Preimage Attacks on MD, HAVAL, SHA, and Others

MD4
MD5

HAVAL-3
HAVAL-4
HAVAL-5

SHA-0
SHA-1
SHA-2

HAS-160
RIPEMD

Yu Sasaki and Kazumaro Aoki
NTT Information Sharing Platform Laboratories

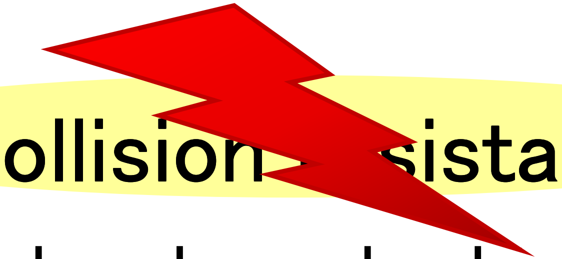
Security of Hash Functions

- Collision resistance
  - has been broken in many hash functions by Prof. Wang's great work.

- Preimage resistance
  - is more important.
  - is not analyzed well yet.

We propose preimage attacks on 10 hash functions.

Security of Hash Functions



- Collision resistance
  - has been broken in many hash functions by Prof. Wang’s great work.

- Preimage resistance
  - is more important.
  - is not analyzed well yet.

We propose preimage attacks on 10 hash functions.

Security of Hash Functions

Chinese Trick

- Collision resistance
  - has been broken in many hash functions by Prof. Wang’ s great work.

- Preimage resistance
  - is more important.
  - is not analyzed well yet.

We propose preimage attacks on 10 hash functions.

Security of Hash Functions

- Collision resistance
  - has been broken in many hash functions by Prof. Wang’s great work.

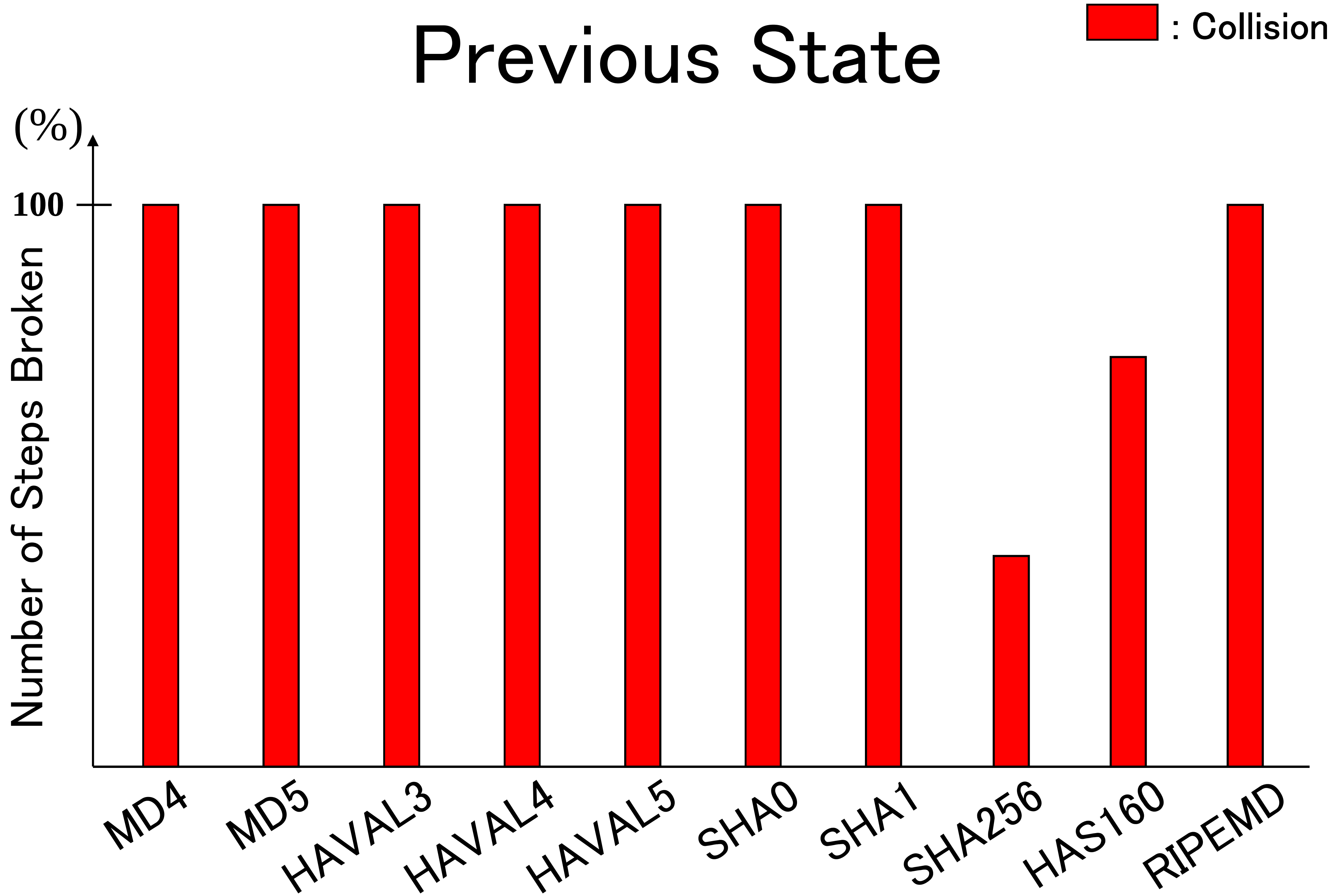
Chinese Trick

- Preimage resistance
  - is more important.
  - is not analyzed well yet.

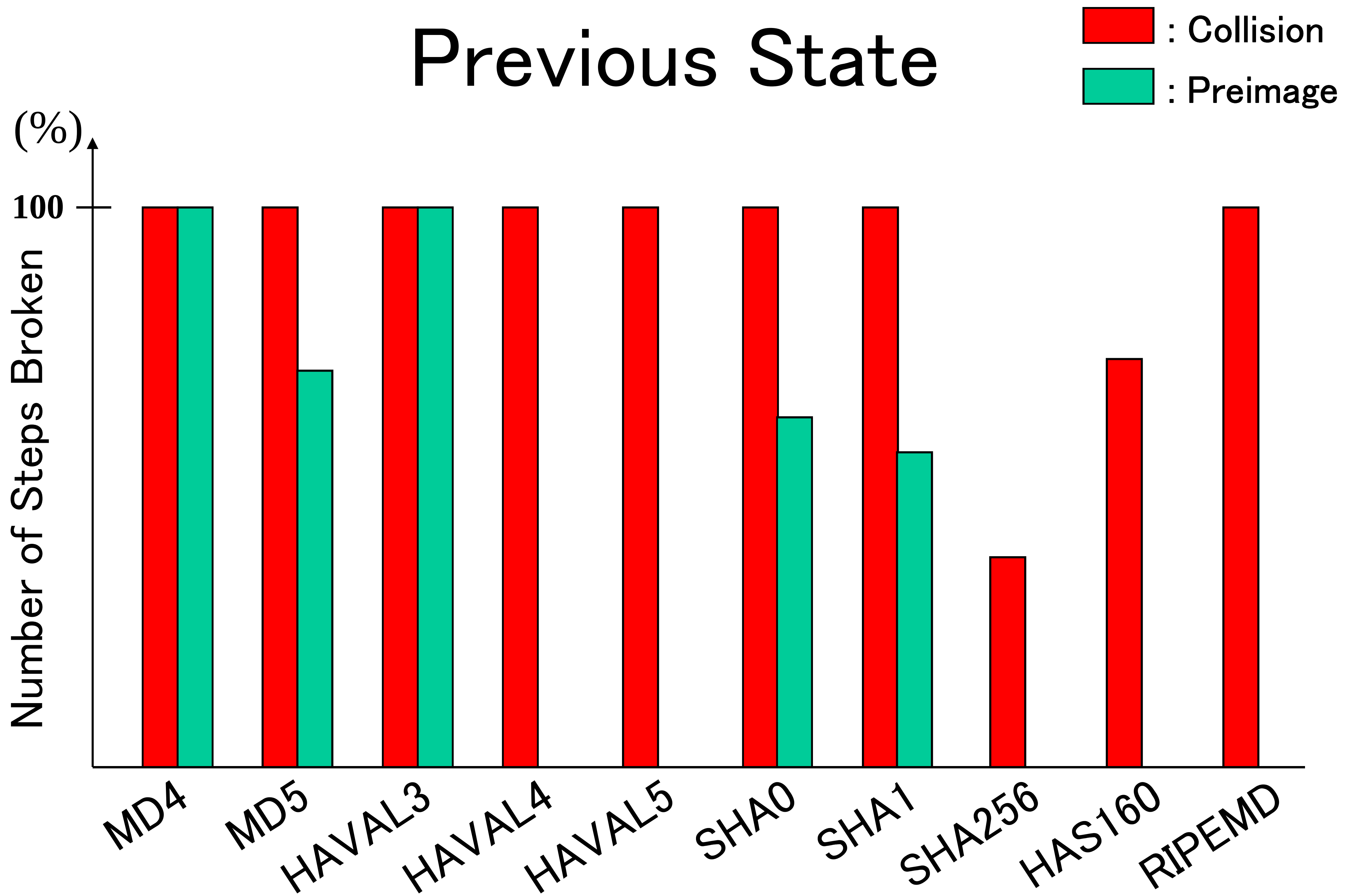
Japanese Illusion !!

