Converting MITM Preimage Attack into Pseudo Collision Attack: Application to SHA-2

Ji Li[1], Takanori Isobe[2] and Kyoji Shibutani[2]

[1]Sony China Research Laboratory

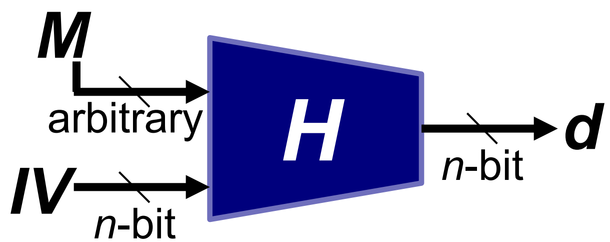
[2]Sony Corporation

FSE 2012, March 20, 2012

Outline

- **Background and summary of results**
- **Propose conversion of MITM preimage attack into pseudo collision attack**
  - Partial target preimage attack ⇒ pseudo collision attack
  - MITM preimage attack ⇒ partial target preimage attack
- **Applications**
  - Pseudo collision attacks on reduced SHA-2 family, Skein-512 and BLAKE

Background



- **Collision attack**
  - Find (M, M') s.t. $M \neq M'$ and $H(IV,M) = H(IV, M')$
- **Preimage attack**
  - Given d (= $H(IV, M)$), find M' s.t. $H(IV, M') = d$
- **Relation between collision security and preimage security**
  - Theory: no implication [RS04]
  - Practice: ?

Open question

- **Can we efficiently convert (pseudo) preimage attack to (pseudo) collision attack ?**
  - e.g. SHA-256

Best collision attack
32 steps

Best preimage attack
45 steps

?

Better collision attack?

Summary (pseudo collision attacks)

