Quantum Collision Attacks on Reduced SHA-256 and SHA-512

Akinori Hosoyamada (NTT Corporation / Nagoya University)
Yu Sasaki (NTT Corporation)

@Crypto 2021

Results

- First dedicated quantum collision attacks on SHA-2
  - 38-step attack on SHA-256 & 39-step attack on SHA-512
  - Classical collision attacks: 31-step for SHA-256 & 27-step for SHA-512
  - Still far from full-step attacks (64 steps / 80 steps)

- We convert classical semi-free-start collisions on 38-step SHA-256 & 39-step SHA-512 into collisions in the quantum setting

- Our attacks are valid in the setting of time-space tradeoff
  - Invalid in other quantum settings

Basics of
Classical Collision Attacks

Valid Classical Collision Attacks

- Generic Attack: Birthday Attack (Time $2^{n/2}$)
- A dedicated attack is valid iff $\boldsymbol{T < 2^{n/2}}$

The number of attacked steps

NTT

Input

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

Step 7

Step 8

Step 9

Step 10

Output

The number of attacked steps

Input

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

Step 7

Step 8

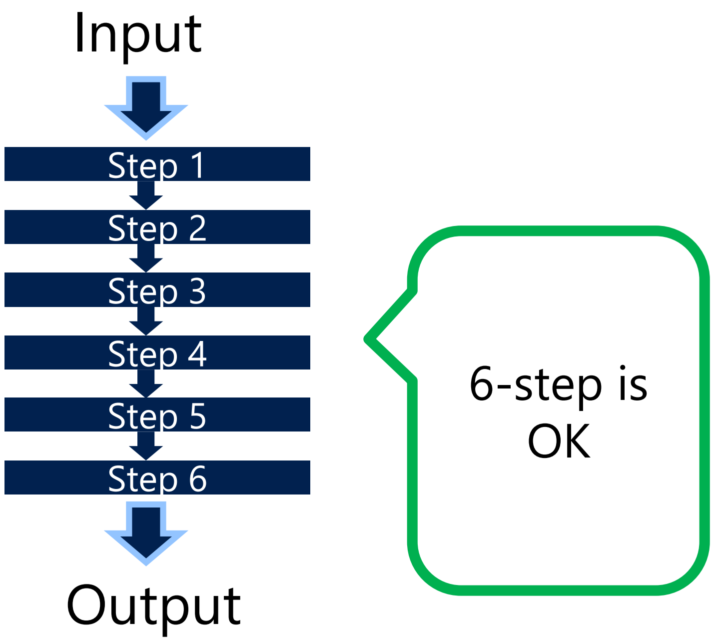
Step 9

Step 10

Output

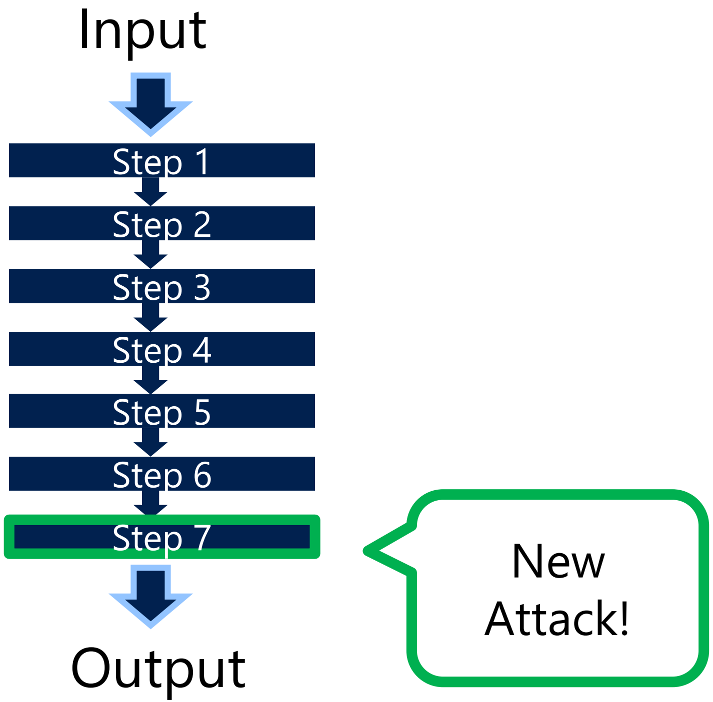
10-step is hard to break…

The number of attacked steps



- When an original primitive is hard to break, usually symmetric-key cryptanalysts try to break its reduced-step variants

The number of attacked steps



- What is important: <u>**How many steps can we break?**</u>
  (rather than the actual complexity)

Valid Classical Collision Attacks

- Generic Attack: Birthday Attack (Time $2^{n/2}$)
- A dedicated attack is valid iff $\boldsymbol{T < 2^{n/2}}$

Valid Classical Collision Attacks

- Generic Attack: Birthday Attack (Time $2^{n/2}$)
- A dedicated attack is valid iff $\boldsymbol{T < 2^{n/2}}$

- Basic approach: Differential cryptanalysis
- A suitable differential trail of which probability is p

  $\rightarrow$ Collision attack of time $T = 1/p$

The differential trail leads to a valid attack only if

$$\boldsymbol{p > 2^{-n/2}}$$

Some Observations on Dedicated Quantum Collision Attacks at Eurocrypt 2020 [HY20]

[HY20] Akinori Hosoyamada, Yu Sasaki: Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound. Eurocrypt 2020.

Generic Quantum Collision Attacks

NTT

Three settings depending on available computational resources

1. Small quantum computer + Large qRAM

Best algorithm: BHT ($T = 2^{n/3}$ & qRAM $2^{n/3}$) [BHT98]

2. Efficiency is measured by Time-Space tradeoff (No qRAM)

Quantum computer of size S + Classical computer of size S

Best algorithm: Parallel rho (Tradeoff $T = 2^{n/2}/S$) [Ber09]

3. Small quantum computer + Large classical memory (No qRAM)

Best algorithm: CNS ($T = 2^{2n/5}$, $2^{n/5}$classical memory) [CNS17]

[BHT98] Gilles Brassard, Peter Høyer, Alain Tapp: Quantum Cryptanalysis of Hash and Claw-Free Functions. LATIN 1998

[Ber09] D. J. Bernstein: Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?. SHARCS 2009.

[CNS17] A. Chailloux, M. Naya-Plasencia, A. Schrottenloher: An efficient quantum collision search algorithm and implications on symmetric cryptography. Asiacrypt 2017.

Generic Quantum Collision Attacks

NTT

Three settings depending on available computational resources

1. Small quantum computer + Large qRAM

Best algorithm: BHT ($T = 2^{n/3}$ & qRAM $2^{n/3}$) [BHT98]

2. Efficiency is measured by Time-Space tradeoff (No qRAM)
Quantum computer of size S + Classical computer of size S

Best algorithm: Parallel rho (Tradeoff $T = 2^{n/2}/S$) [Ber09]

3. Small quantum computer + Large classical memory (No qRAM)

Best algorithm: CNS ($T = 2^{2n/5}, 2^{n/5}$classical memory) [CNS17]

Quantum speed-up for generic collision attack is always <u>less-than-quadratic</u>

[BHT98] Gilles Brassard, Pe
[Ber09] D. J. Bernstein: Co
[CNS17] A. Chailloux, M. N ... ic cryptography. Asiacrypt 2017.

Speed-up for Differential Cryptanalysis

Very roughly speaking, the time to find a collision with a differential path of prob. p is

Classical… $T = 1/p$

Quantum… $T = \sqrt{1/p}$ (with the Grover search)[KLLN16]

<u>Quadratic</u> speed-up for Differential Cryptanalysis

[KLLN16] M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia: Improved rebound attack on the finalist Grostl. *IACR Trans. Symmetric Cryptol.*, 2016(1) pp. 71-94, 2016.

Our Observation @ EC2020: Speed-up gap

Attack	Speed-up
Generic Collision	Less-than-Quadratic
Differential Cryptanalysis	Quadratic

Differential cryptanalysis becomes relatively stronger in the quantum setting

The validity condition $p > 2^{-n/2}$ can be relaxed

Example: Small quantum computer + Large qRAM

- Generic algorithm (BHT): $T = 2^{n/3}$

- Differential cryptanalysis: $T = \sqrt{1/p}$

- Collision attack based on differential cryptanalysis is valid only if

$$\sqrt{1/p} < 2^{n/3} \iff \boldsymbol{p > 2^{-2n/3}}$$

Relaxed from the classical condition $p > 2^{-n/2}$
p may lead to a valid attack even if $2^{-n/2} \geq p$

Example: Time-Space Tradeoff

NTT

- Generic algorithm (parallel rho): $T = 2^{n/2}/S$
- Differential cryptanalysis: $T = \sqrt{1/p}$
- Collision attack based on differential cryptanalysis that requires space S is valid only if

$$\sqrt{1/p} < 2^{n/2}/S \Leftrightarrow \boldsymbol{p > 2^{-n} \cdot S^2}$$

p may lead to a valid attack even if p is very close to 2^{-n}

Results @ EC2020

- The condition for p is relaxed → dedicated quantum collision attacks can reach more steps than classical attacks
  - We indeed showed dedicated quantum collision attacks on AES-MMO and Whirlpool that break more steps than classical attacks

Results @ EC2020

- The condition for p is relaxed → dedicated quantum collision attacks can reach more steps than classical attacks
  - We indeed showed dedicated quantum collision attacks on AES-MMO and Whirlpool that break more steps than classical attacks