We propose preimage attacks on 10 hash functions.

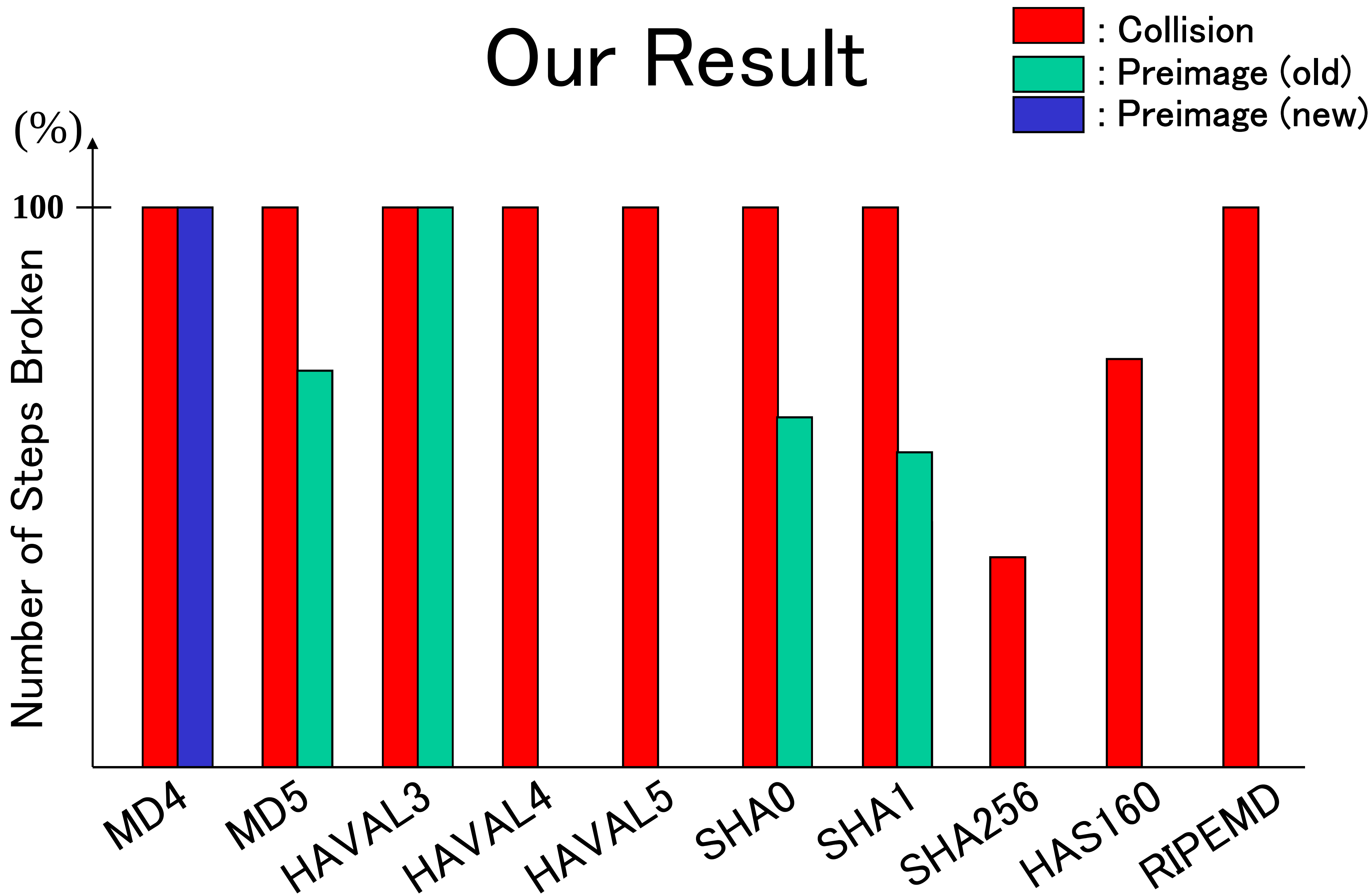
Previous State



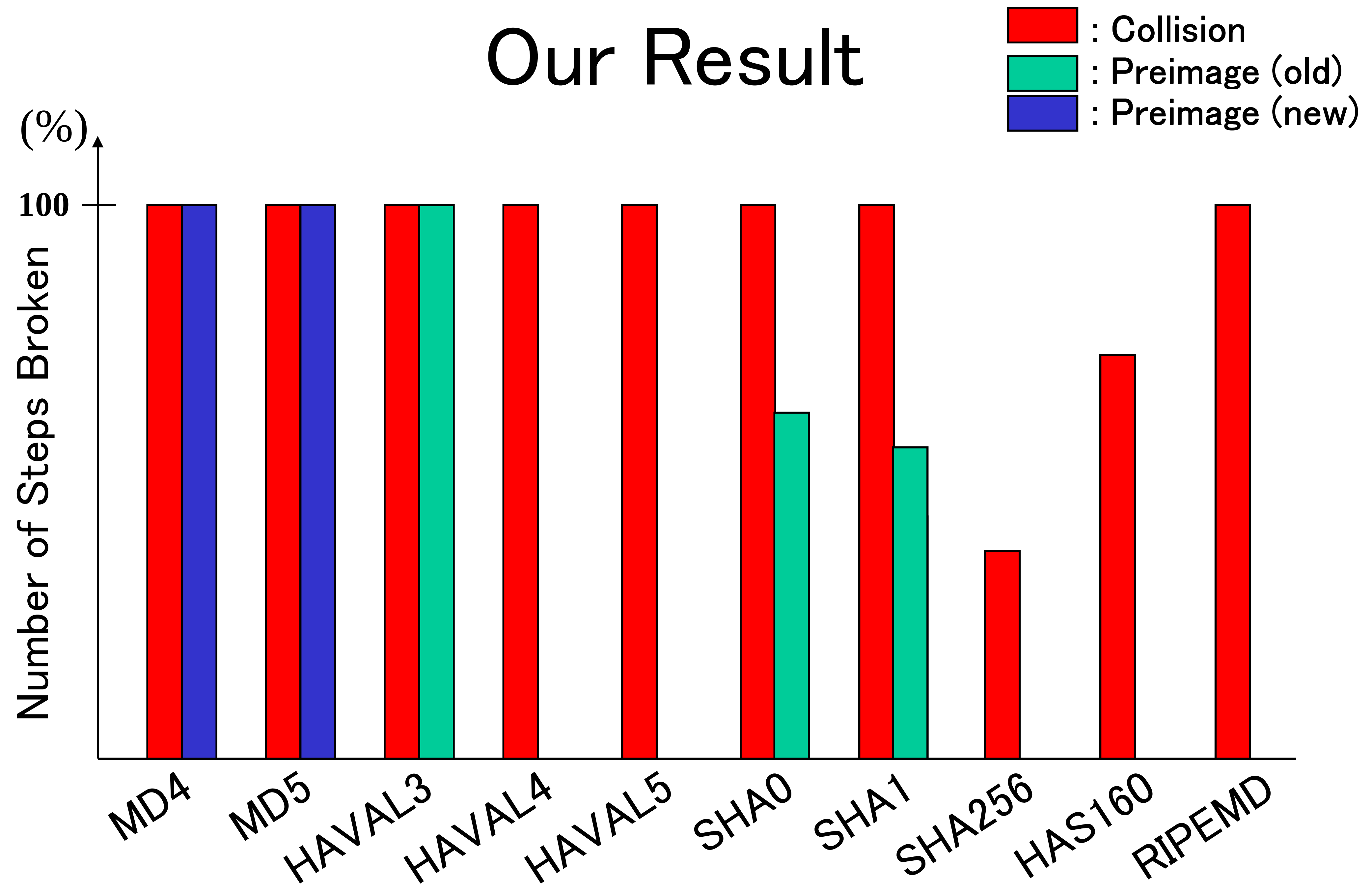
Previous State



Our Result