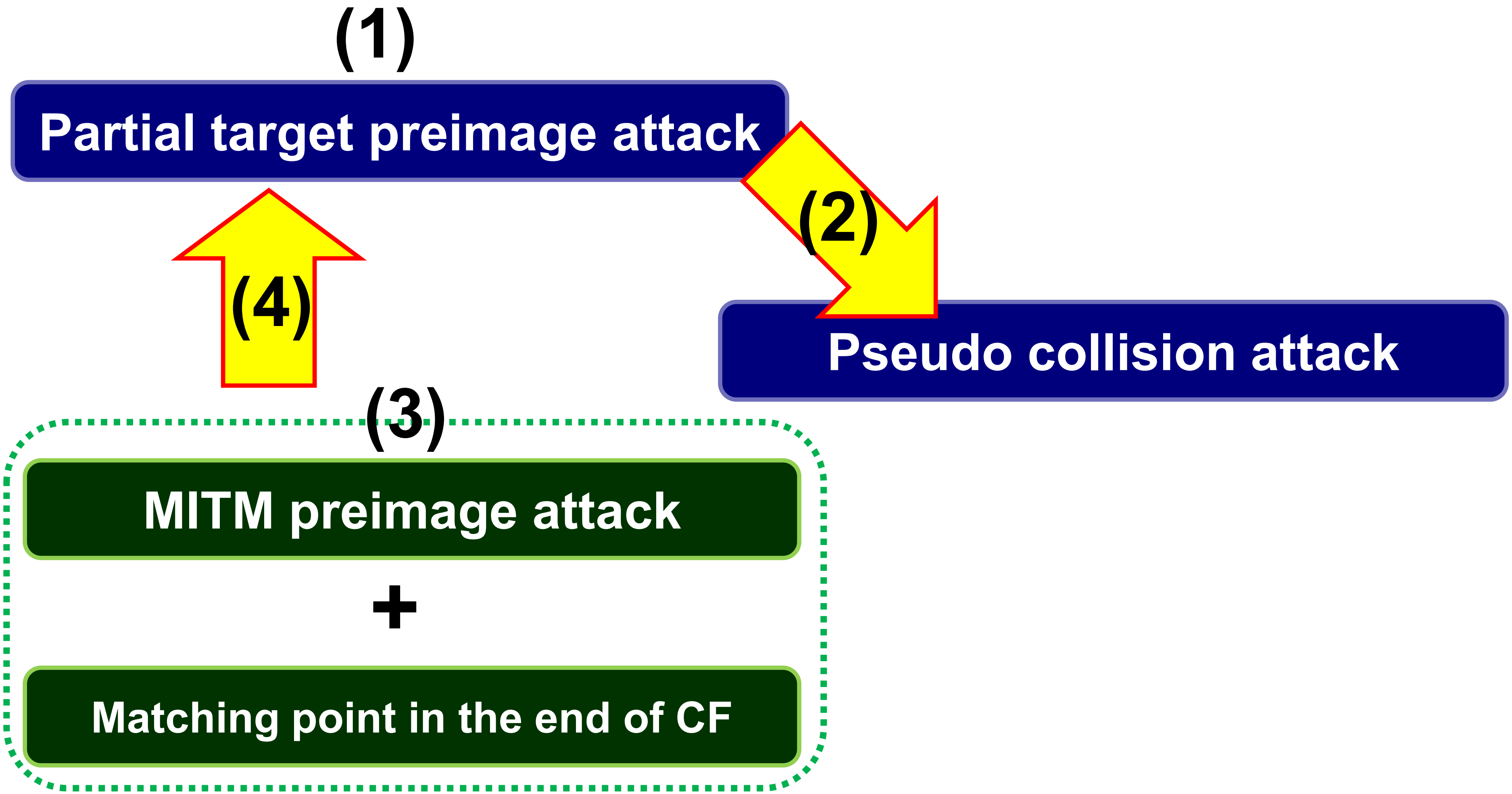
algorithm (# steps/rounds)	# attacked steps/rounds	complexity	reference
SHA-256 (64)	32*1	practical	[MNS11]
	43	2^{126}	
	52	$2^{127.5}$	
SHA-512 (80)	24	$2^{28.5}$	[IMPR09]
	46	$2^{254.5}$	
	57	$2^{255.5}$	
Skein-512 (72)	**22**	$2^{253.8}$	
	37	$2^{255.7}$	
BLAKE-256 (14)	**4** (w/o initialization)	2^{112}	

*1: semi-free-start-collision attack

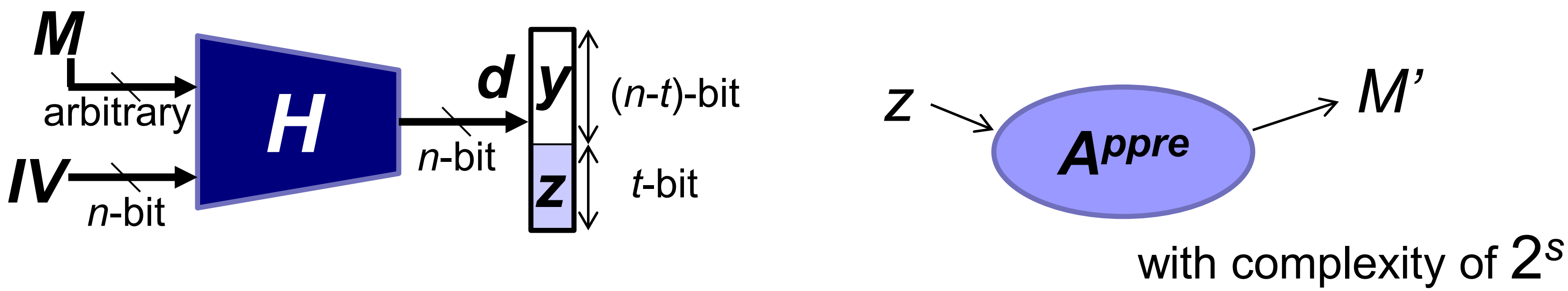
[MNS11] F.Mendel,T.Nad,M.Schlaffer, “Finding SHA-2 characteristics: Searching through a minefield of contradictions”, ASIACRYPT 2011.

