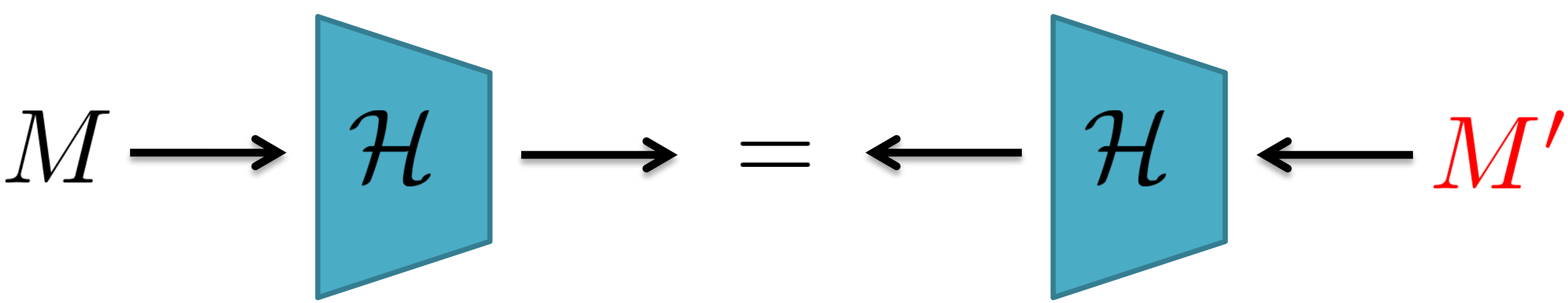
Security Notions

- **Second peimage** attack

  Given M, find M' such that $M \neq M'$ and $\mathcal{H}(M) = \mathcal{H}(M')$

- Second preimage **resistance**

  Finding a second preimage takes **no less than 2^n** computations (n is digest bit size).



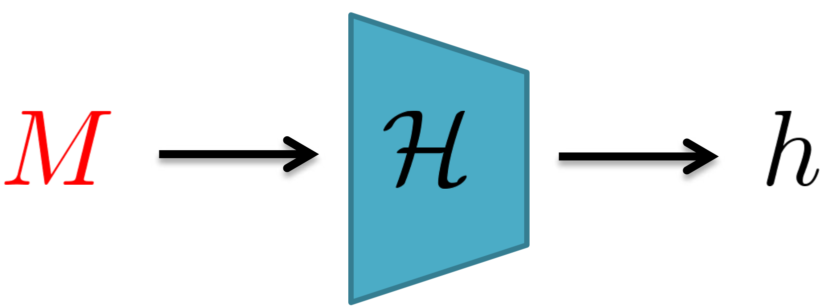
Security Notions

- **Peimage** attack

  Given h, find a M such that $\mathcal{H}(M) = h$

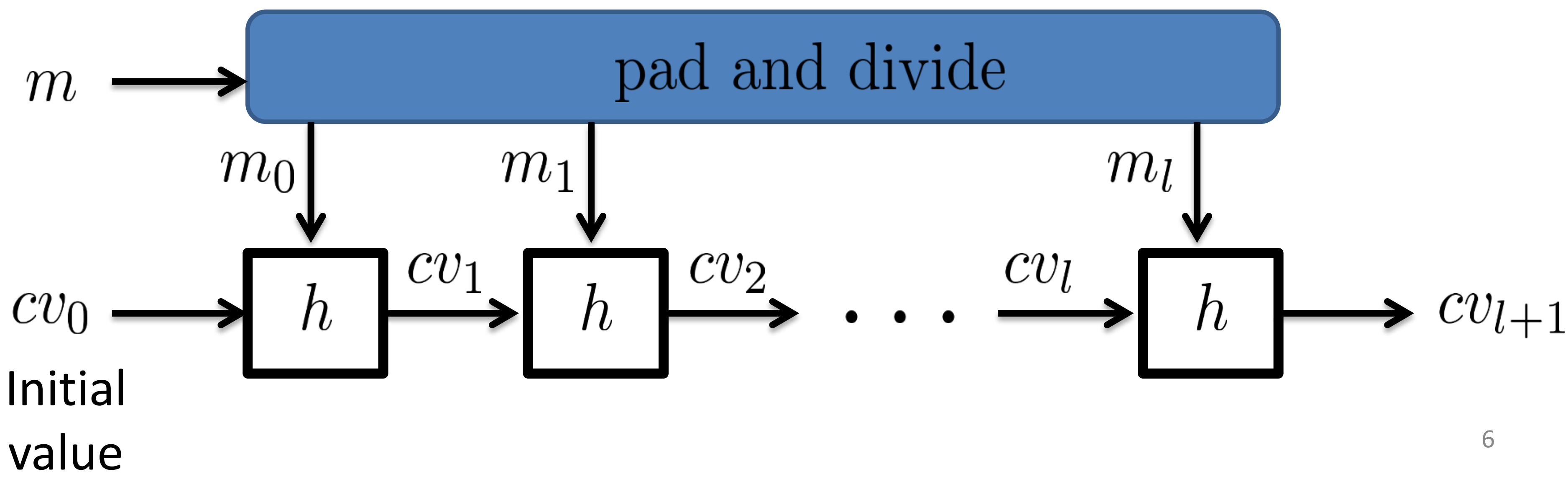
- Preimage **resistance**

  Finding a preimage takes **no less than 2^n** computations (n is digest bit size).



Iterative Hash Function Design

- **Compression function:** public function for which the input and output **size** is **fixed**.
- **Domain extension:** an algorithm which iterates the compression function to handle arbitrary long messages.
  - e.g., **Merkle-Damgård** mode



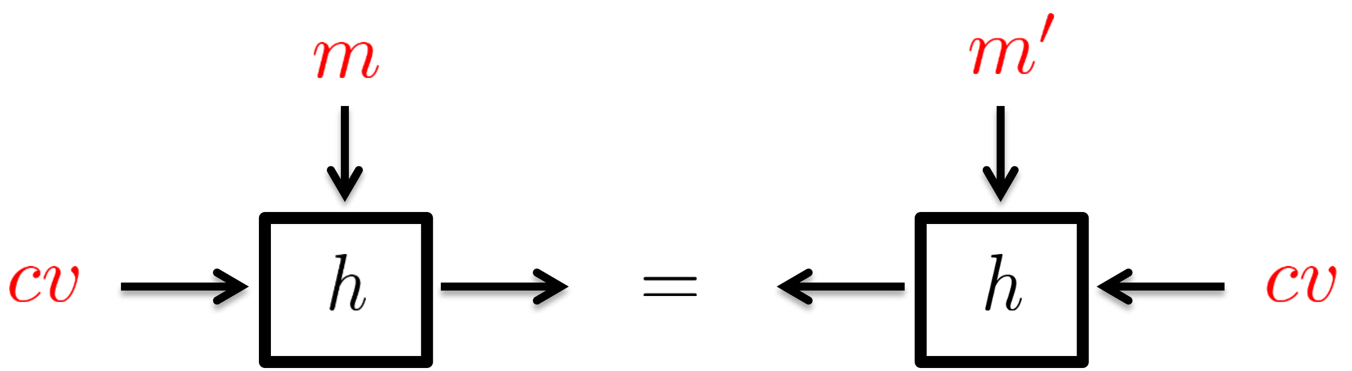
A security notion on compression function

- **Semi-free-start** collision attack

Find cv, m and m' such that $m \neq m'$

$$h(cv, m) = h(cv, m')$$

- **Resistance** requirement: **no less than $2^{n/2}$**



MD-SHA Family

- Well-known **dedicated** hash functions since 1990s
- **Merkle-Damgård** mode
- Compression function
  - ➢ **Addition-Rotation-Xor**
  - ➢ Bitwise **Boolean function**
  - ➢ Unbalanced **Feistel Network**

MD-SHA Family

- **Broken** hash functions

  - MD4, MD5, SHA-0, SHA-1, HAVAL, RIPEMD-0, RIPEMD-128

- **Unbroken** hash functions

  - **RIPEMD-160**, SHA-2

Security State of RIPEMD-160

- After **17 years** since 1996

Target	Type	#Steps	Complexity	Ref.
Compression	Preimage	31	2^{148}	OSS12
Hash	Preimage	31	2^{155}	OSS12
Compression	Non-randomness	48	low	MNSS12
Compression	Non-randomness	52	2^{158}	SW12
Compression	Semi-free-start collision	36	low	MNSS12
Compression	**Semi-free-start collision**	**42**	$\mathbf{2^{75.5}}$	**Ours**
Compression	**Semi-free-start collision**	**36***	$\mathbf{2^{70.4}}$	**Ours**

*: Our 36-step attack **starts from the first step**.

Outline

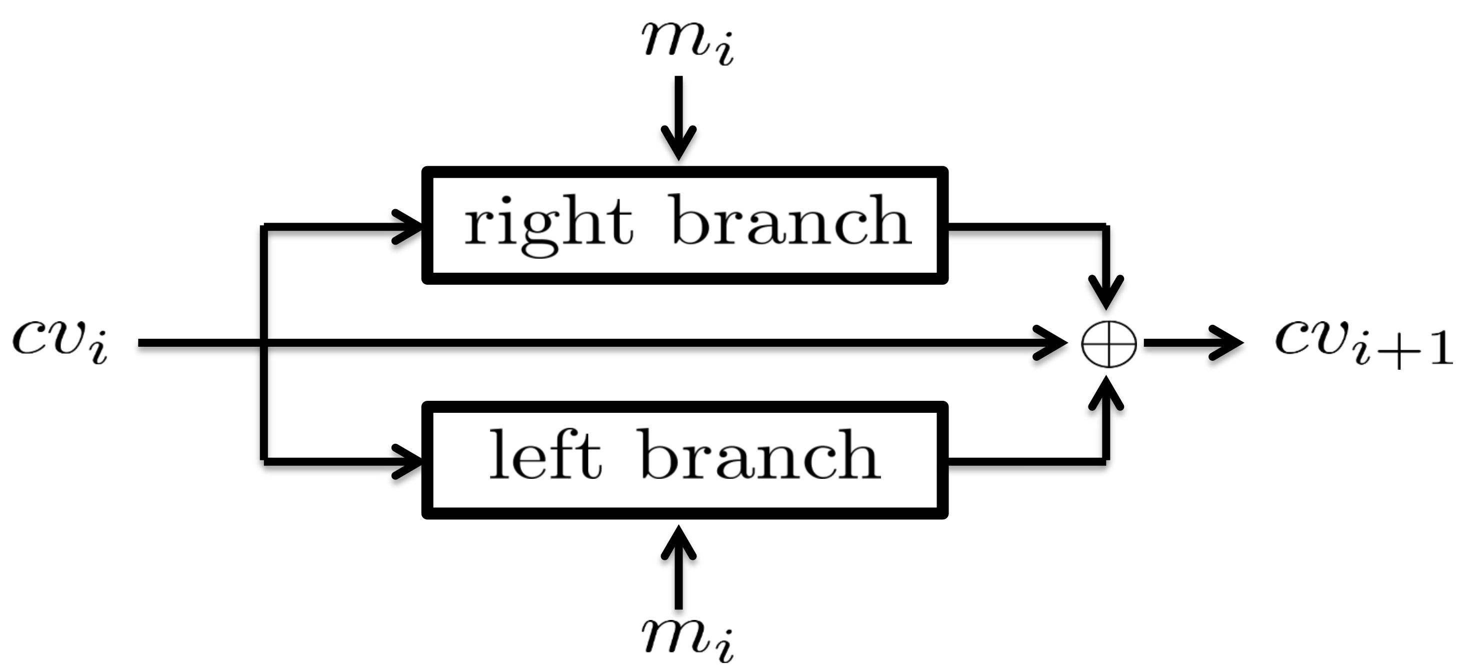
- RIPEMD-160 specification
- Attack overview
- Find a differential path
- Find a confirming pair
- Conclusion

