Rump Session Presentation:
Recent Progress on SHA-1

Adi Shamir
(On behalf of Xiaoyun Wang)
New Collision Search for SHA-1

by

Xiaoyun Wang, Andrew Yao and Frances Yao
Outline

- Current status: attack of SHA-1 with complexity $2^{69}$
- Obstacles for further improvement
- New collision path for SHA-1
- Comparing new collision path with previous path
- Strategies for message modification
- The complexity for searching collision of SHA-1
Obstacles for Further Improvement

- $2^{69}$ complexity comes from 68 conditions in the 2-iteration attack

- Can we eliminate even more conditions by applying message modification in steps 10-16?

- Difficult, because message space available is tight:
  -- 50 message conditions in steps 17-80
  -- hence 50 message conditions in steps 12-16
  -- resulting in 50 message bit equations
  -- most message bits are involved
  -- in addition, 51 chaining variable conditions in steps 10-16
  -- extra chaining variable conditions and message conditions coming from the message modification
**New Collision Path for SHA-1**

- We give a new collision differential path for SHA-1.

**Comparison:**

<table>
<thead>
<tr>
<th></th>
<th>Old</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Message conditions</td>
<td>50</td>
<td>43</td>
</tr>
<tr>
<td>2. Chaining variable conditions</td>
<td>51</td>
<td>30</td>
</tr>
<tr>
<td>3. Message space in steps 10-16 available for direct modification</td>
<td>$2^{47}$</td>
<td>$2^{55}$</td>
</tr>
<tr>
<td>4. Message space in steps 10-16 available for searching collision before advanced message modification</td>
<td>$2^{123}$</td>
<td>$2^{151}$</td>
</tr>
</tbody>
</table>
Strategies for Message Modification

- Determine which message bits are *possible candidates* for modification.

- The message modification process *must respect* all chaining variable conditions and message conditions.
  -- may require adding *extra chaining variable* conditions in steps 1-16 and message conditions.
  -- message modification follow certain *topological order* coming from correlations among chaining variable conditions.
Complexity Estimation for New Collision Search of SHA-1

- There are 83 conditions in steps 17-80
- Message modification can correct about 18 chaining variable conditions in steps 17-26
- Searching for three conditions in steps 26-27 by one computation
- Relax one condition in the final step
- 61 conditions left
- Factor of 4 from 2 iterations and error correction

$2^{63}$ complexity