Message Modification for Step 21-23 on SHA-0

Yusuke Naito[1], Yu Sasaki[1], Takeshi Shimoyama[2], Jun Yajima[2],
Noboru Kunihiro[1] and Kazuo Ohta[1]

[1]The University of Electro-Communications
Chofugaoka 1-5-1, Chofu-shi, Tokyo, 182-8585, Japan
[2]FUJITSU LABORATORIES LTD
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, 211-8585, Japan

Abstract. In CRYPTO 2005, Xiaoyun Wang, Hongbo Yu and Yiqun Lisa Yin proposed an efficient collision attack on SHA-0. Collision messages are found with complexity 2^{39} SHA-0 operations by using their method. Collision messages can be obtained when a message satisfying all sufficient conditions is found. In their paper, they proposed message modifications that can satisfy all sufficient conditions of step 1-20. However, they didn't propose message modifications for sufficient conditions after step 21. In this paper, we propose message modifications for sufficient conditions of step 21-23. By using our message modifications, collision messages are found with complexity 2^{36} SHA-0 operations.

1 Introduction

In CRYPTO 2005, Wang et al. proposed an efficient collision attack on SHA-0 [1]. This attack is a differential attack using modular subtraction. The complexity of their attack is 2^{39} SHA-0 operations. One important parts of their attack is "sufficient condition". Sufficient conditions are conditions for finding collision messages. A procedure of the collision search is as follows.

Procedure 1. Find messages $(m_0, ..., m_{15})$ satisfying all sufficient conditions of step 1-16 by using message modifications.

Procedure 2. Modify a message m_{15} by using message modifications in order to satisfy all sufficient conditions of step 17-20.

Procedure 3. If message produced in procedure 1, 2 satisfies all sufficient conditions, go to procedure 4. Otherwise, go to procedure 1. However, messages $m_0, ..., m_{13}$ is not changed and messages m_{14}, m_{15} is changed.

Procedure 4. Calculate M' as $M' = M + \Delta M$ where M is the message produced in procedure 1, 2, 3, and ΔM is a message differential. Then M and M' are collision messages.

Message modifications in these procedures can find messages satisfying sufficient conditions of step 1-20 with probability 1.

In the method of Wang et al., they proposed message modifications for sufficient conditions of step 1-20. However, message modifications for sufficient conditions after step 21 were not proposed. In this paper, we propose message modifications for sufficient conditions from step 21-23. By using our message modifications, we can find collision messages with complexity 2^{36} SHA-0 operations.

2 Message Modifications for Sufficient Conditions of Step 21-23

In the method of Wang et al., all sufficient conditions of step 1-20 can be satisfied with probability 1. However, they didn't propose message modifications for sufficient conditions after step 21. In this section, we propose message modifications for sufficient conditions of step 21-23.

Step	Message Modification	Differential of Chaining Values	Extra Conditions
6	$m_5 \leftarrow m_5 \oplus 2^5$	$\Delta a_6 = \pm 2^5$	$a_{6,6} = m_{5,6}$
7	$m_6 \leftarrow m_6 \oplus 2^{10}$	$\Delta b_7 = \pm 2^5$	$m_{6,11} \neq m_{5,6}$
8	$m_7 \leftarrow m_7 \oplus 2^5$	$\Delta c_8 = \pm 2^3$	$m_{7,6} = m_{5,6}$
9		$\Delta d_9 = \pm 2^3$	$a_{7,4} = 0$
10		$\Delta e_{10} = \pm 2^3$	$a_{8,4} = 1$
11	$m_{10} \leftarrow m_{10} \oplus 2^3$		$m_{10,4} \neq m_{5,6}$

Table 1. Modification for "$a_{21,4} = a_{20,4}$ (or $a_{21,4} \neq a_{20,4}$)"

2.1 Message Modification for Sufficient Condition "$a_{21,4} = a_{20,4}$ (or $a_{21,4} \neq a_{20,4}$)" of Step 21

A sufficient condition "$a_{21,4} = a_{20,4}$ (or $a_{21,4} \neq a_{20,4}$)" exists in step 21. We correct this condition by using a modification in Table 1.