Outline

- **RIPEMD-160 specification**
- Attack overview
- Find a differential path
- Find a confirming pair
- Conclusion

RIPEMD-160

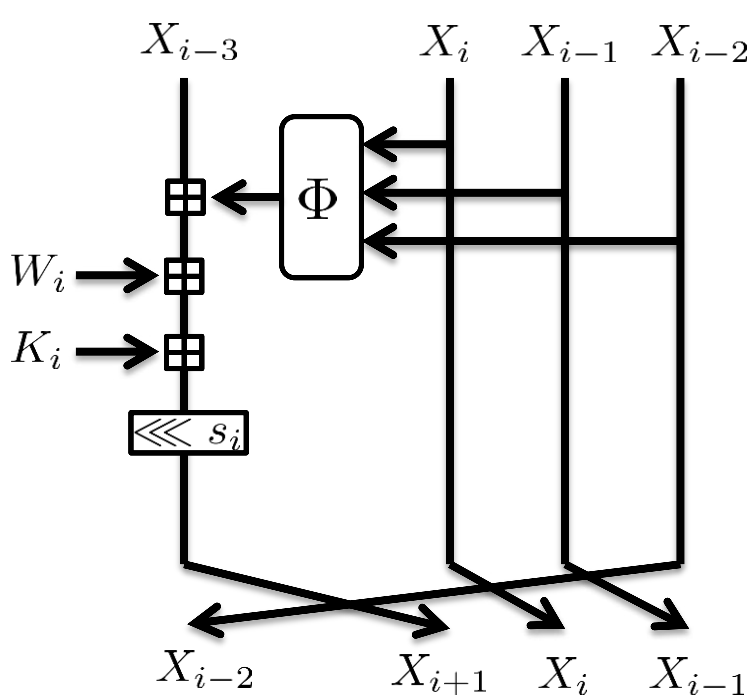
- Designed by Dobbertin, Bosselaers and Preneel
- Worldwide ISO/IEC standard
- **Double-branch** compression function



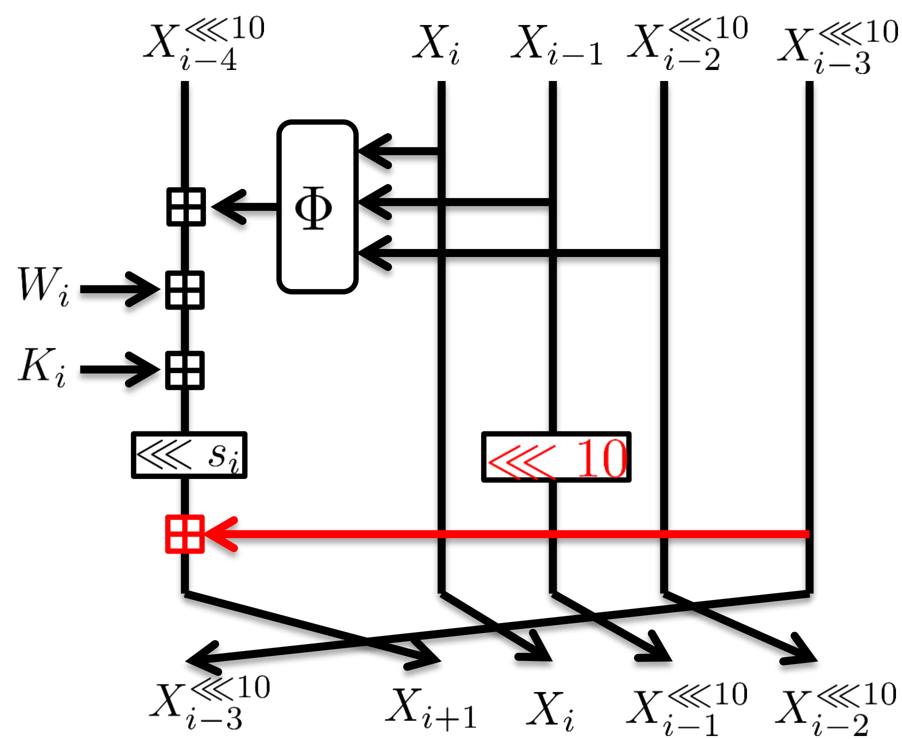
Compared to RIPEMD-128

- Our attacks are based on recent analysis approach of RIPEMD-128 [LP13]
- Larger digest size: 128 $\longrightarrow$ 160
- Increased number of steps: 64 $\longrightarrow$ 80
- **The step function has stronger diffusion and one "free term"**
  - Significant **impact** to **differential path**
  - The **reason** that **#attacked steps** is **less.**

RIPEMD-128



RIPEMD-160



$\boxplus$: modular addition

Φ : Boolean function

$\lll$: left cyclic rotation

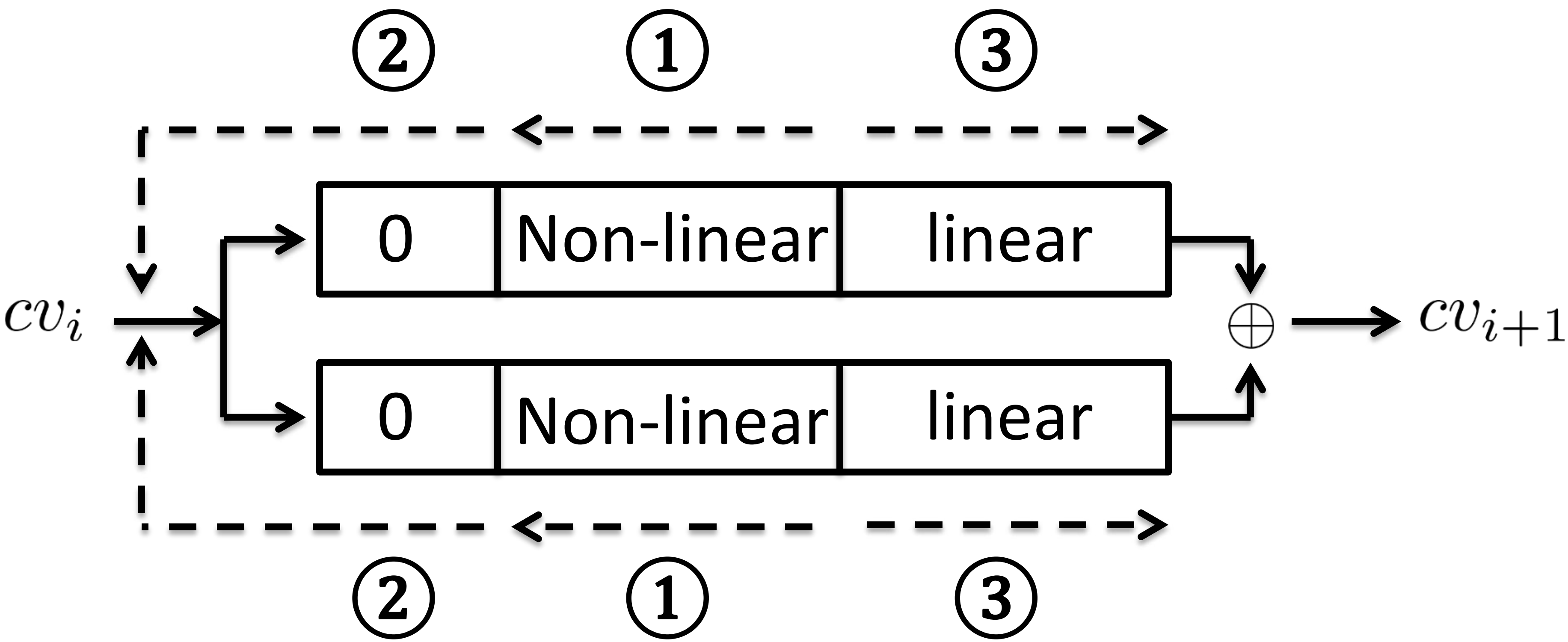
K_i, s_i : constants

Outline

- RIPEMD-160 specification
- **Attack overview**
- Find a differential path
- Find a confirming pair
- Conclusion

Attack Overview

- The same with the attacks on RIPEMD-128 [LP13]



Rationale of Our Attack Strategy

- 80 steps are re-grouped into 5 rounds
- Each round has a distinct Boolean function
- The **Boolean function** has significant **impact** to **non-linear differential path** search

XOR: $x \oplus y \oplus z$ IFZ: $(x \wedge z) \oplus (y \wedge \overline{z})$ ONZ: $(x \vee \overline{y}) \oplus z$

IFX: $(x \wedge y) \oplus (\overline{x} \wedge z)$ ONX: $x \oplus (y \vee \overline{z})$

Rationale of Our Attack Strategy

- **Absorption**: an input bit difference does not necessarily propagate to the output bit

  - **Strong** absorption: IFX, IFZ
  - **Weak** absorption: ONX, ONZ
  - **No** absorption: XOR