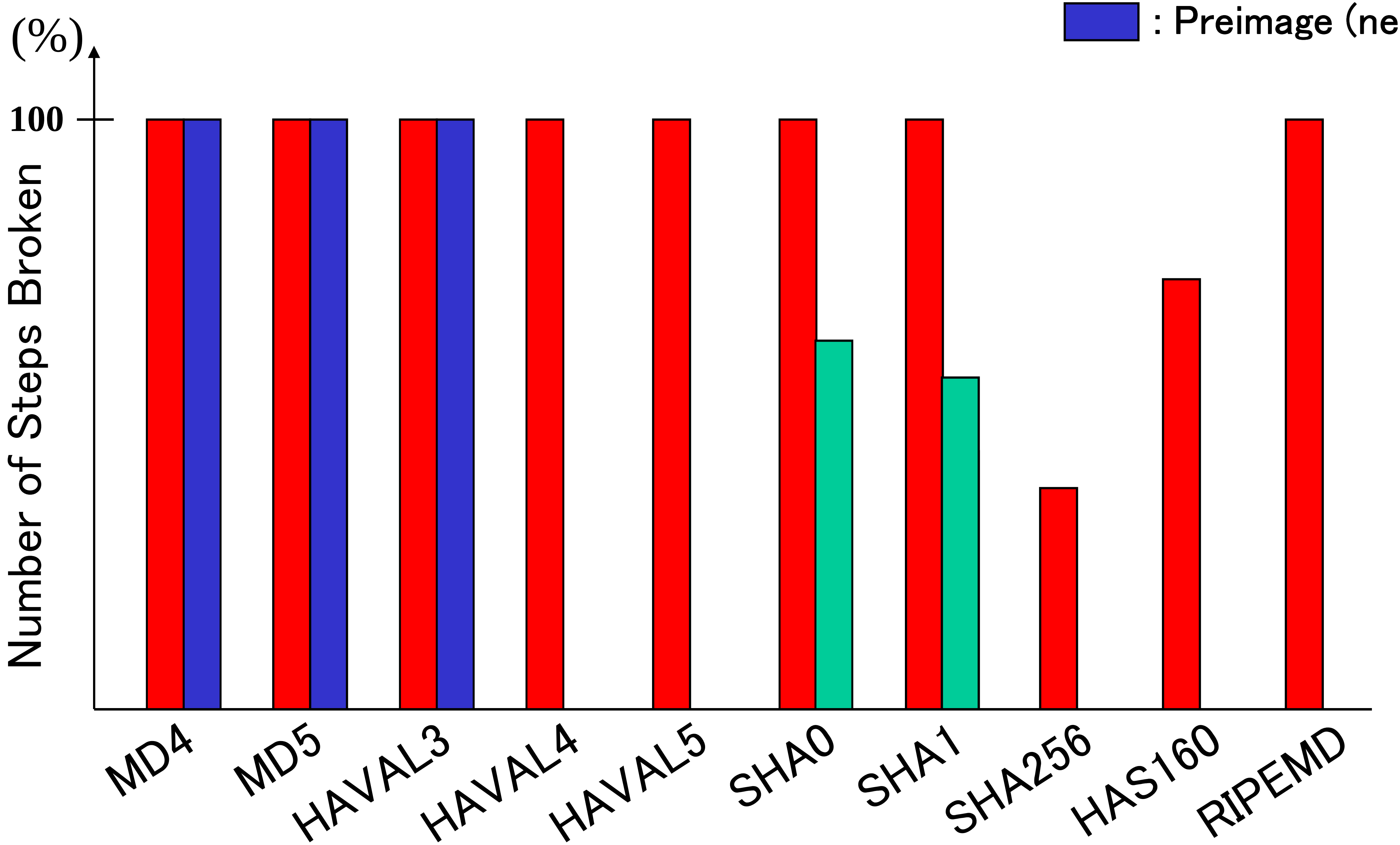

🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)
(%)
100
Number of Steps Broken
MD4
MD5
HAVAL3
HAVAL4
HAVAL5
SHA0
SHA1
SHA256
HAS160
RIPEMD

