Preimages for Step-Reduced SHA-2

Kazumaro Aoki[1], Jian Guo[2], Krystian Matusiewicz[3], Yu Sasaki[1,4], and Lei Wang[4]

[1]NTT Corporation, Japan

[2]Nanyang Technological University, Singapore

[3]Technical University of Denmark, Denmark

[4]University of Electro-Communications, Japan

ASIACRYPT 2009, 10 Dec 2009

Talk Overview

1. Motivation

2. Description of SHA-2
   - General View
   - Message Expansion
   - Step Function

3. MITM Preimage Attacks on SHA-2
   - Message Compensation
   - Precomputated Initial Structure
   - (Indirect) Partial Matching
   - Partial Fixing

4. Conclusions

Motivation

- MD5, SHA-0 and SHA-1 are broken [Wang05]

Motivation

- MD5, SHA-0 and SHA-1 are broken [Wang05]
- SHA-3, wait until 2012?

Motivation

- MD5, SHA-0 and SHA-1 are broken [Wang05]
- SHA-3, wait until 2012?
- use **SHA-2** !

NIST’s Policy on Hash Functions

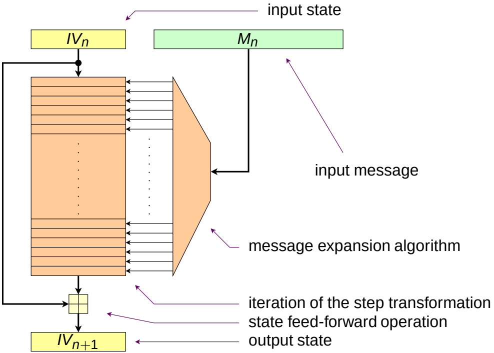
“*The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms. Federal agencies should **stop using SHA-1** for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and **must use the SHA-2** family of hash functions for these applications after 2010 ...*”

How much do we know about SHA-2 ?

- 24 steps collisions [FSE08, ACISP08,SAC08,...]
- 24 steps preimages [FSE09]

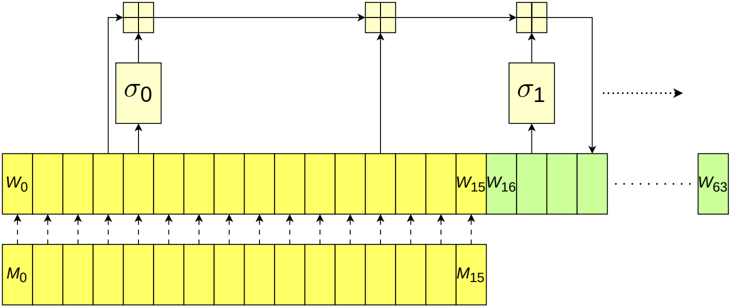
Full SHA-256 has 64 steps; SHA-512 has 80 steps.

SHA-2 Compression Function


input state
IV_n
M_n
input message
message expansion algorithm
iteration of the step transformation
state feed-forward operation
output state
IV_{n+1}

- Step Function: update internal chaining
- Message Expansion: expand 16 message words to 64 (SHA-256) or 80 (SHA-512)

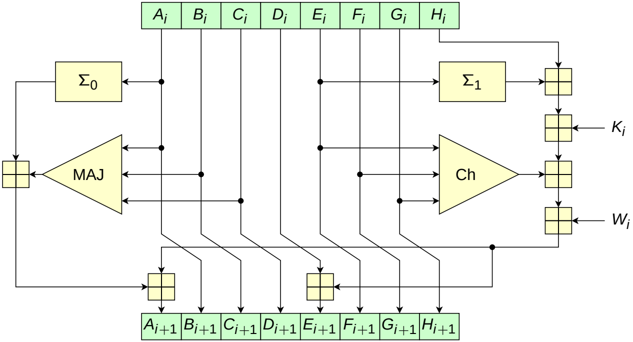
SHA-2 Message Expansion



$$W_i = \begin{cases} M_i & \text{for } 0 \le i < 16\,, \\ \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15}) + W_{i-16} & \text{for } 16 \le i < 64, 80\,. \end{cases}$$