Rationale of Our Attack Strategy

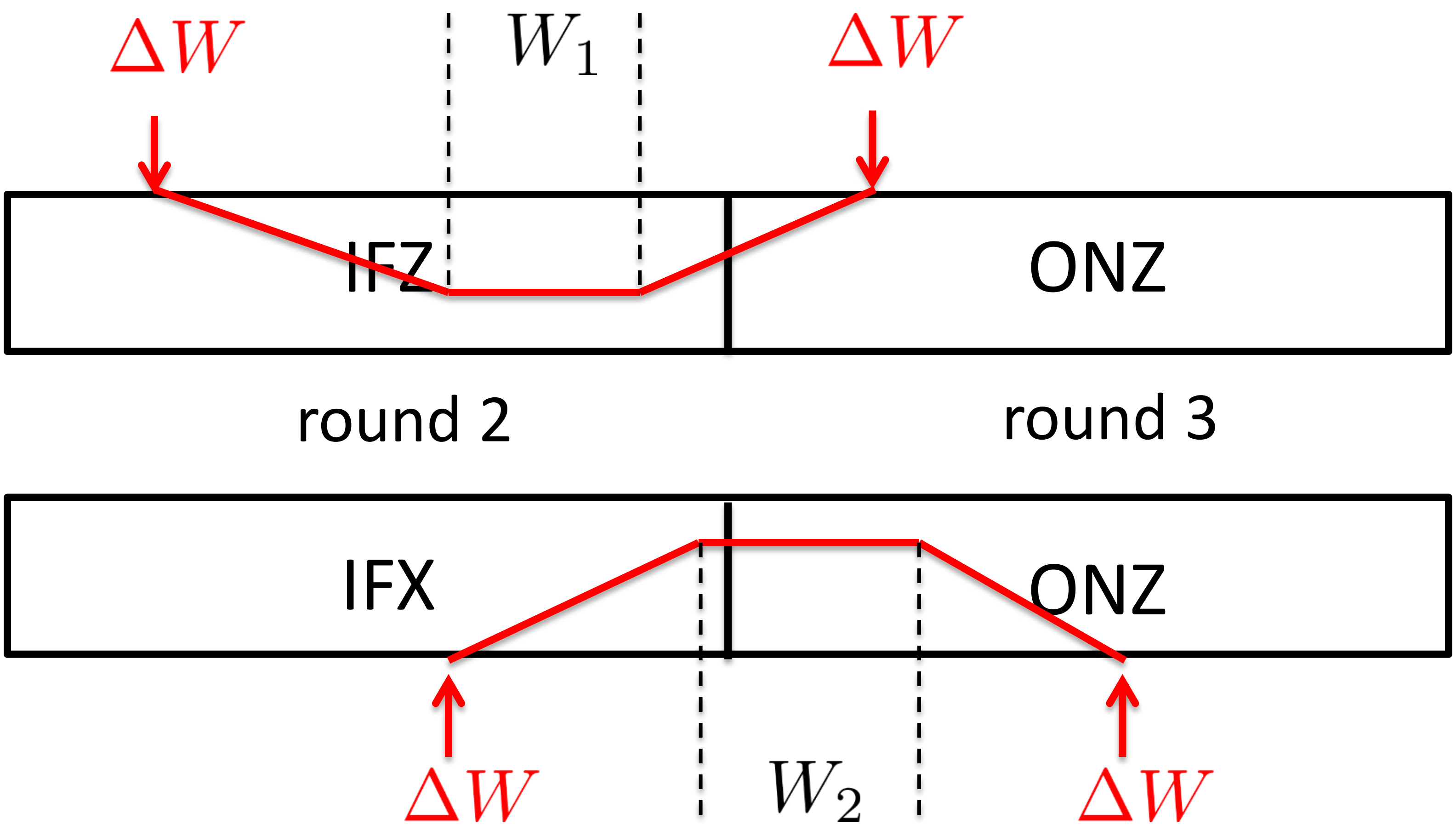
- **Non-linear** differential **path** should **locate** in **rounds** with a **strong absorption** Boolean function.
  - ➢ **Easier** to **search** non-linear path
  - ➢ **Sparser** non-linear paths

Rationale of Our Attack Strategy

- Attack starts from the **second round**
- Discuss attacks starting from the first round **later**.

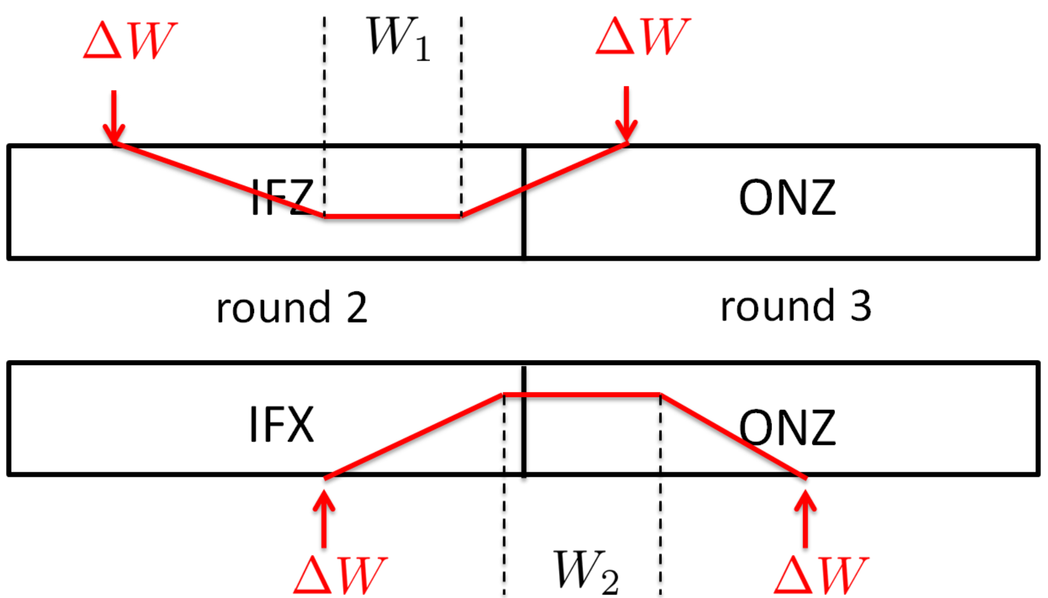
Rationale of Our Attack Strategy

- Message words locate in **different steps** between the two branches



Rationale of Our Attack Strategy

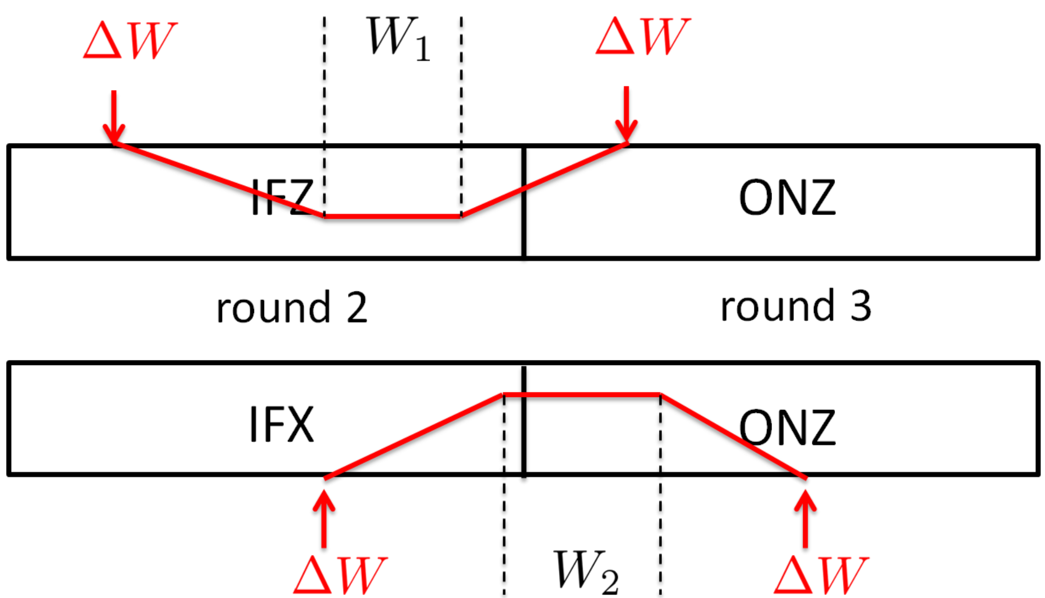
- A **waste** of message word **freedom** exists if the search **starts** from the **beginning step**.



Rationale of Our Attack Strategy

- A **waste** of message word **freedom** exists if the search **starts** from the beginning **step**.
- W_1, W_2 : two subsets of the message words in the **dense part** of the two **differential paths**