Our Result

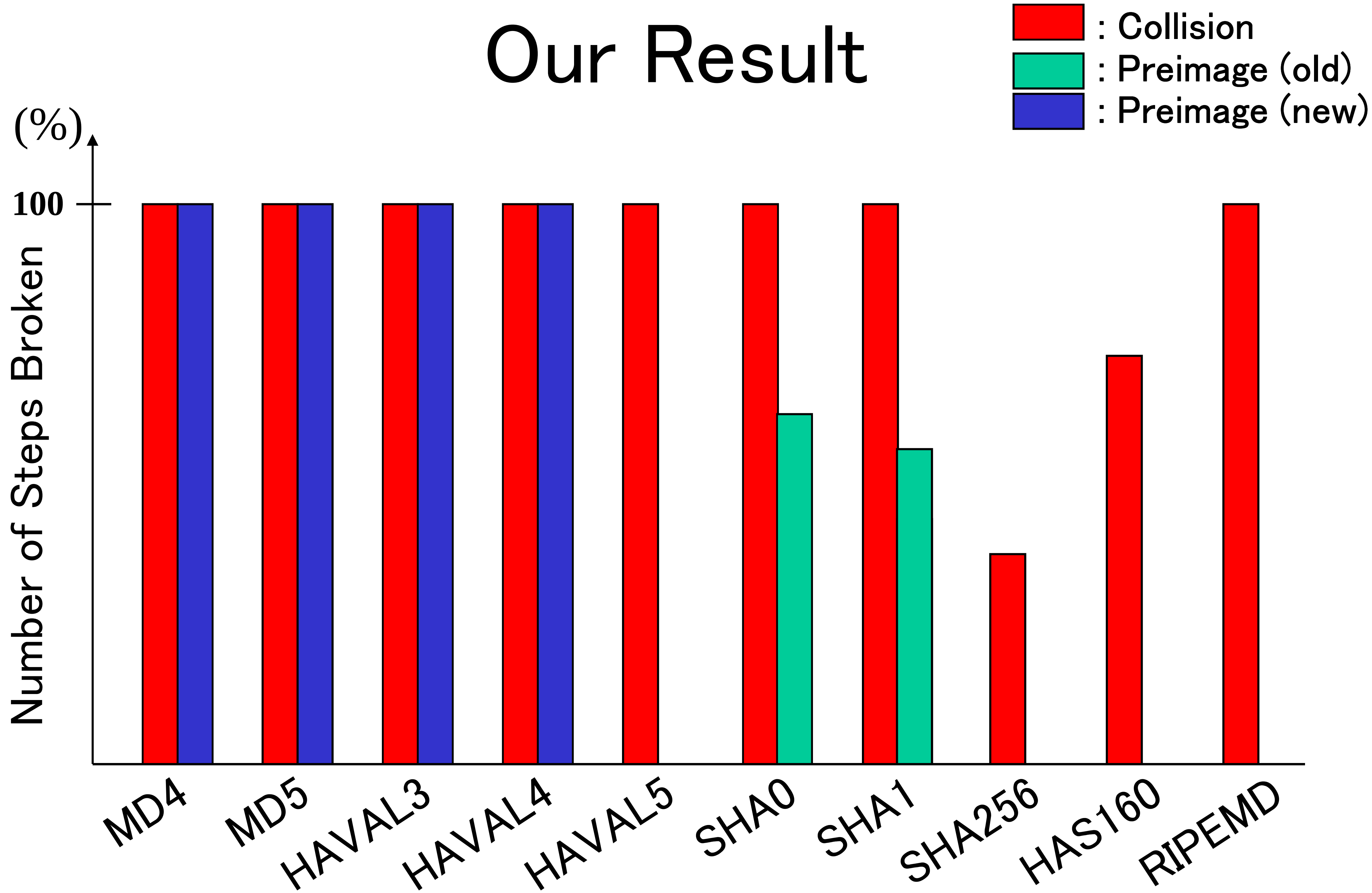

🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)
(%)
100
Number of Steps Broken
MD4
MD5
HAVAL3
HAVAL4
HAVAL5
SHA0
SHA1
SHA256
HAS160
RIPEMD

Our Result

🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)

