Institute for Infocomm Research

SKLOIS
信息安全国家重点实验室

(Pseudo) Preimage Attack on Reduced-Round Grøstl Hash Function and Others

Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong, Jian Zou

March 20, 2012

中国科学院软件研究所
Institute of Software, Chinese Academy of Sciences

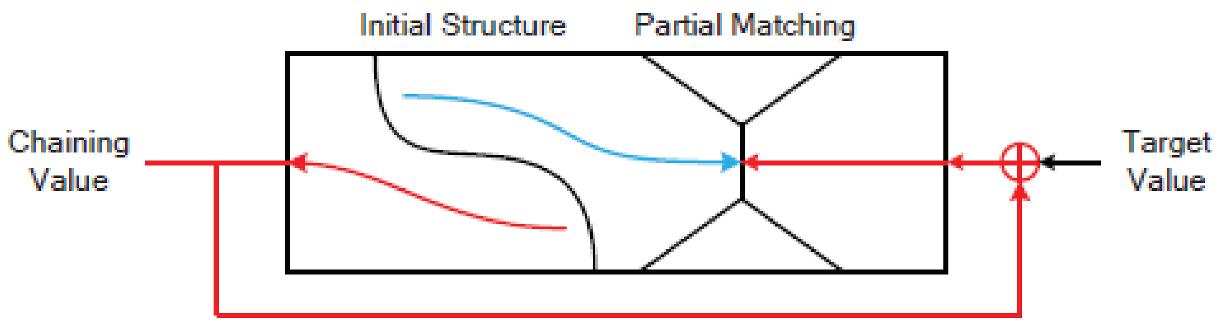
Institute for Infocomm Research, Singapore

Outline

- Introduction
- Attack on Grøstl
- Other results
- Conclusion

Introduction

- Meet-in-the-Middle pre-image attacks
  - Applied to full MD4, MD5,HAVAL-3/4,Tiger and reduced-round HAS-160, RIPEMD, SHA-0/1, SHA-2 etc.
  - Tricks:
    - Splice and Cut Techniques
    - Bicliques, Initial Structure (Message Stealing), local collision
    - Partial-Matching (Relations between deterministic values)



Introduction

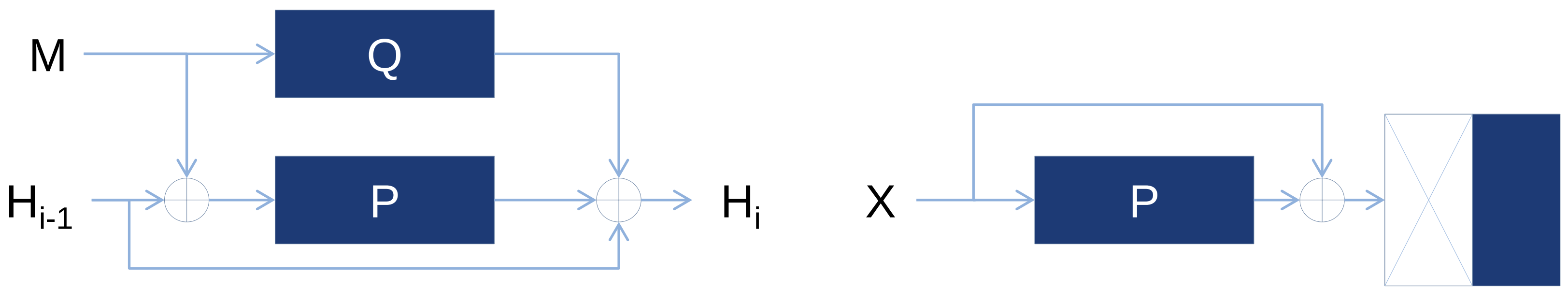
- Meet-in-the-Middle pre-image attacks
  - Yu Sasaki proposed the MitM preimage attack on AES-like structures for the first time at FSE 2011
    - Target: Whirlpool and AES hash modes
  - Use freedom degrees of the state for chunk separation

Outline

- Introduction
- Attack on Grøstl
- Other results
- Conclusion

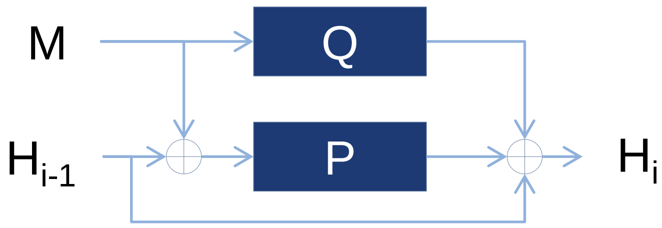
Pseudo-Preimage Attack on 5-round Grøstl-256