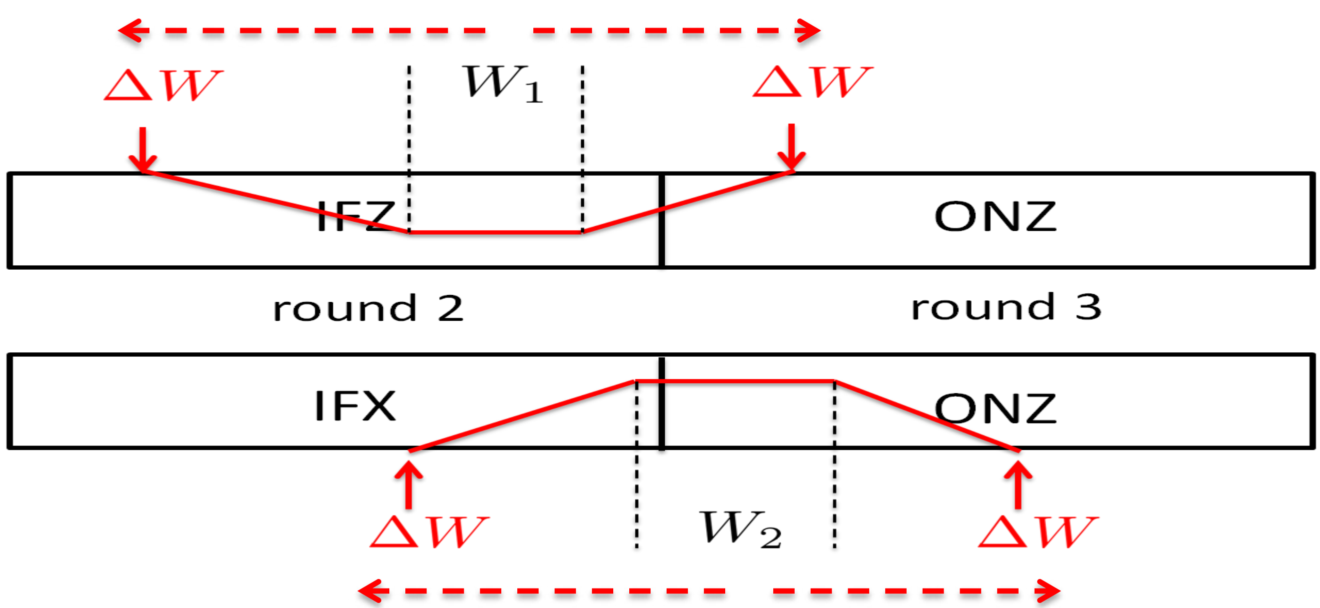
  - $W_1 \neq W_2$



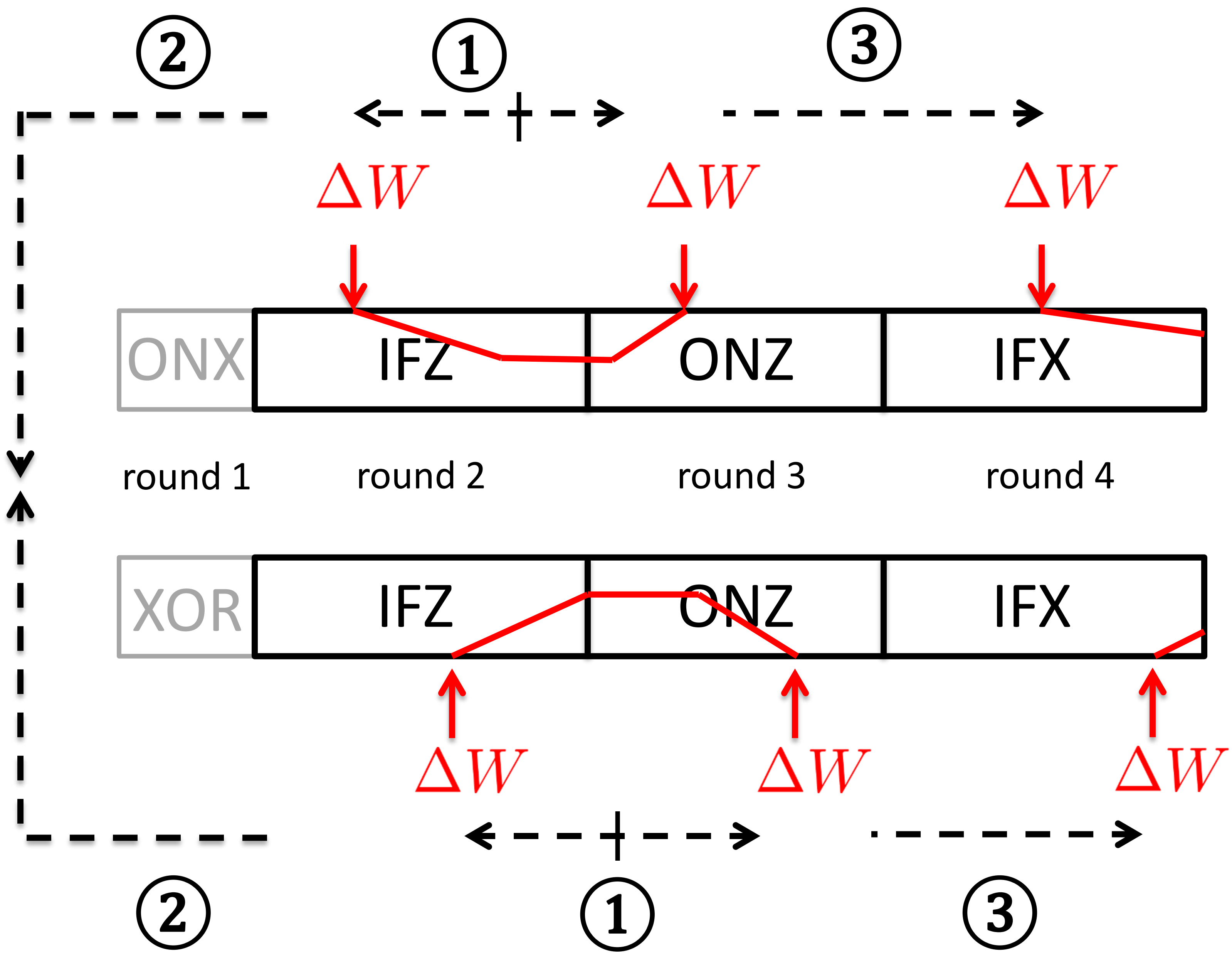
Rationale of Our Attack Strategy

- Satisfy **dense parts** firstly by **using** the **freedom** of **internal state** and the **message words**.

  - Use the independency between W_1 and W_2
  - **Start-from-the-middle** procedures



Wrapping up



②
①
③
ΔW
ΔW
ΔW
ONX
IFZ
ONZ
IFX
round 1
round 2
round 3
round 4
XOR
IFZ
ONZ
IFX
ΔW
ΔW
ΔW
②
①
③

Outline

- RIPEMD-160 specification
- Attack overview
- **Find a differential path**
  - **Choose message difference**
  - **Search non-linear path**
- Find a confirming pair
- Conclusion

The Choice of Message Word

- **Single** message word difference
- Examine the **potential #attacked steps** for each messages word with respect to
  - ➢ short non-linear paths in both branch
  - ➢ early step of the two non-linear path are near
  - ➢ sparse later steps of non-linear path
  - ➢ output difference cancellation of the two branches by the feed-forward operation

The Choice of Message Word

Message word	W_0	W_1	W_2	W_3
#attacked steps	51	46	52	48

Message word	W_4	W_5	W_6	W_7
#attacked steps	42	50	39	56

Message word	W_8	W_9	W_{10}	W_{11}
#attacked steps	36	39	37	38

Message word	W_{12}	W_{13}	W_{14}	W_{15}
#attacked steps	38	34	58	43

The Choice of Message Word

Message word	W_0	W_1	W_2	W_3
#attacked steps	51	46	52	48

Message word	W_4	W_5	W_6	W_7
#attacked steps	42	50	39	**56**

Message word	W_8	W_9	W_{10}	W_{11}
#attacked steps	36	39	37	38

Message word	W_{12}	W_{13}	W_{14}	W_{15}
#attacked steps	38	34	**58**	43

Automatic Non-Linear Path Search

- **Bit-slices** for all operations including **modular addition** in the **step function** developed in [CR06]

- Generalized conditions for two bits x and $x*$

(x, x^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
?	✓	✓	✓	✓
-	✓	-	-	✓
x	-	✓	✓	-
0	✓	-	-	-
u	-	✓	-	-
n	-	-	✓	-
1	-	-	-	✓
#	-	-	-	-

(x, x^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
3	✓	✓	-	-
5	✓	-	✓	-
7	✓	✓	✓	-
A	-	✓	-	✓
B	✓	✓	-	✓
C	-	-	✓	✓
D	✓	-	✓	✓
E	-	✓	✓	✓

Automatic Non-Linear Path Search

- **Bit-slices** for all operations including **modular addition** in the **step function** developed in [CR06]

- Generalized conditions for two bits x and $x*$
  - ➢ Initialize each bit as ?

(x, x^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
?	✓	✓	✓	✓
-	✓	-	-	✓
x	-	✓	✓	-
0	✓	-	-	-
u	-	✓	-	-
n	-	-	✓	-
1	-	-	-	✓
#	-	-	-	-

(x, x^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
3	✓	✓	-	-
5	✓	-	✓	-
7	✓	✓	✓	-
A	-	✓	-	✓
B	✓	✓	-	✓
C	-	-	✓	✓
D	✓	-	✓	✓
E	-	✓	✓	✓

Automatic Non-Linear Path Search

- **Bit-slices** for all operations including **modular addition** in the **step function** developed in [CR06]
- Generalized conditions for two bits x and $x*$
  - Initialize each bit as ?
  - Finalize each bit as one of {-, u, n, 0, 1}

(x, x^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
?	✓	✓	✓	✓
-	✓	-	-	✓
x	-	✓	✓	-
0	✓	-	-	-
u	-	✓	-	-
n	-	-	✓	-
1	-	-	-	✓
#	-	-	-	-

(x, x^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
3	✓	✓	-	-
5	✓	-	✓	-
7	✓	✓	✓	-
A	-	✓	-	✓
B	✓	✓	-	✓
C	-	-	✓	✓
D	✓	-	✓	✓
E	-	✓	✓	✓

Automatic Non-Linear Path Search

- Use the algorithm developed in [MNS11, MNS12]

Decision (Guessing)

1. Pick randomly an unrestricted decision bit.
2. Impose new constraints on this decision bit.

Deduction (Propagation)

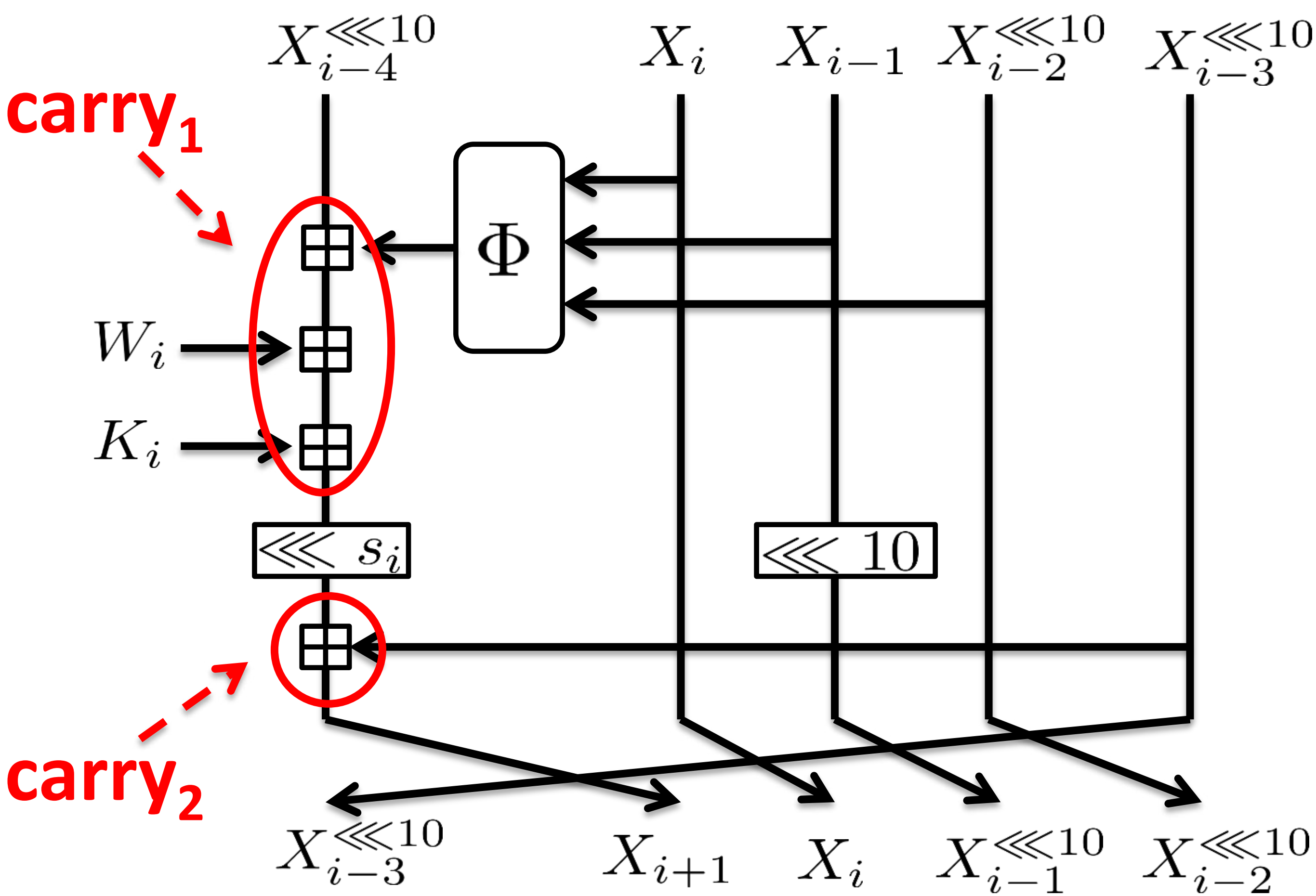
3. Propagate the new information to other variables and equations
4. If an inconsistency is detected start backtracking, else continue with step 1.

