Analysis of Step-Reduced SHA-256

Florian Mendel and Norbert Pramstaller and
Christian Rechberger and Vincent Rijmen

FSE 2006, Graz

Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

SHA-256 is Interesting and Challenging

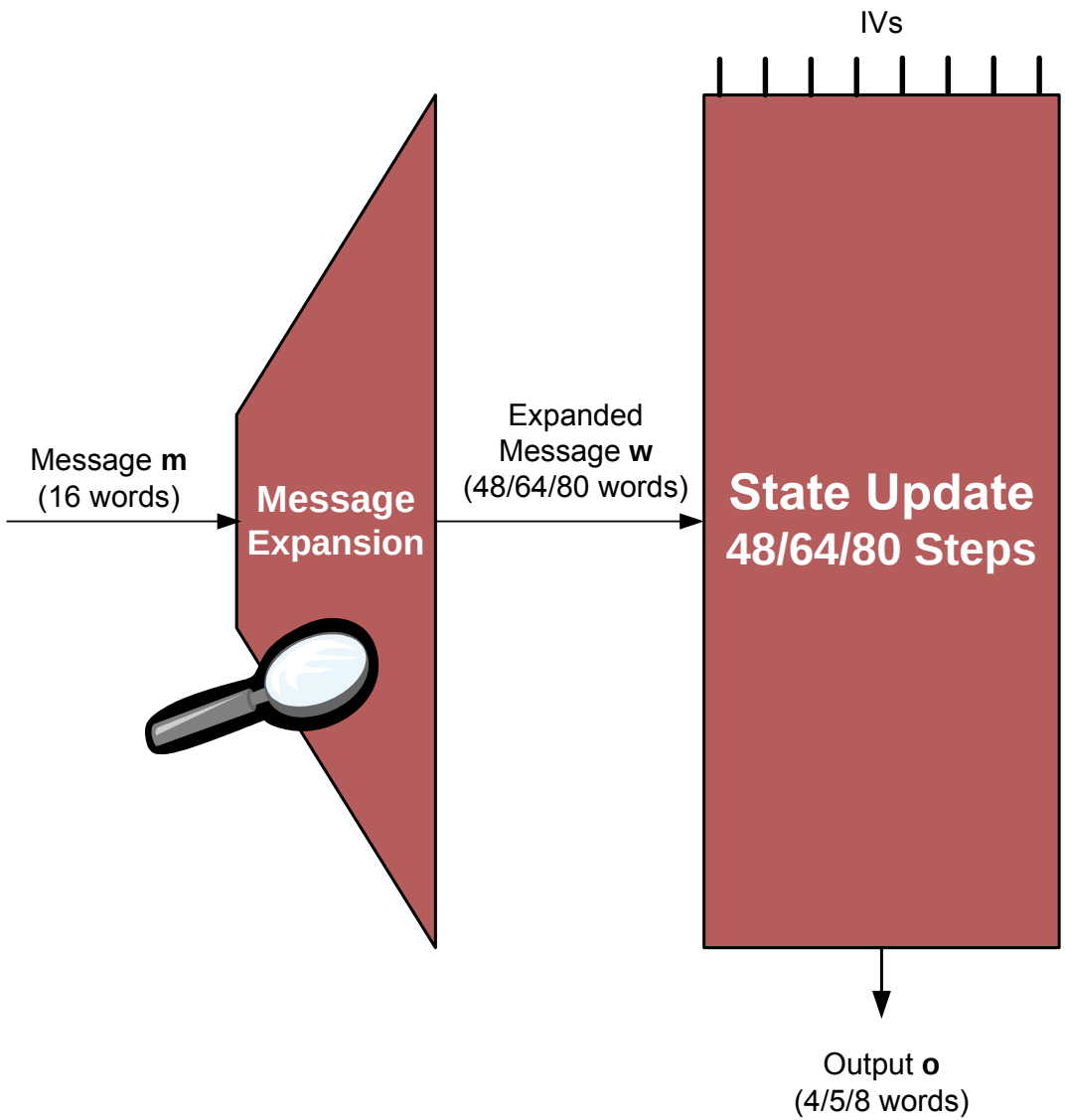
FIPS Standard since 2002

Option for a SHA-1 upgrade

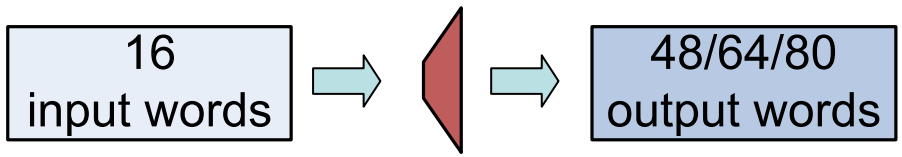
Prudent to know:

How hard is it to find collisions for SHA-256?
What about step-reduced variants (security margin)?

