Collision Search Attacks on SHA1

Xiaoyun Wang* Yiqun Lisa Yin† Hongbo Yu‡

February 13, 2005

1 Introduction

In this note, we summarize the results of our new collision search attacks on SHA1. Technical details will be provided in a forthcoming paper.

We have developed a set of new techniques that are very effective for searching collisions in SHA1. Our analysis shows that collisions of SHA1 can be found with complexity less than 2^{69} hash operations. This is the first attack on the *full* 80-step SHA1 with complexity less than the 2^{80} theoretical bound. Based on our estimation, we expect that real collisions of SHA1 reduced to 70-steps can be found using today's supercomputers.

In the past few years, there have been significant research advances in the analysis of hash functions. The techniques developed in the early work provide an important foundation for our new attacks on SHA1. In particular, our analysis is built upon the original differential attack on SHA0, the near collision attack on SHA0, the multi-block collision techniques, as well as the message modification techniques used in the collision search attack on MD5. Breaking SHA1 would not be possible without these powerful analytical techniques.

Our attacks naturally apply to SHA0 and all reduced variants of SHA1. For SHA0, the attack is so effective that we were able to find real collisions of the full SHA0 with less than 2^{39} hash operations. We also implemented the attack on SHA1 reduced to 58 steps and found real collisions with less than 2^{33} hash operations. Two collision examples are given in this note.

*Shandong University, China. Email:xywang@sdu.edu.cn.
†Independent security consultant, USA. Email:yyin@princeton.edu.
‡Shandong University, China. Email:yhb@mail.sdu.edu.cn.

2 A collision example for SHA0

$$
\begin{aligned}
h_1 &= compress(h_0, M_0) \\
h_2 &= compress(h_1, M_1) = compress(h_1, M_1')
\end{aligned}
$$

h_0:	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
M_0:	65c24f5c	0c0f89f6	d478de77	ef255245	
	83ae3a1f	2a96e508	2c52666a	0d6fad5a	
	9d9f90d9	eb82281e	218239eb	34e1fbc7	
	5c84d024	f7ad1c2f	d41d1a14	3b75dc18	
h_1:	39f3bd80	c38bf492	fed57468	ed70c750	c521033b
M_1:	474204bb	3b30a3ff	f17e9b08	3ffa0874	
	6b26377a	18abdc01	d320eb93	b341ebe9	
	13480f5c	ca5d3aa6	b9f3bd88	21921a2d	
	4085fca1	eb65e659	51ac570c	54e8aae5	
M_1':	c74204f9	3b30a3ff	717e9b4a	3ffa0834	
	6b26373a	18abdc43	5320eb91	3341ebeb	
	13480f1c	4a5d3aa6	39f3bdc8	a1921a2f	
	4085fca3	6b65e619	d1ac570c	d4e8aaa5	
h_2:	2af8aee6	ed1e8411	62c2f3f7	3761d197	0437669d

Table 1: A collision of the full 80-step SHA0. The two messages that collide are (M_0, M_1) and (M_0, M_1'). Note that padding rules were not applied to the messages.

3 A collision example for 58-step SHA1

$$h_1 \quad = \quad compress(h_0, M_0) = compress(h_0, M_0')$$

h_0:	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
M_0:	132b5ab6	a115775f	5bfddd6b	4dc470eb	
	0637938a	6cceb733	0c86a386	68080139	
	534047a4	a42fc29a	06085121	a3131f73	
	ad5da5cf	13375402	40bdc7c2	d5a839e2	
M_0':	332b5ab6	c115776d	3bfddd28	6dc470ab	
	e63793c8	0cceb731	8c86a387	68080119	
	534047a7	e42fc2c8	46085161	43131f21	
	0d5da5cf	93375442	60bdc7c3	f5a83982	
h_1:	9768e739	b662af82	a0137d3e	918747cf	c8ceb7d4

Table 2: A collision of SHA1 reduced to 58 steps. The two messages that collide are M_0 and M_0'. Note that padding rules were not applied to the messages.