New Records in Collision Attacks on SHA-2

Yingxin Li[1],Fukang Liu[2], Gaoli Wang[1]

[1]East China Normal University
[2]Tokyo Institute of Technology

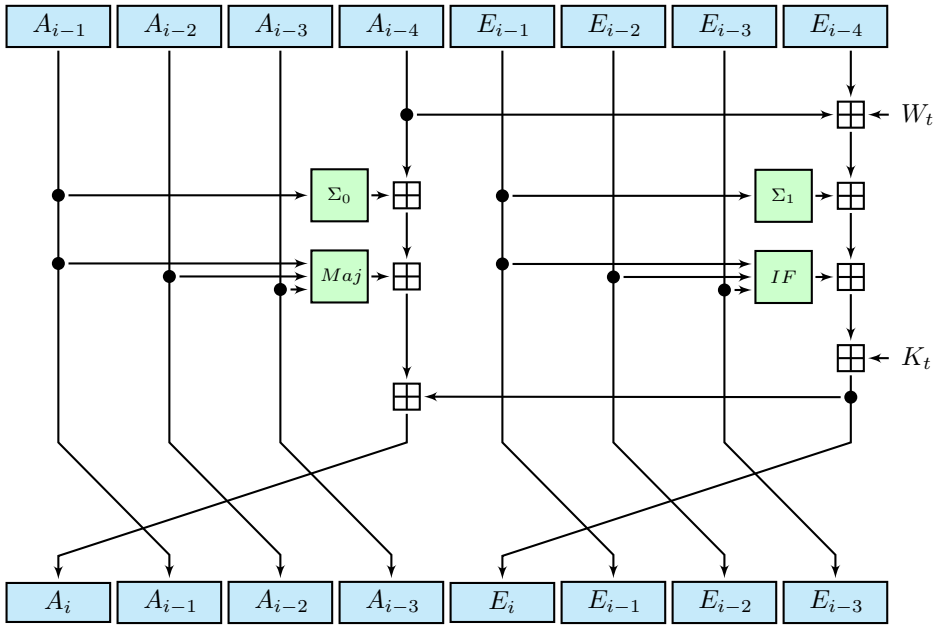
EUROCRYPT 2024

Overview

SHA-2

- A popular hash function family standardized by NIST.
- Strengthening SHA-1 (more complex compression function).
- Two main versions: SHA-256 and SHA-512.
- Used worldwide, e.g. SHA-256 is used in Bitcoin.

Compression Functions of SHA-256



- Step function

$$
\begin{aligned}
E_i &= A_{i-4} \boxplus E_{i-4} \boxplus \Sigma_1(E_{i-1}) \boxplus \mathrm{IF}(E_{i-1}, E_{i-2}, E_{i-3}) \boxplus K_i \boxplus W_i, \\
A_i &= E_i \boxminus A_{i-4} \boxplus \Sigma_0(A_{i-1}) \boxplus \mathrm{MAJ}(A_{i-1}, A_{i-2}, A_{i-3}).
\end{aligned}
$$

Compression Functions of SHA-256

- Boolean function $\Sigma_0, \Sigma_1, \mathrm{IF}$ and MAJ are given by

$$\begin{aligned}
\mathrm{IF}(x, y, z) &= (x \wedge y) \oplus (x \wedge z) \oplus z, \\
\mathrm{MAJ}(x, y, z) &= (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z), \\
\Sigma_0(x) &= (x \ggg 2) \oplus (x \ggg 13) \oplus (x \ggg 22), \\
\Sigma_1(x) &= (x \ggg 6) \oplus (x \ggg 11) \oplus (x \ggg 25).
\end{aligned}$$

Compression Functions of SHA-256

■ Message expansion

The message expansion of SHA-256 splits the 512-bit message block M_j into 16 words m_i, $i = 0, \cdots, 15$, and expands them into 64 expanded message words W_i

$$W_i = \begin{cases} m_i & 0 \le i \le 15, \\ \sigma_1(W_{i-2}) \boxplus W_{i-7} \boxplus \sigma_0(W_{i-15}) \boxplus W_{i-16} & 16 \le i \le 63. \end{cases}$$