By this modification, differentials $\Delta m_{18} = \pm 2^3$, $\Delta m_{19} = \pm 2^5$, and $\Delta m_{20} = \pm 2^{10}$ are appeared from the message expansion. If we consider a situation where carry is not caused, following differentials are caused by these differentials .

$$\begin{array}{l} a_{19} = (a_{18} \lll 5) + f(b_{18}, c_{18}, d_{18}) + e_{18} + m_{18} + k_{18} \\ \quad 2^3 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad 2^3 \\ a_{20} = (\ a_{19} \lll 5) + f(b_{19}, c_{19}, d_{19}) + e_{19} + m_{19} + k_{19} \\ \quad 2^8 \qquad 2^3 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad 2^5 \\ \quad 2^5 \\ a_{21} = (\ a_{20} \lll 5) + f(\ b_{20}\ , c_{20}, d_{20}) + e_{20} + m_{20} + k_{20} \\ 2^{13} \qquad 2^8 \qquad\qquad 2^3 \qquad\qquad\qquad\qquad\qquad\quad 2^{10} \\ 2^{10} \qquad 2^5 \\ \quad 2^3 \end{array}$$

A meaning of $2^3, 2^8, ...$ in an above figure is a differential caused by this message modification. For simplicity, we ignore signs for these differentials. This sufficient condition can be corrected from a differential $\Delta a_{21} = \pm 2^3$. Moreover, we confirmed that this sufficient condition can be corrected with probability almost 100% by a computer experiment if we consider a situation where carry is caused.

2.2 Message Modification for Sufficient Condition "$a_{22,2} = m_{21,2}$" of Step 22

A sufficient condition "$a_{22,2} = m_{21,2}$" exists in step 22. We correct this condition by using a modification described in Table 2.

Step	Message Modification	Differential of Chaining Values	Extra Conditions
11	$m_{10} \leftarrow m_{10} \oplus 2^{20}$	$\Delta a_{11} = \pm 2^{20}$	$a_{11,21} = m_{10,21}$
12	$m_{11} \leftarrow m_{11} \oplus 2^{25}$	$\Delta b_{12} = \pm 2^{20}$	$m_{11,26} \neq m_{10,21}$
13		$\Delta c_{13} = \pm 2^{18}$	$a_{10,23} = a_{9,23}$
14		$\Delta d_{14} = \pm 2^{18}$	$a_{12,19} = 0$
15		$\Delta e_{15} = \pm 2^{18}$	$a_{13,19} = 1$
16	$m_{15} \leftarrow m_{15} \oplus 2^{18}$		$m_{15,19} \neq m_{10,21}$

Table 2. Modification for "$a_{22,2} = m_{21,2}$"

By this modification, differentials $\Delta m_{18} = \pm 2^{18} \pm 2^{20}$, $\Delta m_{19} = \pm 2^{25}$, and $\Delta m_{21} = \pm 2^{18} \pm 2^{20}$ are appeared from the message expansion. If we consider a situation where carry is not caused, following differentials are caused by these differentials.

$$
\begin{array}{l}
a_{19} = (a_{18} \lll 5) + f(b_{18}, c_{18}, d_{18}) + e_{18} + m_{18} + k_{18} \\
\begin{array}{ll} 2^{20} & \\ 2^{18} & \end{array} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \begin{array}{l} 2^{20} \\ 2^{18} \end{array} \\
a_{20} = (\begin{array}{ll} a_{19} & \lll 5) \end{array} + f(b_{19}, c_{19}, d_{19}) + e_{19} + m_{19} + k_{19} \\
\begin{array}{ll} 2^{23} & \\ & 2^{20} \\ & 2^{18} \end{array} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \begin{array}{l} 2^{25} \end{array} \\
a_{21} = (\begin{array}{ll} a_{20} & \lll 5) \end{array} + f(\begin{array}{ll} b_{20} & , c_{20}, d_{20}) \end{array} + e_{20} + m_{20} + k_{20} \\
\begin{array}{ll} 2^{28} & \\ 2^{20} & \\ 2^{18} & \end{array} \qquad \begin{array}{l} 2^{23} \end{array} \qquad\qquad \begin{array}{l} 2^{20} \\ 2^{18} \end{array} \\
a_{22} = (\begin{array}{ll} a_{21} & \lll 5) \end{array} + f(\begin{array}{lll} b_{21} & , c_{21} & , d_{21}) \end{array} + e_{21} + m_{21} + k_{21} \\
\begin{array}{ll} 2 & \\ 2^{25} & \\ \ldots & \\ 2^{16} & \end{array} \qquad \begin{array}{l} 2^{28} \\ 2^{20} \\ 2^{18} \end{array} \qquad\qquad \begin{array}{l} 2^{23} \end{array} \qquad \begin{array}{l} 2^{18} \\ 2^{16} \end{array} \qquad\qquad \begin{array}{l} 2^{20} \\ 2^{18} \end{array}
\end{array}
$$

