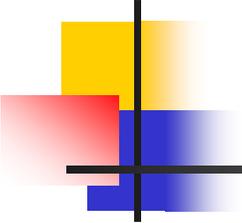


Cryptanalysis on SHA-1

Xiaoyun Wang, Andrew C Yao, and Frances Yao

Xiaoyun Wang	Tsinghua University & Shandong University
Andrew C Yao	Tsinghua University
Frances Yao	City University of Hong Kong



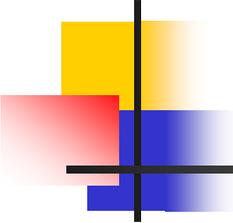
Outline

- Obstacles for further improvement on SHA-1 attack
- New collision path for SHA-1 (First iteration path)
- Comparing new collision path with previous path
- Strategies for message modification
- Details of message modification
- The complexity of searching for collisions

Obstacles for Further Improvement on SHA-1 Attack

- Unlike SHA-0 and MD5, many message conditions and chaining variable conditions must co-exist in each step of differential path

	$m_{6,1} = 1, m_{6,2} = 0, m_{6,5} = 1, m_{6,7} = 0, m_{6,29} = 0, m_{6,31} = 0, m_{6,32} = 0$
	$a_{7,1} = 0, a_{7,3} = 1, a_{7,4} = 0, a_{7,6} = 0, a_{7,7} = 0, a_{7,9} = 0, a_{7,10} = 1$ $a_{7,12} = 0, a_{7,16} = 1, a_{7,17} = 1, a_{7,18} = 1, a_{7,19} = 1, a_{7,20} = 1, a_{7,21} = 1, a_{7,22} = 1$ $a_{7,23} = 1, a_{7,24} = 1, a_{7,25} = 1, a_{7,26} = 1, a_{7,27} = 1, a_{7,28} = 0, a_{7,30} = 0$
m_6	$m_{23,7} = m_{22,1}, m_{23,6} = m_{23,7} + 1, m_{23,30} = m_{19,5}, m_{25,7} = m_{24,1} + 1, m_{27,6} = m_{26,1} + 1,$ $m_{27,31} = 1 + m_{22,1}, m_{29,7} = m_{28,2} + 1, m_{30,7} = m_{29,2} + 1, m_{31,6} = m_{30,1} + 1, m_{31,31} = m_{26,1} + 1$ $m_{34,7} = m_{33,2} + 1, m_{34,2} = m_{34,1} + 1, m_{35,6} = m_{35,7} + 1, m_{35,7} = m_{34,2} + 1, m_{35,31} = m_{30,1} + 1$ $m_{37,7} = m_{36,1} + 1, m_{38,7} = m_{37,2} + 1, m_{39,31} = m_{34,2} + 1, m_{41,7} = m_{40,2} + 1, m_{42,2} = m_{40,2} + 1$ $m_{45,7} = m_{44,2} + 1, m_{47,7} = m_{44,2} + 1, m_{49,7} = m_{44,2} + 1, m_{51,7} = m_{44,2} + 1, m_{52,2} = m_{44,2} + 1$ $m_{67,8} = m_{66,3} + 1, m_{70,9} = m_{69,4} + 1, m_{71,1} = m_{66,3} + 1, m_{73,10} = m_{72,5} + 1, m_{74,2} = m_{69,4} + 1$ $m_{75,9} = m_{74,4} + 1, m_{76,11} = m_{75,6} + 1, m_{77,3} = m_{72,5} + 1, m_{79,12} = m_{78,7} + 1, m_{79,2} = m_{74,4} + 1$



Obstacles for Further Improvement on SHA-1 Attack (continued)