Backtracking (Correction)

5. Try a different choice for the decision bit.
6. If all choices result in an inconsistency, mark the bit as critical.
7. Jump back until the critical bit can be resolved.
8. Continue with step 1.

Specific Configuration for RIPEMD-160

- Two carries to handle in one step function
  - ➢ Computed and stored together as a **3-bit condition**



Resulted Differential Path

- Use message word M_7
- **48** steps (16-64)

Step	X_i	W_i^l	Π_i^l
12	-------- -------- -------- --------		
13	-------- -------- -------- --------		
14	-------- -------- -------- --------		
15	-------- -------- -------- --------		
16	-------- -------- -------- --------	x------- -------- -------- --------	7
17	-------- -------- -------- -n------	-------- -------- -------- --------	4
18	-------- -------- -------- -0------	-------- -------- -------- --------	13
19	-------- -------1 -------- -1------	-------- -------- -------- --------	1
20	-------- -------0 -------- --------	-------- -------- -------- --------	10
21	-------- -------n -------- --------	-------- -------- -------- --------	6
22	-------- -------0 -------- --------	-------- -------- -------- --------	15
23	-----1-- -------0 -------- --------	-------- -------- -------- --------	3
24	1----1-- -------- -------- --------	-------- -------- -------- --------	12
25	-----n-- ---1--1- ------0- --------	-------- -------- -------- --------	0
26	001-00-- ------un nnnn--nu u1--0---	-------- -------- -------- --------	9
27	-n--n-un -u--0100 0000--11 1010----	-------- -------- -------- --------	5
28	1010001- ----00nu --n0-nu- u-un0110	-------- -------- -------- --------	2
29	0-nun-0- 11-u--0u -1010101 1-u0nnu-	-------- -------- -------- --------	14
30	-000-111 uu010n10 1u-1nu1n -00nn000	-------- -------- -------- --------	11
31	-n---1-u 0uu1-0-1 000011n0 0001n---	-------- -------- -------- --------	8
32	-10----0 -010---u -1--1u10 ----01--	-------- -------- -------- --------	3
33	-n-----u --u----1 -----1-- 1----0--	-------- -------- -------- --------	10
34	-11----0 --0----- ----1--- u-------	-------- -------- -------- --------	14
35	-------n --n----- -------- 1--1----	-------- -------- -------- --------	4
36	-------1 --0----- ----0--- u----1--	-------- -------- -------- --------	9
37	-------- --n---1- -------- 1----0--	-------- -------- -------- --------	15
38	-------- --0---0- -------- --------	-------- -------- -------- --------	8
39	-------- -------- -------- --------	-------- -------- -------- --------	1
40	-------- -------- -------- --------	-------- -------- -------- --------	2
41	-------- -------- -------- --------	x------- -------- -------- --------	7
42	-------- -------- -------- --------	-------- -------- -------- --------	0
43	-------- -------- -------- --------	-------- -------- -------- --------	6
44	-------- -------- -------- --------	-------- -------- -------- --------	13
45	-------- -------- -------- --------	-------- -------- -------- --------	11
46	-------- -------- -------- --------	-------- -------- -------- --------	5
47	-------- -------- -------- --------	-------- -------- -------- --------	12
48	-------- -------- -------- --------	-------- -------- -------- --------	1
49	-------- -------- -------- --------	-------- -------- -------- --------	9
50	-------- -------- -------- --------	-------- -------- -------- --------	11
51	-------- -------- -------- --------	-------- -------- -------- --------	10
52	-------- -------- -------- --------	-------- -------- -------- --------	0
53	-------- -------- -------- --------	-------- -------- -------- --------	8
54	-------- -------- -------- --------	-------- -------- -------- --------	12
55	-------- -------- -------- --------	-------- -------- -------- --------	4
56	-------- -------- -------- --------	-------- -------- -------- --------	13
57	-----0-- -------- -------- --------	-------- -------- -------- --------	3
58	-----1-- -------- -------- --------	x------- -------- -------- --------	7
59	-------- -------- -------- ---n----	-------- -------- -------- --------	15
60	-------- -------- -------- --------	-------- -------- -------- --------	14
61	-------- -------- -------- --01----	-------- -------- -------- --------	5
62	-------- -------- -------- --------	-------- -------- -------- --------	6
63	-------- -------- nu------ --------	-------- -------- -------- --------	2
64	-------- -------- -------- --------		

Step	Y_i	W_i^r	Π_i^r
12	-------- -------- -------- --------		
13	-------- -------- -------- --------		
14	-------- -------- -------- --------		
15	-------- -------- -------- --------		
16	-------- -------- -------- --------	-------- -------- -------- --------	6
17	-------- -------- -------- --------	-------- -------- -------- --------	11
18	--01---- 01------ -------- --------	-------- -------- -------- --------	3
19	---1---- -------- -------1 --------	x------- -------- -------- --------	7
20	11------ -----100 -------1 -u---001	-------- -------- -------- --------	0
21	11-01--- -----u10 1-----11 1----111	-------- -------- -------- --------	13
22	---unn-- --0--1-1 0--nuuuu 01----0u	-------- -------- -------- --------	5
23	---00un- 011-uuu- --0----- -un0----	-------- -------- -------- --------	10
24	u11n1--- ----11-1 1-0-u--- -1nn0010	-------- -------- -------- --------	14
25	0-u110-- n-0----1 11--u10- -1-0n1nu	-------- -------- -------- --------	15
26	----1--1 -11---1- 00-n1nnn -nnnu---	-------- -------- -------- --------	8
27	1---1u-- 0-uu--1n 1---00-- ---0-unn	-------- -------- -------- --------	12
28	----u--- --n1--00 0--011-- --n0--n1	-------- -------- -------- --------	4
29	-------- ---u--1- 0u-11u-- ---0---0	-------- -------- -------- --------	9
30	-0--n--- --n----- 1---1--- --------	-------- -------- -------- --------	1
31	-1------ --1----- -----u-- --1-----	-------- -------- -------- --------	2
32	-------- --u----- -----1-- --0-----	-------- -------- -------- --------	15
33	-------- -------- -------- --------	-------- -------- -------- --------	5
34	-------- -------- -------- --------	-------- -------- -------- --------	1
35	-------- -------- -------- --------	-------- -------- -------- --------	3
36	-------- -------- -------- --------	x------- -------- -------- --------	7
37	-------- -------- -------- --------	-------- -------- -------- --------	14
38	-------- -------- -------- --------	-------- -------- -------- --------	6
39	-------- -------- -------- --------	-------- -------- -------- --------	9
40	-------- -------- -------- --------	-------- -------- -------- --------	11
41	-------- -------- -------- --------	-------- -------- -------- --------	8
42	-------- -------- -------- --------	-------- -------- -------- --------	12
43	-------- -------- -------- --------	-------- -------- -------- --------	2
44	-------- -------- -------- --------	-------- -------- -------- --------	10
45	-------- -------- -------- --------	-------- -------- -------- --------	0
46	-------- -------- -------- --------	-------- -------- -------- --------	4
47	-------- -------- -------- --------	-------- -------- -------- --------	13
48	-------- -------- -------- --------	-------- -------- -------- --------	8
49	-------- -------- -------- --------	-------- -------- -------- --------	6
50	-------- -------- -------- --------	-------- -------- -------- --------	4
51	-------- -------- -------- --------	-------- -------- -------- --------	1
52	-------- -------- -------- --------	-------- -------- -------- --------	3
53	-------- -------- -------- --------	-------- -------- -------- --------	11
54	-------- -------- -------- --------	-------- -------- -------- --------	15
55	-------- -------- -------- --------	-------- -------- -------- --------	0
56	-------- -------- -------- --------	-------- -------- -------- --------	5
57	-------- -------- -------- --------	-------- -------- -------- --------	12
58	-------- -------- -------- --------	-------- -------- -------- --------	2
59	-------- -------- -------- --------	-------- -------- -------- --------	13
60	-------- -------- -------- --------	-------- -------- -------- --------	9
61	-------- -------- -------- --------	x------- -------- -------- --------	7
62	-------- -------- -------- ---u----	-------- -------- -------- --------	10
63	-------- -------- -------- ---0----	-------- -------- -------- --------	14
64	-------- -------- -------- --------		

Resulted Differential Path

- Use message word M_7
- **48** steps (16-64)

Dense parts

Step	X_i	W_i^l	Π_i^l
12	-------- -------- -------- --------		
13	-------- -------- -------- --------		
14	-------- -------- -------- --------		
15	-------- -------- -------- --------		
16	-------- -------- -------- --------	x------- -------- -------- --------	7
17	-------- -------- -------- -n------	-------- -------- -------- --------	4
18	-------- -------- -------- -0------	-------- -------- -------- --------	13
19	-------- -------1 -------- -1------	-------- -------- -------- --------	1
20	-------- -------0 -------- --------	-------- -------- -------- --------	10
21	-------- -------n -------- --------	-------- -------- -------- --------	6
22	-------- -------0 -------- --------	-------- -------- -------- --------	15
23	-----1-- -------0 -------- --------	-------- -------- -------- --------	3
24	1----1-- -------- -------- --------	-------- -------- -------- --------	12
25	-----n-- ---1--1- ------0- --------	-------- -------- -------- --------	0
26	001-00-- ------un nnnn--nu u1--0---	-------- -------- -------- --------	9
27	-n--n-un -u--0100 0000--11 1010----	-------- -------- -------- --------	5
28	1010001- ----00nu --n0-nu- u-un0110	-------- -------- -------- --------	2
29	0-nun-0- 11-u--0u -1010101 1-u0nnu-	-------- -------- -------- --------	14
30	-000-111 uu010n10 1u-1nu1n -00nn000	-------- -------- -------- --------	11
31	-n---1-u 0uu1-0-1 000011n0 0001n---	-------- -------- -------- --------	8
32	-10----0 -010---u -1--1u10 ----01--	-------- -------- -------- --------	3
33	-n-----u --u----1 -----1-- 1----0--	-------- -------- -------- --------	10
34	-11----0 --0----- ----1--- u-------	-------- -------- -------- --------	14
35	-------n --n----- -------- 1--1----	-------- -------- -------- --------	4
36	-------1 --0----- ----0--- u----1--	-------- -------- -------- --------	9
37	-------- --n---1- -------- 1----0--	-------- -------- -------- --------	15
38	-------- --0---0- -------- --------	-------- -------- -------- --------	8
39	-------- -------- -------- --------	-------- -------- -------- --------	1
40	-------- -------- -------- --------	-------- -------- -------- --------	2
41	-------- -------- -------- --------	x------- -------- -------- --------	7
42	-------- -------- -------- --------	-------- -------- -------- --------	0
43	-------- -------- -------- --------	-------- -------- -------- --------	6
44	-------- -------- -------- --------	-------- -------- -------- --------	13
45	-------- -------- -------- --------	-------- -------- -------- --------	11
46	-------- -------- -------- --------	-------- -------- -------- --------	5
47	-------- -------- -------- --------	-------- -------- -------- --------	12
48	-------- -------- -------- --------	-------- -------- -------- --------	1
49	-------- -------- -------- --------	-------- -------- -------- --------	9
50	-------- -------- -------- --------	-------- -------- -------- --------	11
51	-------- -------- -------- --------	-------- -------- -------- --------	10
52	-------- -------- -------- --------	-------- -------- -------- --------	0
53	-------- -------- -------- --------	-------- -------- -------- --------	8
54	-------- -------- -------- --------	-------- -------- -------- --------	12
55	-------- -------- -------- --------	-------- -------- -------- --------	4
56	-------- -------- -------- --------	-------- -------- -------- --------	13
57	-----0-- -------- -------- --------	-------- -------- -------- --------	3
58	-----1-- -------- -------- --------	x------- -------- -------- --------	7
59	-------- -------- -------- ---n----	-------- -------- -------- --------	15
60	-------- -------- -------- --------	-------- -------- -------- --------	14
61	-------- -------- -------- --01----	-------- -------- -------- --------	5
62	-------- -------- -------- --------	-------- -------- -------- --------	6
63	-------- -------- nu------ --------	-------- -------- -------- --------	2
64	-------- -------- -------- --------		