The functions $\sigma_0(x)$ and $\sigma_1(x)$ are given by

$$\begin{aligned} \sigma_0(x) &= (x \ggg 7) \oplus (x \ggg 18) \oplus (x \gg 3), \\ \sigma_1(x) &= (x \ggg 17) \oplus (x \ggg 19) \oplus (x \gg 10). \end{aligned}$$

(FS/SFS) Collision Attacks on SHA-2

Finding a valid attack requires attackers to finish the following three tasks:

Three tasks

- Task 1: Select the message difference to construct a local collision;
- Task 2: Search for a corresponding differential trail in (W_i, A_i, E_i);
- Task 3: Find a conforming message pair to verify the differential trail.

Our contribution is Task 2:

- Use a SAT/SMT-based method to solve Task 2;

SFS Collision Attack on 39-step SHA-256

Search for the 39-step differential trail:

1. **Minimize the Hamming weight of ΔW_i.** The nonzero message differences are injected in $(W_8, \ldots, W_{12}, W_{16}, W_{17}, W_{24}, W_{26})$. The only goal is to find the minimal value $t_w = \sum_{i=0}^{38} \mathbf{H}(\Delta W_i)$.

i	ΔA_i	ΔE_i	ΔW_i
-4	================================	================================	
-3	================================	================================	
-2	================================	================================	
-1	================================	================================	
0	================================	================================	================================
1	================================	================================	================================
2	================================	================================	================================
3	================================	================================	================================
4	================================	================================	================================
5	================================	================================	================================
6	================================	================================	================================
7	================================	================================	================================
8	????????????????????????????????	????????????????????????????????	????????????????????????????????
9	????????????????????????????????	????????????????????????????????	????????????????????????????????
10	????????????????????????????????	????????????????????????????????	????????????????????????????????
11	????????????????????????????????	????????????????????????????????	????????????????????????????????
12	????????????????????????????????	????????????????????????????????	????????????????????????????????
13	????????????????????????????????	????????????????????????????????	================================
14	????????????????????????????????	????????????????????????????????	================================
15	????????????????????????????????	????????????????????????????????	================================
16	????????????????????????????????	????????????????????????????????	????????????????????????????????
17	????????????????????????????????	????????????????????????????????	????????????????????????????????
18	????????????????????????????????	????????????????????????????????	================================
19	================================	????????????????????????????????	================================
20	================================	????????????????????????????????	================================
21	================================	????????????????????????????????	================================
22	================================	????????????????????????????????	================================
23	================================	================================	================================
24	================================	================================	????????????????????????????????
25	================================	================================	================================
26	================================	================================	????????????????????????????????
27	================================	================================	================================
28	================================	================================	================================
29	================================	================================	================================
30	================================	================================	================================
31	================================	================================	================================
32	================================	================================	================================
33	================================	================================	================================
34	================================	================================	================================
35	================================	================================	================================
36	================================	================================	================================
37	================================	================================	================================
38	================================	================================	================================

SFS Collision Attack on 39-step SHA-256

2. **Minimize the Hamming weight of ΔA_i.** Under the

$$\delta A_{19\le i\le 38} = 0, \delta E_{23\le i\le 38} = 0, \sum_{i=0}^{38} \mathbf{H}(\Delta W_i) = t_w$$

find the minimal value of $t_A = \sum_{i=0}^{38} \mathbf{H}(\Delta A_i)$ such that there exists a solution. Still, we only aim at the minimal value t_A, and do not fix $(\Delta W_i, \Delta A_i, \Delta E_i)$.

i	ΔA_i	ΔE_i	ΔW_i
-4	==========	==========	
-3	==========	==========	
-2	==========	==========	
-1	==========	==========	
0	==========	==========	==========
1	==========	==========	==========
2	==========	==========	==========
3	==========	==========	==========
4	==========	==========	==========
5	==========	==========	==========
6	==========	==========	==========
7	==========	==========	==========
8	??????????	??????????	??????????
9	??????????	??????????	??????????
10	??????????	??????????	??????????
11	??????????	??????????	??????????
12	??????????	??????????	??????????
13	??????????	??????????	==========
14	??????????	??????????	==========
15	??????????	??????????	==========
16	??????????	??????????	??????????
17	??????????	??????????	??????????
18	??????????	??????????	==========
19	==========	??????????	==========
20	==========	??????????	==========
21	==========	??????????	==========
22	==========	??????????	==========
23	==========	==========	==========
24	==========	==========	??????????
25	==========	==========	==========
26	==========	==========	??????????
27	==========	==========	==========
28	==========	==========	==========
29	==========	==========	==========
30	==========	==========	==========
31	==========	==========	==========