- 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

$$\begin{aligned} m_{13,29} = & m_{0,2} + m_{0,24} + m_{0,25} + m_{0,28} + m_{0,29} + m_{0,30} + m_{1,0} + m_{1,3} + m_{1,26} + m_{1,27} + m_{1,28} + m_{1,29} \\ & + m_{1,30} + m_{2,0} + m_{2,2} + m_{2,3} + m_{2,24} + m_{2,25} + m_{2,29} + m_{2,30} + m_{2,31} + m_{3,2} + m_{3,3} + m_{3,4} + m_{3,25} + m_{3,27} \\ & + m_{3,28} + m_{3,31} + m_{4,2} + m_{4,3} + m_{4,4} + m_{4,28} + m_{4,30} + m_{4,31} + m_{5,0} + m_{5,3} + m_{5,25} + m_{5,26} + m_{5,29} + m_{5,31} + m_{6,0} \\ & + m_{6,3} + m_{6,26} + m_{6,27} + m_{7,1} + m_{7,4} + m_{7,28} + m_{7,29} + m_{8,2} + m_{8,3} + m_{8,24} + m_{8,25} + m_{8,26} + m_{8,27} + m_{8,28} + m_{8,29} \\ & + m_{8,31} + m_{9,0} + m_{9,1} + m_{9,2} + m_{9,3} + m_{9,4} + m_{9,26} + m_{9,28} + m_{9,31} + m_{10,1} + m_{10,2} + m_{10,3} + m_{10,5} + m_{10,28} + m_{10,29} \\ & + m_{11,0} + m_{11,2} + m_{11,3} + m_{11,25} + m_{11,26} + m_{11,27} \\ & + m_{11,28} + m_{11,29} + m_{11,30} + m_{11,31} + m_{12,1} + m_{12,2} + m_{12,5} + m_{12,28} + m_{12,30} + m_{13,0} + m_{13,1} + m_{13,3} + m_{13,24} + m_{13,25} + m_{13,} \end{aligned}$$

- in addition, 51 chaining variable conditions in steps 10-16
- extra chaining variable conditions and message conditions coming from the message modification

Table 1 New Collision Path for SHA-1 (First Iteration)

i	x_{i-1}	Δm_{i-1}	Δa_i	Δb_i	Δc_i	Δd_i	Δe_i
1	80000001	1,-2 -30,-32	32,-1 30,-31				
2		-5,6 30	-3,30	32,-1 30,-31			
3	40000001	30,31	-31,32 3, 8,9,...,-23	-3,30	30,-31 28,-29		
4	2	-2,-4,-6 -30,31,-32	-2, 6,-7 8,13,-14, 32	-31,32 3,8,9,-23	-1, 28	30,-31 28,-29	
5	2	-1,2,7,30	5,-6 8,-9, -23, 28	-2,6,-7 8,13,-14, 32	-29,30 1,6,7,...-21	-1,28	30,-31 28,-29
6	80000002	-7 29,-30,-32	-32 -11,12	5,-6 8,-9,-23,28	-32, 4,-5 6,11,-12, 30	-29,30 1,6,7,...-21	-1,28
7	1	-1,2,-5,7 29,31,32	1 -16,-27,28	-32 -11,12	5,-6 6,-7, -21,26	-32, 4,-5 6,11,-12, 30	-29,30 1,6,7,...-21
8		-2,6 29, 31,32	4	1 -16,-27,28	-30 -9,10	5,-6 6,-7, -21,26	-32,4,-5 6,11,-12, 30
9	80000001	-30	32,1 9,-10	4	31 -14,-25,26	-30 -9,10	5,-6 6,-7, -21,26
10	2	-2,5,6 30,-31	2	32,1 9,-10	2	31 -14,-25,26	-30 -9,10
11	2	1,-2,-7 30,31	9,-10	2	30,31 7,-8	2	31 -7 -14,-25,26
12	2	7,-30	2	9,-10	32	30,31 7,-8	2
13		-2,-7 -30,31,32		2	7,-8	32	30,31 7,-8
14		2,-30,-31			32	7,-8	32
15	1	1,32	1			32	
16		6		1			32