- Specification of Grøstl hash function
  - Wide-pipe MD structure with output transformation
  - Permutations P and Q are AES-like structures with 8×8 states(Grøstl-256) and 8×16 states(Grøstl-512)
    - 10 rounds for Grøstl-256 and 14 rounds for Grøstl-512



Pseudo-Preimage Attack on 5-round Grøstl-256

- Properties of the compression function
  - 2n-bit state, $F(H,M) = P(H \oplus M) \oplus Q(M) \oplus H$
    - With $H' = H \oplus M$, $F(H',M) = P(H') \oplus H' \oplus Q(M) \oplus M$
  - Bounds for generic attacks
    - Pre-image attack: 2^n
      - $P(H') \oplus H' \oplus Q(M) \oplus M = T$
      - birthday attack on 2n-bit state
    - Collision attack: $2^{\frac{2n}{3}}$
      - $P(H_1') \oplus H_1' \oplus Q(M_1) \oplus M_1 \oplus P(H_2') \oplus H_2' \oplus Q(M_2) \oplus M_2 = 0$
      - generalized birthday attack on 2n-bit state with four entries

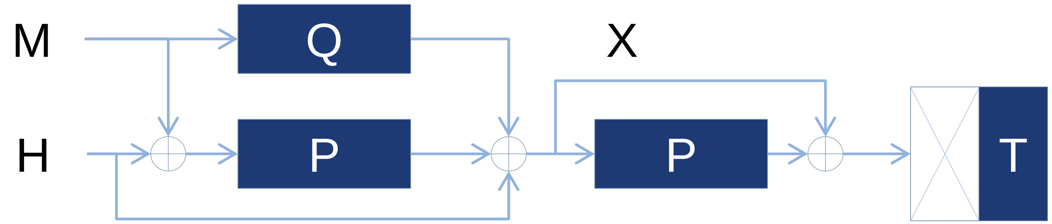


Outline of the attack

Pseudo-Preimage Attack on 5-round Grøstl-256

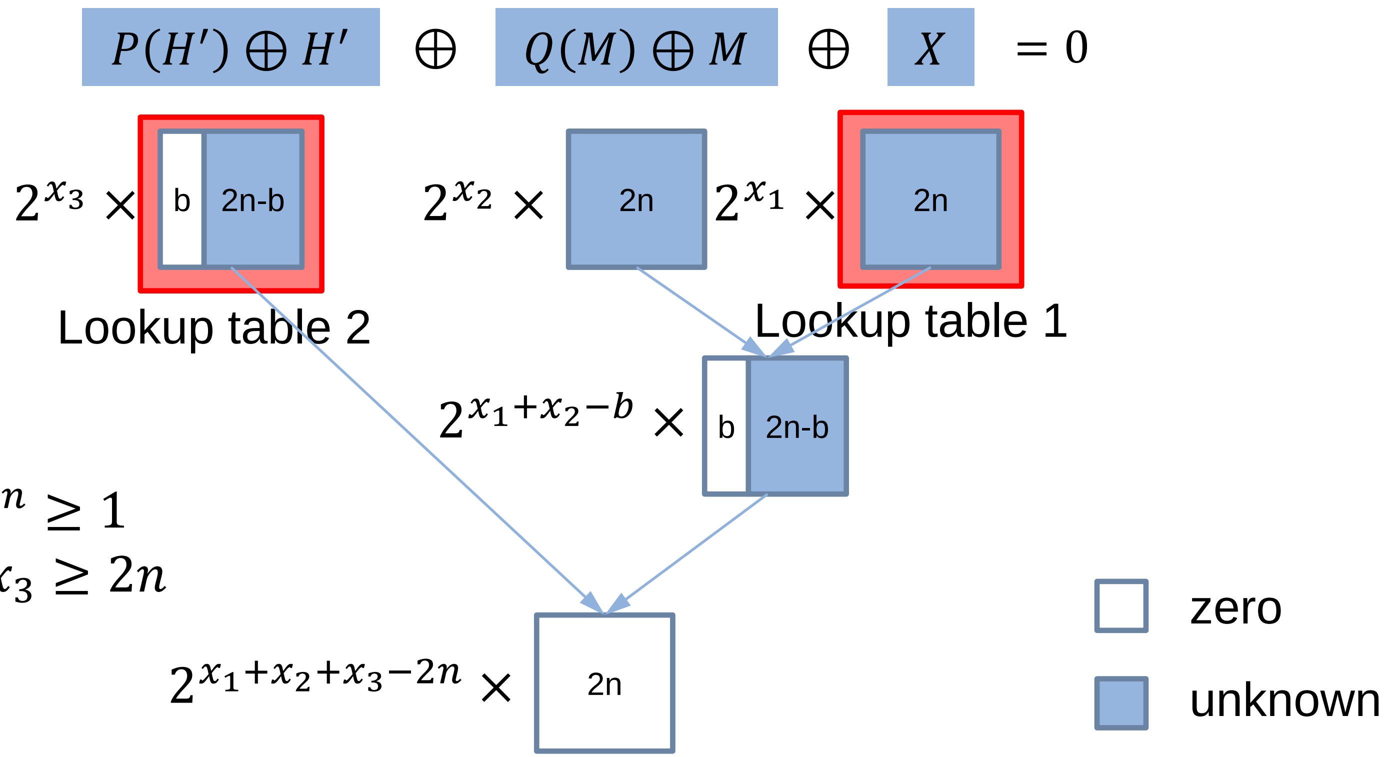
- Attack outline
  - Pseudo pre-image (H,M)
    - $F(H,M) = X, P(X) \oplus X =* ||T$
    - X is a pre-image of the output transformation
  - With $H' = H \oplus M$,