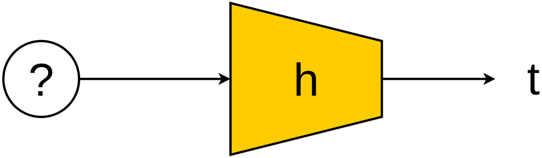
- Any consecutive 16 words determine all words.

SHA-2 Step Function



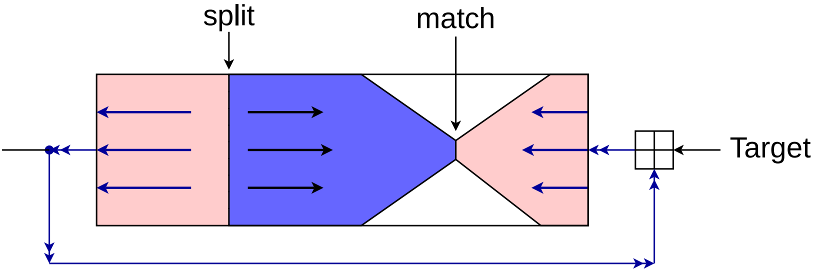
$$\begin{aligned}
\mathrm{MAJ}(A,B,C) &= (A \wedge B) \vee (A \wedge C) \vee (B \wedge C) \;, \\
\mathrm{Ch}(E,F,G) &= (E \wedge F) \vee (\neg E \wedge G) \;, \\
\Sigma_0(x) &= (x \ggg 2) \oplus (x \ggg 13) \oplus (x \ggg 22) \;, \\
\Sigma_1(x) &= (x \ggg 6) \oplus (x \ggg 11) \oplus (x \ggg 25) \;.
\end{aligned}$$

Preimage Attack – the Problem



Given the hash function h with n-bit hash digest and a target t, find a message m, such that $h(m) = t$, in less than 2^n computations

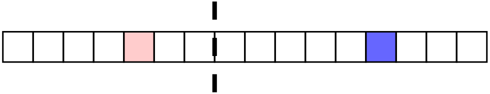
MITM Preimage Attack – in general



l bit neutral word, pseudo-preimage in 2^{n-l}, then preimage in $2^{n-l/2+1}$

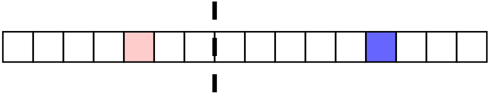
Attack Overview

Start with the simplest 16-step attack.



Attack Overview

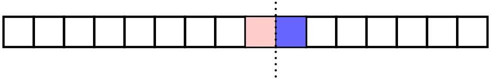
Start with the simplest 16-step attack.



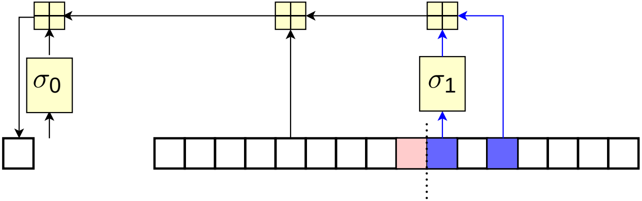
Extend number of steps attacked by:

- Message Compensation
- Precomputed Initial Structure
- Indirect Partial Matching
- Partial Fixing

