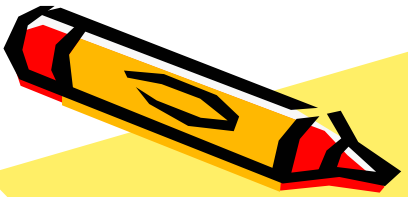


X. Wang, H. Yu and Y. Lisa Yin
"Efficient Collision Search Attack on SHA-0"
CRYPTO 2005

Improving the Collision Search on SHA-0

Yusuke Naito†, Yu Sasaki,
Takeshi Shimoyama, Jun Yajima,
Noboru Kunihiro and Kazuo Ohta

†:The University of Electro-Communications, Japan

Contribution

1. We find two conditions ($b_{0,9}$=0,$b_{0,11}$=1) are necessary in sufficient conditions of Wang et al.
2. We propose new message modifications for sufficient conditions in step 21-24.

	Complexity
Method of Wang et al	~~2^{39}~~ $\rightarrow 2^{41}$ SHA-0 operations
Our Method	2^{36} SHA-0 operations

Main Idea of Message Modifications for Step 21-24

- **Message modifications of the method of Wang et al.**
  - Sufficient conditions in step 17-20 are corrected by inputting a differential in m_{15}.
    (A start point of a differential is step 16)
- **Problem of the method of Wang et al.**
  - It is difficult to correct sufficient conditions after step 20 by inputting a differential in m_{15}.
- **Solution of this problem**
  - We solve this problem by using an idea of local collision.
  - By using this idea, a start point of a differential changes from step 16 to step 19.
  - We can correct sufficient conditions until step 24

Outline of Our Message Modification

Step	Differential	
11	$\Delta a_{11}=2^j$	←Input a differential in m_{10}
.	⋮	Execute a certain procedure to cancel this differential
.	$\Delta e_{15}=2^{j-2}$	
16	0	Differentials of chaining values are 0 (Non differential)
.	⋮	
.	0	
19	$\Delta a_{19}=2^k$	←A differential is appeared from message expansion
.	correct ↓	By this differential, sufficient conditions until step 24 can be corrected
.	Sufficient condition	
24		

Example of Our Message Modification ($a_{22,2}=m_{21,2}$)

- We input a differential 2^{20} in m_{10} ($m_{10} \leftarrow m_{10} \oplus 2^{20}$).
- This differential is canceled by following procedure in six steps.

	step	Message Modify	Differentials	Extra Conditions
Input a differential →	11	$m_{10} \leftarrow m_{10} \oplus 2^{20}$	$\nabla a_{11} = \pm 2^{20}$	$a_{11,21} = m_{10,21}$
Canceling the differential	12	$m_{11} \leftarrow m_{11} \oplus 2^{25}$	$\nabla b_{12} = \pm 2^{20}$	$m_{11,26} \neq m_{10,21}$
	13		$\nabla c_{13} = \pm 2^{18}$	$a_{10,23} = a_{9,23}$
	14		$\nabla d_{14} = \pm 2^{18}$	$a_{12,19} = 0$
	15		$\nabla e_{15} = \pm 2^{18}$	$a_{13,19} = 1$
	16	$m_{15} \leftarrow m_{15} \oplus 2^{18}$	Non Differential	$m_{15,19} \neq m_{10,21}$

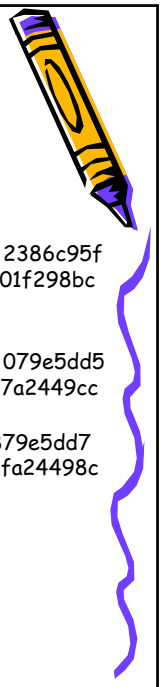
Example of Our Message Modification ($a_{22,2}=m_{21,2}$)

- From message expansion, differential $\nabla m_{18} = \pm 2^{18}$ is appeared in step 19.
- By this differential, the differential moves a_{22} as follows.

  $\nabla a_{19} = \pm 2^{18} \rightarrow \nabla a_{20} = \pm 2^{23} \rightarrow \nabla a_{21} = \pm 2^{28} \rightarrow \nabla a_{22} = \pm 2$
- By the differential $\nabla a_{22} = \pm 2$, $a_{22,2}$ is corrected.

Message modifications for sufficient conditions $a_{21,4} = (\neq) a_{20,4}$, $a_{22,4} = (\neq) a_{21,4}$, and $a_{23,2} = m_{22,2}$ are similar to this message modification

Example of Collision



M1= f459644c b87cdae1 ed98d4a6 7f5c304b a8606648 073dda8d 9f044c3a 2386c95f
8b611aa4 d66ed3b9 c4854f6e d57662b3 d687ebe0 f61cefe5 6d0252c2 01f298bc

M2= 76c21fb3 8a725c5a 13a6039c a23c1950 53e65762 b70bbb88 705ec5b6 079e5dd5
f58793f6 d67d305e 352ee1b8 87c36500 fd012cb5 a51c4269 6a72aabd 7a2449cc

M2'= f6c21ff1 8a725c5a 93a603de a23c1910 53e65722 b70bbbca f05ec5b4 879e5dd7
f58793b6 567d305e b52ee1f8 07c36502 fd012cb7 251c4229 ea72aabd fa24498c

H(M1||M2)=H(M1||M2')

Thank you