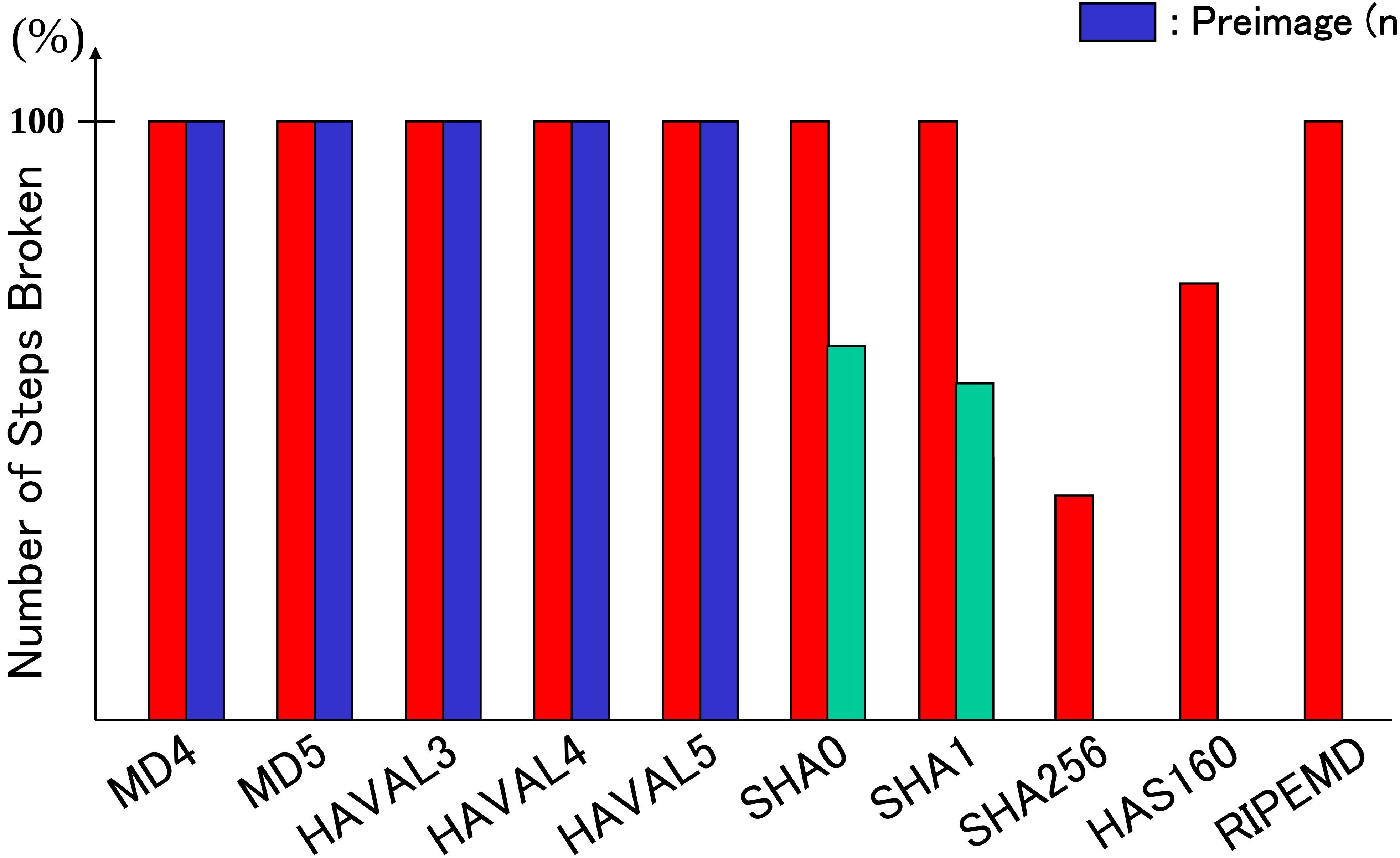


Our Result

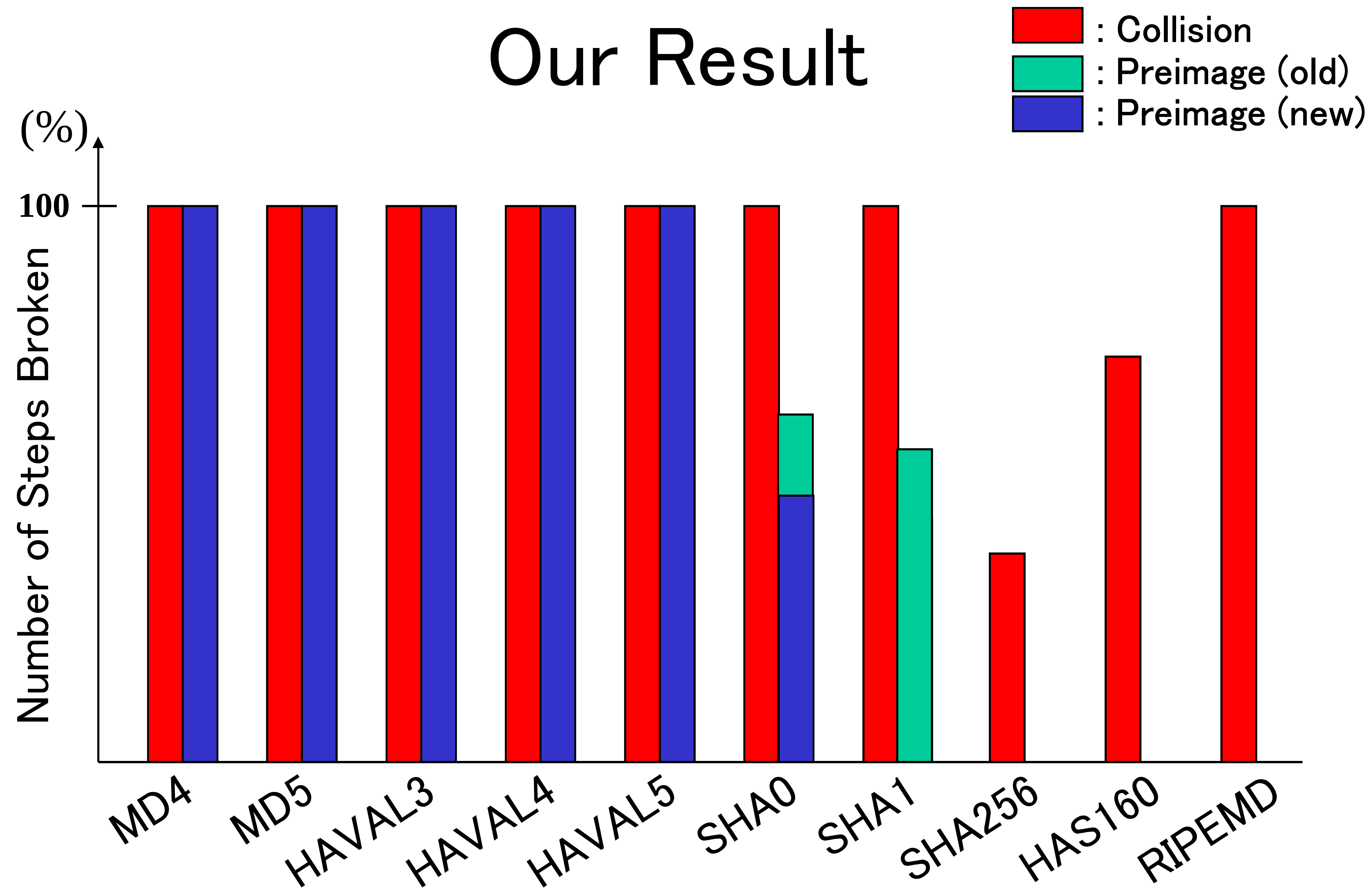

🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)
(%)
100
Number of Steps Broken
MD4
MD5
HAVAL3
HAVAL4
HAVAL5
SHA0
SHA1
SHA256
HAS160
RIPEMD

Our Result

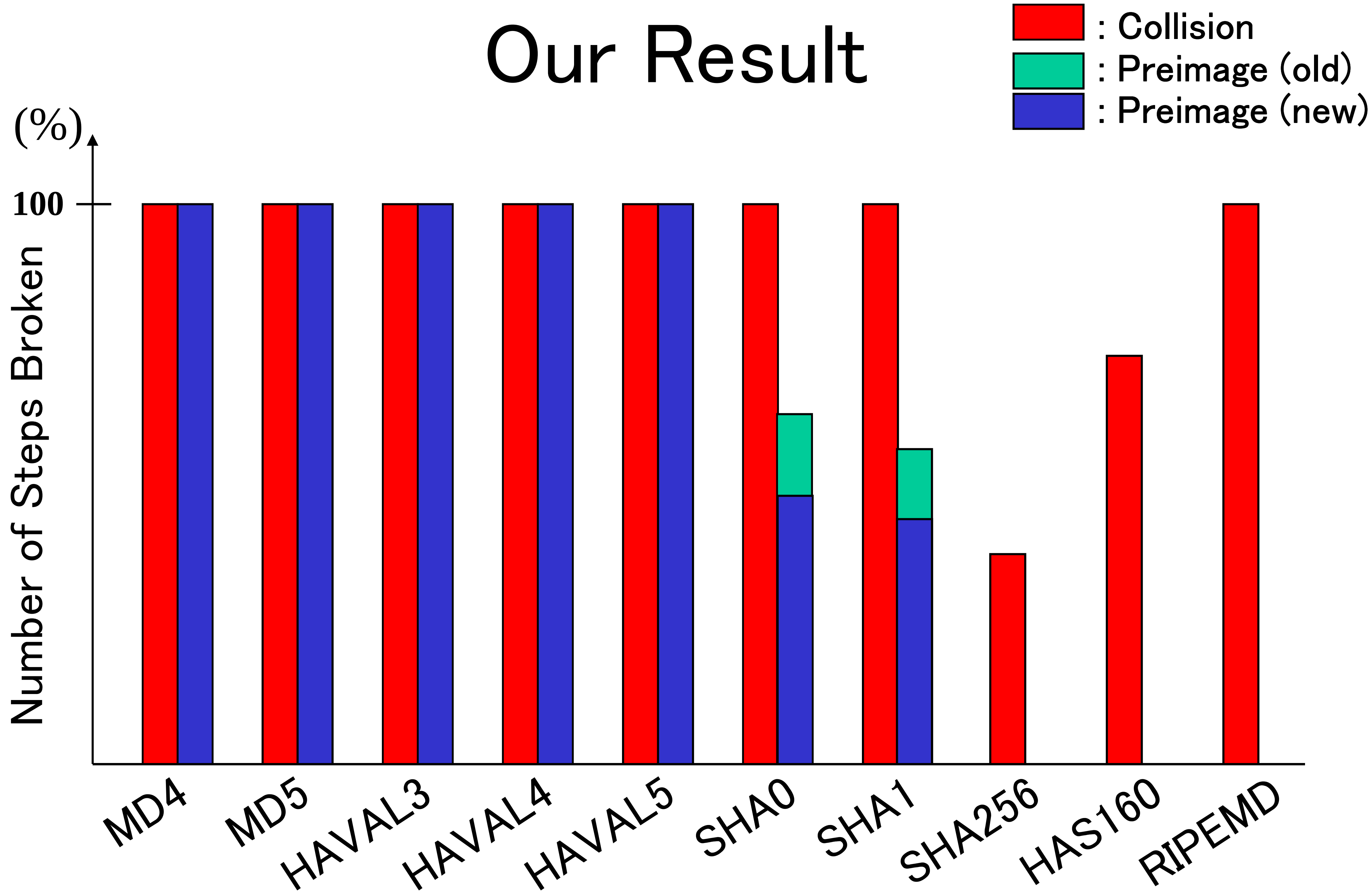
🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)