[IMPR09] S.Indesteege et al., “Collisions and other non-random properties for step-reduced SHA-256”, SAC 2009.

MITM preimage to pseudo collision

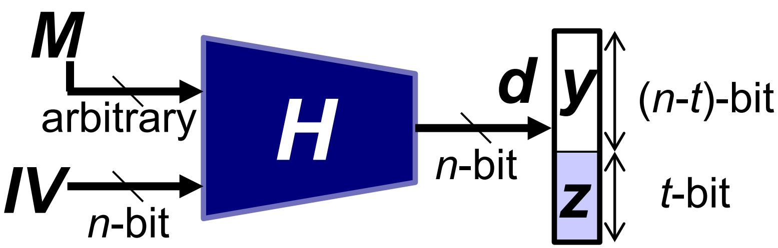


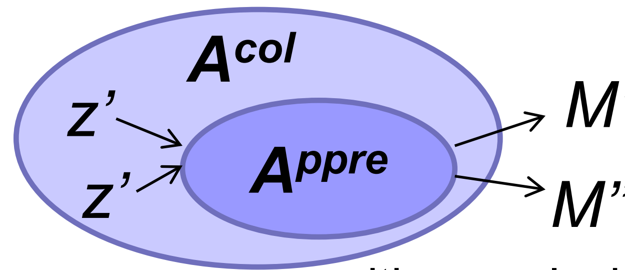
Partial target preimage attack



- **(t-bit) partial target preimage attack**
  - Given z, find M' s.t. $trunc_t(H(IV,M')) = z$,
    where $trunc_t(x)$: t-bit truncation of x
- A^{pre} finds a (t-bit) partial target preimage with 2^s computations

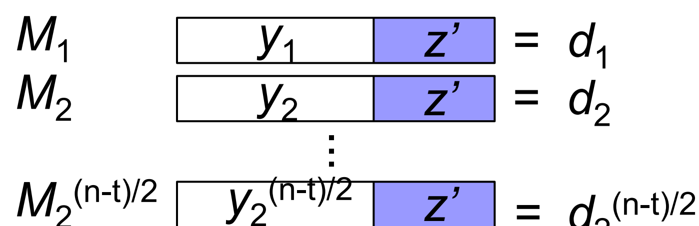
Collision attack (from A^{ppre})