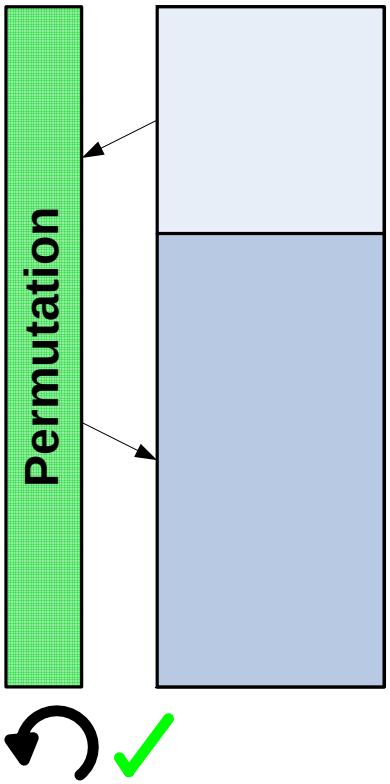
Outline of MD4-style Hash Functions



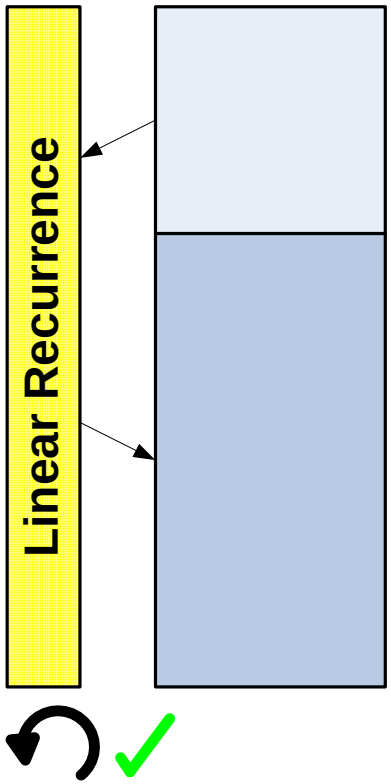
Message Expansions in the MD4 family



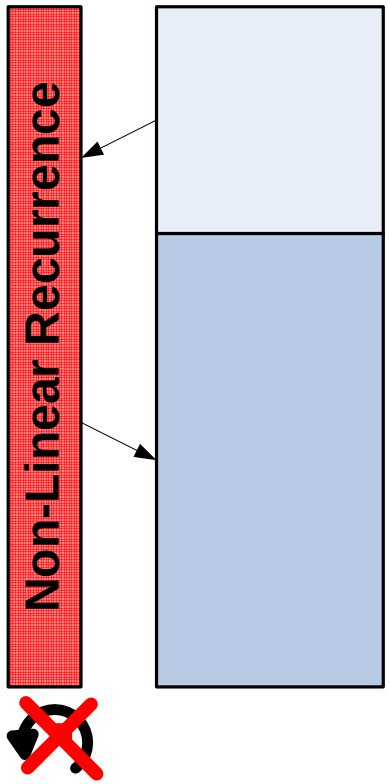
MD4/5, RIPEMD



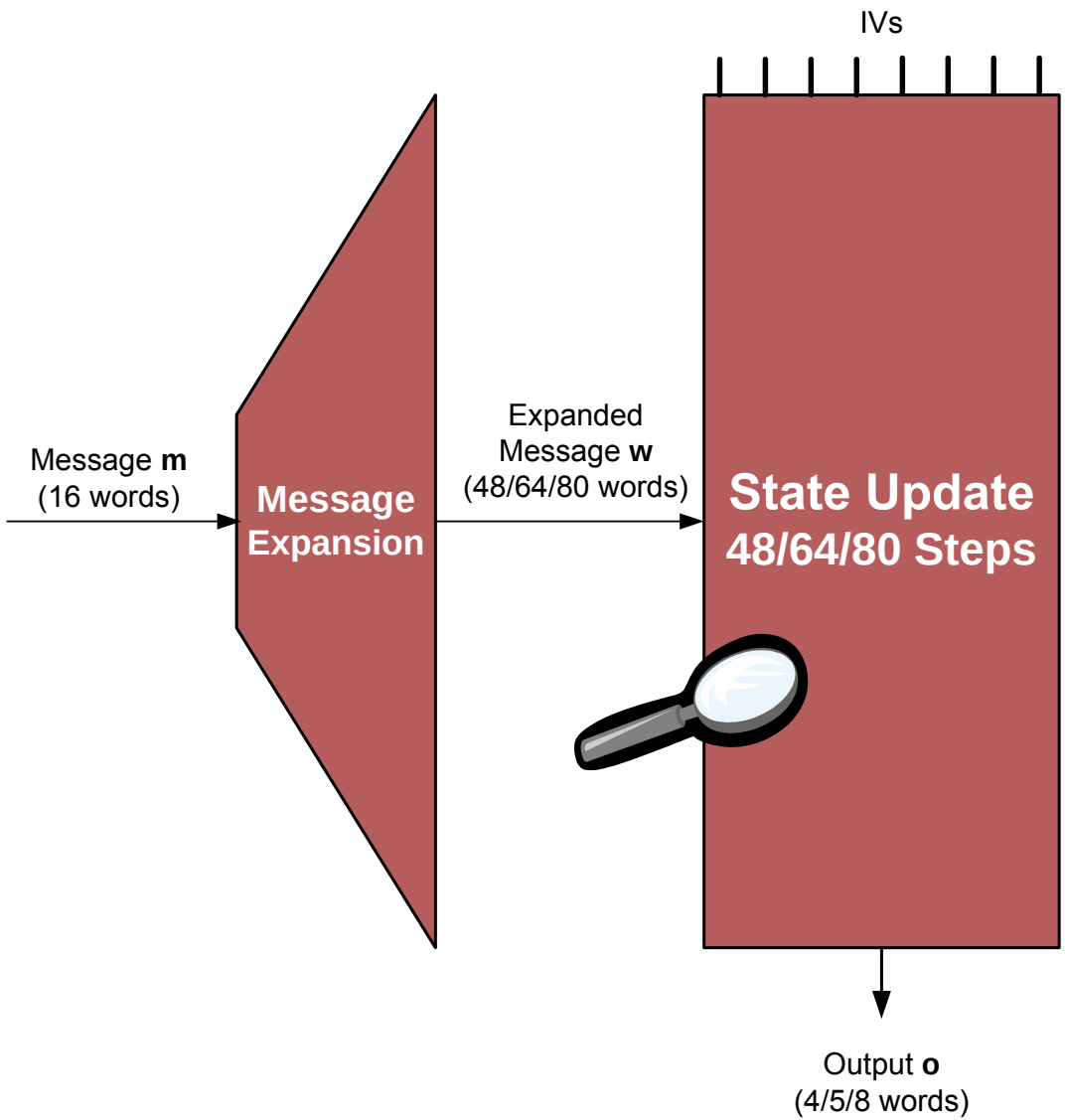
SHA-0 / SHA-1