SFS Collision Attack on 39-step SHA-256

Search for the 39-step differential trail:

3. **Minimize the Hamming weight of ΔE_i.** In addition to the conditions at Step 2, we further add the condition $\sum_{i=0}^{38} \mathbf{H}(\Delta A_i) = t_A$. Under these conditions, find and output the solution of $(\Delta W_i, \Delta A_i, \Delta E_i)$ for $0 \leq i \leq 38$ that minimizes $\sum_{i=0}^{38} \mathbf{H}(\Delta E_i)$.

i	ΔA_i	ΔE_i	ΔW_i
-4	================================	================================	
-3	================================	================================	
-2	================================	================================	
-1	================================	================================	
0	================================	================================	================================
1	================================	================================	================================
2	================================	================================	================================
3	================================	================================	================================
4	================================	================================	================================
5	================================	================================	================================
6	================================	===0============================	================================
7	================================	===1========1======11======0===	================================
8	===u============================	unnn1=1110=0=0101==000=====1110=	===u============================
9	============n=u====u======n===	010n0n0111010nu01001un011n10n=10	======n===u==========u==========
10	================================	0101u1n=1n0n010=u0=11nuu=1u00=n1	===n============================
11	================================	=100010==0=0101=0===0010=10=1=0=	=======nn=======n===n===nn==uu=n
12	================================	=unn010000=1000011=00011==0=101=	============u=======nn=========
13	================================	10110nuuuuuuuuu0u101un000010n111	================================
14	================================	=111=0000000000=0=1=001111111=1=	================================
15	============================n===	1100110110100000001nuuuuuuuu001	================================
16	=======u=u=======u==============	010100unu000001001u1000110unn=n1	======n===u==========u==========
17	================================	11=0111u00nn=100110=u1u00unn000n	===n============================
18	===n============================	uuu1uuuu01000=110n000111101=0101	================================
19	================================	000u0n1000101=0un01=1100=u11n000	================================
20	================================	011100un0u001unnnn11000000001111	================================
21	================================	=110=111=0===000=1=======1==1===	================================
22	================================	=nuu==0110===00101=0110=====110=	================================
23	================================	=000============================	================================
24	================================	=111============================	=======n=n=======n==============
25	================================	================================	================================
26	================================	================================	===u============================
27	================================	================================	================================
28	================================	================================	================================
29	================================	================================	================================
30	================================	================================	================================
31	================================	================================	================================
32	================================	================================	================================
33	================================	================================	================================
34	================================	================================	================================
35	================================	================================	================================

SFS Collision Attack on 39-step SHA-256

Finding a conforming message pair:

1. Extract all the constraints on (W_i, A_i, E_i) for this differential trail.
2. Add these constraints to the SAT/SMT model for the value transitions of SHA-256.
3. Solve the model find a solution of these variables.

The 39-step SHA-256 SFS colliding message pair (M, M')

CV	02b19d5a	88e1df04	5ea3c7b7	f2f7d1a4	86cb1b1f	c8ee51a5	1b4d0541	651b92e7
M	c61d6de7 f72b8c2f	755336e8 0def947c	5e61d618 a0eab159	18036de6 8021370c	a79f2f1d 4b0d8011	f2b44c7b 7aad07f6	4c0ef36b 33cd6902	a85d45cf 3bad5d64
M'	c61d6de7 e72b8c2f	755336e8 0fcf907c	5e61d618 b0eab159	18036de6 81a1bfc1	a79f2f1d 4b098611	f2b44c7b 7aad07f6	4c0ef36b 33cd6902	a85d45cf 3bad5d64
hash	431cadcd	ce6893bb	d6c9689a	334854e8	3baae1ab	038a195a	ccf54a19	1c40606d

