Freestart collision for 76-step SHA-1

Pierre Karpman[1,2], Thomas Peyrin[2], Marc Stevens[3]

1 Inria, France
2 NTU, Singapore
3 CWI, Netherlands

https://marc-stevens.nl/research/sha1freestart

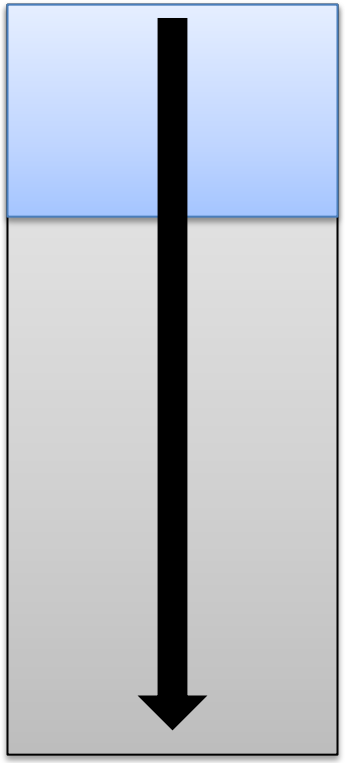
Freestart attack

- Attack on the compression function only
- Search for colliding pairs

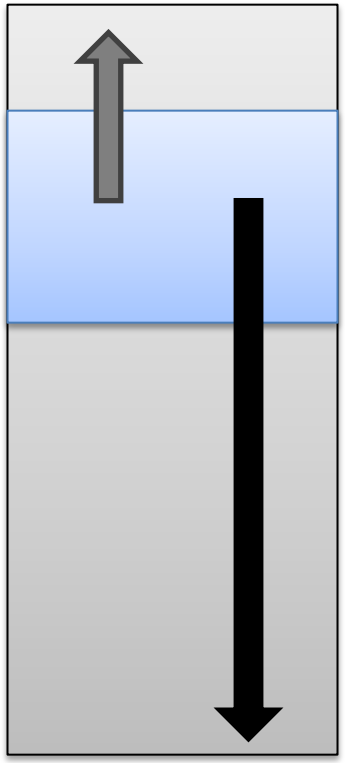
$$\text{Compress}(IV,M) = \text{Compress}(IV',M')$$

with IV,M,IV',M' free

Attack design



normal



freestart

Conditions optimized using Joint Local Collision Analysis

Collision search:

1. Solve steps 0-16
2. Use 51 neutral bits to solve steps 17-26
3. Verify steps 27-75

Neutral bits:

- Alter steps 0-5 backward
- (Almost) don't interfere with pre-fulfilled conditions

Complexity

- i5-4570 @ 3.2 GHz: $2^{49.1}$ eqv. SHA-1 compress
  606.12 cpucore days
- GTX 970 @ 1.2 GHz: $2^{50.1}$ eqv. SHA-1 compress
  4.94 gpu days
- Raw SHA-1: 1 GPU ≈ 256 CPU cores
- Our attack: 1 GPU ≈ 123 CPU cores !

```
-4 11110001010000100001111000100011
-3 11101001010000001010001101010110
-2 00001111101001101001111000111P0
-1 01000001101110000011101101011P0P
 0 10000001101111110010001100000110

 1 10010001100110011110000000P0110
 2 00111M1101101101111100P110111M11
 3 10000M01011110010P000011M1001M00
 4 0M0100111001P101100M1111M10010P1
 5 1P0010100011110M0101M000111P0P110
 6 000M1M1M1MMPPPP001P0M1MM1110100M
 7 1P0M1PM0MP10PM00PPMP11100P010111
 8 PM1100PMMMMMMMMMMMM1MPP110M11P0
 9 MMP0011010110000010PM001100M11101
10 M1001011100011101100100111011001
11 111M1111100111001001101000011100
12 P0P1010101110110110011110101101l
13 01P0101111111101000101l000M10000
14 00P0000110110111000110100l000101
15 1M1101001000011011111101110l1011
16 P0010001010001100111101000011110
17 P1M1100110110110000100001011l100
18 P0001011010100101001111010000100
19 1M0110011000011010101111010000l1
20 M0010001100110011000110111011110
21 M1M1001010010000100000001110lll0
22 M1000001101101000111110101011101
23 M0P1010101101011011000111101010
24 0011110111010001011100110111l101
25 11M0011101100011001100110000001l
26 M0000100110110110101010100101001
27 0MM1001111100010010001010l011001
28 1101111010001100001100l011100001
29 0001000101100101011011110111l010
30 M0010000010001110100000000111000
31 M0011001111000101110101110011101
32 0101000001000111110010001100010l
33 1111101110110010111001110110000l
34 0101011011000110100110001100110l
35 1010100010010001001101001011001l
36 0000000110000111001010011111111l
37 M0000111011010010010110111000011
38 0110110010101000100100011111010l
39 P0110110010010000101101000000111
40 1110101101111101011111110010100l
41 M1000111100011110100000101001010
42 0000011000010010001000011101101l
43 1P1001000000101100001101011101001
44 1001101011000011101100111111110l
45 1001010000101111010010000111111O
46 P1011111110011011000111001011010
47 0101001110111101110001011110110l
48 0011110101110000101011110101011l
49 1010111111000000110010001110101O
50 0010101011111101001011111000110l
51 P1010000001010000101111000000100
52 0111110010000111000010110001101O
53 1110101010011011101101011110111O
54 0001110100101011110010110111010l
55 0000111000000010101000011111010l
56 0111110011010111101000111100111O
57 M1000000110100011011110011100011
58 0011100010100010100101111101101O
59 M0010110110101001001001111011101
60 0111011000111111000010010001001O
61 1010110001111101000000110110001O
62 1100111111010111111011010011000O
63 1000100111110111011000001110011O
64 1011010111010110101111000110111l
65 0011101110110011010111001110101l
66 1101001100111110100101111111011l
67 1011001101000100000110011100100O
68 0100101011111111001011010000101O
69 1100001011100101101011110010101l
70 0111011111101101010100010000101l
71 0011100100111110110101000110101P

72 0110101000101000011011100111001l
73 1000101001011111001010110111100O
74 1000001011010010011110111010001M
75 0001000011001001111110011010011M
76 0010110110001010001110100000101O

 0 1010111101001001010111010001000O
 1 0101001010000010001101010000001l
 2 1110010010011110010001100111100O
 3 1101110011100111111100111011001l
 4 1101011011011010101000110010010O
```

Example collision

https://marc-stevens.nl
/research/sha1freestart

Outlook

- Freestart collision for 80-step SHA-1
- Same disturbance vector: x 274
  1355 gpu days
- Better disturbance vector: > x10 ?
  > 50 gpu days