Step	Y_i	W_i^r	Π_i^r
12	-------- -------- -------- --------		
13	-------- -------- -------- --------		
14	-------- -------- -------- --------		
15	-------- -------- -------- --------		
16	-------- -------- -------- --------	-------- -------- -------- --------	6
17	-------- -------- -------- --------	-------- -------- -------- --------	11
18	--01---- 01------ -------- --------	-------- -------- -------- --------	3
19	---1---- -------- -------1 --------	x------- -------- -------- --------	7
20	11------ -----100 -------1 -u---001	-------- -------- -------- --------	0
21	11-01--- -----u10 1-----11 1----111	-------- -------- -------- --------	13
22	---unn-- --0--1-1 0--nuuuu 01----0u	-------- -------- -------- --------	5
23	---00un- 011-uuu- --0----- -un0----	-------- -------- -------- --------	10
24	u11n1--- ----11-1 1-0-u--- -1nn0010	-------- -------- -------- --------	14
25	0-u110-- n-0----1 11--u10- -1-0n1nu	-------- -------- -------- --------	15
26	----1--1 -11---1- 00-n1nnn -nnnu---	-------- -------- -------- --------	8
27	1---1u-- 0-uu--1n 1---00-- ---0-unn	-------- -------- -------- --------	12
28	----u--- --n1--00 0--011-- --n0--n1	-------- -------- -------- --------	4
29	-------- ---u--1- 0u-11u-- ---0---0	-------- -------- -------- --------	9
30	-0--n--- --n----- 1---1--- --------	-------- -------- -------- --------	1
31	-1------ --1----- -----u-- --1-----	-------- -------- -------- --------	2
32	-------- --u----- -----1-- --0-----	-------- -------- -------- --------	15
33	-------- -------- -------- --------	-------- -------- -------- --------	5
34	-------- -------- -------- --------	-------- -------- -------- --------	1
35	-------- -------- -------- --------	-------- -------- -------- --------	3
36	-------- -------- -------- --------	x------- -------- -------- --------	7
37	-------- -------- -------- --------	-------- -------- -------- --------	14
38	-------- -------- -------- --------	-------- -------- -------- --------	6
39	-------- -------- -------- --------	-------- -------- -------- --------	9
40	-------- -------- -------- --------	-------- -------- -------- --------	11
41	-------- -------- -------- --------	-------- -------- -------- --------	8
42	-------- -------- -------- --------	-------- -------- -------- --------	12
43	-------- -------- -------- --------	-------- -------- -------- --------	2
44	-------- -------- -------- --------	-------- -------- -------- --------	10
45	-------- -------- -------- --------	-------- -------- -------- --------	0
46	-------- -------- -------- --------	-------- -------- -------- --------	4
47	-------- -------- -------- --------	-------- -------- -------- --------	13
48	-------- -------- -------- --------	-------- -------- -------- --------	8
49	-------- -------- -------- --------	-------- -------- -------- --------	6
50	-------- -------- -------- --------	-------- -------- -------- --------	4
51	-------- -------- -------- --------	-------- -------- -------- --------	1
52	-------- -------- -------- --------	-------- -------- -------- --------	3
53	-------- -------- -------- --------	-------- -------- -------- --------	11
54	-------- -------- -------- --------	-------- -------- -------- --------	15
55	-------- -------- -------- --------	-------- -------- -------- --------	0
56	-------- -------- -------- --------	-------- -------- -------- --------	5
57	-------- -------- -------- --------	-------- -------- -------- --------	12
58	-------- -------- -------- --------	-------- -------- -------- --------	2
59	-------- -------- -------- --------	-------- -------- -------- --------	13
60	-------- -------- -------- --------	-------- -------- -------- --------	9
61	-------- -------- -------- --------	x------- -------- -------- --------	7
62	-------- -------- -------- ---u----	-------- -------- -------- --------	10
63	-------- -------- -------- ---0----	-------- -------- -------- --------	14
64	-------- -------- -------- --------		

Outline

- RIPEMD-160 specification
- Attack overview
- Find a differential path
- **Find a confirming pair**
  - **Merge two branches**
  - **Evaluate complexity**
- Conclusion

Merge Two Branches

- Refer to the paper for detailed procedure

Phase 1. fix some free bits to **fulfill in advance** some **conditions** in differential path

Phase 2. **start-from-the-middle adaptively** choose free bits **sequentially** to fulfill conditions in **dense part** of differential path

Phase 3. use remaining free bits to merge the internal states of both branches to a **freely chosen** cv

Merge Two Branches

Step	X_i	W_i^l	Π_i^l	Step	Y_i	W_i^r	Π_i^r
12	-------- -------- -------- --------			12	-------- -------- -------- --------		
13	-------- -------- -------- --------			13	-------- -------- -------- --------		
14	-------- -------- -------- --------			14	-------- -------- -------- --------		
15	-------- -------- -------- --------			15	-------- -------- -------- --------		
16	-------- -------- -------- --------	x------- -------- -------- --------	7	16	-------- -------- -------- --------	-------- -------- -------- --------	6
17	-------- -------- -------- -n------	-------- -------- -------- --------	4	17	-------- -------- -------- --------	-------- -------- -------- --------	11
18	-------- -------- -------- -0------	-------- -------- -------- --------	13	18	--01---- 01------ -------- --------	-------- -------- -------- --------	3
19	-------- -------1 -------- -1------	-------- -------- -------- --------	1	19	---1---- -------- -------1 --------	x------- -------- -------- --------	7
20	-------- -------0 -------- --------	-------- -------- -------- --------	10	20	11------ -----100 -------1 -u---001	-------- -------- -------- --------	0
21	-------- -------n -------- --------	-------- -------- -------- --------	6	21	11-01--- -----u10 1-----11 1----111	-------- -------- -------- --------	13
22	-------- -------0 -------- --------	-------- -------- -------- --------	15	22	---unn-- --0--1-1 0--nuuuu 01----0u	-------- -------- -------- --------	5
23	-----1-- -------0 -------- --------	-------- -------- -------- --------	3	23	---00un- 011-uuu- --0----- -un0----	-------- -------- -------- --------	10
24	1----1-- -------- -------- --------	-------- -------- -------- --------	12	24	u11n1--- ----11-1 1-0-u--- -1nn0010	-------- -------- -------- --------	14
25	-----n-- ---1--1- ------0- --------	-------- -------- -------- --------	0	25	0-u110-- n-0----1 11--u10- -1-0n1nu	-------- -------- -------- --------	15
26	001-00-- ------un nnnn--nu u1--0---	-------- -------- -------- --------	9	26	----1--1 -11---1- 00-n1nnn -nnnu---	-------- -------- -------- --------	8
27	-n--n-un -u--0100 0000--11 1010----	-------- -------- -------- --------	5	27	1---1u-- 0-uu--1n 1---00-- ---0-unn	-------- -------- -------- --------	12
28	1010001- ----00nu --n0-nu- u-un0110	-------- -------- -------- --------	2	28	----u--- --n1--00 0--011-- --n0--n1	-------- -------- -------- --------	4
29	0-nun-0- 11-u--0u -1010101 1-u0nnu-	-------- -------- -------- --------	14	29	-------- ---u--1- 0u-11u-- ---0---0	-------- -------- -------- --------	9
30	-000-111 uu010n10 1u-1nu1n -00nn000	-------- -------- -------- --------	11	30	-0--n--- --n----- 1---1--- --------	-------- -------- -------- --------	1
31	-n---1-u 0uu1-0-1 000011n0 0001n---	-------- -------- -------- --------	8	31	-1------ --1----- -----u-- --1-----	-------- -------- -------- --------	2
32	-10----0 -010---u -1--1u10 ----01--	-------- -------- -------- --------	3	32	-------- --u----- -----1-- --0-----	-------- -------- -------- --------	15
33	-n-----u --u----1 -----1-- 1----0--	-------- -------- -------- --------	10	33	-------- -------- -------- --------	-------- -------- -------- --------	5
34	-11----0 --0----- ----1--- u-------	-------- -------- -------- --------	14	34	-------- -------- -------- --------	-------- -------- -------- --------	1
35	-------n --n----- -------- 1--1----	-------- -------- -------- --------	4	35	-------- -------- -------- --------	-------- -------- -------- --------	3
36	-------1 --0----- ----0--- u----1--	-------- -------- -------- --------	9	36	-------- -------- -------- --------	x------- -------- -------- --------	7
37	-------- --n---1- -------- 1----0--	-------- -------- -------- --------	15	37	-------- -------- -------- --------	-------- -------- -------- --------	14
38	-------- --0---0- -------- --------	-------- -------- -------- --------	8	38	-------- -------- -------- --------	-------- -------- -------- --------	6
39	-------- -------- -------- --------	-------- -------- -------- --------	1	39	-------- -------- -------- --------	-------- -------- -------- --------	9
40	-------- -------- -------- --------	-------- -------- -------- --------	2	40	-------- -------- -------- --------	-------- -------- -------- --------	11