The First Practical FS Collision for 40-step SHA-224

In SHA-224, the last one output word $(E_{60} + E_{-4})$ was truncated. We inject differences in E_{-4} and (W_0, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{17}, W_{18}, W_{25}, W_{27}) to mount a FS collision attack. The searching strategy is almost the same as the 39-step SHA-256.

i	ΔA_i	ΔE_i	ΔW_i
-4	================================	===u============================	
-3	================================	================================	
-2	================================	================================	
-1	================================	================================	
0	================================	================================	===n============================
1	================================	================================	================================
2	================================	================================	================================
3	================================	================================	================================
4	================================	================================	================================
5	================================	================================	================================
6	================================	================================	================================
7	================================	0111============================	================================
8	================================	1000========10======1===1==1===	================================
9	===u============================	unnn1=0=00=0=00=01=1=100=0110=1=	===u============================
10	==============n=u====u======n===	100n0n110111=nu00011un101n11n=00	======n===u==========u==========
11	================================	0101u0n=1n0n010=u0=10nun=1u01=n1	===n============================
12	================================	=10001000010001=0===0110=10=1=0=	=======nn=======n===n===nn==uu=u
13	================================	=unn00000001100011=00011==0=101=	==============u=======nn========
14	================================	11100nuuuuuuuuu1u=01un000001n001	================================
15	================================	=111=0000000000=0=1=001111111=1=	================================
16	============================n===	1100110111010000000101nuuuuuuuu001	================================
17	=======u=u=======u==============	010100unu000001001u1000110unn=n1	======n===u==========u==========
18	================================	1100111u00nn=100110=u1u00unn000n	===n============================
19	===n============================	uuu1uuuu01000=110n000111101=0101	================================
20	================================	000u0n1000101=0un01=1100=u11n000	================================
21	================================	011100un1u001unnnn11000000101111	================================
22	================================	=110=111=0===11101=======1==1===	================================
23	================================	=nuu==0110===00101=0110=====110=	================================
24	================================	=000============================	================================
25	================================	=111============================	=======n=n=======n==============
26	================================	================================	================================
27	================================	================================	===u============================
28	================================	================================	================================
29	================================	================================	================================
30	================================	================================	================================
31	================================	================================	================================
32	================================	================================	================================
33	================================	================================	================================
34	================================	================================	================================
35	================================	================================	================================
36	================================	================================	================================
37	================================	================================	================================
38	================================	================================	================================
39	================================	================================	================================

The FS colliding message pair for 40-step SHA-224

The 40-step SHA-224 FS colliding message pair (M, M')

CV	791c9c6b	baa7f900	f7c53298	9073cbbd	c90690c5	5591553c	43a5d984	af92402d
CV'	791c9c6b	baa7f900	f7c53298	9073cbbd	c90690c5	5591553c	43a5d984	bf92402d
M	f41d61b4	ce033ba2	dd1bc208	a268189b	ee6bda2c	5ddbe94d	9675bbd3	32c1ba8a
	7eba797d	88b06a8f	3bc3015c	d36f38cc	cfcb88e0	3c70f7f3	faa0c1fe	35c62535
M'	e41d61b4	ce033ba2	dd1bc208	a268189b	ee6bda2c	5ddbe94d	9675bbd3	32c1ba8a
	7eba797d	98b06a8f	39e3055c	c36f38cc	ce4b002d	3c74f1f3	faa0c1fe	35c62535
hash	9af50cac	c165a72f	b6f1c9f3	ef54bad9	af0cfb1f	57d357c9	c6462616	

The Collision Attacks on 31-Step SHA-512

Search for the 31-step differential trail:

1. Find a solution of $(\Delta W_i)_{0\leq i\leq 30}$ with the minimal $\sum_{i=0}^{30} \mathbf{H}(\Delta W_i)$, while keeping the minimal $\mathbf{H}(\Delta W_{16})$ and $\mathbf{H}(\Delta W_{18})$, which allows a local collision in the message expansion.