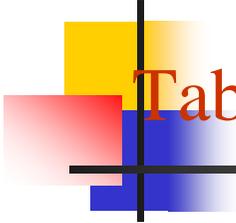
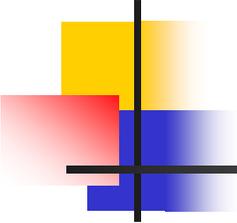


Table 2 An Sample Solution to 1-10 Steps Differential

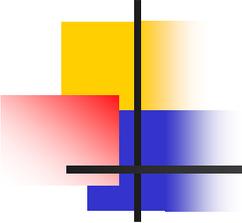
M	b67fd432 172193ca	15fdd1d6 2132f639	8627ed48 58de2ce	a5fcd96b 7c7e019a	83dad005 ccceb003
M'	167fd431 a721938a	35fdd1e6 f132f66a	e627ed48 d58de2ec	45fcd941 5c7e019a	a3dad046 acceeb031
ΔM	a0000003 b0000040	20000030 d0000053	60000000 d0000022	e000002a 20000000	20000043 60000032



Comparison between New Collision Path and Previous Collision Path

■ Comparison:

	Old		New
1. <u>Message conditions</u>	50		42
2. <u>Chaining variable conditions in steps 10-16</u>	51		
3. <u>Message space in steps 10-16 available for direct modification</u>	2^{47}		2^{55}
4. <u>Message space in steps 10-16 available for searching collision before advanced message modification</u>		30	
	2^{123}		2^{151}



Strategies for Message Modification

- Determine which message bits are *possible candidates (control bits)* for modification (Table 3).
- The message modification process *must respect* all chaining variable conditions and message conditions.
 - require adding *extra chaining variable* conditions in steps 1-16 and message conditions.
Especially Consider the carry effect.
 - message modification follow certain *topological order* coming from correlations among chaining variable conditions.

42 Message Conditions in Steps 17-80 for SHA-1 First Iteration

0	$m_{17,7} = m_{16,2} + 1, m_{17,31} = 1$
1	$m_{18,7} = m_{17,2} + 1, m_{18,31} = 0$
2	$m_{19,30} = m_{17,5}, m_{19,31} = 1$
3	$m_{23,7} = m_{22,1}, m_{23,6} = m_{23,7} + 1, m_{23,30} = m_{19,5}$
6-7	$m_{25,7} = m_{24,1} + 1, m_{26,7} = m_{25,2} + 1$
8	$m_{27,6} = m_{26,1} + 1, m_{27,31} = 1 + m_{22,1}$
10-12	$m_{29,7} = m_{28,2} + 1, m_{30,7} = m_{29,2} + 1, m_{31,6} = m_{30,1} + 1$
13-15	$m_{31,31} = m_{26,1} + 1, m_{34,7} = m_{33,2} + 1, m_{34,2} = m_{34,1} + 1$
16-18	$m_{35,6} = m_{35,7} + 1, m_{35,7} = m_{34,2} + 1, m_{35,31} = m_{30,1} + 1$
19-21	$m_{37,7} = m_{36,1} + 1, m_{38,7} = m_{37,2} + 1, m_{39,31} = m_{34,2} + 1$
22-24	$m_{41,7} = m_{40,2} + 1, m_{42,2} = m_{40,2} + 1, m_{45,7} = m_{44,2} + 1$
25-27	$m_{47,7} = m_{44,2} + 1, m_{49,7} = m_{44,2} + 1, m_{51,7} = m_{44,2} + 1$
28-30	$m_{52,2} = m_{44,2} + 1, m_{67,8} = m_{66,3} + 1, m_{70,9} = m_{69,4} + 1$
31-33	$m_{71,1} = m_{66,3} + 1, m_{73,10} = m_{72,5} + 1, m_{74,2} = m_{69,4} + 1$
34-36	$m_{75,9} = m_{74,4} + 1, m_{76,11} = m_{75,6} + 1, m_{77,3} = m_{72,5} + 1$
37-38	$m_{79,12} = m_{78,7} + 1, m_{79,2} = m_{74,4} + 1$

