SHA-1 collisions now $2^{52}$

Cameron McDonald, Philip Hawkes and Josef Pieprzyk

cmcdonal@ics.mq.edu.au

Macquarie University and Qualcomm, Australia
Motivation and Achievements

In November 2008, Stéphane Manuel published a new disturbance vector for SHA-1 with complexity $2^{57}$. He provided no differential path through the first 20 steps.

Using Joux and Peyrin’s boomerang attack with $n$ auxiliary differentials, the complexity can be reduced to $2^{57-n}$.

Our goal is to find a non-linear main differential path through the first 20 steps where a maximum number of auxiliary differentials can be applied.

Achieved: A differential path with 5 independent auxiliary paths - complexity $2^{52}$.
Method

- **Manual**
  Aided by a web based tool written in javascript. Allows tweaking of conditions, the resulting differences are propagated through the function.

- **Automated Path Tool**
  Tree searching algorithm that exhaustively searches differences generated by the modular addition and boolean $f$ function. Has the option to specify weight (number of conditions/differences), neutral bits and auxiliary conditions.

- **SAT Solving**
  Convert the problem into a corresponding propositional formula and attempt to find a solution using a SAT solver.

*Best results have come from using a combination of all three methods!*
# Example Path - $2^{52}$ (5 Aux)

<table>
<thead>
<tr>
<th>$i$</th>
<th>$A_i$</th>
<th>$W_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>-4</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-1</td>
<td>.v1v....v...vv...v...v...v...0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1...0...........10.......0</td>
<td></td>
</tr>
</tbody>
</table>
| 1   | 1+.-v-a...v.dvvgjvvv.m01...v1.+1 | .++++a...d..gj...m.........+
| 2   | 0+-0...-01...11...11...1+-...00...x0 | -ã-----ã̃.g̃j...m..........+-+
| 3   | 1--10+b00...e00hk00+-n...0...101...++...0 | .+...b...e...hk...n.........+
| 4   | --+1011101v00...+00...1100101.0000 | .b+...+ã̃.ã̃hk...ã̃ñj...m......+++
| 5   | 1.0-0+++0...0...00...00010...-00-- | ++--++.ã...ã̃.g̃j...m....++
| 6   | +100111-+++++++1...l...l+111-- | .---.ã...ã̃.g̃j...m.......-+
| 7   | +++...000.1111111...0v1-100++ | +++.ã...ã̃.g̃j...m....++
| 8   | 0-00...11001111...0...1+++-- | .---.ã...ã̃.g̃j...m....++
| 9   | 0++11l...v...vv...v1v0vvv--...01- | .+++..........................---+
| 10  | 0...01l...1...+.00010-- | +-----++..........................++
| 11  | --.l...c...f...il...p-+++++101+- | .-+-c...f...il...p.........+
| 12  | ++01l...0...0...0...00...01111-+010 | .ã̃...ã̃f...il...p.........+-
| 13  | ++000...0...0...0...00...0011111++ | +---..........................---+
| 14  | -++10------------------0110 | +..........................++
| 15  | ++--.l...1........................-- | .+++.ã...ã̃f...il...p.........+
| 16  | +................................. | .---.ã...ã̃f...il...p.........+
| 17  | -++............................. | .-+-..........................++
| 18  | .................................. | .---..........................++
| 19  | +.................................. | .---..........................++
| 20  | +.................................. | .---..........................++

SHA-1 collisions now $2^{52} - p$.  

Conclusion

- Until now, the best complete differential path (to our knowledge) has complexity $2^{63}$.

- The new path presented has complexity $2^{52}$ - a significant reduction.

- Practical collisions are within resources of a well funded organisation.

- We are continuing our search for differential paths where the boomerang attack can be used with maximum effect.

- Paper will appear on eprint soon.