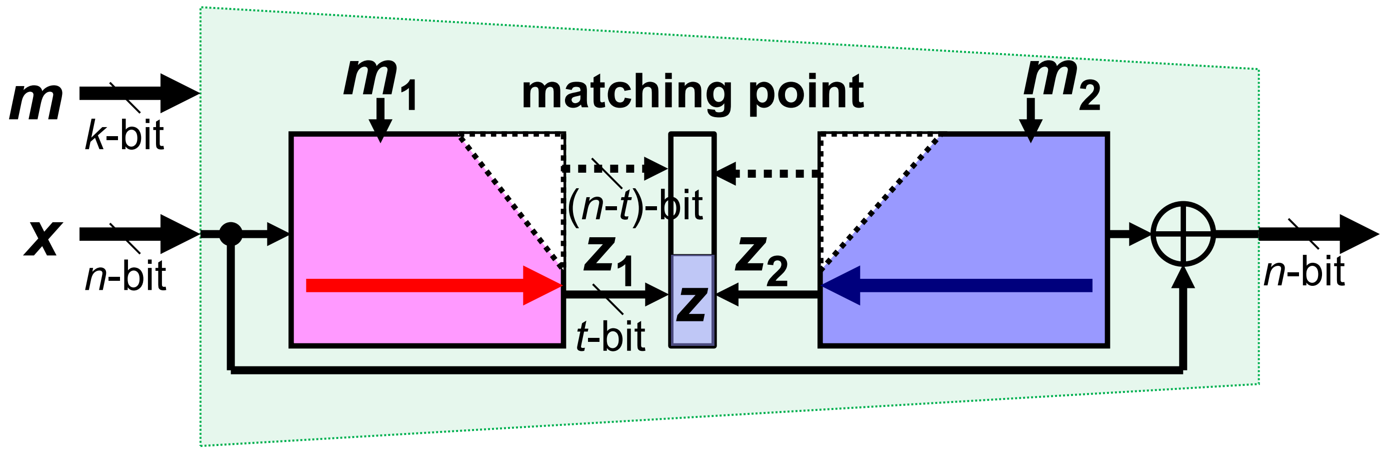
with complexity of 2^s

- **Collision attack**
  - A^{col} : calling A^{ppre} $2^{(n-t)/2}$ times with same z'
  - Time complexity: $2^{(n-t)/2} \times 2^s$ computations
  - Condition: if $s < t / 2$, faster than generic collision attack



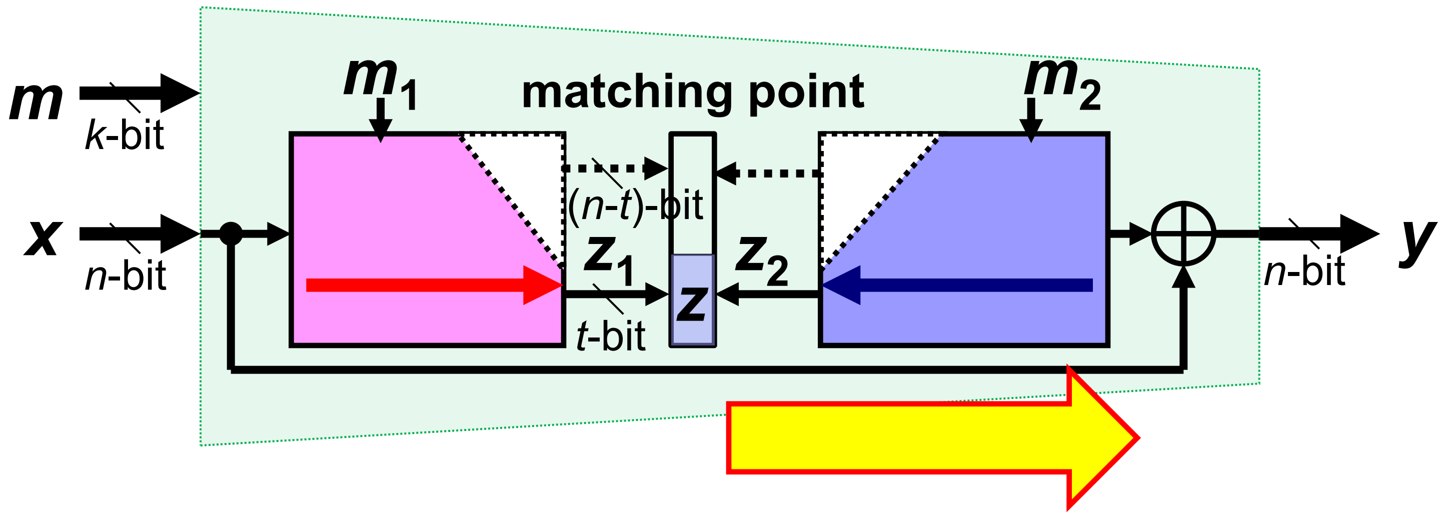
How to construct efficient partial target preimage attack?