Merge Two Branches

Step	X_i	W_i^l	Π_i^l
12	-------- -------- -------- --------		
13	-------- -------- -------- --------		
14	-------- -------- -------- --------		
15	-------- -------- -------- --------		
16	-------- -------- -------- --------	x------- -------- -------- --------	7
17	-------- -------- -------- -n------	-------- -------- -------- --------	4
18	-------- -------- -------- -0------	-------- -------- -------- --------	13
19	-------- -------1 -------- -1------	-------- -------- -------- --------	1
20	-------- -------0 -------- --------	-------- -------- -------- --------	10
21	-------- -------n -------- --------	-------- -------- -------- --------	6
22	-------- -------0 -------- --------	-------- -------- -------- --------	15
23	-----1-- -------0 -------- --------	-------- -------- -------- --------	3
24	1----1-- -------- -------- --------	-------- -------- -------- --------	12
25	-----n-- ---1--1- ------0- --------	-------- -------- -------- --------	0
26	001-00-- ------un nnnn--nu u1--0---	-------- -------- -------- --------	9
27	-n--n-un -u--0100 0000--11 1010----	-------- -------- -------- --------	5
28	1010001- ----00nu --n0-nu- u-un0110	-------- -------- -------- --------	2
29	0-nun-0- 11-u--0u -1010101 1-u0nnu-	-------- -------- -------- --------	14
30	-000-111 uu010n10 1u-1nu1n -00nn000	-------- -------- -------- --------	11
31	-n---1-u 0uu1-0-1 000011n0 0001n---	-------- -------- -------- --------	8
32	-10----0 -010---u -1--1u10 ----01--	-------- -------- -------- --------	3
33	-n-----u --u----1 -----1-- 1----0--	----	[illegible]
34	-11----0 --0----- ----1--- u-------	----	[illegible]
35	-------n --n----- -------- 1--1----	----	[illegible]
36	-------1 --0----- ----0--- u----1--	-------- -------- -------- --------	9
37	-------- --n---1- -------- 1----0--	-------- -------- -------- --------	15
38	-------- --0---0- -------- --------	-------- -------- -------- --------	8
39	-------- -------- -------- --------	-------- -------- -------- --------	1
40	-------- -------- -------- --------	-------- -------- -------- --------	2

Step	Y_i	W_i^r	Π_i^r
12	-------- -------- -------- --------		
13	-------- -------- -------- --------		
14	-------- -------- -------- --------		
15	-------- -------- -------- --------		
16	-------- -------- -------- --------	-------- -------- -------- --------	6
17	-------- -------- -------- --------	-------- -------- -------- --------	11
18	--01---- 01------ -------- --------	-------- -------- -------- --------	3
19	---1---- -------- -------1 --------	x------- -------- -------- --------	7
20	11------ -----100 -------1 -u---001	-------- -------- -------- --------	0
21	11-01--- -----u10 1-----11 1----111	-------- -------- -------- --------	13
22	---unn-- --0--1-1 0--nuuuu 01----0u	-------- -------- -------- --------	5
23	---00un- 011-uuu- --0----- -un0----	-------- -------- -------- --------	10
24	u11n1--- ----11-1 1-0-u--- -1nn0010	-------- -------- -------- --------	14
25	0-u110-- n-0----1 11--u10- -1-0n1nu	-------- -------- -------- --------	15
26	----1--1 -11---1- 00-n1nnn -nnnu---	-------- -------- -------- --------	8
27	1---1u-- 0-uu--1n 1---00-- ---0-unn	-------- -------- -------- --------	12
28	----u--- --n1--00 0--011-- --n0--n1	-------- -------- -------- --------	4
29	-------- ---u--1- 0u-11u-- ---0---0	-------- -------- -------- --------	9
30	-0--n--- --n----- 1---1--- --------	-------- -------- -------- --------	1
31	-1------ --1----- -----u-- --1-----	-------- -------- -------- --------	2
32	-------- --u----- -----1-- --0-----	-------- -------- -------- --------	15
[illegible]	[illegible]	----	5
[illegible]	[illegible]	----	1
[illegible]	[illegible]	----	3
36	-------- -------- -------- --------	x------- -------- -------- --------	7
37	-------- -------- -------- --------	-------- -------- -------- --------	14
38	-------- -------- -------- --------	-------- -------- -------- --------	6
39	-------- -------- -------- --------	-------- -------- -------- --------	9
40	-------- -------- -------- --------	-------- -------- -------- --------	11

Fix these internal state words

Merge Two Branches

Step	X_i	W^l_i	Π^l_i	Step	Y_i	W^r_i	Π^r_i
12	-------- -------- -------- --------			12	-------- -------- -------- --------		
13	-------- -------- -------- --------			13	-------- -------- -------- --------		
14	-------- -------- -------- --------			14	-------- -------- -------- --------		
15	-------- -------- -------- --------			15	-------- -------- -------- --------		
16	-------- -------- -------- --------	x------- -------- -------- --------	7	16	-------- -------- -------- --------	-------- -------- -------- --------	6
17	-------- -------- -------- -n------	-------- -------- -------- --------	4	17	-------- -------- -------- --------	-------- -------- -------- --------	11
18	-------- -------- -------- -0------	-------- -------- -------- --------	13	18	--01---- 01------ -------- --------	-------- -------- -------- --------	3
19	-------- -------1 -------- -1------	-------- -------- -------- --------	1	19	---1---- -------- -------1 --------	x------- -------- -------- --------	7
20	-------- -------0 -------- --------	-------- -------- -------- --------	10	20	11------ -----100 -------1 -u---001	-------- -------- -------- --------	0
21	-------- -------n -------- --------	-------- -------- -------- --------	6	21	11-01--- -----u10 1-----11 1----111	-------- -------- -------- --------	13
22	-------- -------0 -------- --------	-------- -------- -------- --------	15	22	---unn-- --0--1-1 0--nuuuu 01----0u	-------- -------- -------- --------	5
23	-----1-- -------0 -------- --------	-------- -------- -------- --------	3	23	---00un- 011-uuu- --0----- -un0----	-------- -------- -------- --------	10
24	1----1-- -------- -------- --------	-------- -------- -------- --------	12	24	u11n1--- ----11-1 1-0-u--- -1nn0010	-------- -------- -------- --------	14
25	-----n-- ---1--1- ------0- --------	-------- -------- -------- --------	0	25	0-u110-- n-0----1 11--u10- -1-0n1nu	-------- -------- -------- --------	15
26	001-00-- ------un nnnn--nu u1--0---	-------- -------- -------- --------	9	26	----1--1 -11---1- 00-n1nnn -nnnu---	-------- -------- -------- --------	8
27	-n--n-un -u--0100 0000--11 1010----	-------- -------- -------- --------	5	27	1---1u-- 0-un--1n 1---00-- ---0-unn	-------- -------- -------- --------	12
28	1010001- ----00nu --n0-nu- u-un0110	-------- -------- -------- --------	2	28	----u--- --n1--00 0--011-- --n0--n1	-------- -------- -------- --------	4
29	0-nun-0- 11-u--0u -1010101 1-u0nnu-	-------- -------- -------- --------	14	29	-------- ---u--1- 0u-11u-- ---0---0	-------- -------- -------- --------	9
30	-000-111 uu010n10 1u-1nu1n -00nn000	-------- -------- -------- --------	11	30	-0--n--- --n----- 1---1--- --------	-------- -------- -------- --------	1
31	-n---1-u 0u1-0--1 000011n0 0001n---	-				--- --------	2
32	-10----0 -010---u -1--1u10 ----01--	-				--- --------	15
33	-n-----u --1----1 -----1-- 1----0--	-				--- --------	5
34	-11----0 --0----- ----1--- u-------	-				--- --------	1
35	-------n --n----- -------- 1--1----	-				--- --------	3
36	-------1 --0----- ----0--- u----1--	-				--- --------	7
37	-------- --n---1- -------- 1----0--	-				--- --------	14
38	-------- --0---0- -------- --------	-				--- --------	6
39	-------- -------- -------- --------	-------- -------- -------- --------	1	39	-------- -------- -------- --------	-------- -------- -------- --------	9
40	-------- -------- -------- --------	-------- -------- -------- --------	2	40	-------- -------- -------- --------	-------- -------- -------- --------	11

Adaptively choose message words forward and backward to fulfill the conditions

A “Starting Point” after Phase 2

Step	X_i	W_i^l	Π_i^l
12	-------- -------- -------- --------		
13	-------- -------- -------- --------		
14	-------- -------- -------- --------		
15	-------- -------- -------- --------		
16	-------- -------- -------- --------	x------- -------- -------- --------	7
17	-------- -------- -------- -n------	-------- -------- -------- --------	4
18	-------- -------- -------- -0------	-------- -------- -------- --------	13
19	-------- -------1 -------- -1------	-------- -------- -------- --------	1
20	-------- -------0 -------- --------	00000011 00100101 10100111 00001111	10
21	-------- -------n -------- --------	-------- -------- -------- --------	6
22	-------- -------0 00111100 0-----00	11110110 11100100 10110100 00010001	15
23	01101110 00100100 11111101 10111000	01001111 11011100 00000100 11100000	3
24	11010101 00011001 01001010 10110101	11101100 10100110 10100100 11100111	12
25	11101n11 11110111 01100001 10110000	-------- -------- -------- --------	0
26	00110001 001001un nnnn00nu u1010001	-----011 01000010 -------- --------	9
27	0n00n1un 0u110100 00001111 10101010	01100000 11111110 10100110 01000000	5
28	10100010 101100nu 00n00nu1 u0un0110	01101100 10101011 01110010 00010011	2
29	01nun101 110u110u 11010101 11u0nnu1	11000000 00110011 00110000 01100000	14
30	00001111 uu010n10 1u11nu1n 000nn000	01100111 01010111 01001110 11101100	11
31	1n00110u 0uu11001 000011n0 0001n000	10001110 10111001 11000010 10010100	8
32	11011010 1010011u 01101u10 00010111	01001111 11011100 00000100 11100000	3
33	1n01101u 10u01101 11100110 11111001	00000011 00100101 10100111 00001111	10
34	11100110 10010010 01101000 u1100011	11000000 00110011 00110000 01100000	14
35	0111100n 00n00000 11110101 10110010	-------- -------- -------- --------	4
36	-------1 --0----- -------- u----1--	-----011 01000010 -------- --------	9
37	-------- --n---1- -------1 11111010	11110110 11100100 10110100 00010001	15
38	-------- --0---00 00000--- --------	10001110 10111001 11000010 10010100	8
39	-------- -------- -------- --------	-------- -------- -------- --------	1
40	-------- -------- -------- --------	01101100 10101011 01110010 00010011	2