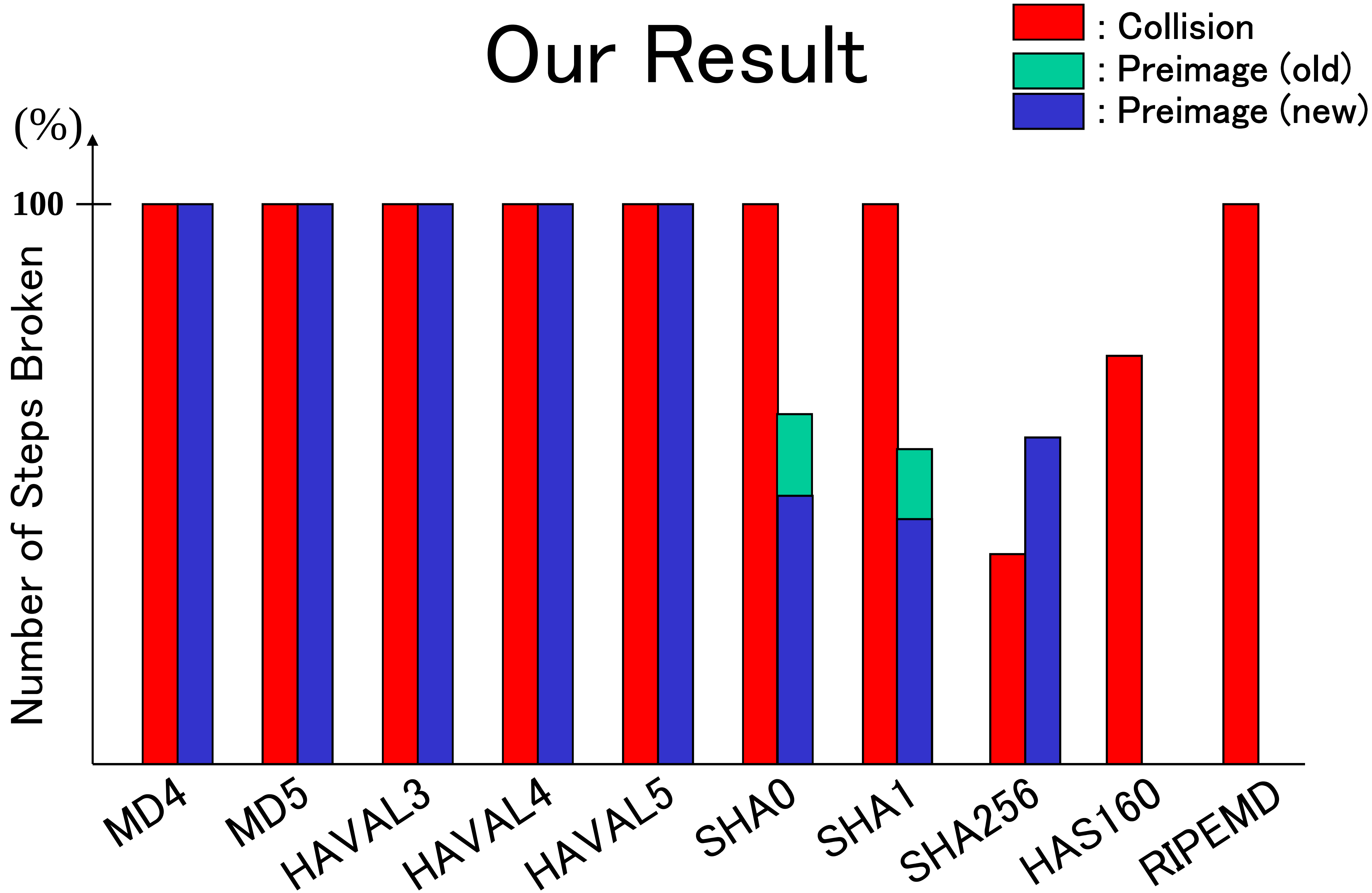
Our Result


🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)
(%)
100
Number of Steps Broken
MD4
MD5
HAVAL3
HAVAL4
HAVAL5
SHA0
SHA1
SHA256
HAS160
RIPEMD

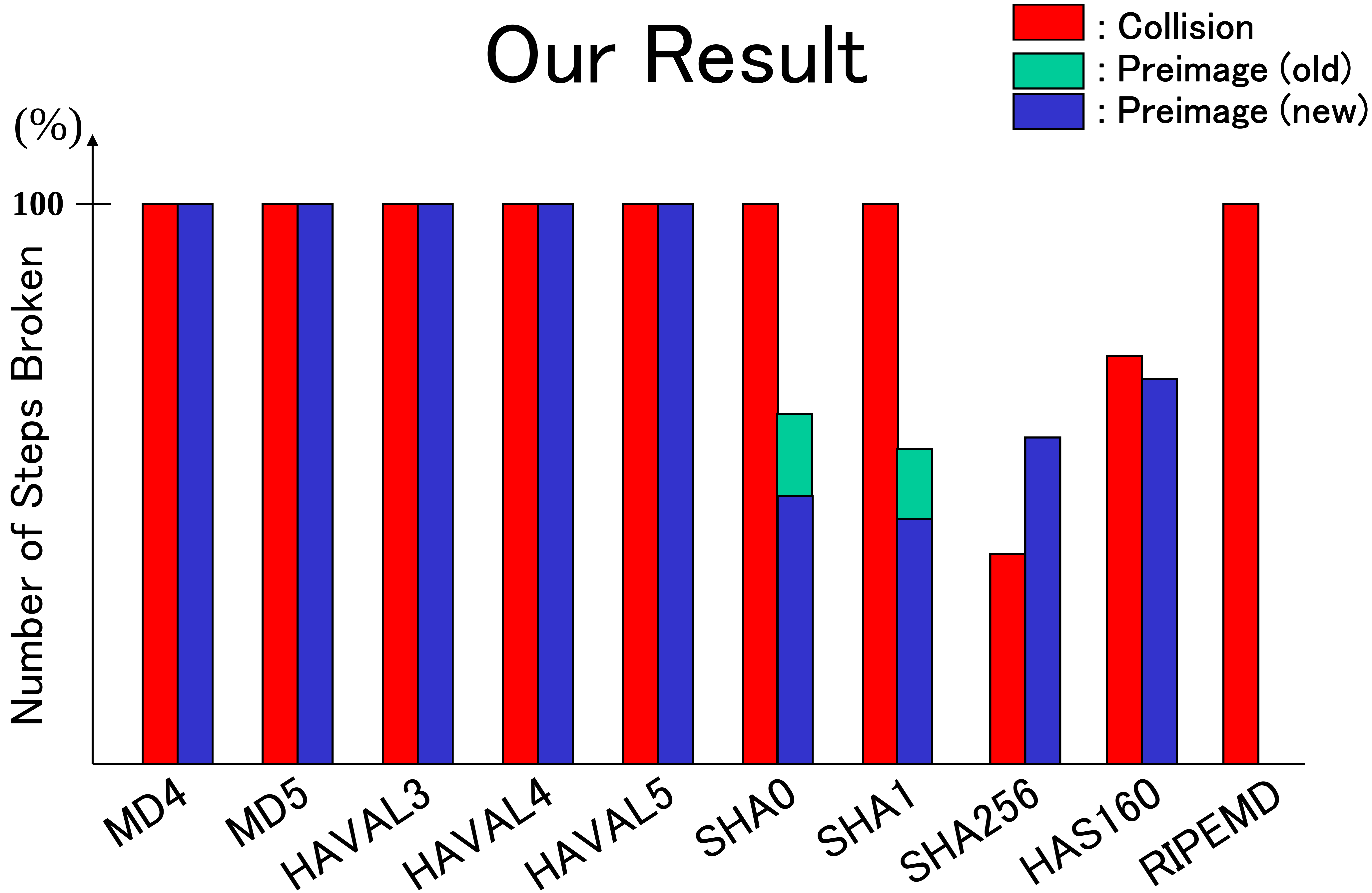
Our Result


🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)
(%)
100
Number of Steps Broken
MD4
MD5
HAVAL3
HAVAL4
HAVAL5
SHA0
SHA1
SHA256
HAS160
RIPEMD