Meet-in-the-middle preimage attack



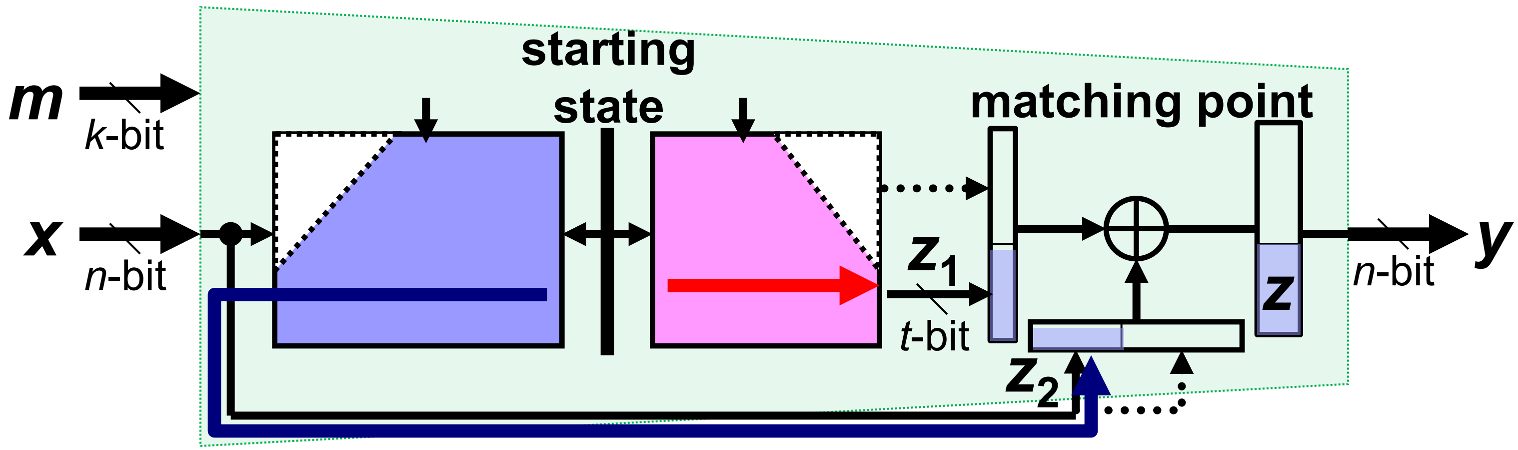
- Narrow-pipe Merkle-Damgard + Davies-Meyer mode
- Neutral message words m_1 and m_2
  - z_1, z_2 are independently computed from m_2, m_1, respectively
- $2^{|m1|+|m2|}$ $(z_1 + z_2)$ with a complexity of $2^{|m1|}+2^{|m2|}$ $(\ll 2^{|m1|+|m2|})$
  - $2^{|m1|}$ of z_1 with a complexity $2^{|m1|}$, $2^{|m2|}$ of z_2 with a complexity $2^{|m2|}$
- Total complexity = $2^{n-(|m1|+|m2|)}$ x $\max(2^{|m1|},2^{|m2|})$

Moving matching point of MITM



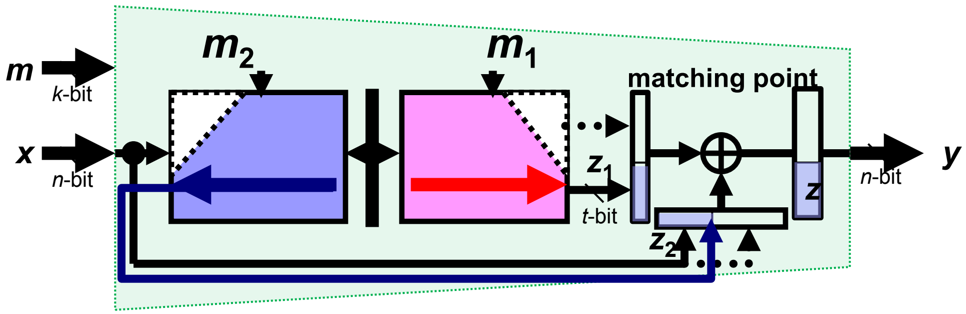
- Splice-and-Cut [AS08]
  - Starting/matching point can be moved to any position