$$P(H') \oplus H' \oplus Q(M) \oplus M \oplus X = 0$$



Pseudo-Preimage Attack on 5-round Grøstl-256

- How to convert the partial pre-images of $P(X) \oplus X$ into pseudo pre-image of the hash function



$$2^{x_1+x_2+x_3-2n} \geq 1$$
$$\Rightarrow x_1 + x_2 + x_3 \geq 2n$$

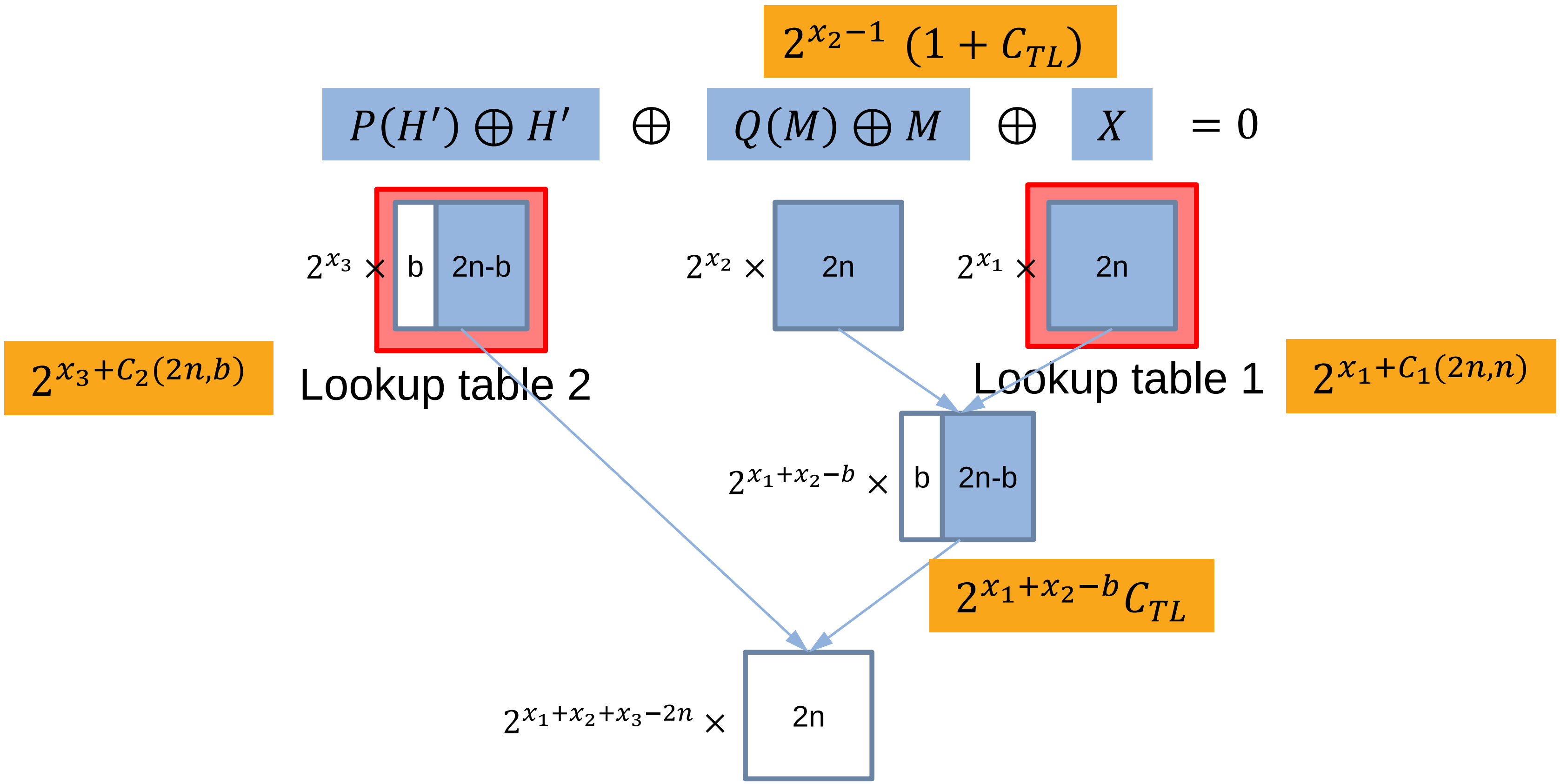
Pseudo-Preimage Attack on 5-round Grøstl-256