Details for Message Modification —

Control bit and Control path

- Choices for control bit: a message bit $m_{\{i',j'\}}$ ($i' < 16$) which does not appear explicitly in 42 message conditions or chaining variable conditions. (marked by 0* and 0 in Table 3)

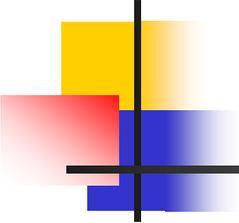
0*: No appearance in 42 message bit equations and no chaining variable condition in the same bit position

0 : No appearance in 42 message bit equation, but a chaining variable condition in the same bit position

- Control Path: A chain of intermediate variable bits which can transmit a bit change from control bit $m_{\{i',j'\}}$ to the target bit $a_{\{i,j\}}$.

- An example for Control Path:

$m_{14,10} \longrightarrow a_{18,11} \longrightarrow a_{20,11} \longrightarrow a_{21,16} \longrightarrow a_{22,21} \longrightarrow a_{23,26} \longrightarrow a_{24,31}$



Details for Message Modification — Topological Order

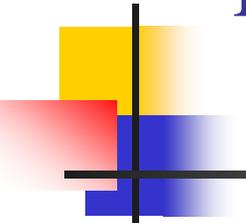
- A preferred order for processing a set of conditions $a_{\{i,j\}}$ so as to minimize the chance that a previously enforced condition may later get undone.
- An example of topological order

$a_{18,2} \rightarrow a_{17,31} \rightarrow a_{17,32} \rightarrow a_{17,2} \rightarrow a_{16,31} \rightarrow a_{17,4} \rightarrow a_{20,4}$

$\rightarrow a_{19,32} \rightarrow a_{19,2} \rightarrow a_{18,30} \rightarrow a_{18,32} \rightarrow a_{20,30} \rightarrow a_{21,30} \rightarrow a_{21,2} \rightarrow a_{22,3}$

$\rightarrow a_{24,4} \rightarrow a_{23,1} \rightarrow a_{24,31} \rightarrow a_{25,31}$

$a_{18,29} \rightarrow (a_{19,2}, a_{18,30})$



Details for Message Modification

-----Error Probability

- **Error probability** In spite of topological order, there is some probability that at the end of the message modification process, not all conditions are satisfied . We refer to this probability as **error probability**.
- Calculation of error probability (See Table 4)

Table 4 An Example for One Condition Correction

step	Δw_i	Additional Cons	Control bits	Closest Cons	Pr_1	Pr_2
11	2^{11}	$a_{11,12} = m_{10,12}$	$a_{11,12}$	$a_{11,30}$	$\frac{1}{2^{18}}$	
12	2^{16}	$m_{11,17} = 1 + m_{10,12}$				
13		$c_{12,12} = d_{12,12}$		$a_{13,32}$		
14		$b_{13,10} = 0$		$a_{14,32}$		
15		$b_{14,10} = 1$		$a_{15,1}$		
16	2^9	$m_{15,10} = 1 + m_{10,12}$		$a_{16,31}$		
...
19	$2^{10}, 2^{12}$		$a_{19,11}, a_{19,13}$	$a_{19,32}$	$\frac{1}{2^{19}}$	
20	2^{17}		$a_{20,16}, a_{20,18}$	$a_{20,4}$	$\frac{1}{2^{20}}$	
21			$a_{21,11}, a_{21,13}, a_{21,21}, a_{21,23}$	$a_{21,30}$	$\frac{1}{2^9}$	
22	$2^{12}, 2^{13}$		$a_{22,9}, \dots, a_{22,18}, a_{22,26}, a_{22,28}$	$a_{22,3}$	$\frac{1}{2^9}$	
23	2^{18}		$a_{23,1}, \dots, a_{23,23}, a_{23,31}$	$a_{23,1}$		
24			$a_{24,4}, a_{24,6}, a_{24,10}, \dots, a_{24,28}$	$a_{24,31}$		$\frac{1}{2^8}$