Moving matching point of MITM



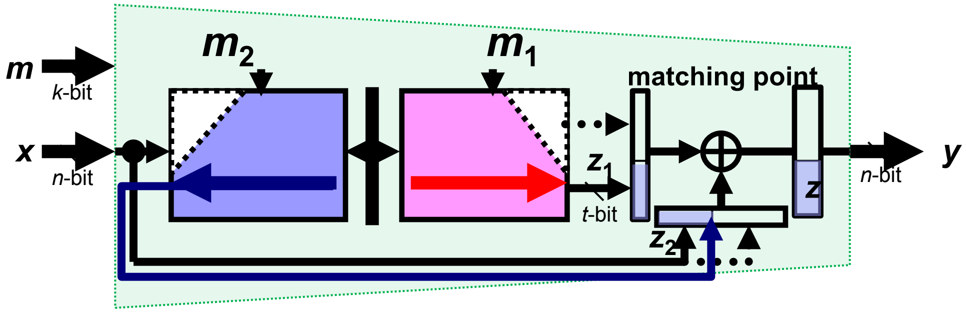
- Splice-and-Cut [AS08]
  - Starting/matching point can be moved to any position
- MITM preimage attack with the matching point at the end is considered as partial target preimage attack

MITM preimage to partial target preimage



- MITM preimage attack with the matching point at the end is considered as partial target preimage attack
  - e.g. $|m_1| = 4$, $|m_2| = 5$, $|z| = 4$
    - 2^4 of $(z_1 + z_2)$ are required to obtain one 4-bit partial target preimage
    - Compute 2^2 of z_1, and 2^2 of z_2 $\Rightarrow$ 2^4 of $(z_1 + z_2)$
    - 1 preimage of the partial target z is derived with a complexity of 2^2
  - Condition for efficient collision attack: $s < t / 2$
  - $t = 4$, $s = 2$ $\Rightarrow$ worse than generic collision attack...

MITM preimage to partial target preimage



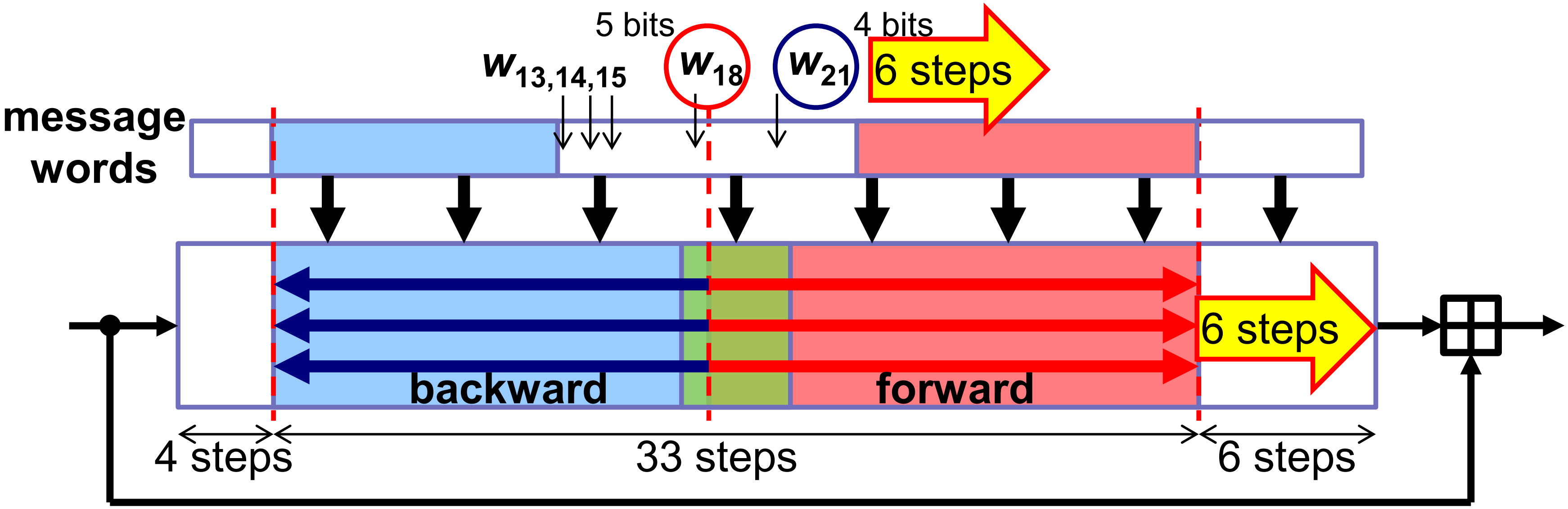
- MITM preimage attack with the matching point at the end is considered as partial target preimage attack
  - e.g. $|m_1| = 4$, $|m_2| = 5$, $|z| = 4$
    - 2^4 of $(z_1 + z_2)$ are required to obtain one 4-bit partial target preimage
    - ~~Compute $\cancel{2^2}$ of z_1, and $\cancel{2^2}$ of z_2 $\Rightarrow$ $\cancel{2^4}$ of $(z_1 + z_2)$~~
      $\mathbf{2^4}$ $\mathbf{2^5}$ $\mathbf{2^9}$
    - $\cancel{1}$ preimage of the partial target z is derived with a complexity of $\cancel{2^2}$
      $\mathbf{2^5}$ $\mathbf{2^5}$
      = 1 preimage of the partial target z is derived with a complexity of **1**
  - Condition for efficient collision attack: $s < t / 2$