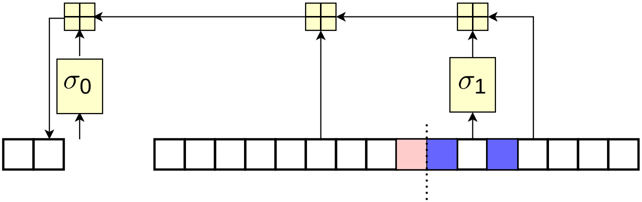
Message Compensation



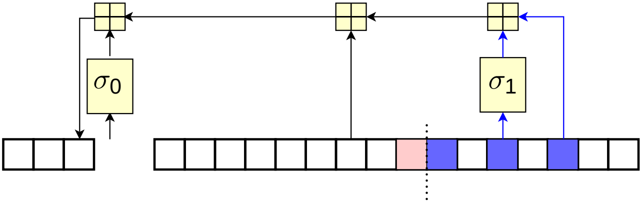
Message Compensation



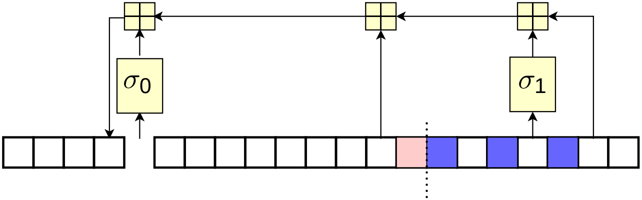
Message Compensation



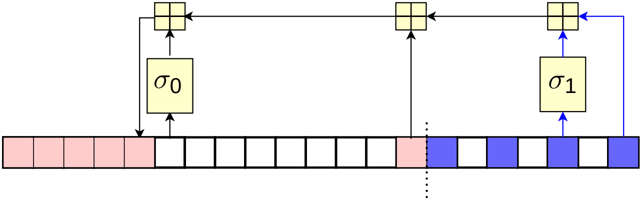
Message Compensation



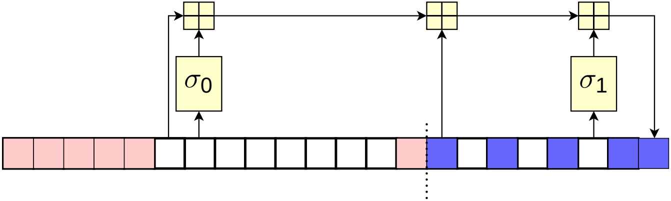
Message Compensation



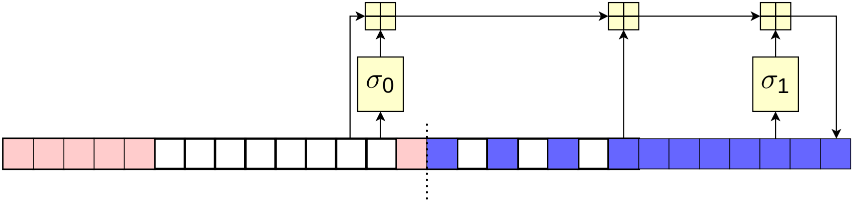
Message Compensation



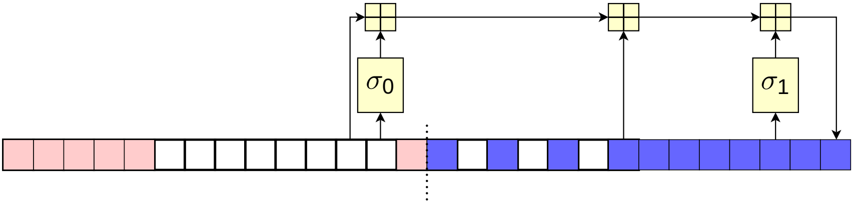
Message Compensation



Message Compensation

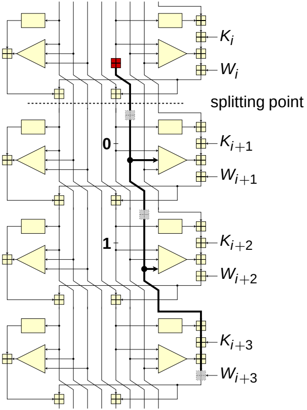


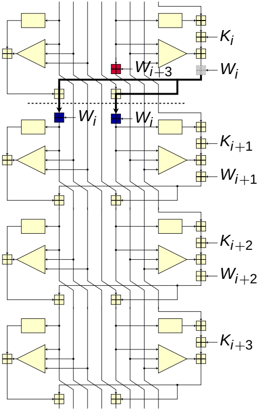
