

Preimages for Step-Reduced SHA-2

Jian Guo¹ and Krystian Matusiewicz²

Nanyang Technological University, Singapore

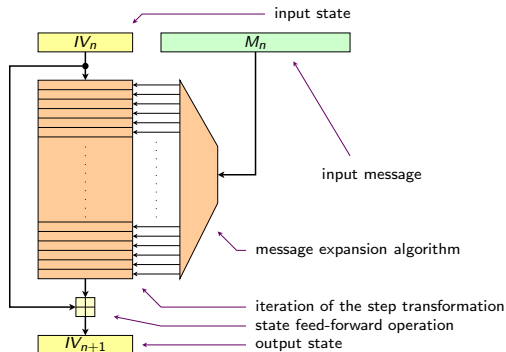
Technical University of Denmark

29 May 2009

Table of contents

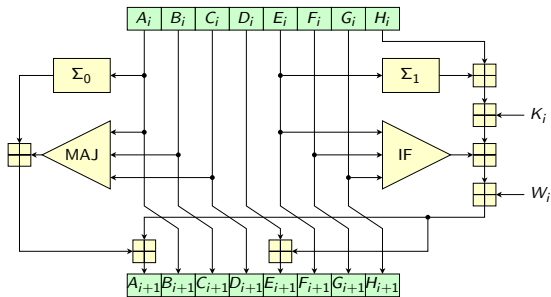
- 1 Description of SHA-2
 - General View
 - Step Function
 - Message Expansion
- 2 Description of Preimage Attack
- 3 Application to SHA-2
 - Overview
 - Message Stealing
 - Message Compensation
 - Extended Partial Matching
- 4 Conclusions

SHA-2 in General



- Step Function: update internal chaining
- Message Expansion: expand 16 message words to 64/80

SHA-2 Step Function



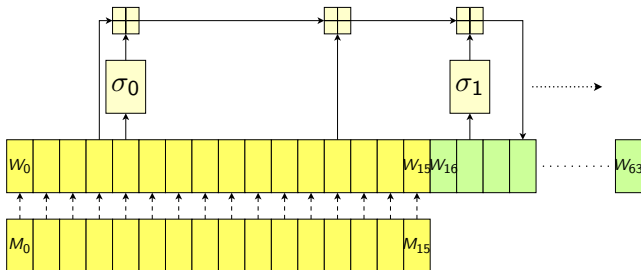
$$\text{MAJ}(A, B, C) = (A \wedge B) \vee (A \wedge C) \vee (B \wedge C) ,$$

$$\text{IF}(E, F, G) = (E \wedge F) \vee (\neg E \wedge G) ,$$

$$\Sigma_0(x) = (x \ggg 2) \oplus (x \ggg 13) \oplus (x \ggg 22) ,$$

$$\Sigma_1(x) = (x \ggg 6) \oplus (x \ggg 11) \oplus (x \ggg 25) .$$

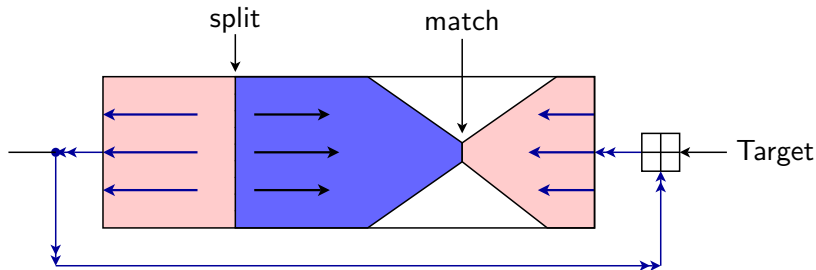
SHA-2 Message Expansion



$$W_i = \begin{cases} M_i & \text{for } 0 \leq i < 16, \\ \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15}) + W_{i-16} & \text{for } 16 \leq i < 64. \end{cases}$$

Note: any consecutive 16 determine all message words.