SHA-2 family

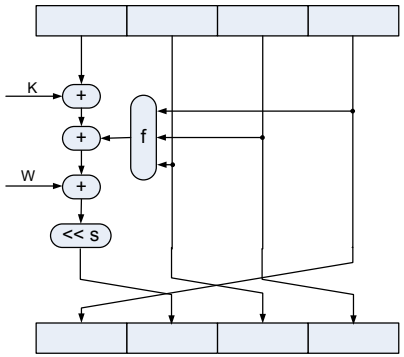


Outline of MD4-style Hash Functions

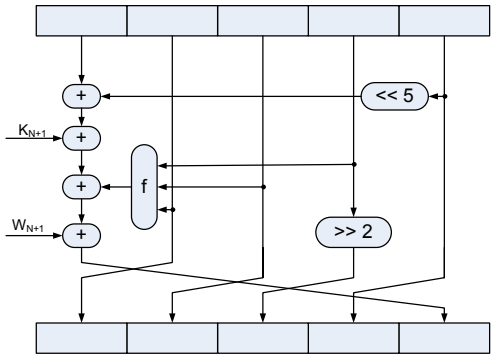


Evolution of the State Updates in the MD4 Family

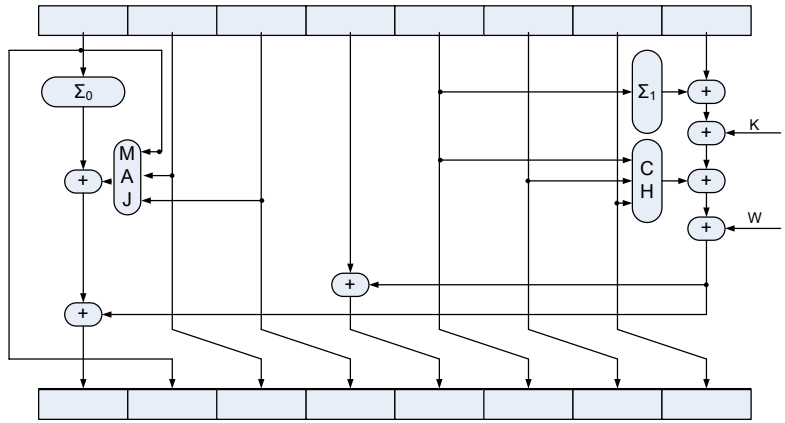
MD4



SHA-0/1



SHA-2 family