i	ΔA_i	ΔE_i	ΔW_i
-4	==========	==========	
-3	==========	==========	
-2	==========	==========	
-1	==========	==========	
0	==========	==========	==========
1	==========	==========	==========
2	==========	==========	==========
3	==========	==========	==========
4	==========	==========	==========
5	??????????	??????????	??????????
6	??????????	??????????	??????????
7	??????????	??????????	??????????
8	??????????	??????????	??????????
9	??????????	??????????	??????????
10	??????????	??????????	==========
11	==========	??????????	==========
12	==========	??????????	==========
13	==========	??????????	==========
14	==========	??????????	==========
15	==========	==========	==========
16	==========	==========	??????????
17	==========	==========	==========
18	==========	==========	??????????
19	==========	==========	==========
20	==========	==========	==========
21	==========	==========	==========
22	==========	==========	==========
23	==========	==========	==========
24	==========	==========	==========
25	==========	==========	==========
26	==========	==========	==========
27	==========	==========	==========
28	==========	==========	==========
29	==========	==========	==========
30	==========	==========	==========

The Collision Attacks on 31-Step SHA-512

Search for the 31-step differential trail:

2. With the fixed solution of $(\Delta W_i)_{0\leq i\leq 30}$ obtained at Step 1, find a valid solution of $(\Delta A_i, \Delta E_i)_{0\leq i\leq 30}$. We expect to find the smallest possible $\sum_{i=0}^{30} \mathbf{H}(\Delta A_i) = tr$ in a reasonable time at this step.

i	ΔA_i	ΔE_i	ΔW_i
-4	==========	==========	
-3	==========	==========	
-2	==========	==========	
-1	==========	==========	
0	==========	==========	==========
1	==========	==========	==========
2	==========	==========	==========
3	==========	==========	==========
4	==========	==========	==========
5	??????????	??????????	??????????
6	??????????	??????????	??????????
7	??????????	??????????	??????????
8	??????????	??????????	??????????
9	??????????	??????????	??????????
10	??????????	??????????	==========
11	==========	??????????	==========
12	==========	??????????	==========
13	==========	??????????	==========
14	==========	??????????	==========
15	==========	==========	==========
16	==========	==========	??????????
17	==========	==========	==========
18	==========	==========	??????????
19	==========	==========	==========
20	==========	==========	==========
21	==========	==========	==========
22	==========	==========	==========
23	==========	==========	==========
24	==========	==========	==========
25	==========	==========	==========
26	==========	==========	==========
27	==========	==========	==========
28	==========	==========	==========
29	==========	==========	==========
30	==========	==========	==========

The Collision Attacks on 31-Step SHA-512

Search for the 31-step differential trail:

3. With the fixed solution of $(\Delta A_i, \Delta W_i)_{0\le i\le 30}$, find a valid solution of $(\Delta E_i)_{0\le i\le 30}$ with the minimal $\sum_{i=0}^{30} \mathbf{H}(\Delta E_i)$, which allows a 31-step collision attack.

i	ΔA_i	ΔE_i	ΔW_i
-4	==	==	
-3	==	==	
-2	==	==	
-1	==	==	
0	==	==	==
1	==	==	==
2	==	==	==
3	==	==	==
4	==	==	==
5	??	??	??
6	??	??	??
7	??	??	??
8	??	??	??
9	??	??	??
10	??	??	==
11	==	??	==
12	==	??	==
13	==	??	==
14	==	??	==
15	==	==	==
16	==	==	??
17	==	==	==
18	==	==	??
19	==	==	==
20	==	==	==
21	==	==	==
22	==	==	==
23	==	==	==
24	==	==	==
25	==	==	==
26	==	==	==
27	==	==	==
28	==	==	==
29	==	==	==
30	==	==	==

The Collision Attacks on 31-Step SHA-512

It is found that the obtained 31-step differential trail is invalid. Therefore, we propose a method to correct this obtained 31-step differential trail.