- Complexity evaluation
  - X: Fixed position partial preimage (n-bit) of $P(X) \oplus X$
    - Let complexity to find one X be $2^{C_1(2n,n)}$
  - M: Randomly chosen message with padding
    - Complexity=one Q call=1/2 compression function call
  - H': Chosen position partial preimage (b-bit) of $P(H') \oplus H'$
    - Let complexity to find one H' be $2^{C_2(2n,b)}$

Pseudo-Preimage Attack on 5-round Grøstl-256

- Overall complexity of the attack is

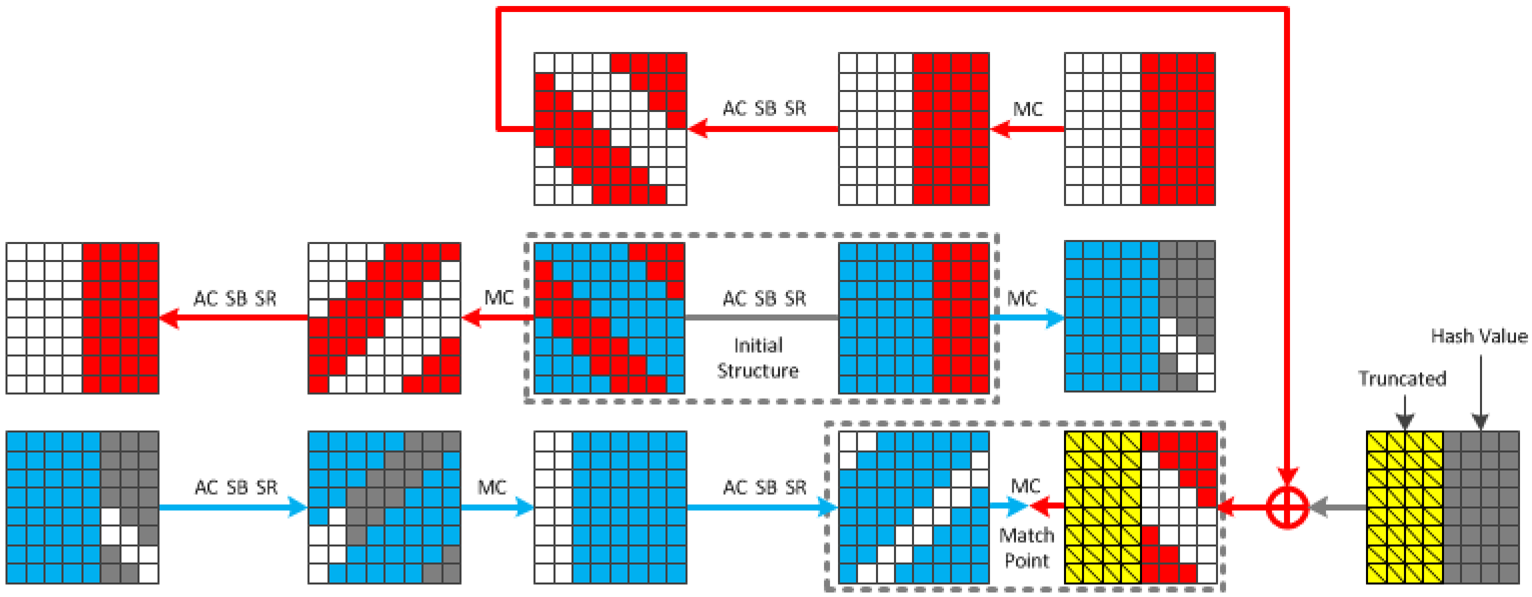
$$2^{x_1+C_1(2n,n)} + 2^{x_3+C_2(2n,b)} + 2^{x_2-1} + 2^{x_1+x_2-b}C_{TL}$$



