SHA-1 Differentials for Boomerang Attack

Cameron McDonald, Philip Hawkes and Josef Pieprzyk

cameronm@qualcomm.com

Macquarie University and Qualcomm, Australia

Collision Attacks

- High probability differential
  - nonlinear differential in round 1
  - low cost disturbance vector (linear differential in rounds 2-4)
- Fast message generation
  - message modification (advanced)
  - neutral bits
  - tunnels
  - boomerang attack

Collision Attacks

- High probability differential
  - nonlinear differential in round 1
  - low cost disturbance vector (linear differential in rounds 2-4)
- Fast message generation
  - message modification (advanced)
  - neutral bits
  - tunnels
  - boomerang attack

Attack complexity depends on all factors!

Path with 7 auxiliaries

i	A_i	W_i
-4	.....	
-3	.....	
-2	.....	
-1	.v.1v....v..vv....v..1v....1...0	
0	0..1.................1.....0..v1	..--+-t....q..mj....g..da....+..
1	++.+v+t..v.qvvmj11v.gvvda.1..+.0	+$\bar{t}$--++$\bar{q}$..$\bar{m}\bar{j}$....$\bar{g}$..$\bar{d}\bar{a}$.....--.-
2	-++1.-.01....1..11....1+-11....0	..-....u....r..nk....h..eb..+....
3	00-.00u00..r.0nk00+-h.0eb00.+1.0	.$\bar{u}$-...-$\bar{r}$.$\bar{t}\bar{n}\bar{k}$..$\bar{q}$.$\bar{h}\bar{m}\bar{j}\bar{e}\bar{b}$..$\bar{g}$..$\bar{d}\bar{a}$+--..
4	.---01.00....0+.00..000..00.001.	-++.-+..$\bar{t}$....$\bar{q}$..$\bar{m}\bar{j}$....$\bar{g}$..$\bar{d}\bar{a}$+.-..
5	0..-10v+0+v0v01v00vv100..00101-	....++..$\bar{t}$....$\bar{q}$..$\bar{m}\bar{j}$....$\bar{g}$..$\bar{d}\bar{a}$...-.
6	-0.110.000.0.00.00.......01110-+	++.....$\bar{u}$....$\bar{r}$..$\bar{n}\bar{k}$....$\bar{h}$..$\bar{e}\bar{b}$-....
7	0--..1-+++++++++++++.....-----	-.--.-..$\bar{u}$....$\bar{r}$..$\bar{n}\bar{k}$....$\bar{h}$..$\bar{e}\bar{b}$--+..
8	0+001...10110000000000000.0...011	..+.-+.....................+..
9	+++11...0000000000000001.1v01110	-.++-+.....................-+...
10	0-0.1....0..00....0..00....+.1+-	-.++..w....s..pl....i..fc..-....
11	1++10.w....s..pl....i..fc...+-++	.$\bar{w}$....$\bar{s}$..$\bar{p}\bar{l}$....$\bar{i}$..$\bar{f}\bar{c}$.......++..
12	+0.00...0....0..00....0..00.v101	+.+++.....................-....
13	+-100...0....0..00....0..00..011	....-.....................-+...
14	+.-0.........................-+	.+-++...$\bar{w}$....$\bar{s}$..$\bar{p}\bar{l}$....$\bar{i}$..$\bar{f}\bar{c}$+....
15	-0+00.......................0v	....+...$\bar{w}$....$\bar{s}$..$\bar{p}\bar{l}$....$\bar{i}$..$\bar{f}\bar{c}$+.-..
16	-00.0.......................0.	.+-+.....................+....
17	+-+.1.......................	+.+-+.....................-+-..
18	..001.......................	+--.+.......................
19	..-.........................	+.++.....................+..
20	.........................+	