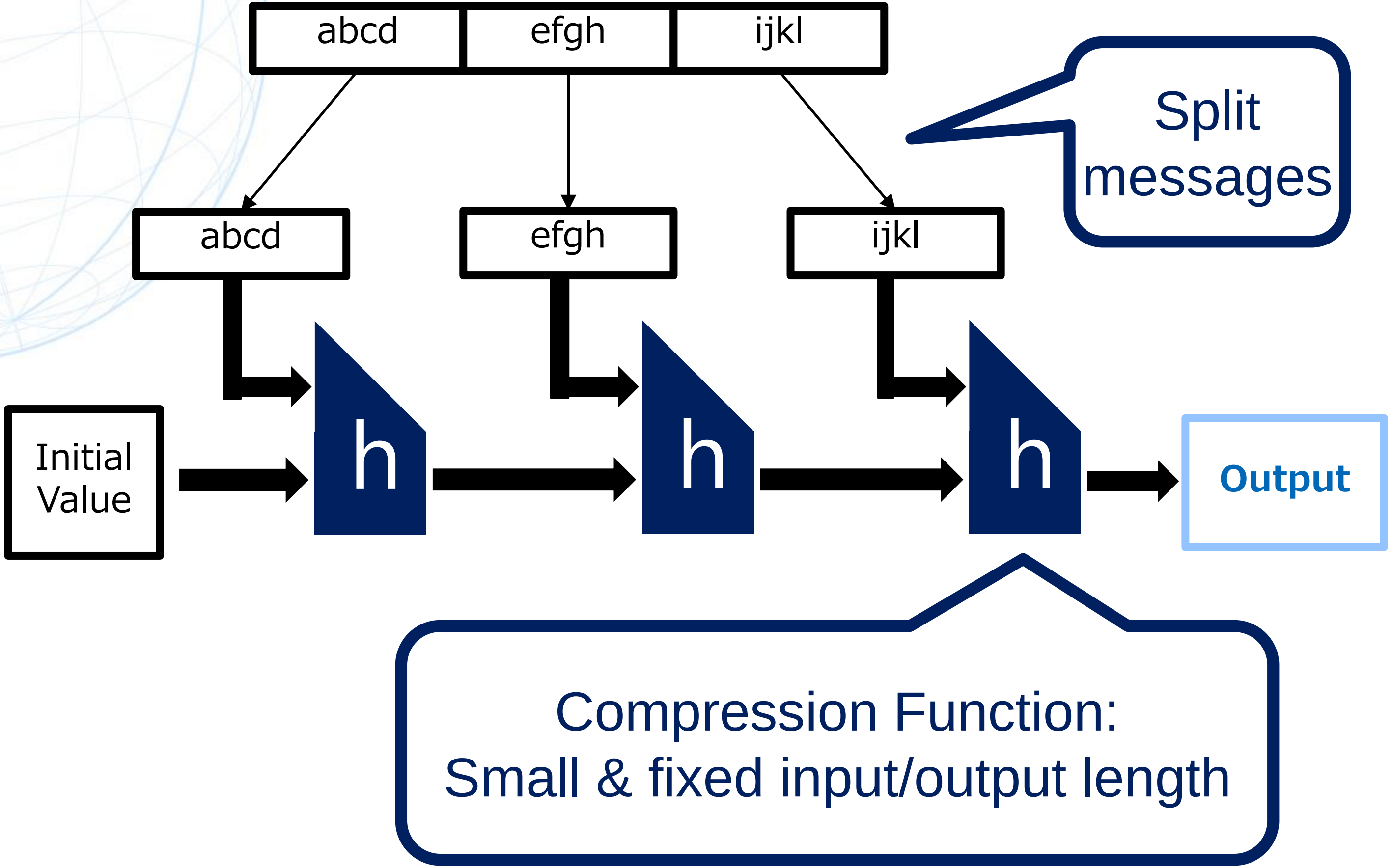
Q. Can we similarly extend the number of attacked steps of SHA-2 in the quantum setting??

Basics of SHA-2

SHA-2

- Current most popular hash function family standardized by NIST
- Consists of several functions:
  - SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
  - SHA-224 is a truncated version of SHA-256
  - SHA-384, SHA-512/224, SHA-512/256 are truncated versions of SHA-512
- Davies-Meyer + Merkle-Damgaard

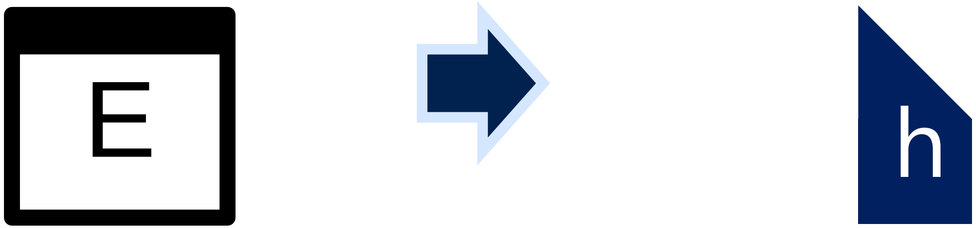
Merkle-Damgaard construction



How to make compression functions

Block cipher

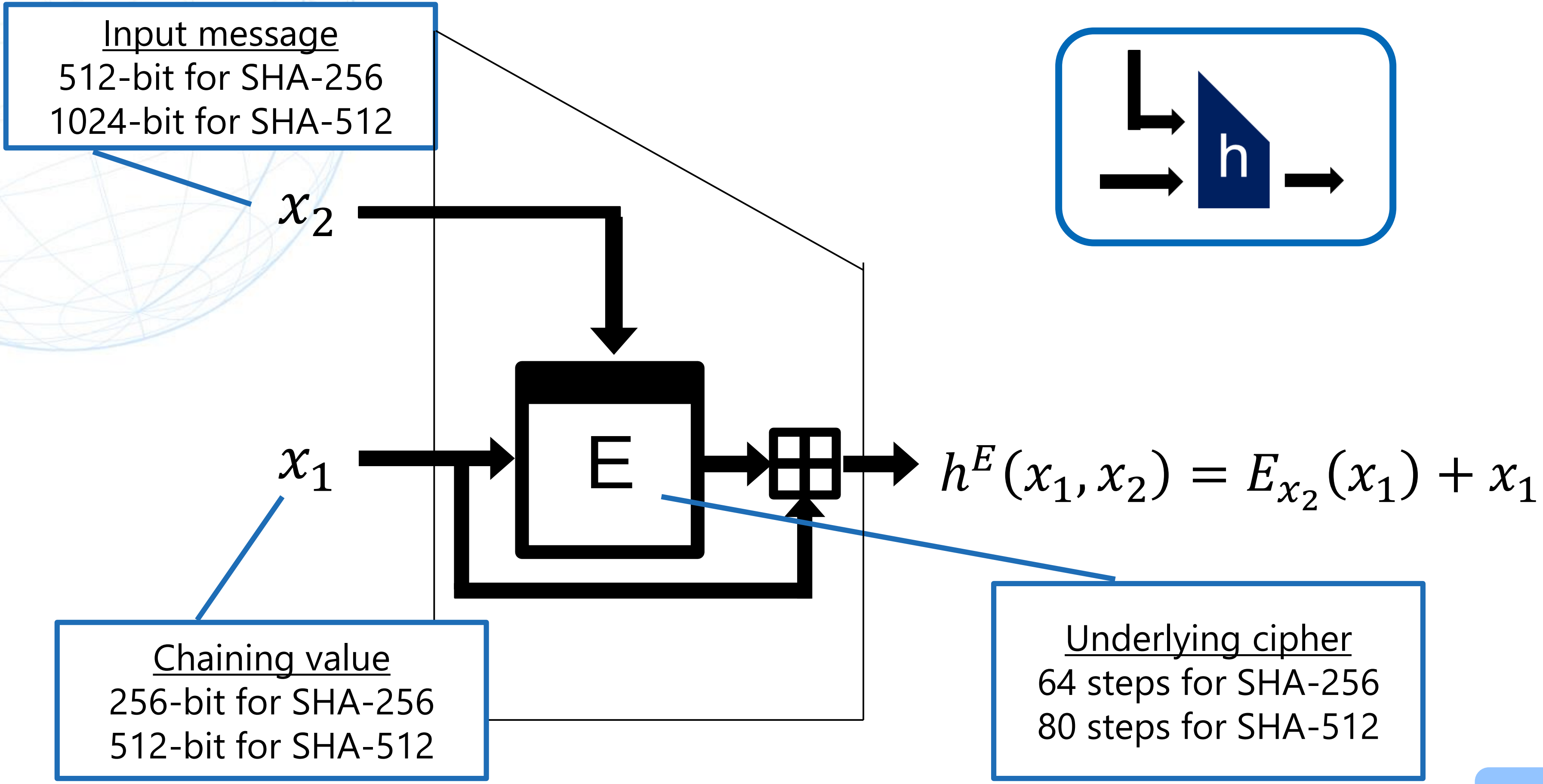
Compression Function



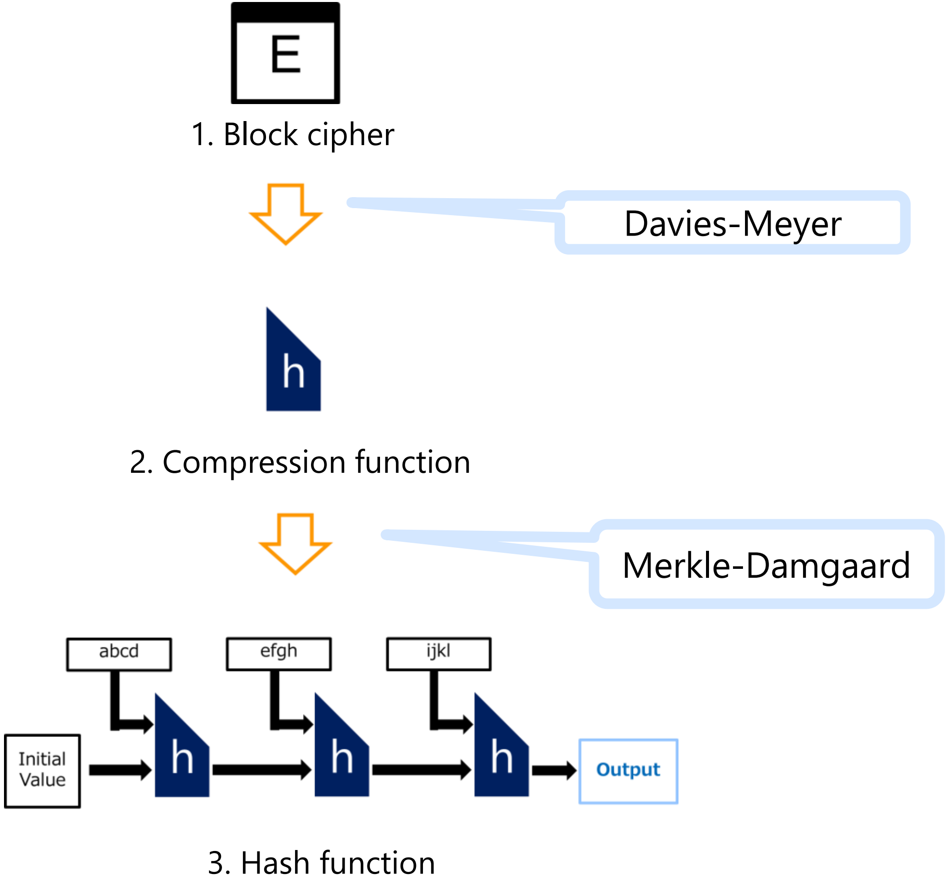
SHA-2

<u>Davies-Meyer Construction</u>,
Matyas–Meyer–Oseas (MMO) Construction,
Miyaguchi-Preneel (MP) Construction,
etc...