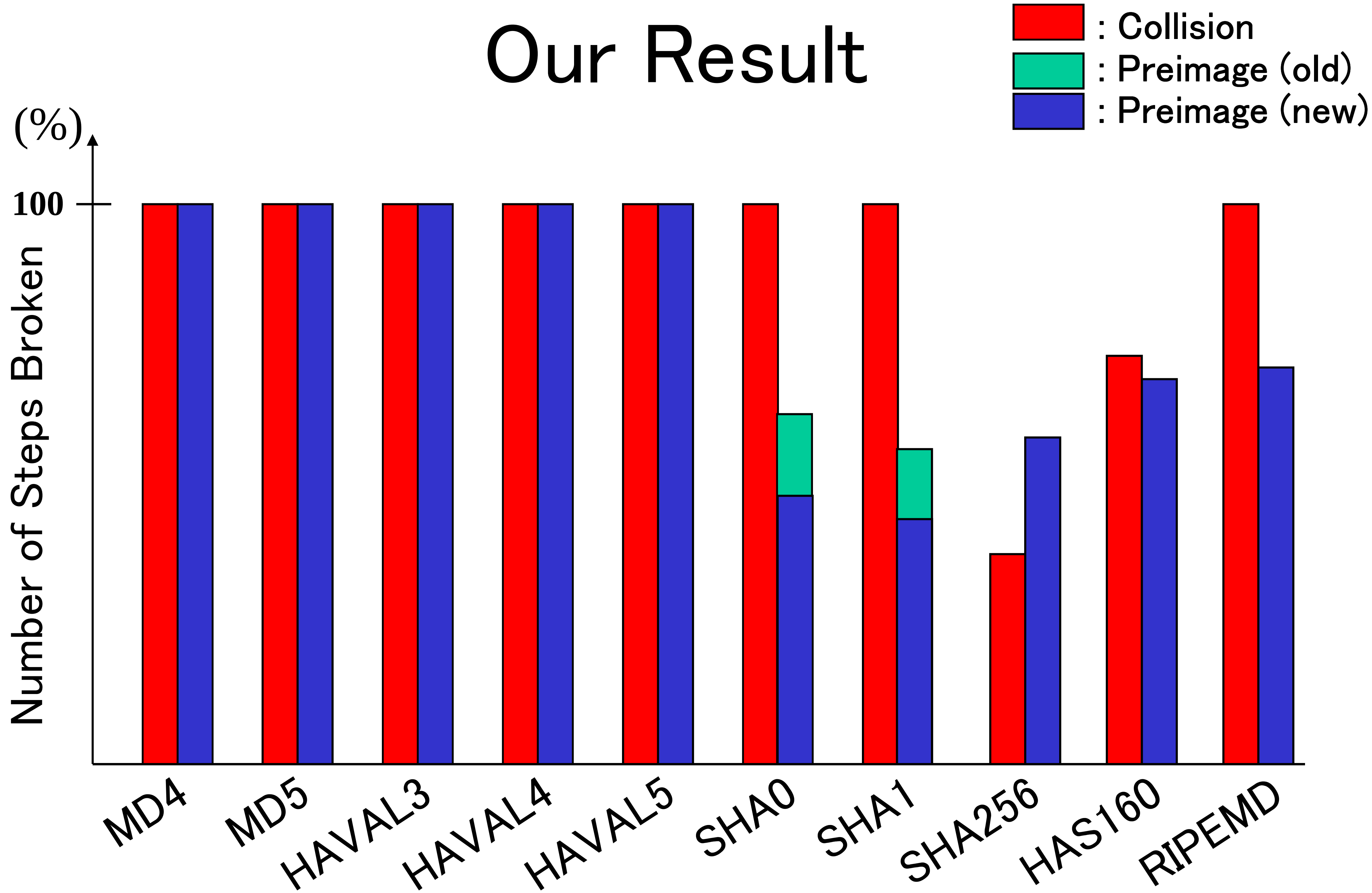
Our Result


🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)
(%)
100
Number of Steps Broken
MD4
MD5
HAVAL3
HAVAL4
HAVAL5
SHA0
SHA1
SHA256
HAS160
RIPEMD

Our Result


: Collision
: Preimage (old)
: Preimage (new)
(%)
100
Number of Steps Broken
MD4
MD5
HAVAL3
HAVAL4
HAVAL5
SHA0
SHA1
SHA256
HAS160
RIPEMD

Our Result


🟥 : Collision
🟩 : Preimage (old)
🟦 : Preimage (new)
(%)
100
Number of Steps Broken
MD4
MD5
HAVAL3
HAVAL4
HAVAL5
SHA0
SHA1
SHA256
HAS160
RIPEMD

MD4 （48-step, 128-bit）

Previous

- Leurent [FSE08]　48-step (full)　$2^{100.5}$

New (SAC08)

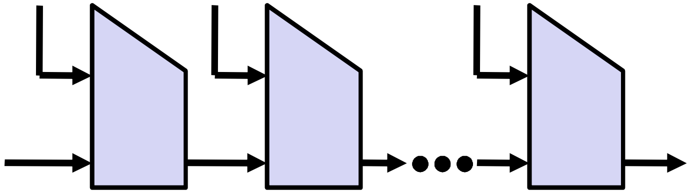
48-step (full)　2^{107}

MD4 (48-step, 128-bit)

Previous

Using iterative structure of Merkle-Damgård

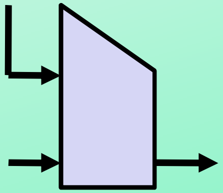
- Leurent [FSE08] 48-step (full) $2^{100.5}$



New (SAC08)

48-step (full) 2^{107}

Attack of single compression function



MD5 (64-step, 128-bit)

Previous

- Aumasson, Meier, Mendel [SAC08] 47-step 2^{102}

New (SAC08)

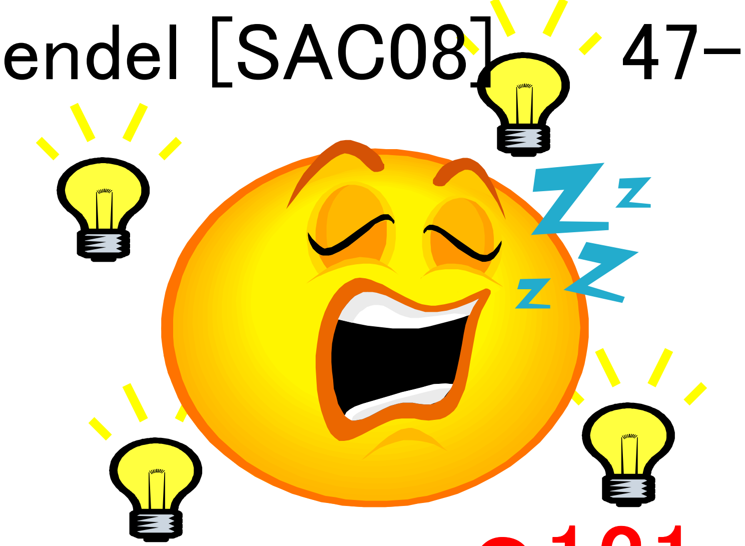
63-step 2^{121}

64-step (full) 2^{127}

MD5 (64-step, 128-bit)

Previous

- Aumasson, Meier, Mendel [SAC08] 47-step 2^{102}



New (SAC08)

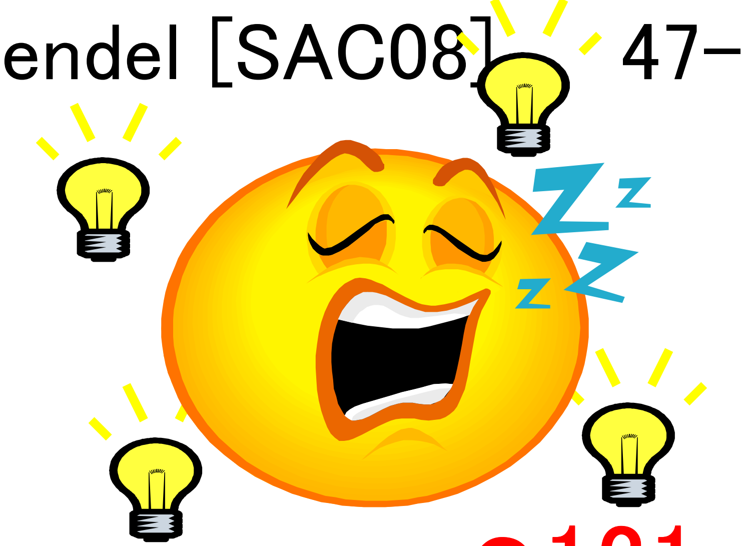
63-step 2^{121}

64-step (full) 2^{127}

MD5 (64-step, 128-bit)

Previous

- Aumasson, Meier, Mendel [SAC08] 47-step 2^{102}



New (SAC08)

63-step 2^{121}

64-step (full) 2^{127}

HAVAL-3 (96-step, 256-bit)

Previous

– Aumasson, Meier, Mendel [SAC08]	96-step (full)	2^{230}

New

To appear in Asiacrypt 2008

96-step (full) 2^{225}

HAVAL-3 (96-step, 256-bit)

Best attack on HAVAL-3 !!