    $t = 4$, $s = 0$ $\Rightarrow$ **better** than generic collision attack !

- **Extra freedom of neutral bits can be exploited!**

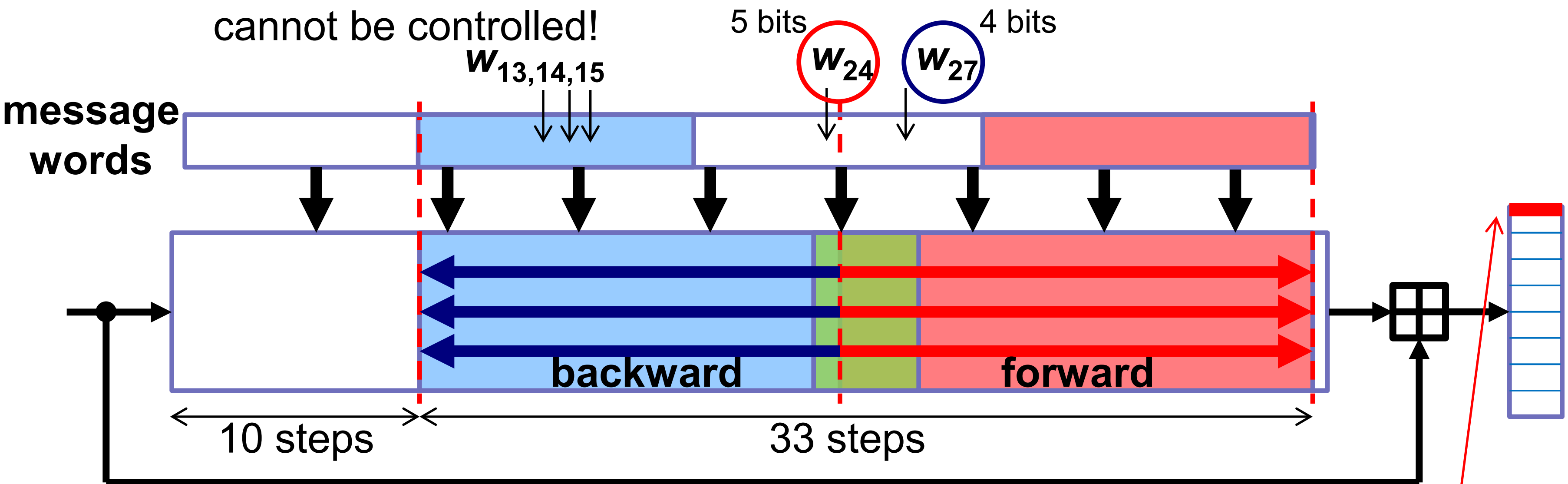
Applications

Conversion (6 steps moving forward)