Message Compensation



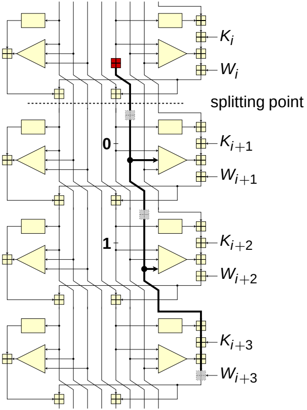
16 → 29 steps

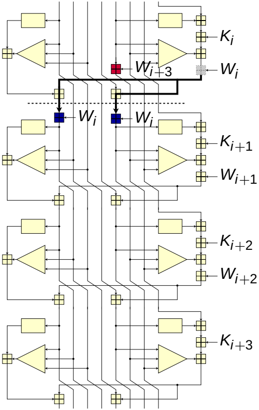
Precomputed Initial Structure





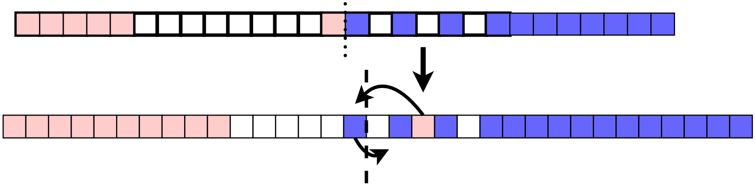
Precomputed Initial Structure





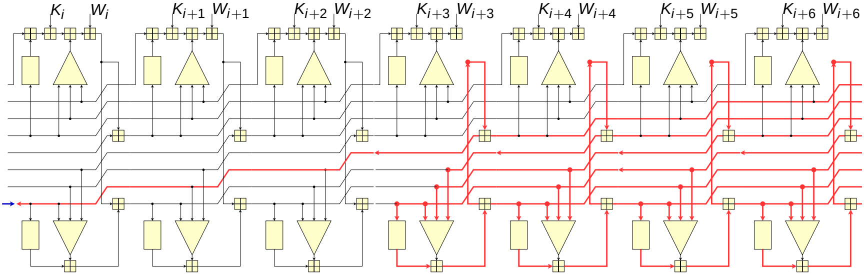
4 more steps

Precomputed Initial Structure – cont

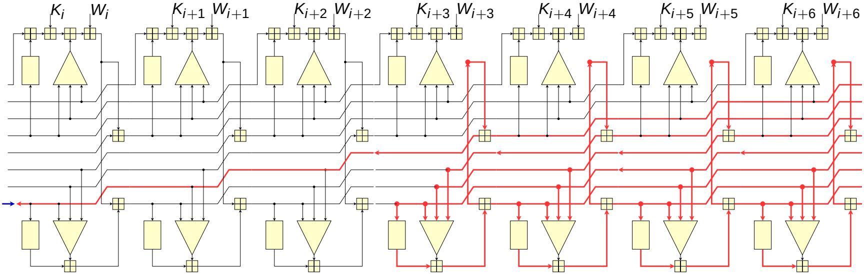


29 → 33 steps

Partial Matching

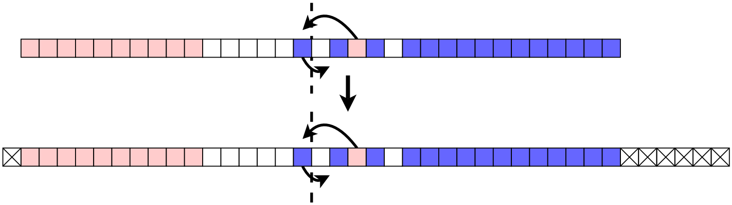


Partial Matching



7 more steps

Partial Matching – cont



33 → 40 steps

Indirect Partial Matching

Find values of x, y, s.t.