The Collision Attacks on 31-Step SHA-512

Correct the 31-step differential trail:

1. Set $(\Delta E_i)_{5\leq i\leq 7}$ as unknown variables. For the remaining $(\Delta E_i)_{0\leq i\leq 30}$ where $i \notin \{5,6,7\}$, keep them the same as those in the obtained solution. For $(\Delta A_i)_{0\leq i\leq 30}$ and $(\Delta W_i)_{0\leq i\leq 30}$, they are also kept the same as those in the obtained solution.

i	ΔA_i	ΔE_i	ΔW_i
-4	==	==	
-3	==	==	
-2	==	==	
-1	==	==	
0	==	==	==
1	==	==	==
2	==	==	==
3	==	==	==
4	==	==	==
5	=nunuuuuuu=====u=====u===unnnu===u=n=====u=====nn===unnnn====	??	==n=====n=====un======u=====u=nunnnnu======u====nn======u====
6	========n======u================un=======u=====unnnn====nuunn=	??	n0u011=01u=====0n====10n====un=============n====uu===u=u=nuuuuu=
7	=n=====nunnu=u=u=u========u=uu=n=u=======nnn====n=====u=u====	??	=u=========n==========u====u==unn=n====u======n=0=1====u
8	==u	11110011001100u000100u1n00n0011==n=0000n=0nu0un0n1n00010n0111110	n=====nu=====u=====nu=====n======u=====u======u=========0=====
9	======================n===	11n1==111=0101110111011unn01000u0=011u1u00=0110010101=1==10101101	==========u==========n==========n======================n
10	==========u==========nu==========n====================nuu	==10==1===111=10u0==101=0n0==11==11010n11=1u=0110=0=0n==1101=nuu	==
11	==	=1u1======un0=n=nn===11001u==un====unnn0n==n=========u==u=10=100	==
12	==	=000======00n=1=11===10==u1==00===1010u11==1=========1==1==0=11u	==
13	==	==1=======110=1=01=======11==11====1111=1==0=========0==1======1	==
14	==	==========u==========n==========n====================n	==
15	==	==========0==========0==========0====================0	==
16	==	==========1==========1==========1====================1	======unnnnn====nuuuuuuuu=======nuuuu==========11====nuuuuuuuu
17	==	==	==
18	==	==	==========n==========u==========u====================u
19	==	==	==
20	==	==	==
21	==	==	==
22	==	==	==
23	==	==	==
24	==	==	==
25	==	==	==
26	==	==	==
27	==	==	==
28	==	==	==
29	==	==	==
30	==	==	==

The Collision Attacks on 31-Step SHA-512

Correct the 31-step differential trail:

2. Add the constraints describing the value transitions for $(A_i, E_i, W_i)_{7 \le i \le 12}$ to the model.

i	ΔA_i	ΔE_i	ΔW_i
-4	==	==	
-3	==	==	
-2	==	==	
-1	==	==	
0	==	==	==
1	==	==	==
2	==	==	==
3	==	==	==
4	==	==	==
5	=nunuuuuuu=====u=====u==unnnu==u=n=====u=====nn==unnnn====	??	==n======n=====un======u=====u=nunnnnu======u=====nn======u====
6	========n======u=================un=======u=====unnnn====nuunn=	??	n0u011=01u=====0n====10n====un=============n====uu===u=u=nuuuuu=
7	=n======nunnu==u=u========u==uu=n=u=======nnn====n=====u=u====	??	=u============n==========u====u==unn==n====u=======n=0=1====u
8	==u	1111001100110 0u000100u1n00n0011==n=0000n=0nu0un0n1n00010n0111110	n=====nu=====u=====nu=====n======u=====u======u=========0======
9	====================n==	11n1==111=0101110111011unn01000u0=011u1u00=0110010101=1==10101101	==========u==========n==========n====================n
10	==========u==========nu==========n====================nuu	==10==1===111=10u0==101=0n0==11==11010n11=1u=0110=0=0n==1101=nuu	==
11	==	=1u1======un0=n=nn===11001u==un====unnn0n==n=========u==u=10=100	==
12	==	=000======00n=1=11==10==u1==00==1010u11==1=========1==1==0=11u	==
13	==	==1=======110=1=01=======11==11====1111=1==0=========0==1======1	==
14	==	==========u==========n==========n====================n	==
15	==	==========0==========0==========0====================0	==
16	==	==========1==========1==========1====================1	=======unnnnn====nuuuuuuuuu=======nuuuuu=========11====nuuuuuuuu
17	==	==	==
18	==	==	==========n==========u==========u====================u
19	==	==	==
20	==	==	==
21	==	==	==
22	==	==	==
23	==	==	==
24	==	==	==
25	==	==	==
26	==	==	==
27	==	==	==
28	==	==	==
29	==	==	==
30	==	==	==