- Preimage attack on 43-step reduced SHA-256 [AGMSW09]
  - Padding words $W_{13,14,15}$ can be controlled
- Neutral message words etc. are moved forward by 6 steps

Conversion (6 steps moving forward)



- Preimage attack on 43-step reduced SHA-256 [AGMSW09]
  - Padding words $W_{13,14,15}$ can be controlled
- Neutral message words etc. are moved forward by 6 steps
- Attack complexity
  - Neutral words: $|W_{24}| = 5$, $|W_{27}| = 4$, bit size of partial target $t = 4$
  - $s = 0$ (2^5 preimages of 4-bit target with complexity of 2^5)
  - Total complexity = 2^{126} (= $2^{(n-t)/2} \times 2^s = 2^{(256-4)/2} \times 2^0$)

More results on SHA-2

- MITM preimage attack on 46-step SHA-512 [AGMSW09]
  - Pseudo collision attack on 46-step SHA-512
- Pseudo collision attacks on SHA-224/384
  - Due to wide-pipe construction, other MITM preimage attacks are required to reduce the total time complexity
  - SHA-224: 40-step pseudo collision attack
  - SHA-384: 40-step pseudo collision attack
- Preimage attacks using bicliques [KRS12]

Preimage attacks on		**Pseudo collision attacks on**
45-step SHA-256 HF	→	45-step SHA-256 HF
50-step SHA-512 HF	→	50-step SHA-512 HF
52-step SHA-256 CF	→	52-step SHA-256 **HF**
57-step SHA-512 CF	→	57-step SHA-512 **HF**

HF: hash function
CF: compression function

Application to Skein and BLAKE

Skein-512

MITM preimage attacks [KRS12]

target	complexity
22-round HF	2^{508}
37-round CF	$2^{511.2}$

Pseudo collision attack

target	complexity
22-round HF	$2^{253.8}$
37-round **HF**	$2^{255.7}$

BLAKE-256 w/o initialization

MITM preimage attacks [WOS09]

target	complexity
4-round CF	2^{224}

Pseudo collision attack

target	complexity
4-round CF	2^{112}

[KRS12] D.Khovratovich, C.Rechberger, A.Savelieva, “Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family”, FSE2012

[WOS09] L.Wang, K.Ohta, K.Sakiyama, “Free-start preimages of round-reduced Blake compression function”, Rump session at ASIACRYPT2009.

Advantages and limitations

- **Advantages**
  - Compared to previous collision attack based on differentials: significantly improve the number of attacked steps/rounds
  - Compared to MITM preimage attack:
    more steps/rounds may be attacked due to relaxed conditions for selecting neutral words (i.e., do not need to care about padding bits)
- **Limitations**
  - Time complexity is likely to be high due to a few gains from MITM
    - e.g.) complexity of pseudo collision attacks on reduced SHA-2 is much larger than previous (pseudo) collision attacks based on differential attacks
  - Hard to extend to collision attack (only a pseudo collision attack)

Conclusion

- **Proposed generic conversion of MITM preimage attack to pseudo collision attack**
- **Applications to SHA-2, Skein, BLAKE**
  - Pseudo collision attacks on
    52-step SHA-256 hash function,
    57-step SHA-512 hash function,
    37-round Skein-512 hash function,
    4-round BLAKE-256 w/o initialization
- **Maybe possible to apply our technique to other hash functions such as Tiger**

Thank you for your attention!