Step	Y_i	W_i^r	Π_i^r
12	-------- -------- -------- --------		
13	-------- -------- -------- --------		
14	-------- -------- -------- --------		
15	-------- -------- -------- --------		
16	-------- -------- -------- --------	-------- -------- -------- --------	6
17	-------- -------- -------- --------	01100111 01010111 01001110 11101100	11
18	10011001 01001100 00000011 10111000	01001111 11011100 00000100 11100000	3
19	10011110 00000100 10101111 00011011	x------- -------- -------- --------	7
20	11001011 10111100 00011101 1u111001	-------- -------- -------- --------	0
21	11001011 10101u10 11111111 10001111	-------- -------- -------- --------	13
22	001unn01 00011101 011nuuuu 0110010u	01100000 11111110 10100110 01000000	5
23	00000un0 0110uuu1 01001010 1un01001	00000011 00100101 10100111 00001111	10
24	u11n1001 11111111 1000u010 11nn0010	11000000 00110011 00110000 01100000	14
25	00u11000 n1010111 1111u100 1110n1nu	11110110 11100100 10110100 00010001	15
26	01111001 11110111 001n1nnn 0nnnu000	10001110 10111001 11000010 10010100	8
27	10001u11 01uu011n 11110001 10100unn	11101100 10100110 10100100 11100111	12
28	1100u001 01n10100 01101101 11n000n1	-------- -------- -------- --------	4
29	00---0-- ---u--1- -u---u-- --------	-----011 01000010 -------- --------	9
30	00--n--- --n----- -------- ---10--0	-------- -------- -------- --------	1
31	-1------ -------- -----u-- --1-----	01101100 10101011 01110010 00010011	2
32	-------- --u----- -----111 000-----	11110110 11100100 10110100 00010001	15
33	-------- -------- -------- --------	01100000 11111110 10100110 01000000	5
34	-------- -------- -------- --------	-------- -------- -------- --------	1
35	-------- -------- -------- --------	01001111 11011100 00000100 11100000	3
36	-------- -------- -------- --------	x------- -------- -------- --------	7
37	-------- -------- -------- --------	11000000 00110011 00110000 01100000	14
38	-------- -------- -------- --------	-------- -------- -------- --------	6
39	-------- -------- -------- --------	-----011 01000010 -------- --------	9
40	-------- -------- -------- --------	01100111 01010111 01001110 11101100	11

Merge Two Branches

Step	X_i	W_i^l	Π_i^l	Step	Y_i	W_i^r	Π_i^r
12	-------- -------- -------- --------			12	-------- -------- -------- --------		
13	-------- -------- -------- --------			13	-------- -------- -------- --------		
14	-------- -------- -------- --------			14	-------- -------- -------- --------		
15	-------- -------- -------- --------			15	-------- -------- -------- --------		
16	-------- -------- -------- --------	x------- -------- -------- --------	7	16	-------- -------- -------- --------	-------- -------- -------- --------	6
17	-------- -------- -------- -n------	-------- -------- -------- --------	4	17	-------- -------- -------- --------	01100111 01010111 01001110 11101100	11
18	-------- -------- -------- -0------	-------- -------- -------- --------	13	18	10011001 01001100 00000011 10111000	01001111 11011100 00000100 11100000	3
19	-------- -------1 -------- -1------	-------- -------- -------- --------	1	19	10011110 00000100 10101111 00011011	x------- -------- -------- --------	7
20	-------- -------0 -------- --------	00000011 00100101 10100111 00001111	10	20	11001011 10111100 00011101 1u111001	-------- -------- -------- --------	0
21	-------- -------n -------- --------	-------- -------- -------- --------	6	21	11001011 10101u10 11111111 10001111	-------- -------- -------- --------	13
22	-------- -------0 00111100 0-----00	11110110 11100100 10110100 00010001	15	22	001unn01 00011101 011nuuuu 0110010u	01100000 11111110 10100110 01000000	5
23	01101110 00100100 11111101 10111000	01001111 11011100 00000100 11100000	3	23	00000un0 0110uuu1 01001010 1un01001	00000011 00100101 10100111 00001111	10
24	11010101 00011001 01001010 10110101	11101100 10100110 10100100 11100111	12	24	u11n1001 11111111 1000u010 11nn0010	11000000 00110011 00110000 01100000	14
25	11101n11 11110111 01100001 10110000	-------- -------- -------- --------	0	25	00u11000 n1010111 1111u100 1110n1nu	11110110 11100100 10110100 00010001	15
26	00110001 001001un nnnn00nu u1010001	-----011 01000010 -------- --------	9	26	01111001 11110111 001n1nnn 0nnnu000	10001110 10111001 11000010 10010100	8
27	0n00n1un 0u110100 00001111 10101010	01100000 11111110 10100110 01000000	5	27	10001u11 01uu011n 11110001 10100unn	11101100 10100110 10100100 11100111	12
28	10100010 101100nu 00n00nu1 u0un0110	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	4
29	01nun101 110u110u 11010101 11u0nnu1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	9
30	00001111 uu010n10 1u11nu1n 000nn000	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1
31	1n00110u 0uu11001 000011n0 0001n000	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	2
32	11011010 1010011u 01101u10 00010111	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	15
33	1n01101u 10u01101 11100110 11111001	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	5
34	11100110 10010010 01101000 u1100011	11000000 00110011 00110000 01100000	14	34	-------- -------- -------- --------	-------- -------- -------- --------	1
35	0111100n 00n00000 11110101 10110010	-------- -------- -------- --------	4	35	-------- -------- -------- --------	01001111 11011100 00000100 11100000	3
36	-------1 --0----- -------- u----1--	-----011 01000010 -------- --------	9	36	-------- -------- -------- --------	x------- -------- -------- --------	7
37	-------- --n---1- -------1 11111010	11110110 11100100 10110100 00010001	15	37	-------- -------- -------- --------	11000000 00110011 00110000 01100000	14
38	-------- --0---00 00000--- --------	10001110 10111001 11000010 10010100	8	38	-------- -------- -------- --------	-------- -------- -------- --------	6
39	-------- -------- -------- --------	-------- -------- -------- --------	1	39	-------- -------- -------- --------	-----011 01000010 -------- --------	9
40	-------- -------- -------- --------	01101100 10101011 01110010 00010011	2	40	-------- -------- -------- --------	01100111 01010111 01001110 11101100	11

Use these remaining free bits to merge the two branches

Evaluate Complexity

- The **uncontrolled** probability of merging is $2^{-77.4}$
  - ➢ #necessary starting points: $2^{77.4}$
- One starting point is generated by 4 step functions, which is $2^{-4.4}$ (=4/42*2)
- The merging for each starting point costs $2^{-1.9}$

Overall complexity: $2^{77.4-4.4} + 2^{77.4-1.9} \approx 2^{75.5}$

Evaluate Complexity

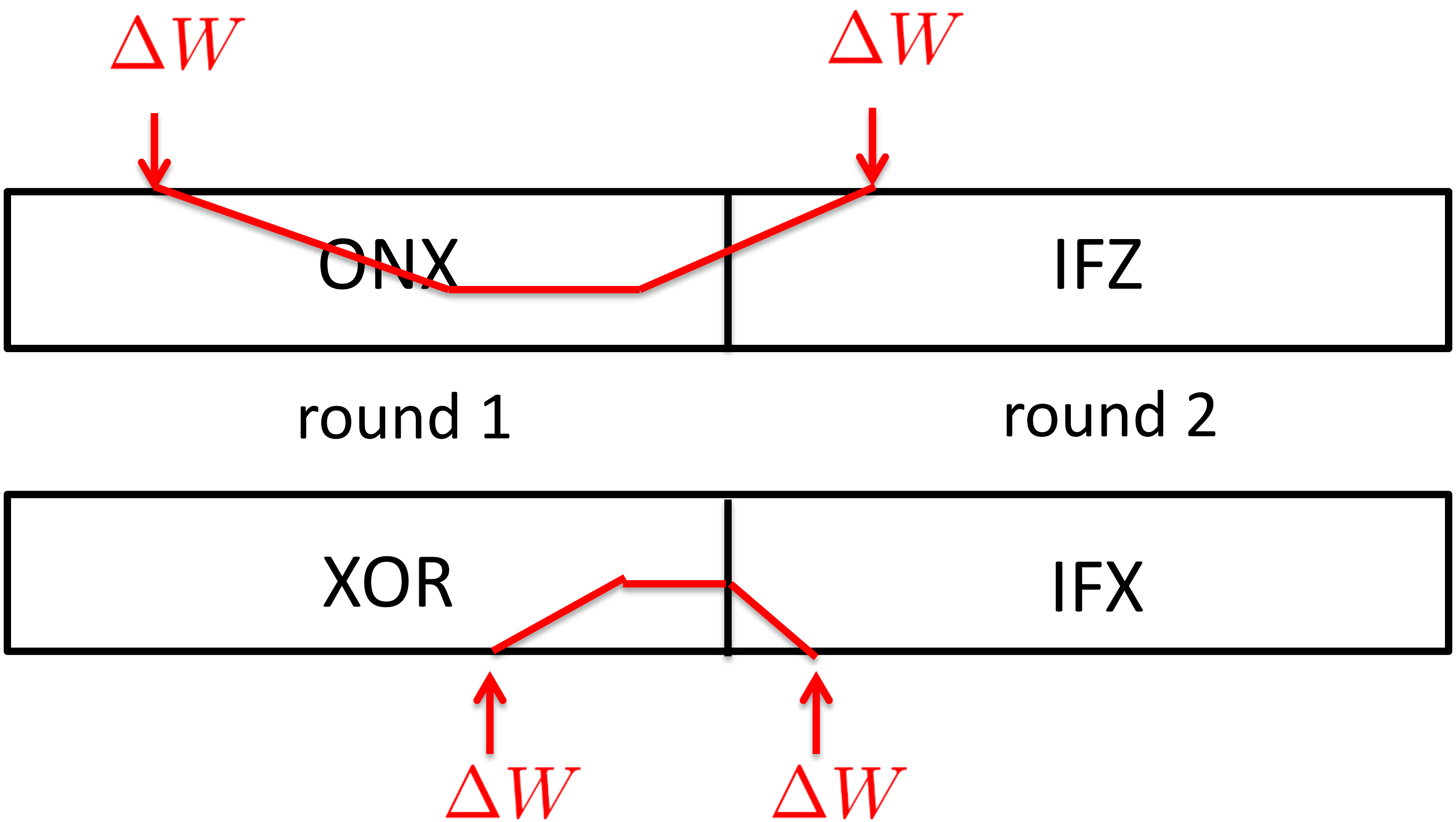
- The **uncontrolled** probability of merging is $2^{-77.4}$
  - #necessary starting points: $2^{77.4}$
- One starting point is generated by 4 step functions, which is $2^{-4.4}$ (=4/42*2)
- The merging for each starting point costs $2^{-1.9}$

Overall complexity: $2^{77.4-4.4} + 2^{77.4-1.9} \approx 2^{75.5}$

We cannot afford the probabilities for steps 58 to 64.
#attacked step is 42, while differential path has 48 steps.

Attack from the First Round

- The **non-linear** path in **XOR** round should be **as short as possible**



Outline

- RIPEMD-160 specification
- Attack overview
- Find a differential path
- Find a confirming pair
- **Conclusion**

Conclusion

- Semi-free-start collision attack on 42 steps
    - **6** steps more compared with [MNSS12]
- Semi-free-start collision attack on **first** 36 steps

Open question:

Can the merging complexity be reduced in order to extend the attack to 48 steps?

Thank you for your attention!