

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)

i	A_i	W_i
-4		
-3		
-2		
-1	.v.1v...v.vv...v...v...0	
0	1..0.....10.....0	
1	1+.-v-a.v.dvvgjvvv.m01..v1+.1	..++-+a...d.gj...m...+..
2	0-+0.-.01...11.11...1+-..0.x0	-a--++d.gj...m...-++.
3	1--10+b00.e00hk00+-n.0.101.++.0	..+...b...e.hk...n...+..
4	--+1011101vvv0+.00.1100101.0000	.b+.+e.ahk.d.ngj...m...+-+.
5	1.0-0-++0+...0.00.00010.-.00--	++-.+-..a...d.gj...m...++.
6	+10011-+++++++1.....1-+111--	a...d.gj...m...-.
7	++-..0.00.1.11111.....0v1-100++	-+.....b...e.hk...n...+..
8	0-.00...110011111..0...1...+--.	-...b...e.hk...n...-+-.
9	0++11...v.vv...v1v0vvv+-..001-	..+..+.....-.
10	0.+01.....1.+...00010--	+...-+.....++.
11	--.1..c...f.il...p-+++++101+-	-.-+..c...f.il...p...+..
12	+. +01...0...0.00...01111-+010	.c...f.il...p...-+..
13	++000...0...0.00...00111111-+	+...-.....-.
14	-+-10.....0110	...+.....++.
15	++-.1.....-+	.++-...c...f.il...p...+..
16	+.....	...-...c...f.il...p...++.
17	-++.....	..-++.....-.
18		-.-+-.....-++.
19	..+.....	..-+-.....
20	+.....	-.-+.....+

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.