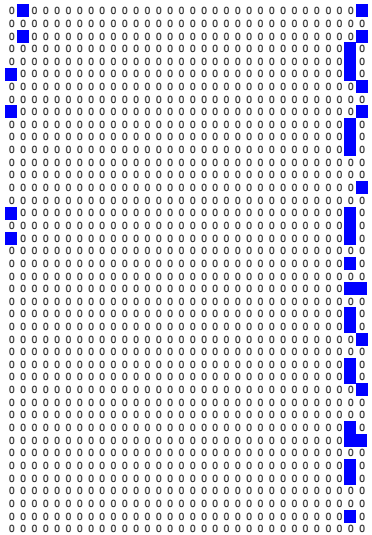
Design Complexity

Overview

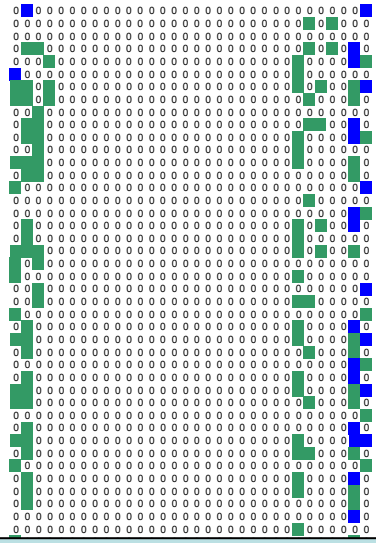
- Top-level review of results on SHA-1
- Applicability to SHA-2 members
- New method overcomes identified obstacles
- Interesting insights and directions for future work