Partial preimage attacks on $P(X) \oplus X$

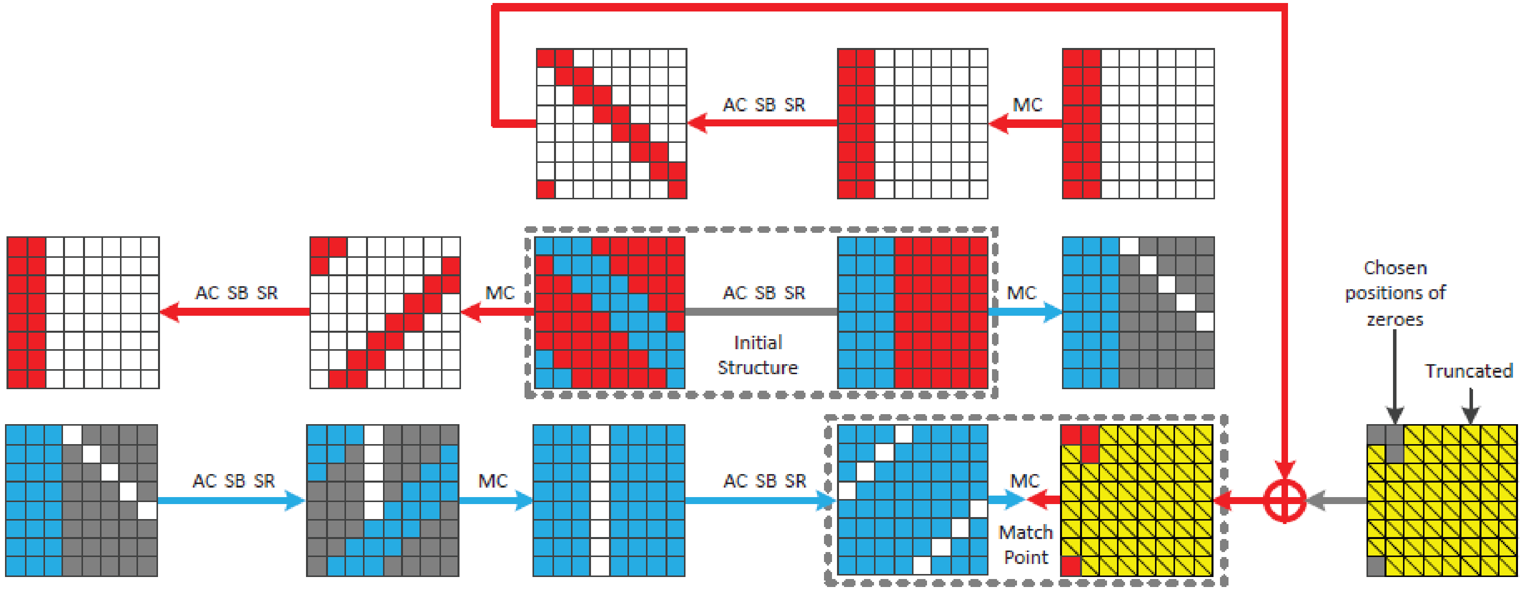
Pseudo-Preimage Attack on 5-round Grøstl-256

- Evaluation of $C_1(2n, n)$ (fixed position partial preimage)
  - Freedom degrees in blue and red bytes: 64 and 48 bits
  - Size of the matching point: 64 bits
  - Size of the full match: 256 bits
  - Complexity: 2^{207} P(X) calls = 2^{206} compression function calls