Then, we add an extra condition "$m_{19,26} \neq m_{18,21}$" in order to cancel a differential "$\Delta a_{19} = \pm 2^{20}$" by a differential "$\Delta m_{19} = \pm 2^{25}$". This sufficient condition can be corrected by a differential $\Delta a_{22} = \pm 2$. Moreover, we confirmed that this sufficient condition can be corrected with probability 97.5 % by a computer experiment if we consider a situation where carry is caused.

2.3 Message Modification for Sufficient Condition "$a_{22,4} = a_{21,4}$ (or $a_{22,4} \neq a_{21,4}$)" of Step 22

A sufficient condition "$a_{22,4} = a_{21,4}$ (or $a_{22,4} \neq a_{21,4}$)" exists in step 22. We correct this condition by using a modification described in Table 3.

Step	Message Modification	Differential of Chaining Values	Extra Conditions
11	$m_{10} \leftarrow m_{10} \oplus 2^7$	$\Delta a_{11} = \pm 2^7$	$a_{11,8} = m_{10,8}$
12	$m_{11} \leftarrow m_{11} \oplus 2^{12}$	$\Delta b_{12} = \pm 2^7$	$m_{11,13} \neq m_{10,8}$
13		$\Delta c_{13} = \pm 2^5$	$a_{10,10} = a_{9,10}$
14		$\Delta d_{14} = \pm 2^5$	$a_{12,6} = 0$
15		$\Delta e_{15} = \pm 2^5$	$a_{13,6} = 1$
16	$m_{15} \leftarrow m_{15} \oplus 2^5$		$m_{15,6} \neq m_{10,8}$

Table 3. Modification for "$a_{22,4} = a_{21,4}$ (or $a_{22,4} \neq a_{21,4}$)"

By this modification, differentials $\Delta m_{18} = \pm 2^5 \pm 2^7$, $\Delta m_{19} = \pm 2^{12}$, and $\Delta m_{21} = \pm 2^5 \pm 2^7$ are appeared from the message expansion. If we consider a situation where carry is not caused, following differentials are caused by these differentials.

$$
\begin{array}{l}
a_{19} = (a_{18} \lll 5) + f(b_{18}, c_{18}, d_{18}) + e_{18} + m_{18} + k_{18} \\
\begin{array}{ll} 2^{7} & \\ 2^{5} & \end{array} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \begin{array}{l} 2^{7} \\ 2^{5} \end{array} \\
a_{20} = (\begin{array}{ll} a_{19} & \lll 5) \end{array} + f(b_{19}, c_{19}, d_{19}) + e_{19} + m_{19} + k_{19} \\
\begin{array}{ll} 2^{10} & \\ & 2^{7} \\ & 2^{5} \end{array} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \begin{array}{l} 2^{12} \end{array}
\end{array}
$$

$$
\begin{array}{l}
a_{21} = (\ a_{20} \lll 5) + f(\ b_{20}\ , c_{20}, d_{20}) + e_{20} + m_{20} + k_{20} \\
\begin{array}{llll}
2^{15} & 2^{10} & 2^{7} & \\
2^{7} & & 2^{5} & \\
2^{5} & & &
\end{array} \\
a_{22} = (\ a_{21} \lll 5) + f(\ b_{21}\ , c_{21}\ , d_{21}) + e_{21} + m_{21} + k_{21} \\
\begin{array}{lllll}
2^{3} & 2^{15} & 2^{10} & 2^{5} & 2^{7} \\
2^{20} & 2^{7} & & 2^{3} & 2^{5} \\
\ldots & 2^{5} & & & \\
2^{5} & & & &
\end{array}
\end{array}
$$

Then, we add an extra condition "$m_{19,13} \neq m_{18,8}$" in order to cancel a differential "$\Delta a_{19} = \pm 2^7$" by a differential "$\Delta m_{19} = \pm 2^{12}$". This sufficient condition can be corrected by a differential $\Delta a_{22} = \pm 2^3$. Moreover, we confirmed that this sufficient condition can be corrected with probability almost 100% by a computer experiment if we consider a situation where carry is caused.