Review of Collision Attacks on SHA-1 [CJ98, BC04, RO05, BCJ05, WYY05]

step 1



apply corrections



perturbation

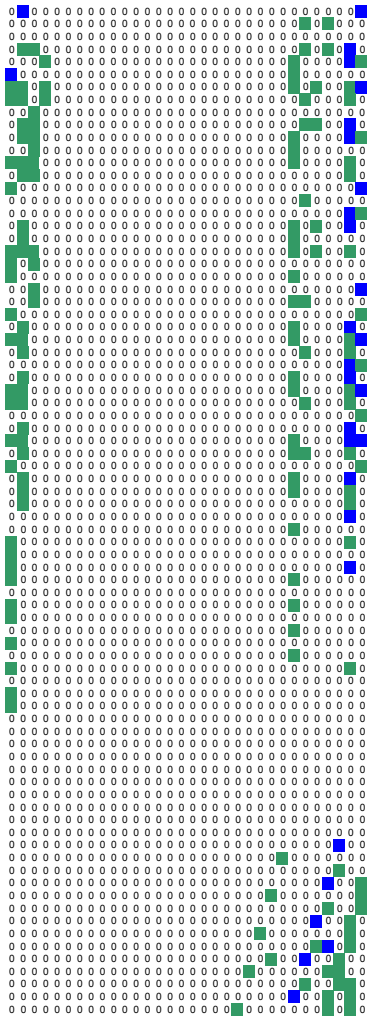
correction

Two properties are needed for that:

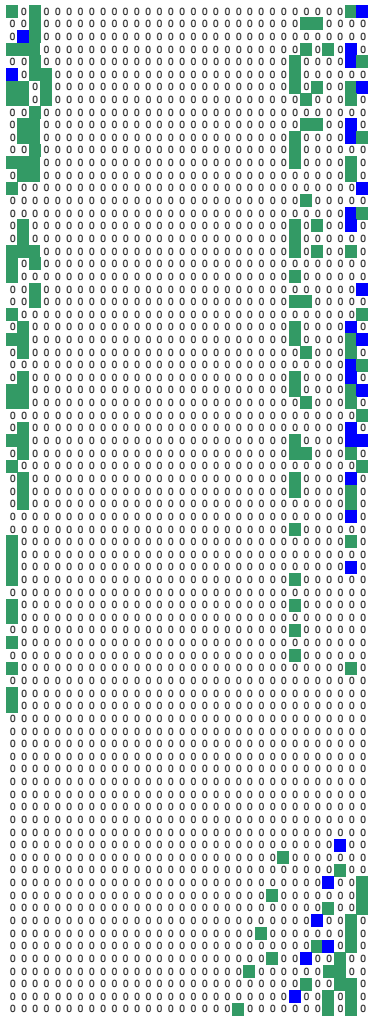
- ME is invariant with respect to rotation
- ME is invariant with respect to translation