Pseudo-Preimage Attack on 5-round Grøstl-256

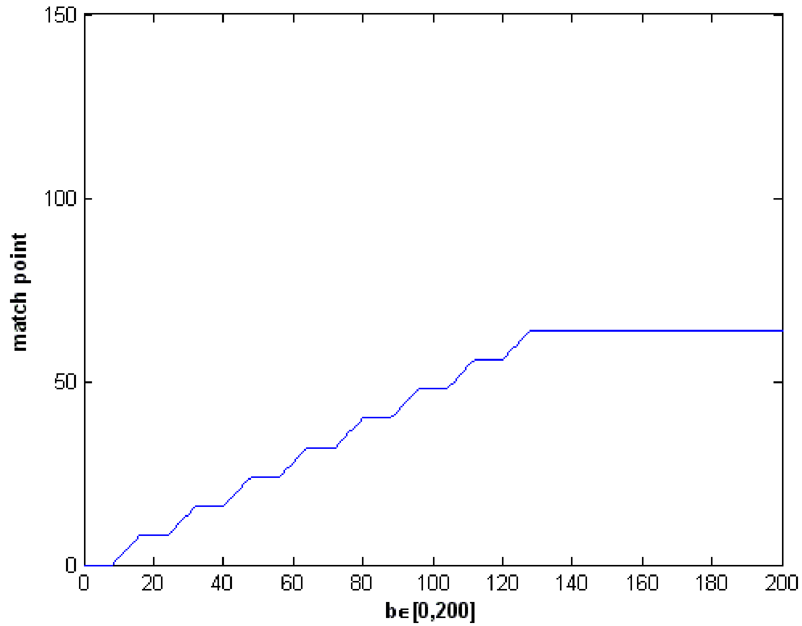
- Evaluation of $C_2(2n, b)$ (chosen position partial preimage)
  - Note: we can choose the positions of the target zero bits
  - Choose optimal positions to maximize the size of the matching point

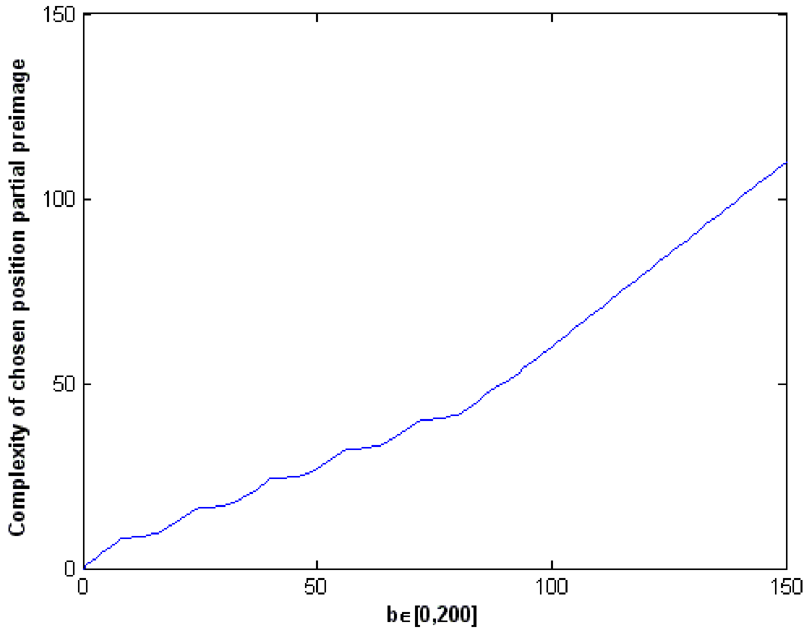


Pseudo-Preimage Attack on 5-round Grøstl-256

- Graphs of $m(b)$ and $C_2(2n, b)$ for different b

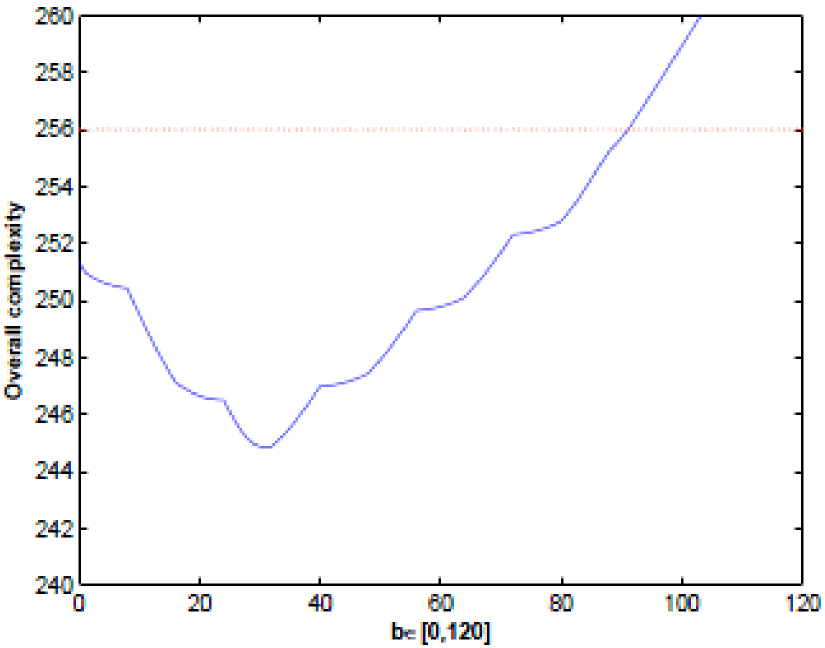
Grøstl-256





Pseudo-Preimage Attack on 5-round Grøstl-256

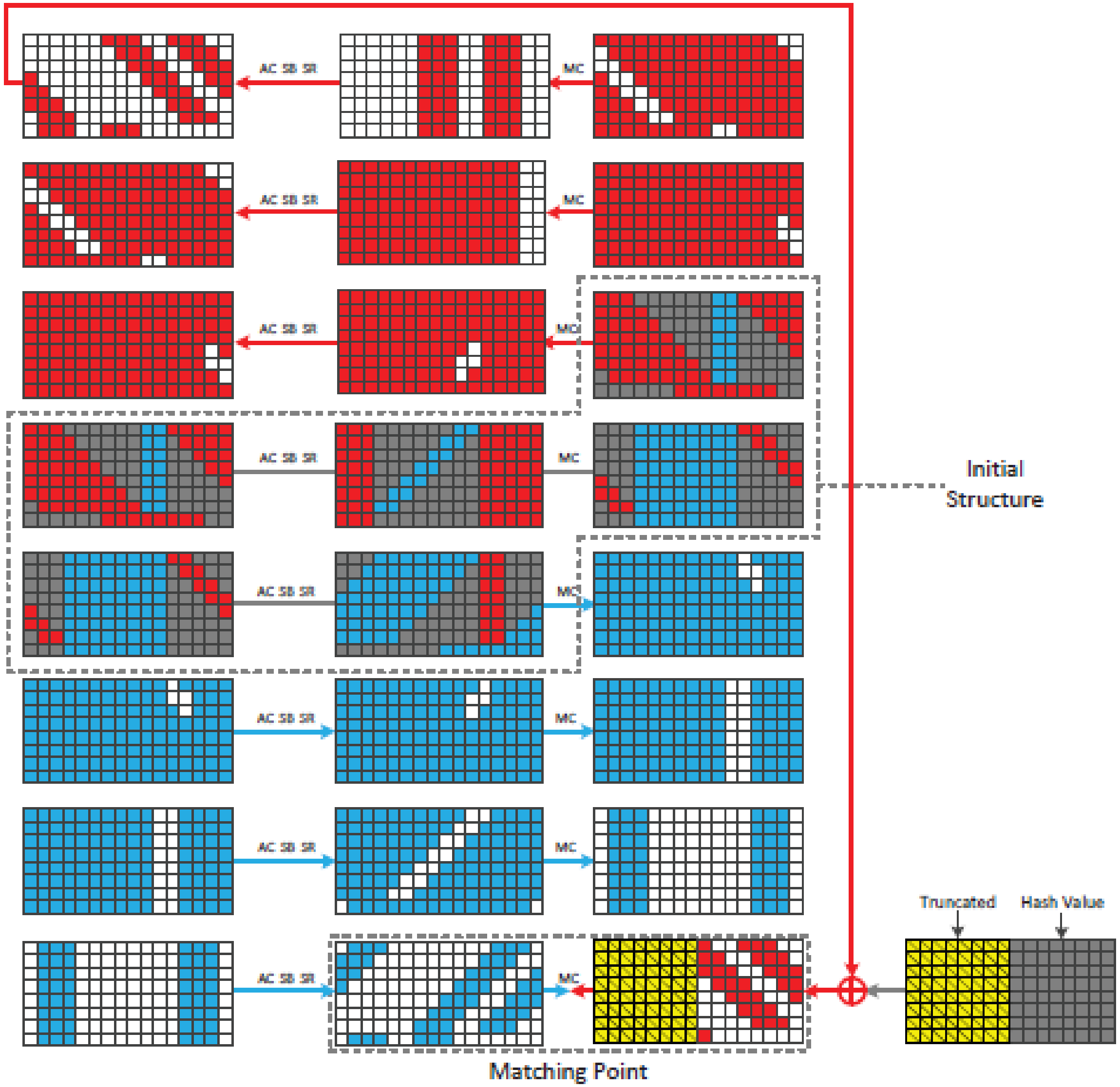
- Overall complexity of pseudo-preimage attack on 5-round Grøstl-256
  - When $b = 35$, the overall complexity reaches its minimum value $2^{244.85}$