Davies-Meyer Construction



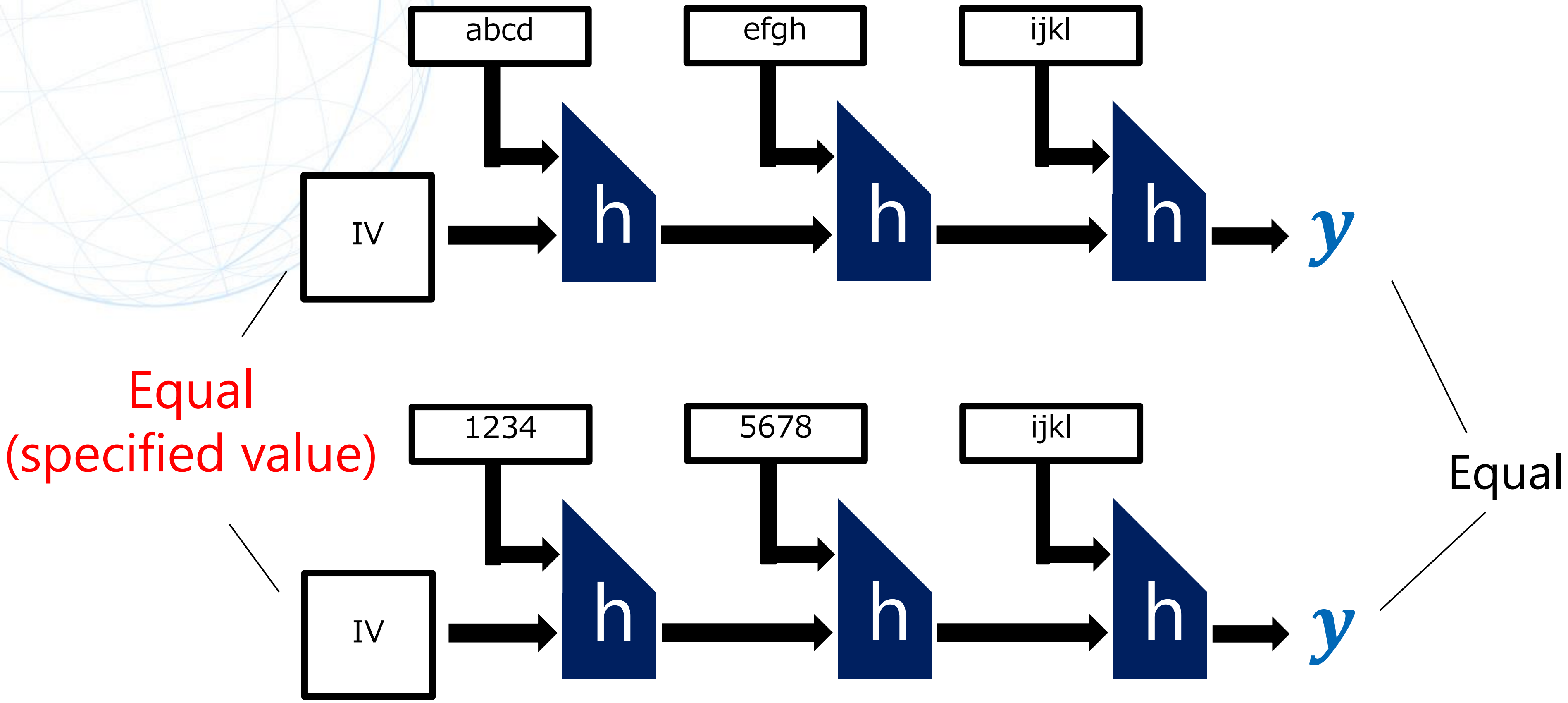
Construction of SHA-2: Summary



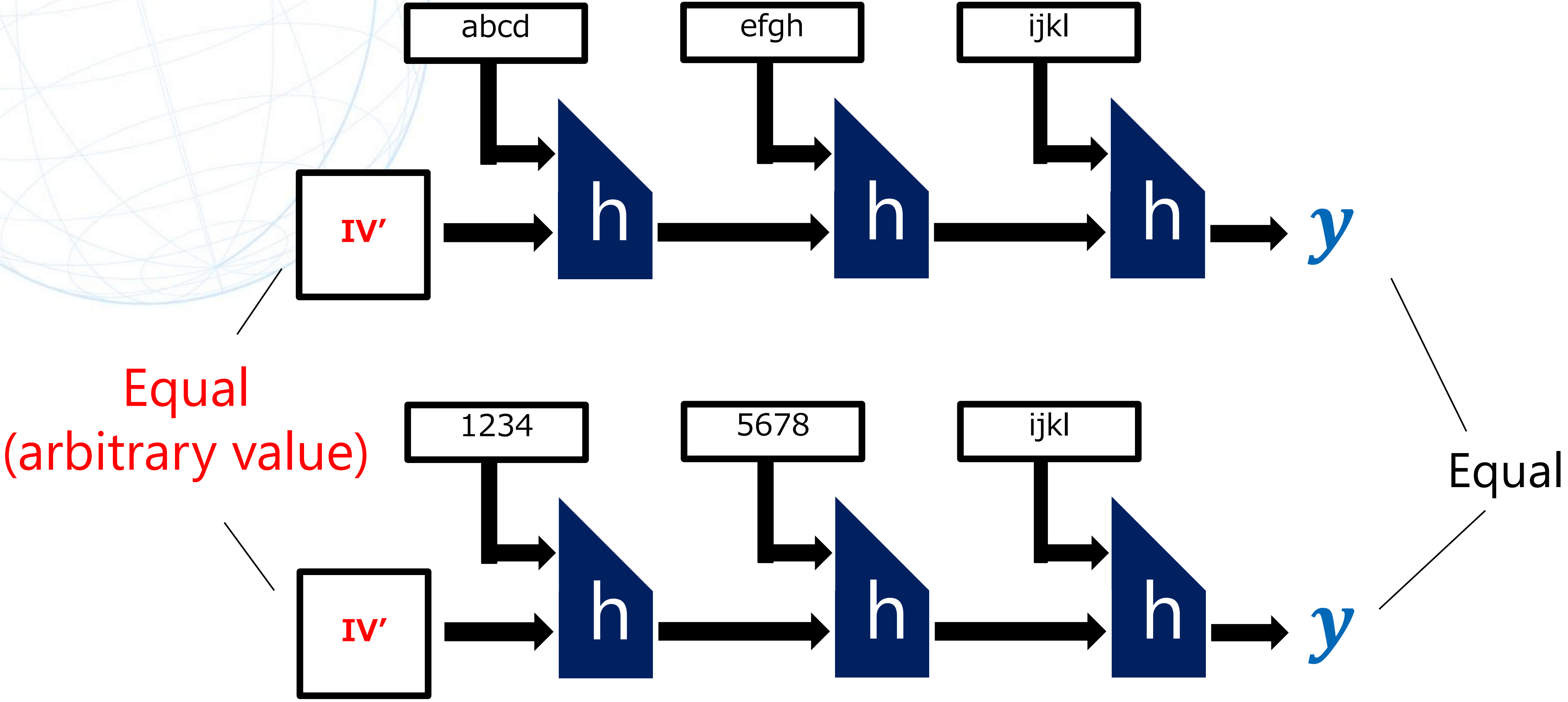
Semi-Free-Start Collision

Collision of a Hash Function

NTT



Semi-Free-Start Collision of a Hash Function



Collision and Semi-Free-Start Collision

NTT

- Collision

  IVs are equal to the specified value

- Semi-Free-Start Collision

  IVs are the same but not equal to the specified value

Previous Work on SHA-256

Previous Classical Work on SHA-256

- Mendel et al. showed
  - 31-step collision attack on SHA-256
  - 38-step semi-free-start collision attack on SHA-256

- The attacks are based on differential cryptanalysis
  - Differential characteristic, (some parts of) conforming message pairs / internal states are searched simultaneously with automated tools
  - Characteristic is very complicated

[MNS13] Florian Mendel and Tomislav Nad and Martin Schläffer: Improving Local Collisions: New Attacks on Reduced SHA-256 (Eurocrypt 2013)

The 31-step characteristic by Mendel et al.