step 80

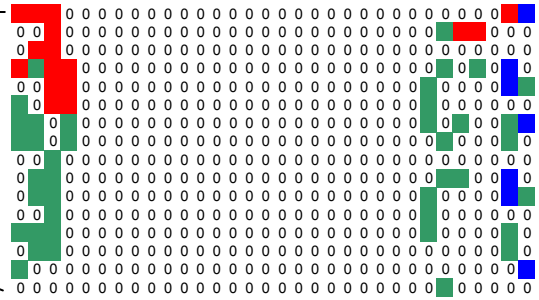
needed



reality



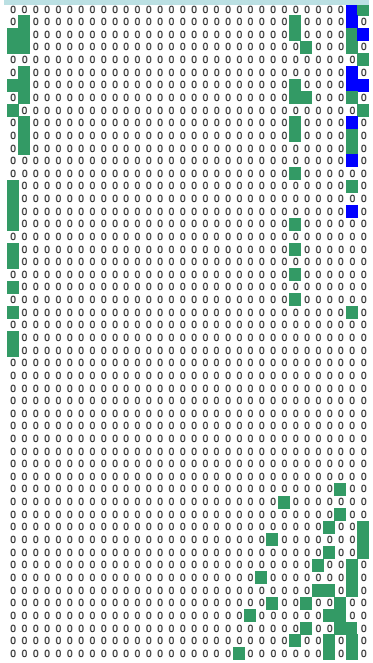
difference



ghost differences of type 1

Review of the [WYY05] Characteristic

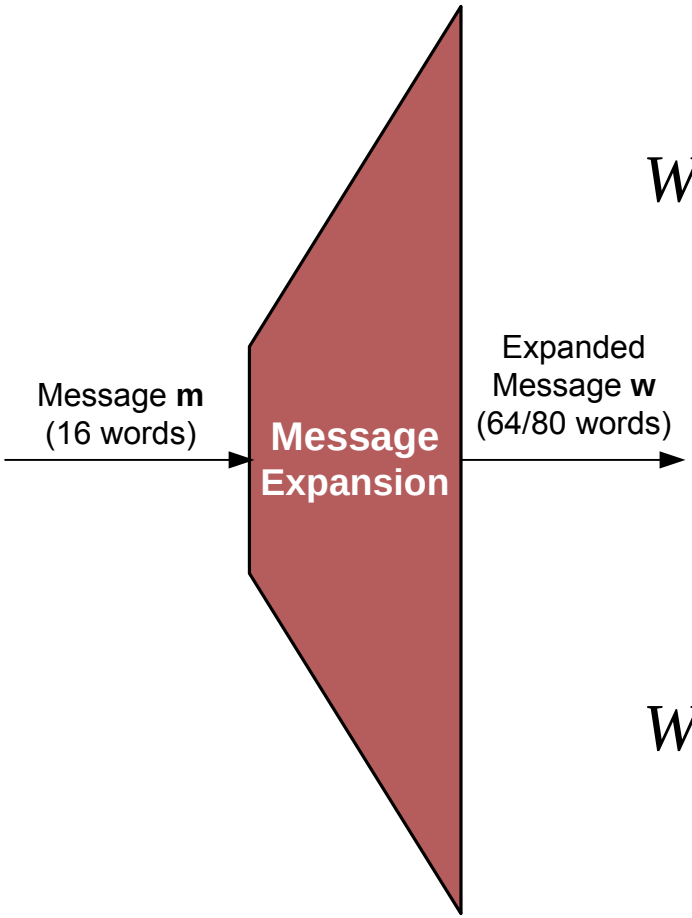
Message Modification improves the probability to 2^{-6x}



Low-probability characteristic

High-probability characteristic (about 2^{-83})

Comparison of SHA Message Expansions



SHA-1

$$W_t = \begin{cases} M_t & for\,(0 \le t \le 15) \\ ROTL^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) & for\,(16 \le t \le 79) \end{cases}$$

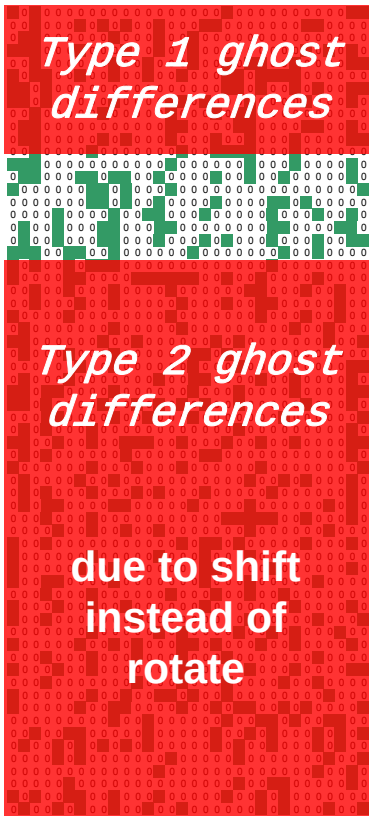
SHA-256

$$W_t = \begin{cases} M_t & for\,(0 \le t \le 15) \\ \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16} & for\,(16 \le t \le 63) \end{cases}$$

