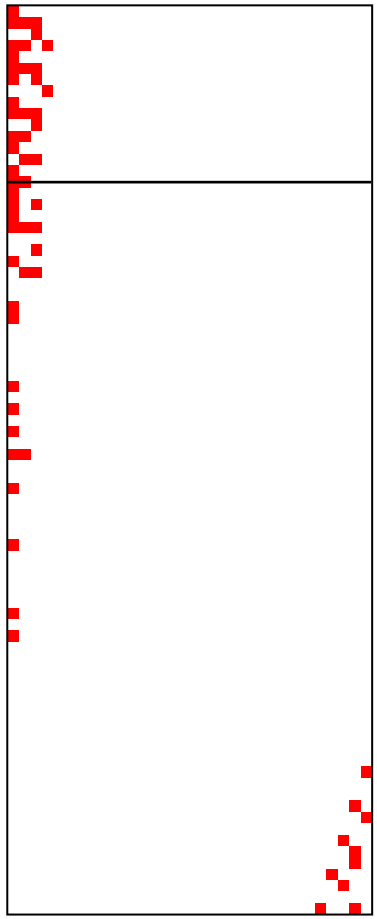
SHA-1: exact joint local collision analysis & new attacks

Marc Stevens

CWI, Amsterdam

Old: local collision analysis



local collision conditions

LC 1 cond p_1

LC 2 cond p_2

LC 3 cond p_3

LC k cond p_k

Adjustments:

LC interaction (msg. bitrel.)

attack conditions

steps 20-79 conditions:

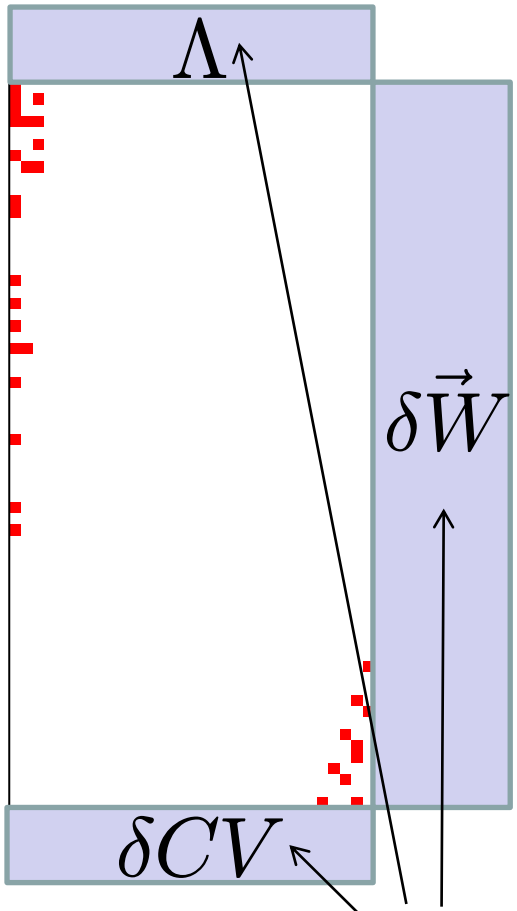
msg. bitrel.

w.s. bitcond

$$p_{\text{attack}} \overset{?}{\leq} p_1 \cdot p_2 \cdots p_k$$

Exact joint local collision analysis

differential path



pre- & post- conditions

$$p_{(\Lambda,\delta\vec{W},\delta CV)} = \sum_{\substack{\text{paths } \mathcal{P} \\ \Lambda,\delta\vec{W},\delta CV}} \Pr[\mathcal{P}]$$

Exactly compute total success probability
- ALL differential paths compatible with DV
- have given pre-/post-conditions

Automatically captures:
- All possible carries
- LC compression
- **LC dependency**

DV	dep	indep	diff
I(48, 0)	71.4	80.5	9.1
I(49, 0)	72.2	79.6	7.4
I(50, 0)	71.9	81.4	9.5
I(51, 0)	73.3	85.8	12.5
I(48, 2)	73.8	75.7	1.9
I(49, 2)	73.8	74.1	0.3
II(50, 0)	73.0	77.4	4.4
II(51, 0)	71.9	77.7	5.8
II(52, 0)	71.8	79.4	7.6

Deriving optimal conditions

$$\{p_{(\Lambda,\delta\vec{W},\delta CV)}\}$$

$$p_{\max} = \max_{\Lambda,\delta\vec{W},\delta CV} p_{(\Lambda,\delta\vec{W},\delta CV)}$$

optimal derivation

attack conditions

steps 20-79 conditions:

msg bitrel.

w.s. bitcond

$$p_{\text{attack}} = p_{\max} > p_1 \cdot p_2 \cdots p_k$$

New SHA-1 attacks

First publicly-verifiable attack implementation!

Project HashClash: http://code.google.com/p/hashclash

- First near-collision attack: $2^{57.5}$
- Second near-collision attack: $\sim 2^{61}$

- Identical-prefix collision attack **$\sim 2^{61}$**
  - First + second near-collision attack

- Chosen-prefix collision attack **$\sim 2^{77.1}$**
  - Birthday search + second near-collision attack

- Optimized success probability over steps 20-79
- Preliminary implementation steps 0-32: room for improvement
- PhD thesis + submitted to CRYPTO