2.4 Message Modification for Sufficient Condition "$a_{23,2} = m_{22,2}$" of Step 23

A sufficient condition "$a_{23,2} = m_{22,2}$" exists in step 23. We correct this condition by using a modification described in Table 4.

Step	Message Modification	Differential of Chaining Values	Extra Conditions
11	$m_{10} \leftarrow m_{10} \oplus 2^{15}$	$\Delta a_{11} = \pm 2^{15}$	$a_{11,16} = m_{10,16}$
12	$m_{11} \leftarrow m_{11} \oplus 2^{20}$	$\Delta b_{12} = \pm 2^{15}$	$m_{11,21} \neq m_{10,16}$
13	$m_{12} \leftarrow m_{12} \oplus 2^{15}$	$\Delta c_{13} = \pm 2^{13}$	$m_{12,16} \neq m_{10,16}$
14		$\Delta d_{14} = \pm 2^{13}$	$a_{12,14} = 0$
15		$\Delta e_{15} = \pm 2^{13}$	$a_{13,14} = 1$
16	$m_{15} \leftarrow m_{15} \oplus 2^{13}$		$m_{15,14} \neq m_{10,16}$

Table 4. Modification for "$a_{23,2} = m_{22,2}$"

By this modification, differentials $\Delta m_{18} = \pm 2^{13} \pm 2^{15}$, $\Delta m_{19} = \pm 2^{20}$, $\Delta m_{20} = \pm 2^{15}$, $\Delta m_{21} = \pm 2^{13} \pm 2^{15}$, and $\Delta m_{22} = \pm 2^{20}$ are appeared from the message expansion. If we consider a situation where carry is not caused, following differentials are caused by these differentials.

$$
\begin{array}{l}
a_{19} = (a_{18} \lll 5) + f(b_{18}, c_{18}, d_{18}) + e_{18} + m_{18} + k_{18} \\
\begin{array}{ll}
2^{15} & 2^{15} \\
2^{13} & 2^{13}
\end{array} \\
a_{20} = (\ a_{19} \lll 5) + f(b_{19}, c_{19}, d_{19}) + e_{19} + m_{19} + k_{19} \\
\begin{array}{lll}
2^{18} & 2^{15} & 2^{20} \\
& 2^{13} &
\end{array} \\
a_{21} = (\ a_{20} \lll 5) + f(\ b_{20}\ , c_{20}, d_{20}) + e_{20} + m_{20} + k_{20} \\
\begin{array}{llll}
2^{23} & 2^{18} & 2^{15} & 2^{15} \\
2^{15} & & 2^{13} & \\
2^{13} & & &
\end{array} \\
a_{22} = (\ a_{21} \lll 5) + f(\ b_{21}\ , c_{21}\ , d_{21}) + e_{21} + m_{21} + k_{21} \\
\begin{array}{lllll}
2^{28} & 2^{23} & 2^{18} & 2^{13} & 2^{15} \\
2^{20} & 2^{15} & & 2^{11} & 2^{13} \\
\ldots & 2^{13} & & & \\
2^{11} & & & &
\end{array}
\end{array}
$$

$$
\begin{array}{lllllll}
a_{23} = (& a_{22} \lll 5) + f(& b_{22} , & c_{22} , & d_{22}) + e_{22} + & m_{22} + k_{22} \\
2 & 2^{28} & 2^{23} & 2^{16} & 2^{13} & 2^{20} & \\
2^{25} & 2^{20} & 2^{15} & & 2^{11} & & \\
... & ... & 2^{13} & & & & \\
2^{11} & 2^{11} & & & & &
\end{array}
$$

Then, we add an extra condition "$m_{19,21} \neq m_{18,16}$" in order to cancel a differential "$\Delta a_{19} = \pm 2^{15}$" by a differential "$\Delta m_{19} = \pm 2^{20}$". This sufficient condition can be corrected by a differential $\Delta a_{23} = \pm 2$. Moreover, we confirmed that this sufficient condition can be corrected with probability 97% by a computer experiment if we consider a situation where carry is caused.

3 Conclusion

We propose message modifications for sufficient conditions of step 21-23. By combining our message modifications and the method of Wang et al., we can find collisions with complexity 2^{36} SHA-0 operations.

References

1. X. Wang, H. Yu and Y. Lisa Yin. *Efficient Collision Search Attack on SHA-0*. CRYPTO'05, LNCS 3621, pp1–16, Springer-Verlag, 2005.
2. NIST. *Secure hash standard*. Federal Information Processing Standard, FIPS-180, May 1993.