$$\sigma_0(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$$

$$\sigma_1(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

Approach does not apply to SHA-2



Low-probability characteristic

~~High-probability characteristic~~

Low-probability characteristic

Carry Effects in the Message Expansion

What about the non-linearity of the Message Expansion?

Theorem:
Preventing *type 2 ghost differences* is not always possible

Approach to avoid *type-2 Ghost Differences*

- Build up on approach originally pioneered by Rijmen and Oswald [RO05]
- Generalization → huge search space 2^{768}

- **Solution:**
  - Generic + heuristic search-space reduction → 2^{64}
  - Probabilistic search using algorithms from coding theory [Leo88,CC98]

Example of 19-step Characteristic

Step	W'	A'	B'	C'	D'	E'	F'	G'	H'
1-4	0	0	0	0	0	0	0	0	0
05	85009008	85009008	0	0	0	85009008	0	0	0
06	a14cae12	a1442610	85009008	0	0	02000802	85009008	0	0
07	0	0	a1442610	85009008	0	084c4120	02000802	85009008	0
08	8200a8a8	00000020	0	a1442610	85009008	00000020	084c4120	02000802	85009008
09	85009008	85009008	00000020	0	a1442610	01008008	00000020	084c4120	02000802
10	0	0	85009008	00000020	0	02000802	01008008	00000020	084c4120
11	0	0	0	85009008	00000020	0	02000802	01008008	00000020
12	0	00000020	0	0	85009008	0	0	02000802	01008008
13	0	0	00000020	0	0	84001000	0	0	02000802
14	00088802	0	0	00000020	0	0	84001000	0	0
15	0	0	0	0	00000020	0	0	84001000	0
16	0	0	0	0	0	00000020	0	0	84001000
17	0	0	0	0	0	0	00000020	0	0
18	0	0	0	0	0	0	0	00000020	0
19	0	0	0	0	0	0	0	0	00000020

1-block collision for SHA-224

Interesting Results

- **Perturbation pattern** is **no valid expanded message**
  - But the sum of perturbations and corrections is
- **More freedom** for the **carry**
  - … to prevent impossible characteristics
- The **overall probability** is **much higher** than the product of the probabilities of each individual local collision
  - Different to SHA-0 / SHA_1
  - Example: low-weight 19-step characteristic
    - 23 local collisions of probability around 2^{-40}
    - Total probability is much higher: instead of 2^{-920} around **2^{-200}**

      (Compare this to a similar probability of the best known 80-step characteristic for SHA-1)

Conclusions

- First analysis of unmodified SHA-256/224 for a nontrivial number of steps

- Collision resistance of SHA-256/224 is not threatened
- All publicly known attacks on SHA-0/1 since 1997 are not directly applicable to any SHA-2 member

- New analysis method
  - Circumvent problem of *ghost differences of type 2*
  - New type of perturbation pattern
  - Probability of a local collision is much less relevant
  - Explicit control of carry extensions is possible and needed

Future Research

1. Ways to reduce the search space for high probability characteristics
2. New message modification techniques
3. Exploiting non-linearity of Message Expansion
4. Apply multi-block approach

Analysis of Step-Reduced SHA-256

Florian Mendel and Norbert Pramstaller and
Christian Rechberger and Vincent Rijmen

http://www.iaik.tugraz.at/research/krypto

Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology