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

Marc Stevens

CWI, Amsterdam
Old: local collision analysis

D.V.

Local collision conditions:
- LC 1 cond
- LC 2 cond
- LC 3 cond
- LC k cond

Adjustments:
LC interaction (msg. bitrel.)

Attack conditions:
- steps 20-79 conditions:
  - msg. bitrel.
  - w.s. bitcond

\[ p_{\text{attack}} \overset{?}{=} p_1 \cdot p_2 \cdot \ldots \cdot p_k \]
Exact joint local collision analysis

Let \( \delta \mathbf{W} \) be the differential path

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

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

<table>
<thead>
<tr>
<th>DV</th>
<th>dep</th>
<th>indep</th>
<th>diff</th>
</tr>
</thead>
<tbody>
<tr>
<td>I(48, 0)</td>
<td>71.4</td>
<td>80.5</td>
<td>9.1</td>
</tr>
<tr>
<td>I(49, 0)</td>
<td>72.2</td>
<td>79.6</td>
<td>7.4</td>
</tr>
<tr>
<td>I(50, 0)</td>
<td>71.9</td>
<td>81.4</td>
<td>9.5</td>
</tr>
<tr>
<td>I(51, 0)</td>
<td>73.3</td>
<td>85.8</td>
<td>12.5</td>
</tr>
<tr>
<td>I(48, 2)</td>
<td>73.8</td>
<td>75.7</td>
<td>1.9</td>
</tr>
<tr>
<td>I(49, 2)</td>
<td>73.8</td>
<td>74.1</td>
<td>0.3</td>
</tr>
<tr>
<td>II(50, 0)</td>
<td>73.0</td>
<td>77.4</td>
<td>4.4</td>
</tr>
<tr>
<td>II(51, 0)</td>
<td>71.9</td>
<td>77.7</td>
<td>5.8</td>
</tr>
<tr>
<td>II(52, 0)</td>
<td>71.8</td>
<td>79.4</td>
<td>7.6</td>
</tr>
</tbody>
</table>
Deriving optimal conditions

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