i	ΔA_i	ΔE_i	ΔW_i
-4	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
-3	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
-2	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
-1	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
0	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
1	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
2	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
3	---- ---- ---- ---- ---- ---- ---- --0-	-0-- ---- ---- ---- --0- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
4	---- ---- ---- ---- ---- ---- ---- --00	-1-- ---- ---1 ---- -01- --1- 0--0 --10	---- ---- ---- ---- ---- ---- ---- ----
5	-nnn -n-n -11- ---n --nu -1-- ---- -0n-	0nnn n1uu -0-1 101n -1nu --0- 11-1 -0n1	u--- uunu ---- ---n ---n ---- ---- --n-
6	unnn n--- ---- ---- ---- ---- ---- --0-	n-n1 0111 n--u 11u0 0n10 u1n- nn1n -1uu	nn1- n--- nu-n n--1 u--0 -un0 --n0 -nn-
7	---- ---- ---- ---- ---n ---- ---- n-0u	101u 0nn1 0-11 011u -n11 1n11 0un1 -nnn	00nn 0n10 1-n1 nnn1 u0nn -n01 1u-1 n0--
8	---- ---- ---- ---- ---- ---- ---- ----	1-uu 1111 0--0 u101 10n- 1010 1010 -0n0	0001 u000 1-00 0nuu un1n 01nn -01n uuuu
9	---- ---- ---- ---- ---- ---- ---- ----	1011 00uu 1111 11nu 1110 01-- 0111 10nn	---- -1-- ---- ---u n--- 0--- --11 un--
10	---- ---- ---- ---- u--- ---- ---- -u--	1-00 u110 1001 101u n00- -000 1--u 1n00	---0 ---- ---- ---- ---- ---- ---- --1-
11	---- ---- ---- ---- ---- ---- ---- ----	0101 00u0 nu1u uuuu u100 1000 000n 1u10	---- ---- ---- ---- ---- ---- ---- ----
12	---- ---- ---- ---- ---- ---- ---- ----	111n uuuu uuuu uuuu u001 1111 0110 0n00	---- ---- ---- ---- ---- ---- ---- ----
13	---- ---- ---- ---- ---- ---- ---- ----	---1 01-1 1-1- ---- 1--- ---- ---0 -0--	---- ---- ---- ---- ---- ---- ---- ----
14	---- ---- ---- ---- ---- ---- ---- ----	---1 00-- -001 1111 u--- ---- 1--- -u--	---- ---- ---- ---- ---- ---- ---- ----
15	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- 0--- ---- ---- -0--	---- ---- ---- ---- ---- ---- ---- ----
16	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- 1--- ---- ---- -1--	---- ---- ---- -unn nunn nnnn nnnn nn--
17	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
18	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- n--- ---- ---- -n--
19	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
20	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
21	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
22	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
23	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
24	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
25	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
26	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
27	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
28	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
29	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
30	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----

The 31-step characteristic by Mendel et al.

NTT

Conditions for Internal states

Conditions for Message words

i	ΔA_i								ΔE_i								ΔW_i							
-4	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----								
-3	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----								
	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----								
	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----								
	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
	----	----	----	----	----	----	----	--0-	-0--	----	----	----	--0-	----	----	----	----	----	----	----	----	----	----	----
	----	----	----	----	----	----	----	--00	-1--	----	---1	----	-01-	--1-	0--0	--10	----	----	----	----	----	----	----	----
	nnn	-n-n	-11-	---n	--nu	-1--	----	-0n-	0nnn	n1uu	-0-1	101n	-1nu	--0-	11-1	-0n1	u---	uunu	----	---n	---n	----	----	--n-
	nnn	n---	----	----	----	----	----	--0-	n-n1	0111	n--u	11u0	0n10	u1n-	nn1n	-1uu	nn1-	n---	nu-n	n--1	u--0	-un0	--n0	-nn-
7	----	----	----	----	---n	----	----	n-0u	101u	0nn1	0-11	011u	-n11	1n11	0un1	-nnn	00nn	0n10	1-n1	nnn1	u0nn	-n01	1u-1	n0--
8	----	----	----	----	----	----	----	----	1-uu	1111	0--0	u101	10n-	1010	1010	-0n0	0001	u000	1-00	0nuu	un1n	01nn	-01n	uuuu
9	----	----	----	----	----	----	----	----	1011	00uu	1111	11nu	1110	01--	0111	10nn	----	-1--	----	---u	n---	0---	--11	un--
10	----	----	----	----	u---	----	----	-u--	1-00	u110	1001	101u	n00-	-000	1--u	1n00	---0	----	----	----	----	----	----	--1-
11	----	----	----	----	----	----	----	----	0101	00u0	nu1u	uuuu	u100	1000	000n	1u10	----	----	----	----	----	----	----	----
12	----	----	----	----	----	----	----	----	111n	uuuu	uuuu	uuuu	u001	1111	0110	0n00	----	----	----	----	----	----	----	----
13	----	----	----	----	----	----	----	----	---1	01-1	1-1-	----	1---	----	---0	-0--	----	----	----	----	----	----	----	----
14	----	----	----	----	----	----	----	----	---1	00--	-001	1111	u---	----	1---	-u--	----	----	----	----	----	----	----	----
15	----	----	----	----	----	----	----	----	----	----	----	----	0---	----	----	-0--	----	----	----	----	----	----	----	----
16	----	----	----	----	----	----	----	----	----	----	----	----	1---	----	----	-1--	----	----	----	-unn	nunn	nnnn	nnnn	nn--
17	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
18	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	n---	----	----	-n--
19	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
20	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
21	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
22	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
23	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
24	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
25	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
26	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
27	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
28	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
29	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----
30	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Previous Classical Work on SHA-256

NTT

- Mendel et al. showed
  - 31-step collision attack on SHA-256
  - 38-step semi-free-start collision attack on SHA-256
- The attacks are based on differential cryptanalysis
  - Differential characteristic, (some parts of) conforming message pairs / internal states are searched simultaneously with automated tools
  - Characteristic is very complicated

[MNS13] Florian Mendel and Tomislav Nad and Martin Schläffer: Improving Local Collisions: New Attacks on Reduced SHA-256 (Eurocrypt 2013)

Previous Classical Work on SHA-256

NTT

- Mendel et al. showed
  - 31-step collision attack on SHA-256
  - 38-step semi-free-start collision attack on SHA-256

- The attacks are based on differential cryptanalysis
  - Differential characteristic, (some parts of) conforming message pairs / internal states are searched simultaneously with automated tools
  - Characteristic is very complicated

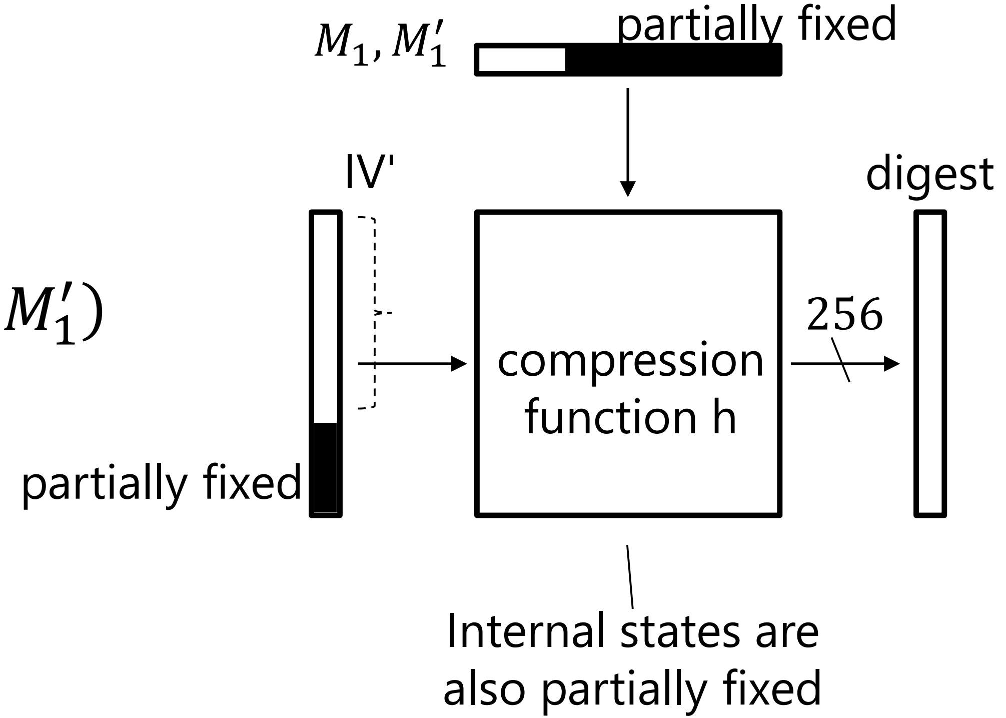
- <u>The 31-step collision attack is mounted by converting 31-step semi-free-start collisions into a collision</u>

[MNS13] Florian Mendel and Tomislav Nad and Martin Schläffer: Improving Local Collisions: New Attacks on Reduced SHA-256 (Eurocrypt 2013)

31-Step collision attack on SHA-256 by Mendel et al.

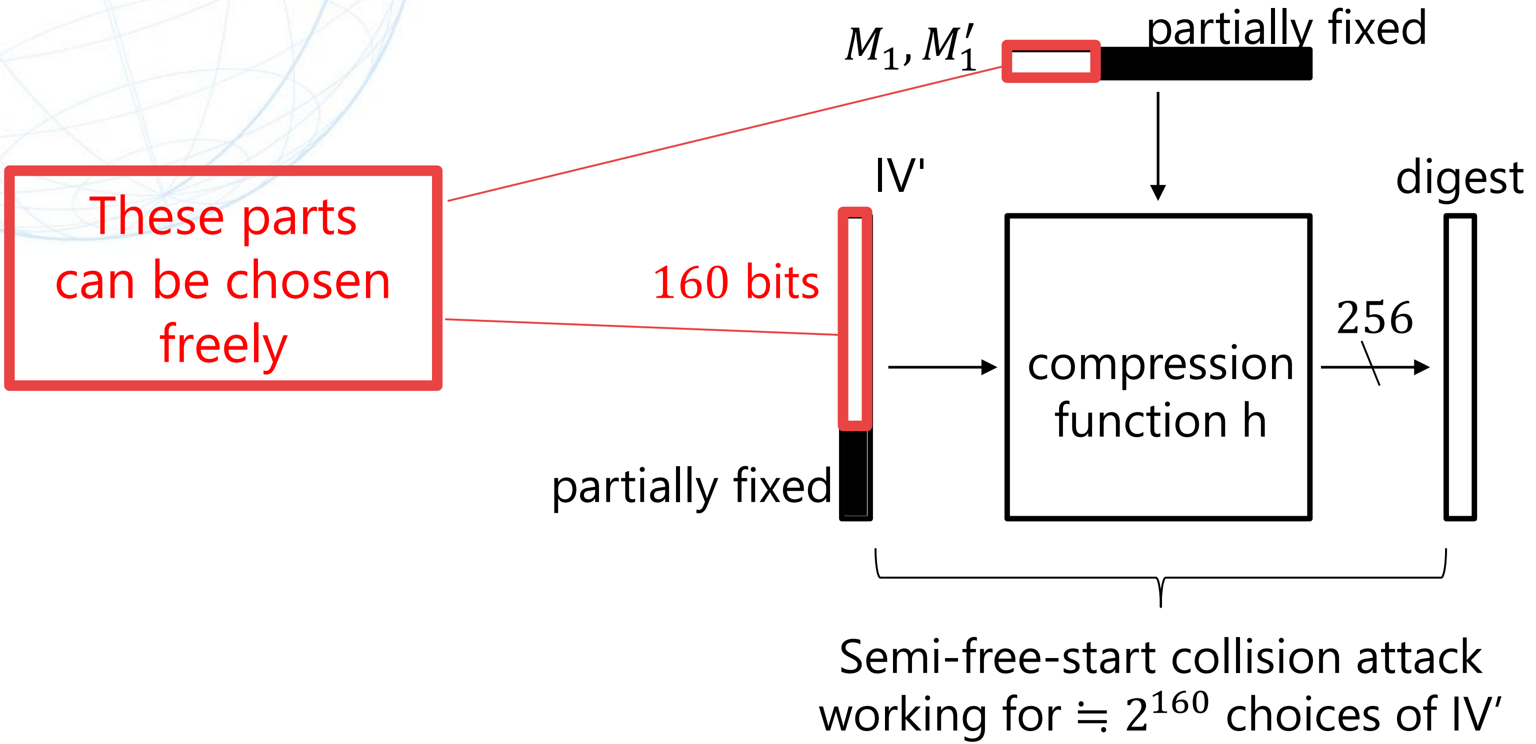
- We can make many <u>semi-free-start collisions</u> of the compression function from the differential characteristic

$$h(\mathrm{IV}', M_1) = h(\mathrm{IV}', M_1')$$



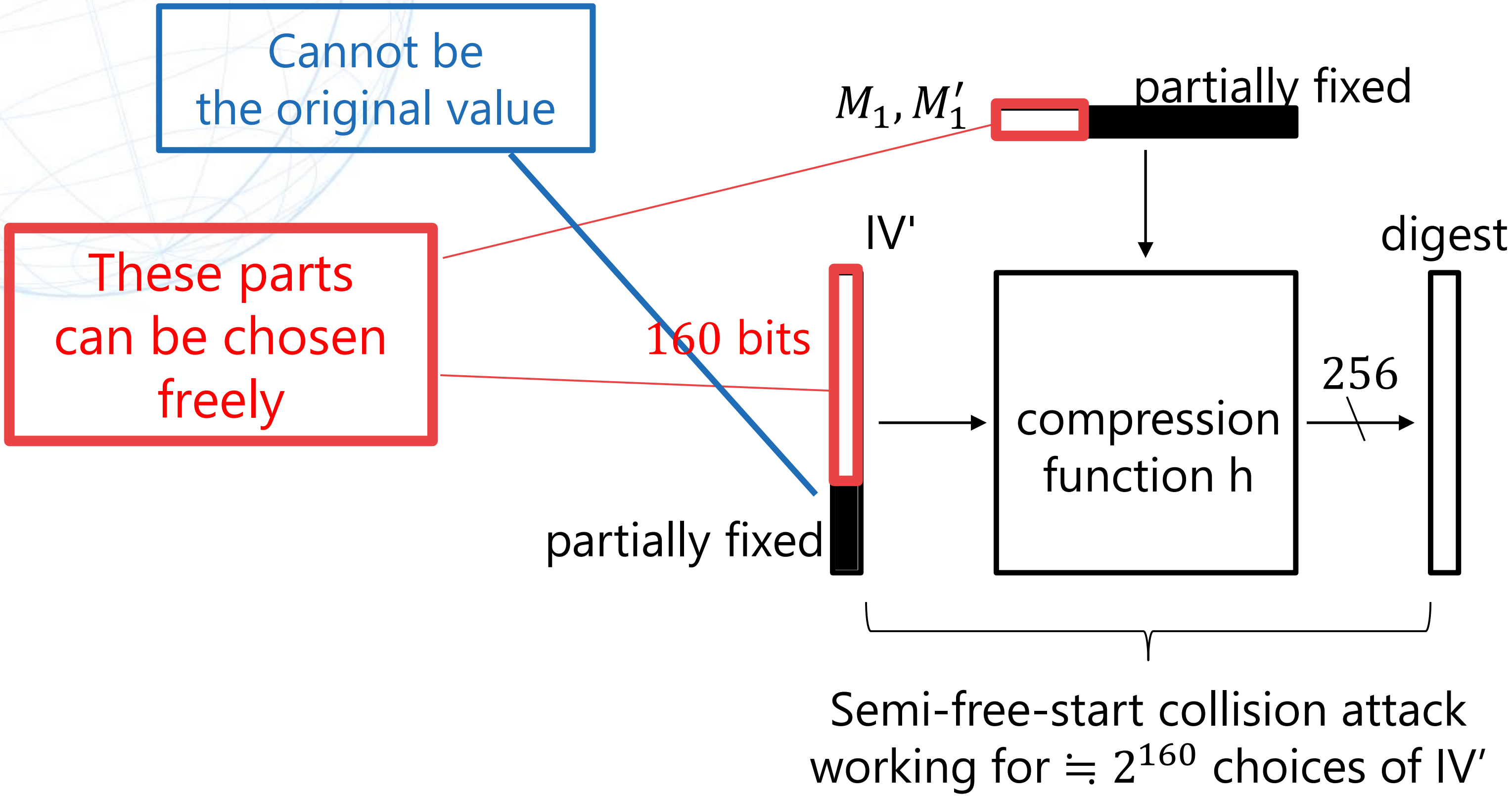
31-Step collision attack on SHA-256 by Mendel et al.

- We can make many <u>semi-free-start collisions</u> of the compression function from the differential characteristic



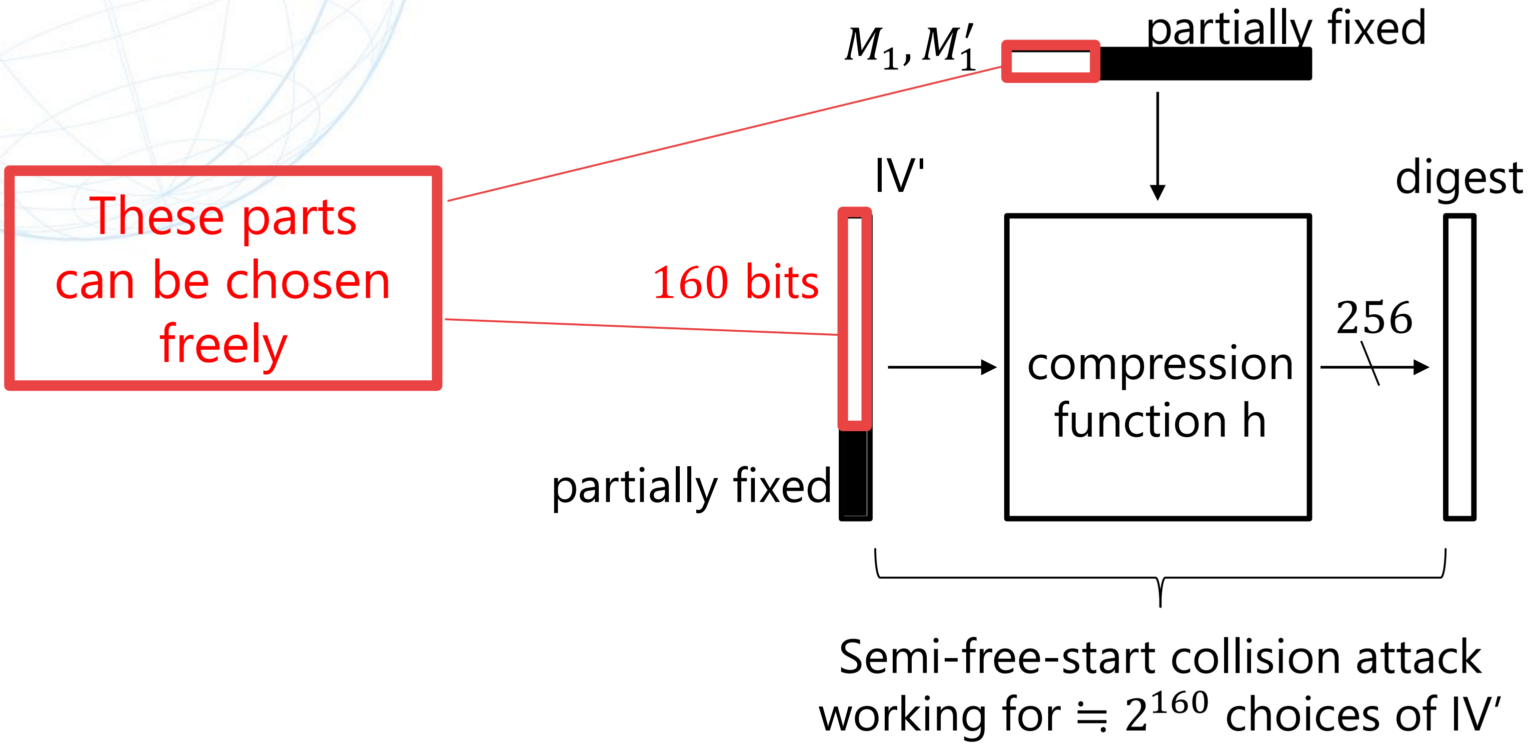
31-Step collision attack on SHA-256 by Mendel et al.

- However, IV’ is not equal to the original IV…

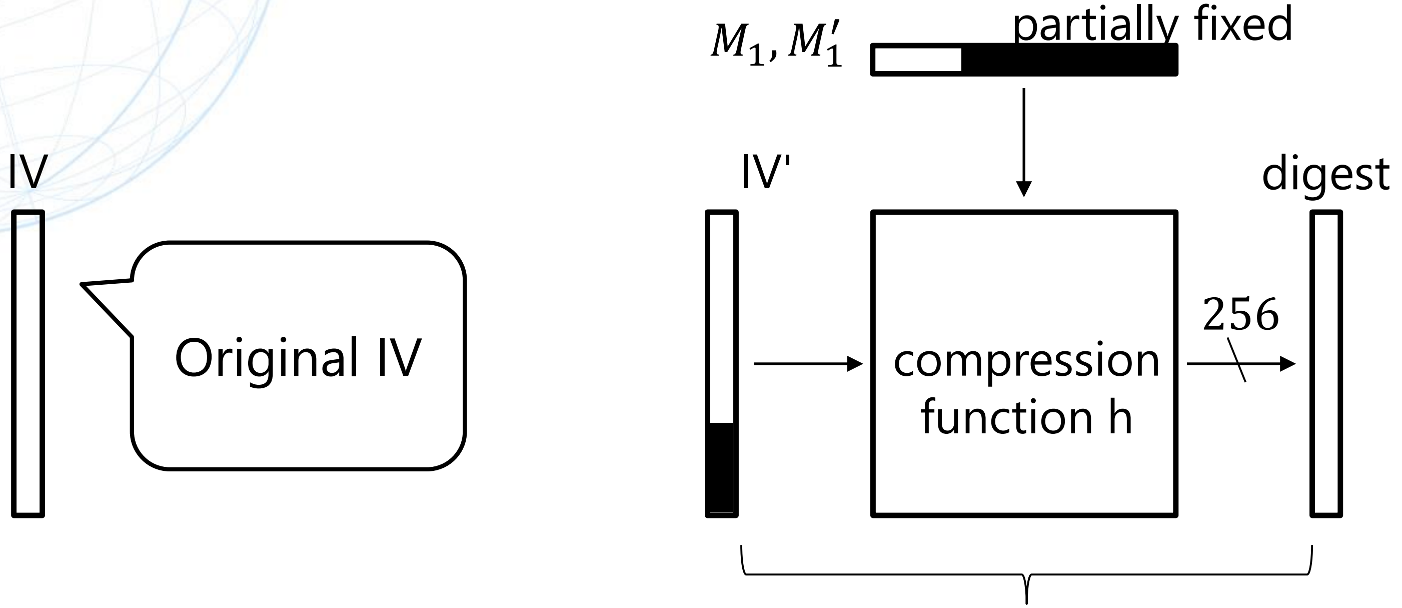


31-Step collision attack on SHA-256 by Mendel et al.

- Convert the semi-free-start collision into a 2-block collision by using the degrees of freedom



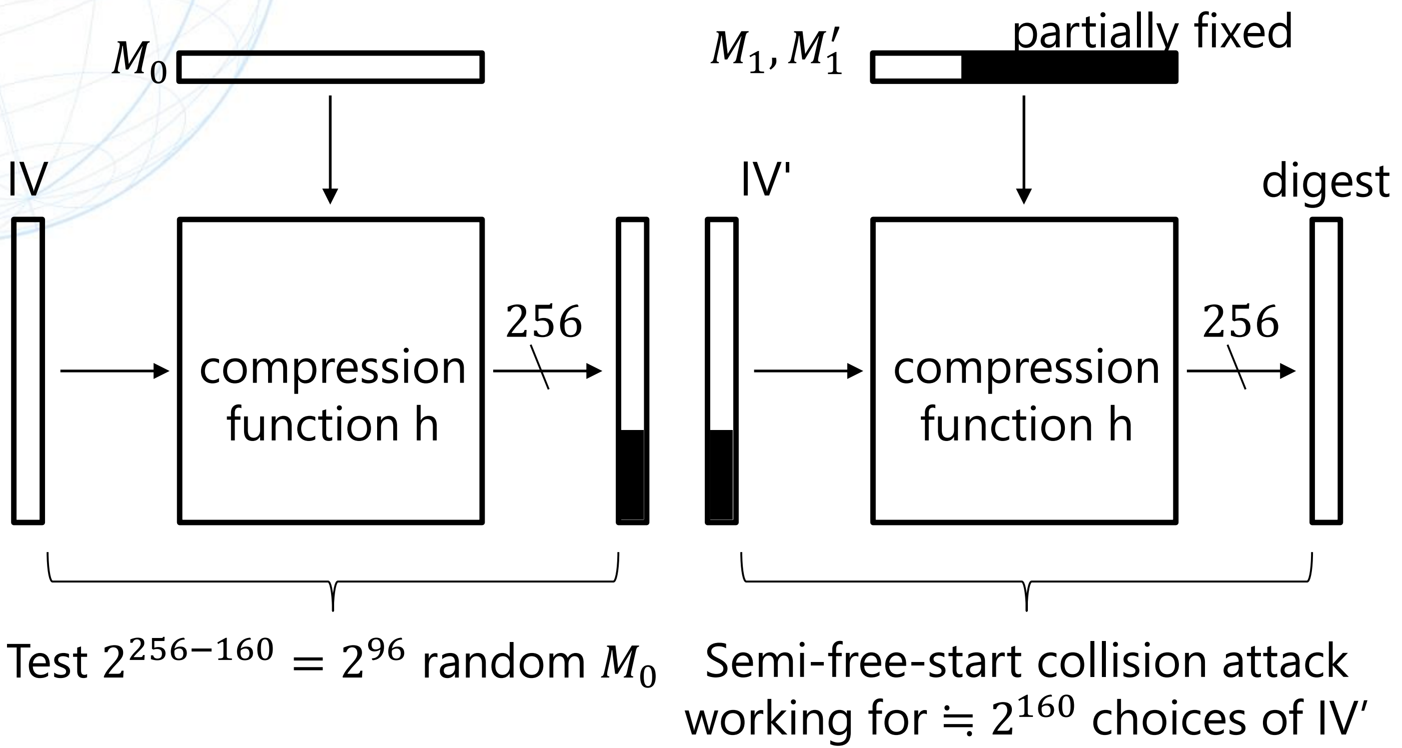
31-Step collision attack on SHA-256 by Mendel et al.



Semi-free-start collision attack working for ≒ 2^{160} choices of IV′

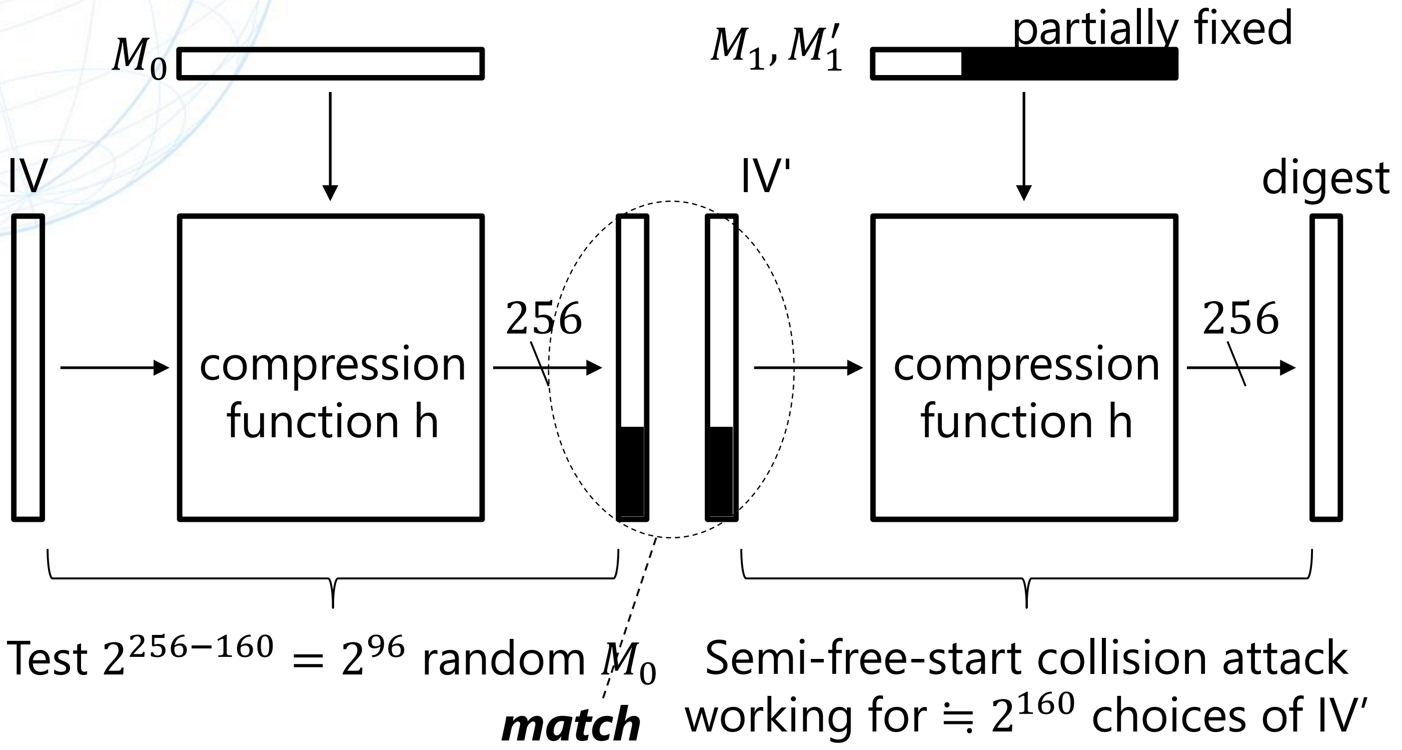
31-Step collision attack on SHA-256 by Mendel et al.

- When we test $2^{256-160} = 2^{96}$ random M_0,



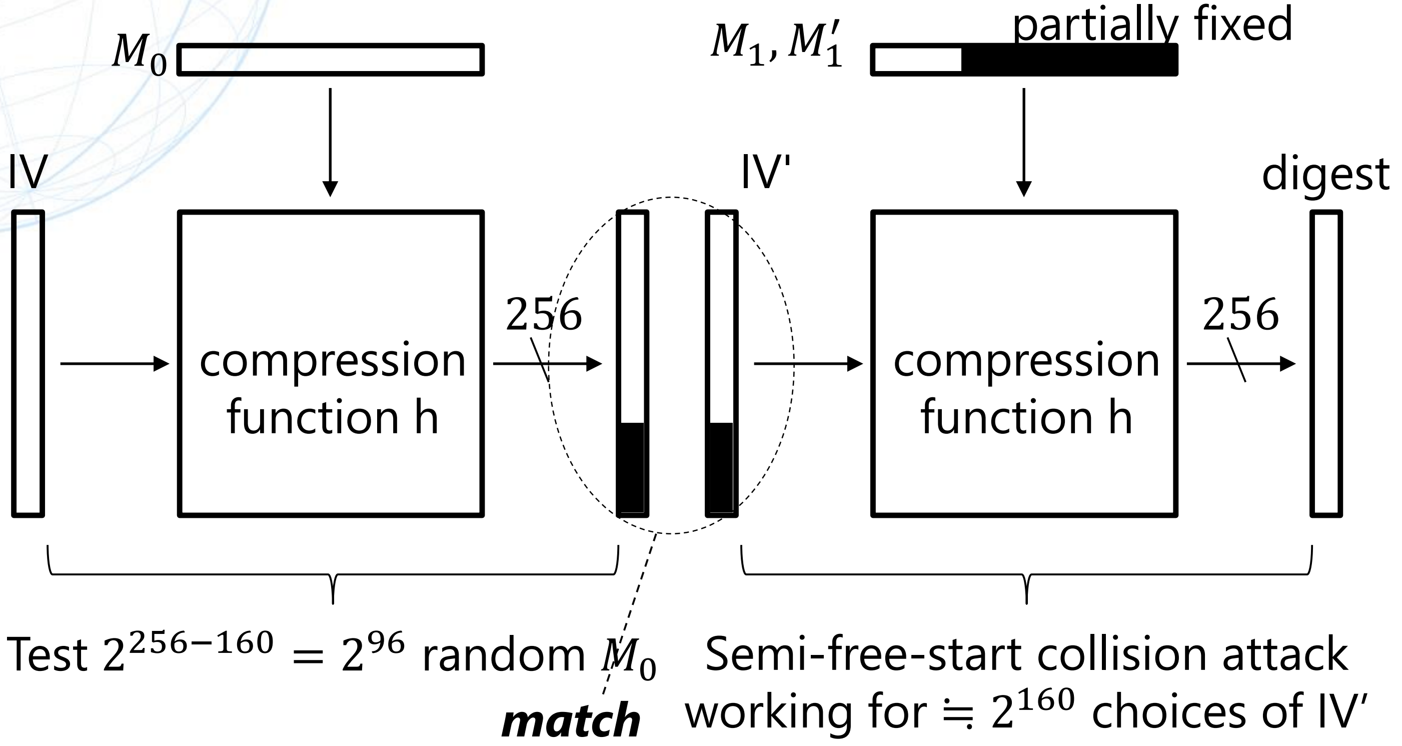
31-Step collision attack on SHA-256 by Mendel et al.

- When we test $2^{256-160} = 2^{96}$ random M_0, one of the outputs will match an IV′ of the second block (among 2^{160} choices of IV′)



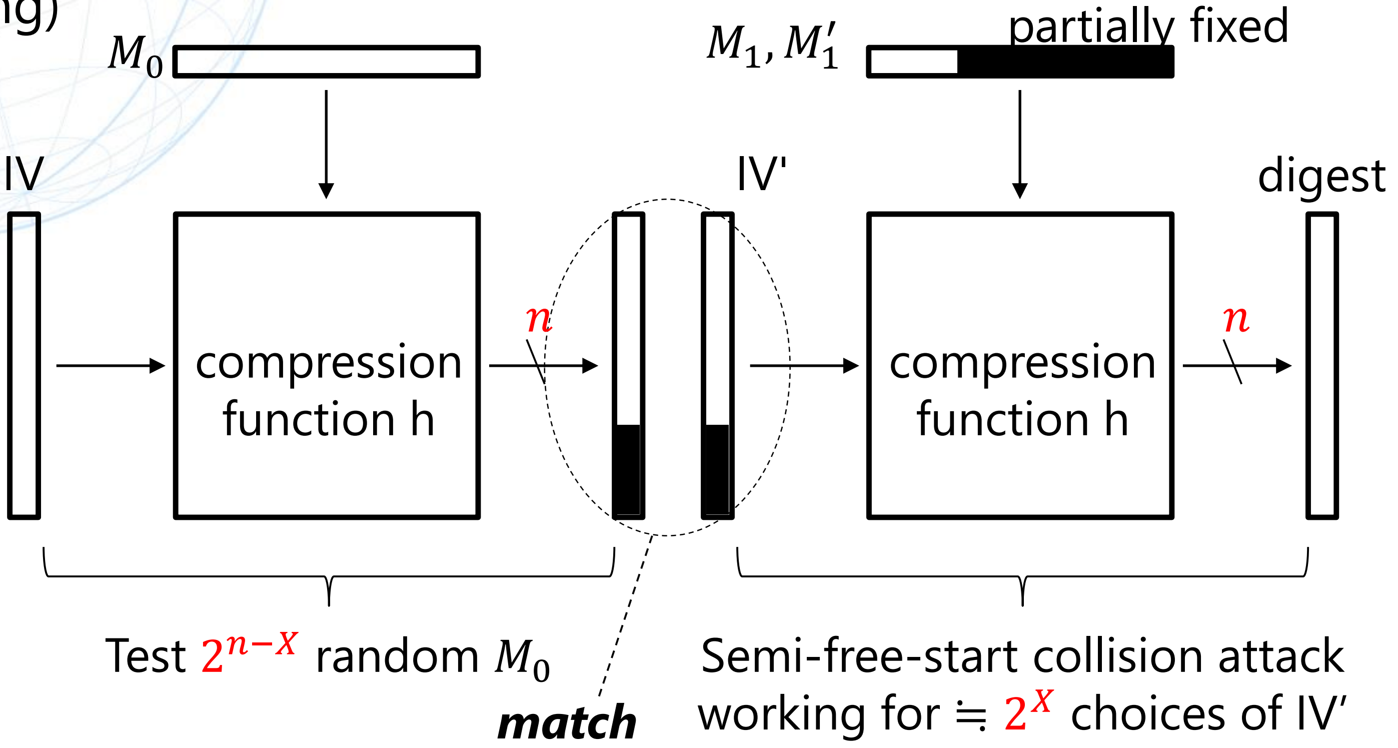
31-Step collision attack on SHA-256 by Mendel et al.

- We can find a 2-block collision in time $2^{96} < 2^{\frac{256}{2}} = 2^{128}$ (actually the attack is more complicated...)



Generalization of the 2-block collision attack

- If we can make many semi-free-start collisions for 2^X choices of IV's, then we can find a 2-block collision in time 2^{n-X} (in the classical setting)



Generalization of the 2-block collision attack

NTT

- If we can make many semi-free-start collisions for 2^X choices of IV's, then we can find a 2-block collision in time 2^{n-X} (in the classical setting)

- The attack is valid only if $2^{n-X} < 2^{n/2}$, i.e., $\boldsymbol{X > n/2}$

- Mendel et al. showed not only the 31-step collision attack but also a 38-step semi-free-start collision attack in the same paper, but it is not converted into a collision attack

  →<u>The parameter X for the 38-step attack is not large enough</u>

Generalization of the 2-block collision attack

NTT

- If we can make many semi-free-start collisions for 2^X choices of IV's, then we can find a 2-block collision in time 2^{n-X} (in the classical setting)

- The attack is valid only if $2^{n-X} < 2^{n/2}$, i.e., $\boldsymbol{X > n/2}$

- Mendel et al. showed not only the 31-step collision attack but also a 38-step semi-free-start collision attack in the same paper, but it is not converted into a collision attack

  →The parameter X for the 38-step attack is not large enough

Idea:

The validity condition may be relaxed in the quantum setting

Conversion of Semi-Free-Start Collisions into Collisions in the Quantum Setting

Generic Quantum Collision Attacks

NTT

Three settings depending on available computational resources

1. Small quantum computer + Large qRAM

Best algorithm: BHT ($T = 2^{n/3}$ & qRAM $2^{n/3}$) [BHT98]

2. Efficiency is measured by Time-Space tradeoff (No qRAM)

Quantum computer of size S + Classical computer of size S

Best algorithm: Parallel rho (Tradeoff $T = 2^{n/2}/S$) [Ber09]

3. Small quantum computer + Large classical memory (No qRAM)

Best algorithm: CNS ($T = 2^{2n/5}, 2^{n/5}$classical memory) [CNS17]

[BHT98] Gilles Brassard, Peter Høyer, Alain Tapp: Quantum Cryptanalysis of Hash and Claw-Free Functions. LATIN 1998

[Ber09] D. J. Bernstein: Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?. SHARCS 2009.

[CNS17] A. Chailloux, M. Naya-Plasencia, A. Schrottenloher: An efficient quantum collision search algorithm and implications on symmetric cryptography. Asiacrypt 2017.

Generic Quantum Collision Attacks

NTT

Three settings depending on available computational resources

1. Small quantum computer + Large qRAM

Best algorithm: BHT ($T = 2^{n/3}$ & qRAM $2^{n/3}$) [BHT98]

Our Focus

2. Efficiency is measured by Time-Space tradeoff (No qRAM)

Quantum computer of size S + Classical computer of size S

Best algorithm: Parallel rho (Tradeoff $T = 2^{n/2}/S$) [Ber09]

3. Small quantum computer + Large classical memory (No qRAM)

Best algorithm: CNS ($T = 2^{2n/5}, 2^{n/5}$classical memory) [CNS17]

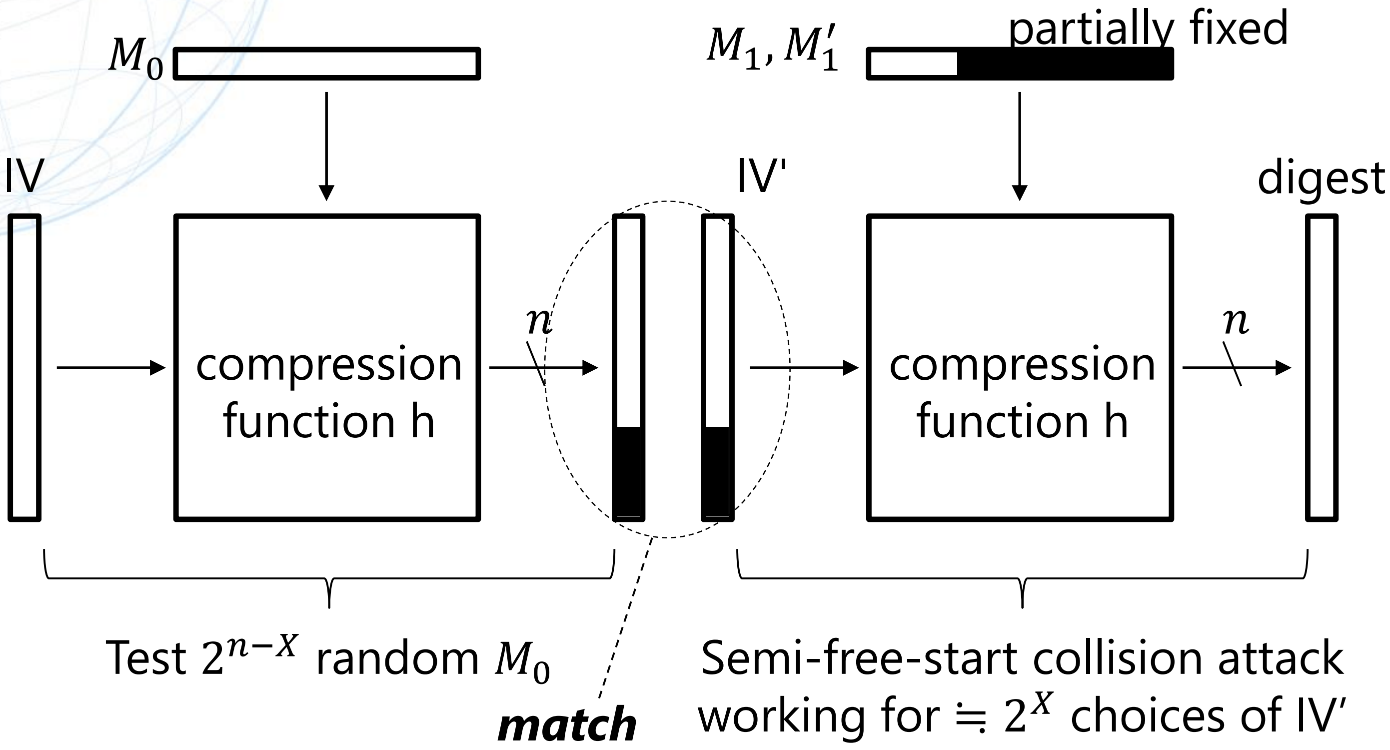
[BHT98] Gilles Brassard, Peter Høyer, Alain Tapp: Quantum Cryptanalysis of Hash and Claw-Free Functions. LATIN 1998

[Ber09] D. J. Bernstein: Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?. SHARCS 2009.

[CNS17] A. Chailloux, M. Naya-Plasencia, A. Schrottenloher: An efficient quantum collision search algorithm and implications on symmetric cryptography. Asiacrypt 2017.

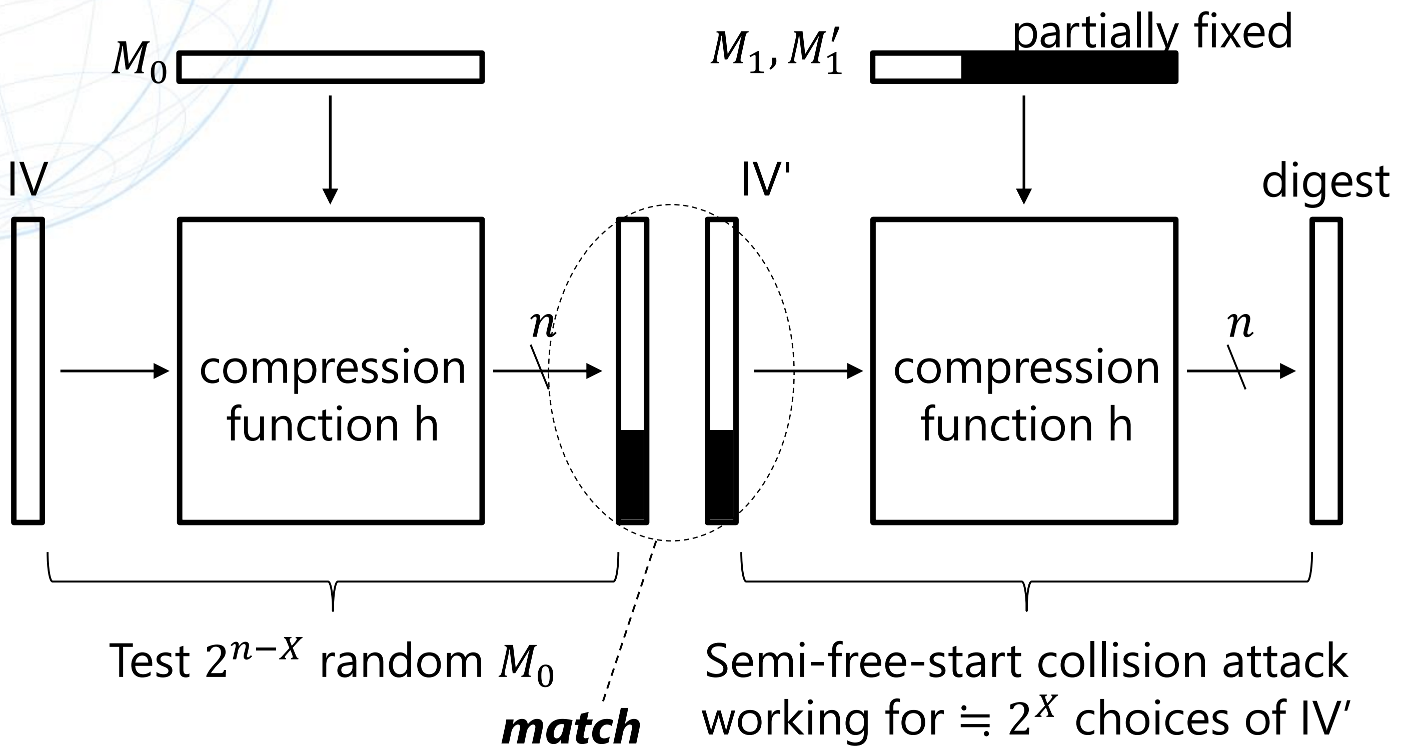
Classical 2-block collision attack

- If we can make many semi-free-start collisions for 2^X choices of IV's, then we can find a 2-block collision in **time 2^{n-X}**



Quantum 2-block collision attack

- If we can make many semi-free-start collisions for 2^X choices of IV's, then we can find a 2-block collision in **time $\sqrt{2^{n-X}}$** (Grover)



Quantum 2-block collision attack

- If S-qubits are available, the attack can be parallelized: $\boldsymbol{T = \sqrt{2^{n-X}/S}}$
- Generic attack… $\boldsymbol{T = \sqrt{2^n}/S}$
- The attack is valid if $\sqrt{2^{n-X}/S} < \sqrt{2^n}/S$, i.e., $\boldsymbol{X > 0}$ (for $S < 2^X$)
- Actually the condition for X will be stronger because here I'm ignoring many things: qubits required to implement Grover, time for sub-procedures, etc.
- Still, the new condition $\boldsymbol{X > 0}$ seems much weaker than $\boldsymbol{X > n/2}$

Main Results

Results on SHA-256 and SHA-512

NTT

- We convert the 38-step semi-free-start collision attack on SHA-256 by Mendel et al. [MNS13] and 39-step semi-free-start collision attack on SHA-512 by Dobraunig et al. [DEM15] into a 2-block collision.
- With some analysis and computer experiments, we confirmed that the attacks are valid in the quantum setting:

Attack Target	Time Complexity	(Generic Complexity)
38-step SHA-256	$2^{121}/\sqrt{S}$ $(2.4 < S < 2^{14})$	$2^{128}/S$
39-step SHA-512	$2^{252.2}/\sqrt{S}$ $(2.5 < S < 2^{7.6})$	$2^{256}/S$

Note: classical best collision attacks are 31-step for SHA-256 and 27-step for SHA-512

Remark: the attacks are invalid in other settings

[MNS13] Florian Mendel and Tomislav Nad and Martin Schläffer: Improving Local Collisions: New Attacks on Reduced SHA-256 (Eurocrypt 2013)
[DEM15] Christoph Dobraunig, Maria Eichlseder, Florian Mendel: Analysis of SHA-512/224 and SHA-512/256. (Asiacrypt 2015)

Summary & Future Directions

Summary & Future Directions

- First dedicated quantum collision attacks on SHA-2
  - 38-step attack on SHA-256 & 39-step attack on SHA-512
  - Classical collision attacks: 31-step for SHA-256 & 27-step for SHA-512
  - Still far from full-step attacks (64 steps / 80 steps)
- We convert classical semi-free-start collisions on 38-step SHA-256 & 39-step SHA-512 into collisions in the quantum setting
- There are many functions which is similar to SHA-2 (RIPEMD-128, RIPEMD-160, SM3, HAS-160, etc……), but so far we haven't found any quantum collision attacks on them: Existing characteristics are not suitable for our idea
- We should revisit differential characteristics search activities
  - Possibility of quantum attacks should be taken into account

Thank you!