$$a_{23,23} \rightarrow a_{23,28} \rightarrow a_{24,1} \rightarrow a_{24,4}$$

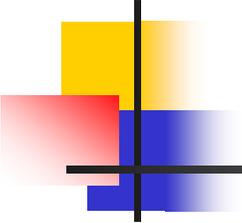
Table 5 Conditions can be Corrected
by Advanced Message Modification (with Star)

10	$a_{10,2} = 0, a_{10,4} = 1, a_{10,7} = 0, a_{10,8} = 0, a_{10,11} = a_{9,11}, a_{10,12} = a_{9,12}, a_{10,30} = 1, a_{10,31} = 1,$
11	$a_{11,4} = 0, a_{11,7} = 1, a_{11,8} = 1, a_{11,9} = 0, a_{11,10} = 1, a_{11,30} = 0, a_{11,31} = 1, a_{11,32} = 1,$
12	$a_{12,2} = 0, a_{12,7} = 1, a_{12,8} = 0, a_{12,32} = 1$
13	$a_{13,7} = 1, a_{13,8} = 1, a_{13,32} = 1$
14	$a_{14,3} = a_{13,4} + 1 = m_{16,1}, a_{14,32} = 1,$
15	$a_{15,1} = 0,$
16	$a_{16,1} = 0, a_{16,2} = a_{15,2}, a_{16,31} = 1$
17	$a_{17,2} = m_{17,2} + m_{19,7} + 1^*, a_{17,32} = m_{20,30}^*, a_{17,4} = m_{19,2} + m_{17,2}^*, a_{17,31} = 0^*$
18	$a_{18,2} = m_{17,2}^*, a_{18,32} = 1^*, a_{18,30} = 1^*$
19	$a_{19,32} = 1 + m_{19,5}^*, a_{19,2} = a_{18,2} + a_{17,2}^*,$
20	$a_{20,30} = 1 + a_{17,32} + a_{18,32}^*, a_{20,4} = m_{22,1} + 1 + a_{19,4}^*$
21	$a_{21,2} = a_{18,4} + a_{17,4}^*, a_{21,2} = m_{21,7} + 1^*, a_{21,30} = 1 + m_{22,30} + a_{20,32}^*$
22	$a_{22,3} = m_{24,1} + a_{21,3}^*$
23	$a_{23,1} = 1 + m_{22,1}^*$
24	$a_{24,4} = w_{26,2} + 1 + a_{23,4}^*, a_{24,31} = w_{25,31} + a_{22,1}^*$
25	$a_{25,2} = m_{24,1}, a_{25,31} = w_{26,31} + a_{23,1}^*$
26	$a_{26,2} = w_{25,2}, a_{26,3} = w_{28,1} + 1 + a_{25,3}$

Complexity Estimation

----Complexity for Second Iteration

- There are 83 conditions in steps 17-80
- After advanced message modification, there are 65 conditions left in 17-80 steps
- Searching for two conditions in steps 25-26 by one computation
- Relax one condition in the final step
- 62 conditions left
- Error probability for correcting 17-25 conditions amounts to one failed condition.
- The complexity is about 2^{63} computations.



Complexity Estimation ---Total Complexity

- Complexity for first iteration: further relax 3 conditions in the final 2 steps.

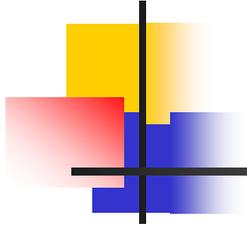
The complexity is about 2^{60} computations

- Complexity for the second iteration

2^{63} computations

- Total complexity

$$2^{63} + 2^{60} = 1.125 \times 2^{63} \sim 2^{63}$$



Thanks!