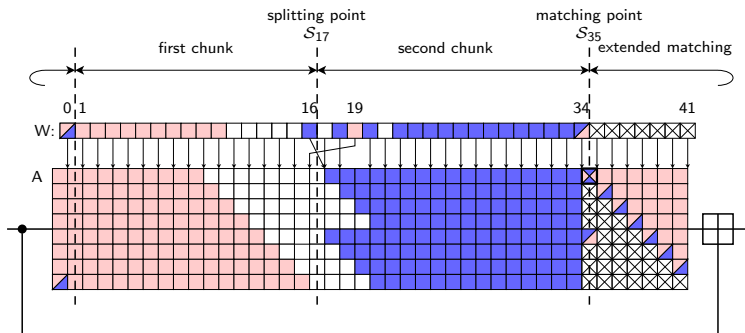
Preimage Attack - in general



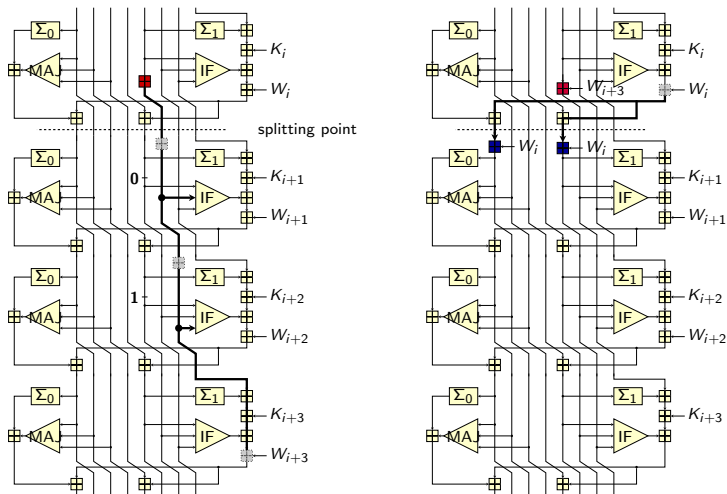
Find pseudo-preimage in 2^l , then preimage in $2^{\frac{n+l}{2}+1}$

Result on SHA-2

- W_{11}, \dots, W_{26} as a basis to generate all message words.
- Neutral words: W_{16} and W_{19}

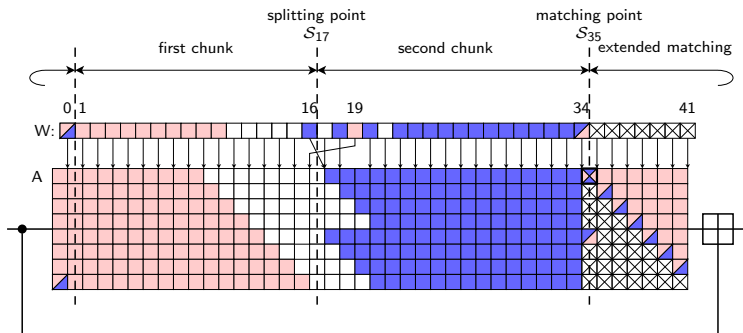


Message Stealing



Result on SHA-2

- W_{11}, \dots, W_{26} as a basis to generate all message words.
- Neutral words: W_{16} and W_{19}



Message Compensation - First Chunk

$$\begin{aligned}W_{10} &= W_{26} - \sigma_1(W_{24}) - W_{19} - \sigma_0(W_{11}) , \\W_9 &= W_{25} - \sigma_1(W_{23}) - W_{18} - \sigma_0(W_{10}) , \\W_8 &= W_{24} - \sigma_1(W_{22}) - W_{17} - \sigma_0(W_9) , \\W_7 &= W_{23} - \sigma_1(W_{21}) - W_{16} - \sigma_0(W_8) , \\W_6 &= W_{22} - \sigma_1(W_{20}) - W_{15} - \sigma_0(W_7) , \\W_5 &= W_{21} - \sigma_1(W_{19}) - W_{14} - \sigma_0(W_6) , \\W_4 &= W_{20} - \sigma_1(W_{18}) - W_{13} - \sigma_0(W_5) , \\W_3 &= W_{19} - \sigma_1(W_{17}) - W_{12} - \sigma_0(W_4) , \\W_2 &= W_{18} - \sigma_1(W_{16}) - W_{11} - \sigma_0(W_3) , \\W_1 &= W_{17} - \sigma_1(W_{15}) - W_{10} - \sigma_0(W_2) , \\W_0 &= W_{16} - \sigma_1(W_{14}) - W_9 - \sigma_0(W_1) .\end{aligned}$$