$$\alpha(x) + \beta(y) = \gamma(x) + \zeta(y)$$

Indirect Partial Matching

Find values of x, y, s.t.

$$\alpha(x) + \beta(y) = \gamma(x) + \zeta(y)$$

Instead, we do:

$$\alpha(x) - \gamma(x) = \zeta(y) - \beta(y)$$

and meet in the middle

Indirect Partial Matching

Find values of x, y, s.t.

$$\alpha(x) + \beta(y) = \gamma(x) + \zeta(y)$$

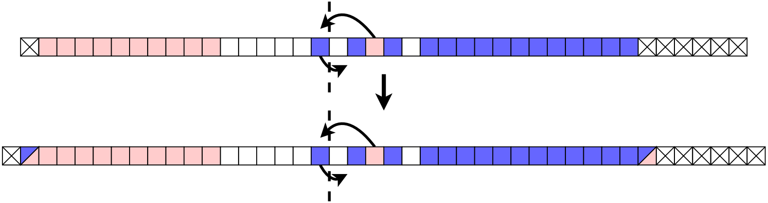
Instead, we do:

$$\alpha(x) - \gamma(x) = \zeta(y) - \beta(y)$$

and meet in the middle

2 more steps

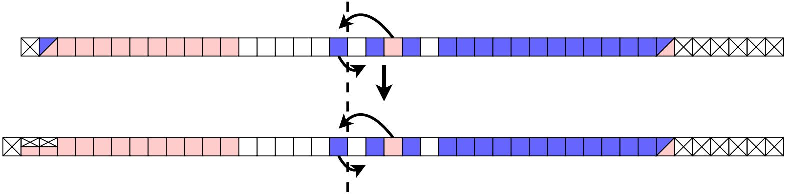
Indirect Partial Matching - cont



40 → 42 steps

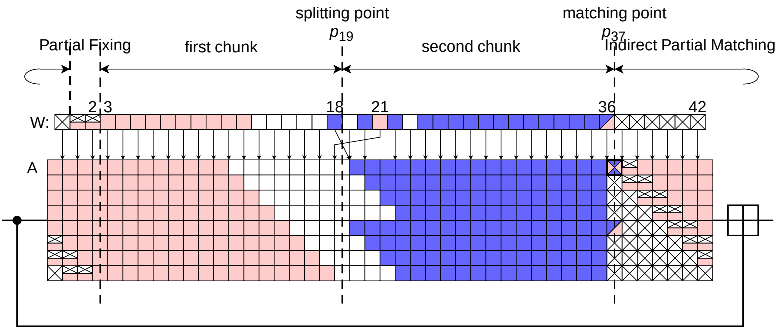
Partial Fixing

Fix few bits of the message word



42 → 43 steps

Full view of Result on SHA-256



Summary of Results

Hash	No. Steps	Mem	Comp.(PseudoPre)	Comp.(Pre)	Techniques
SHA-256	41	2^{32}	2^{224}	2^{241}	IS + IPM
	42	2^{12}	$2^{245.3}$	$2^{251.7}$	PIS + IPM
	43	2^{6}	$2^{251.9}$	$2^{254.9}$	PIS + IPM + PF
SHA-224	43	2^{6}	$2^{219.9}$	N.A.	PIS + IPM +PF
SHA-384	43	2^{19}	2^{386}	N.A.	PIS + IPM +PF
SHA-512	46	2^{6}	2^{509}	$2^{511.5}$	IS + PM + PF

- (P)IS: (Precomputed) Initial Structure
- (I)PM: (Indirect) Partial Matching
- PF: Partial Fixing

Note: Similar tradeoff between (No. Step) and Complexity applies to all other SHA-2 variants.

Q & A

Thank You!