Previous

– Aumasson, Meier, Mendel [SAC08] 96-step (full) 2^{230}

New

To appear in Asiacrypt 2008

96-step (full) 2^{225}

HAVAL-4 (128-step, 256-bit)

Previous

none

New

To appear in Asiacrypt 2008

128-step (full) 2^{241}

HAVAL-4 (128-step, 256-bit)

Previous

none

Surprisingly, 128-steps can be inverted !!

New

To appear in Asiacrypt 2008

128-step (full) 2^{241}

HAVAL-5 (160-step, 256-bit)

Previous

none

New

To appear in Asiacrypt 2008

151-step 2^{241}

160-step (full) 2^{255}

HAVAL-5 (160-step, 256-bit)

Previous

none

Even 151-steps can be inverted !!

New

To appear in Asiacrypt 2008

151-step 2^{241}

160-step (full) 2^{255}

SHA-0 (80-step, 160-bit)

Previous

- Cannière, Rechberger [Crypto08] 49-step 2^{159}

New

36-step 2^{153}

SHA-1 (80-step, 160-bit)

Previous

- Cannière, Rechberger [Crypto08]   44-step 2^{157}

New

34-step $2^{153.5}$

SHA-2 (64-step, 256-bit)

Previous

none

＊ Best collision attack: 24-step

New

36-step 2^{249}

SHA-2 (64-step, 256-bit)

Previous

none

Preimage attack works more steps than collision attack !!

＊ Best collision attack: 24-step

New

36-step 2^{249}

HAS-160 (80-step, 160-bit)

Previous

none

＊ Collision attack until 59-step

New

52-step 2^{153}

RIPEMD (48-step, 128-bit, 2-branch)

Previous

none

New

33-step 2^{125}

RIPEMD (48-step, 128-bit, 2-branch)

Previous

none

Also work for 2-branch hash !!

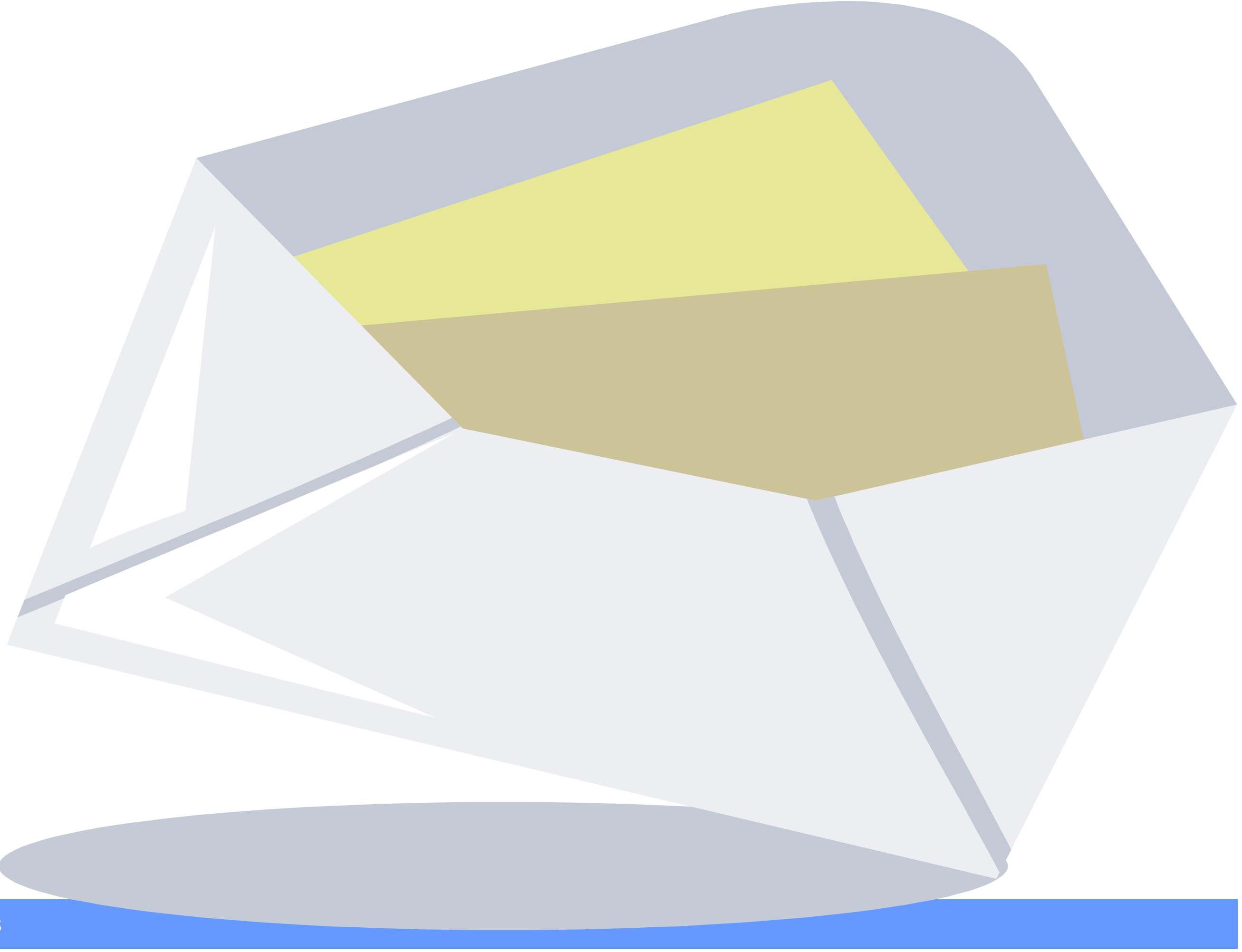
New

33-step 2^{125}

Summary of Our Results

Target	(Step, Output bit)	Previous	New	Comp.
MD4	(48, 128)	48 (Full)	48 (Full)	2^{107}
MD5	(64, 128)	47	64 (Full)	2^{127}
HAVAL-3	(96, 256)	96 (Full)	96 (Full)	2^{225}
HAVAL-4	(128, 256)	–	128 (Full)	2^{241}
HAVAL-5	(160, 256)	–	160 (Full)	2^{255}
SHA-0	(80, 160)	49	36 (45%)	2^{153}
SHA-1	(80, 160)	44	34 (43%)	$2^{153.5}$
SHA-256	(64, 256)	–	36 (56%)	2^{249}
HAS-160	(80, 160)	–	52 (65%)	2^{153}
RIPEMD	(48, 128)	–	33 (69%)	2^{125}

Messages from us



Messages from us

- Need to be careful for preimage attack.
- NIST requires 2^n for preimage resistance.
- Our work is still on going.

Messages from us

- Need to be careful for preimage attack.
- NIST requires 2^n for preimage resistance.
- Our work is still on going.

Thanks for your attention !!