Message Compensation - First Chunk

$$\begin{aligned}W_{10} &= W_{26} - \sigma_1(W_{24}) - W_{19} - \sigma_0(W_{11}) , \\W_9 &= W_{25} - \sigma_1(W_{23}) - W_{18} - \sigma_0(W_{10}) , \\W_8 &= W_{24} - \sigma_1(W_{22}) - W_{17} - \sigma_0(W_9) , \\W_7 &= W_{23} - \sigma_1(W_{21}) - W_{16} - \sigma_0(W_8) , \\W_6 &= W_{22} - \sigma_1(W_{20}) - W_{15} - \sigma_0(W_7) , \\W_5 &= W_{21} - \sigma_1(W_{19}) - W_{14} - \sigma_0(W_6) , \\W_4 &= W_{20} - \sigma_1(W_{18}) - W_{13} - \sigma_0(W_5) , \\W_3 &= W_{19} - \sigma_1(W_{17}) - W_{12} - \sigma_0(W_4) , \\W_2 &= W_{18} - \sigma_1(W_{16}) - W_{11} - \sigma_0(W_3) , \\W_1 &= W_{17} - \sigma_1(W_{15}) - W_{10} - \sigma_0(W_2) , \\W_0 &= W_{16} - \sigma_1(W_{14}) - W_9 - \sigma_0(W_1) .\end{aligned}$$

Message Compensation - First Chunk

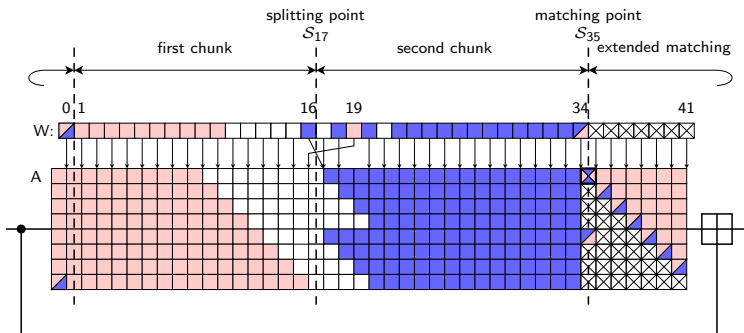
$$\begin{aligned}W_{10} &= W_{26} - \sigma_1(W_{24}) - W_{19} - \sigma_0(W_{11}) , \\W_9 &= W_{25} - \sigma_1(W_{23}) - W_{18} - \sigma_0(W_{10}) , \\W_8 &= W_{24} - \sigma_1(W_{22}) - W_{17} - \sigma_0(W_9) , \\W_7 &= W_{23} - \sigma_1(W_{21}) - W_{16} - \sigma_0(W_8) , \\W_6 &= W_{22} - \sigma_1(W_{20}) - W_{15} - \sigma_0(W_7) , \\W_5 &= W_{21} - \sigma_1(W_{19}) - W_{14} - \sigma_0(W_6) , \\W_4 &= W_{20} - \sigma_1(W_{18}) - W_{13} - \sigma_0(W_5) , \\W_3 &= W_{19} - \sigma_1(W_{17}) - W_{12} - \sigma_0(W_4) , \\W_2 &= W_{18} - \sigma_1(W_{16}) - W_{11} - \sigma_0(W_3) , \\W_1 &= W_{17} - \sigma_1(W_{15}) - W_{10} - \sigma_0(W_2) , \\W_0 &= W_{16} - \sigma_1(W_{14}) - W_9 - \sigma_0(W_1) .\end{aligned}$$

Message Compensation - First Chunk

$$\begin{aligned}
 W_{10} &= W_{26} - \sigma_1(W_{24}) - W_{19} - \sigma_0(W_{11}) , \\
 W_9 &= W_{25} - \sigma_1(W_{23}) - W_{18} - \sigma_0(W_{10}) , \\
 W_8 &= W_{24} - \sigma_1(W_{22}) - W_{17} - \sigma_0(W_9) , \\
 W_7 &= W_{23} - \sigma_1(W_{21}) - W_{16} - \sigma_0(W_8) , \\
 W_6 &= W_{22} - \sigma_1(W_{20}) - W_{15} - \sigma_0(W_7) , \\
 W_5 &= W_{21} - \sigma_1(W_{19}) - W_{14} - \sigma_0(W_6) , \\
 W_4 &= W_{20} - \sigma_1(W_{18}) - W_{13} - \sigma_0(W_5) , \\
 W_3 &= W_{19} - \sigma_1(W_{17}) - W_{12} - \sigma_0(W_4) , \\
 W_2 &= W_{18} - \sigma_1(W_{16}) - W_{11} - \sigma_0(W_3) , \\
 W_1 &= W_{17} - \sigma_1(W_{15}) - W_{10} - \sigma_0(W_2) , \\
 W_0 &= W_{16} - \sigma_1(W_{14}) - W_9 - \sigma_0(W_1) .
 \end{aligned}$$

Result on SHA-2

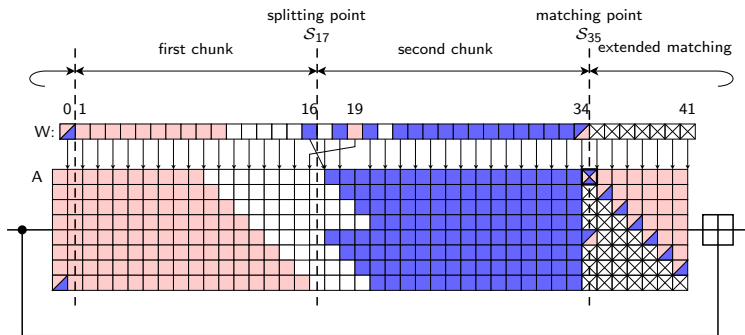
- W_{11}, \dots, W_{26} as a basis to generate all message words.
- Neutral words: W_{16} and W_{19}



Message Compensation - Second Chunk

$$\begin{aligned}W_{27} &= \sigma_1(W_{25}) + W_{20} + \sigma_0(W_{12}) + W_{11} , \\W_{28} &= \sigma_1(W_{26}) + W_{21} + \sigma_0(W_{13}) + W_{12} , \\W_{29} &= \sigma_1(W_{27}) + W_{22} + \sigma_0(W_{14}) + W_{13} , \\W_{30} &= \sigma_1(W_{28}) + W_{23} + \sigma_0(W_{15}) + W_{14} , \\W_{31} &= \sigma_1(W_{29}) + W_{24} + \sigma_0(W_{16}) + W_{15} , \\W_{32} &= \sigma_1(W_{30}) + W_{25} + \sigma_0(W_{17}) + W_{16} , \\W_{33} &= \sigma_1(W_{31}) + W_{26} + \sigma_0(W_{18}) + W_{17} , \\W_{34} &= \sigma_1(W_{32}) + W_{27} + \sigma_0(W_{19}) + W_{18} .\end{aligned}$$

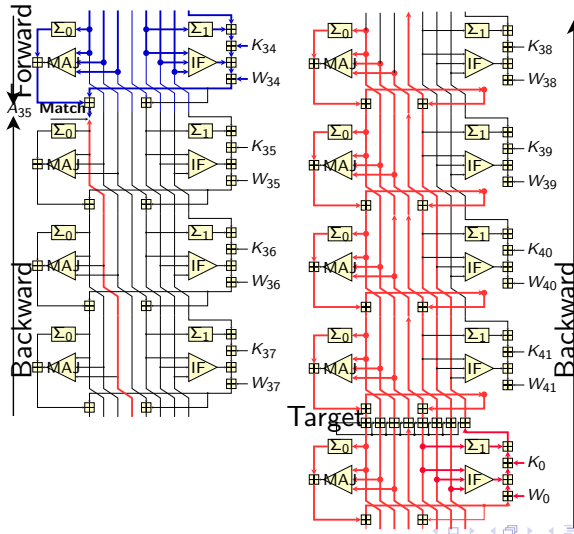
Result on SHA-2



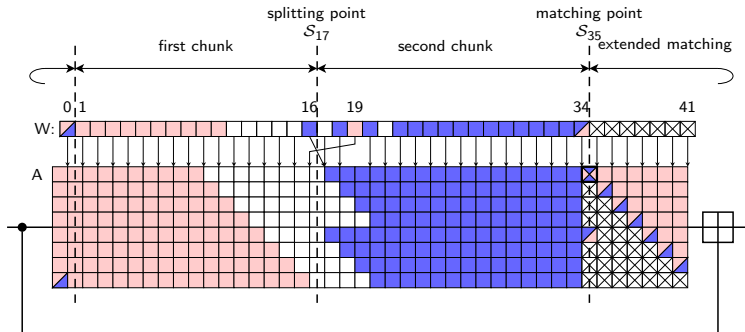
$$W_0 = W_{16} - \sigma_1(W_{14}) - W_9 - \sigma_0(W_1)$$

$$W_{34} = \sigma_1(W_{32}) + W_{27} + \sigma_0(W_{19}) + W_{18}$$

Extended Partial Matching



Result on SHA-2



Conclusions

- We find preimages for 42 out of 64 (66%) step-reduced SHA-256 with complexity 2^{252} and memory requirement of order 2^{12} bits
- The same attack applies to SHA-512 with complexity 2^{502} and memory requirement of order 2^{22}

END

THANK YOU!
QUESTIONS?