Results on Grøstl-512

Pseudo-Preimage Attack on 8-round Grøstl-512

- Preimage attack on the output transformation



Summary of results

Algorithm	Target	Type	Rounds	Time	Memory	Source
Grøstl-256	Hash Function	Collision	3	2^{64}	-	Martin Schlæffer
	Compression Function	Semi-Free-Start Collision	6	2^{112}	2^{64}	Martin Schlæffer
	Permutation	Distinguisher	9	2^{368}	2^{64}	Jérémy Jean et al.
	Permutation	Zero-Sum Distinguisher	10	2^{509}	-	Christina Boura et al.
	Output Transformation	Preimage	5	2^{206}	2^{48}	Ours
	Hash Function	Pseudo Preimage	5	$2^{244.85}$	$2^{230.13}$	Ours
Grøstl-512	Hash Function	Collision	3	2^{192}	-	Martin Schlæffer
	Compression Function	Semi-Free-Start Collision	7	2^{152}	2^{56}	Yu Sasaki
	Permutation	Distinguisher	10	2^{392}	2^{64}	Jérémy Jean et al.
	Output Transformation	Preimage	8	2^{495}	2^{16}	Ours
	Hash Function	Pseudo Preimage	8	$2^{507.32}$	$2^{507.00}$	Ours

Outline

- Introduction
- Attack on Grøstl
- Other results
- Conclusion

Other results in this paper

Algorithm	Target	Type	Rounds	Time	Memory	Source
Whirlpool	Hash Function	2nd Preimage	5	2^{504}	2^{8}	Yu Sasaki
	Hash Function	2nd Preimage	5	2^{448}	2^{64}	Ours
	Hash Function	Preimage	5	$2^{481.5}$	2^{64}	Ours

Algorithm	Hash Mode	Type	Rounds	Time	Memory	Message Length	Source
AES	MMO,MP	2nd Preimage	7	2^{120}	2^{8}	-	Yu Sasaki
	MMO,MP,DM	2nd Preimage	7	2^{128-k}	2^{k}	2^{k} blocks	John Kelsey et at.
	MMO,MP,DM	2nd Preimage	7	$2^{120-\min(k,24)}$	2^{16}	2^{k} blocks	Ours
	DM	Preimage	7	2^{125}	2^{8}	-	Yu Sasaki
	DM	Preimage	7	$2^{122.7}$	2^{16}	$>2^{8}$ blocks	Ours

New Related Result Announcement

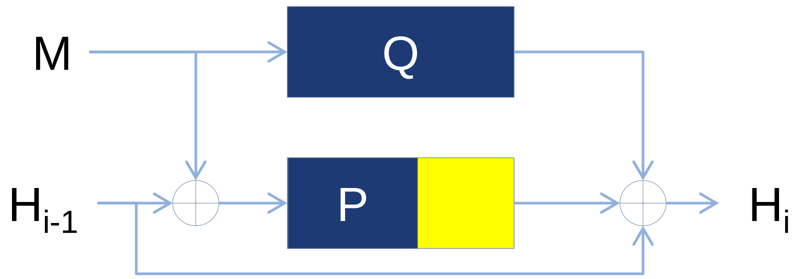
- Converting partial pre-images into pseudo collisions
  - The technique is proposed by Ji Li et al.
  - Target: 8-round Grøstl-512 output transformation
  - The complexity is 2^{248}

Outline

- Introduction
- Attack on Grøstl
- Other results
- Conclusion

Conclusion

- We proposed:
  - Pseudo preimage attack on 5-round Grøstl-256 and 8-round Grøstl-512 for the first time
    - We found that partial preimage attack on $P(X) \oplus X$ (n-bit size) can be converted in to pseudo preimage attack on the hash function
    - An interesting observation: Properties of the permutation Q are not concerned in this attack, i.e. this attack works with any Q.
      - So, our attack works on Grøstl-256 with 5-round P and full 10-round Q and Grøstl-512 with 8-round P and full 14-round Q.



Thank you!

Any questions?