The Collision Attacks on 31-Step SHA-512

We utilize the degrees of freedom in $(\Delta E_i)_{5\leq i\leq 7}$ and the model for value transitions to correct an invalid 31-step differential trail.

i	ΔA_i	ΔE_i	ΔW_i
-4	==	==	
-3	==	==	
-2	==	==	
-1	==	==	
0	==	==	==
1	==	==	==
2	==	==	==
3	==	=11=00000====10=0=====000==101=0===1========0===1==1==011110====	==
4	==	=00011100=11101=1===10111==010=1===0===1=10=01=00==101101011=10=	==
5	=nunuuuuuu======u======u===unnnu===u=n======u======nn==unnnn====	uuu1nuuuuu101unnn10001ununnnnn1n=1unnu10=010u011nu0u11unnnnn1111	==n======n=====un======u=====u=nunnnnu======u=====nn======u====
6	========n=======u================un=======u=====unnnn====nuunn=	00nnnnnnu0unu0u0n111unnn101u010u0011110u0un0nn0uu11uun10n0nn1nu1	n0u011=01u=====0n====10n====un=============n====uu===u=u=nuuuuu=
7	=n======nunnu==u=u=========u==uu=n=u========nnn====n=====u=u====	u1uu11u1n0nuu1000nnu10uu1un1uu0u110un111110nu1uu0n1010011nn=uu1u	=u============n===========u====u==unn==n====u======n=0=1====u
8	==u	11110011001100u000100u1n00n0011==n=0000n=0nu0un0n1n00010n0111110	n=====nu=====u=====nu=====n======u=====u======u=========0======
9	==================n==	11n1==111=0101110111011unn01000u0=011u1u00=0110010101=1==10101101	===========u==========n==========n====================n
10	==========u==========nu==========n==================nuu	==10==1===111=10u0==101=0n0==11==11010n11=1u=0110=0=0n==1101=nuu	==
11	==	=1u1======un0=n=nn===11001u==un====unnn0n==n=========u==u=10=100	==
12	==	=000======00n=1=11===10==u1==00==1010u11==1========1==1==0=11u	==
13	==	==1=======110=1=01=======11==11====1111=1==0========0==1======1	==
14	==	==========u==========n==========n====================n	==
15	==	==========0==========0==========0====================0	==
16	==	==========1==========1==========1====================1	=======unnnnn====nuuuuuuuu=======nuuuuu=========11====nuuuuuuuu
17	==	==	==
18	==	==	==========n==========u==========u====================u
19	==	==	==
20	==	==	==
21	==	==	==
22	==	==	==
23	==	==	==
24	==	==	==
25	==	==	==
26	==	==	==
27	==	==	==
28	==	==	==
29	==	==	==
30	==	==	==

The Collision Attacks on 31-Step SHA-512

To demonstrate that the 31-step differential trail is valid, we provide a 31-step SFS collision message pair.

The SFS colliding message pair (M, M') for 31-step differential trail

CV	e8db5ea7aa921652	b99d911402b6f13b	d67789b44900bbd3	6dd99e5934fa4c36
	022c1b11afc030cd	0b5ab5d050736da3	6624b6d94833584f	0377be3bbc9ee6a9
M	c84e359a94cfa415	8b62e2794d50178a	cc95cf1218bc494a	000000404e263440
	4b1c2f410a70233a	2568946b7b20f000	8e82c5955ff61841	857f82c3b6494b6c
	c272b2af2a91b091	0a209a722f595461	958e7d6a665ca726	b82d422e9e59e3e3
	62188a13372b78d5	00074c63ff27970c	0810031ff62c060a	c007835890369005
M'	c84e359a94cfa415	8b62e2794d50178a	cc95cf1218bc494a	000000404e263440
	4b1c2f410a70233a	0529156e8728c010	2ec244995fe6dd3f	c57e82cbf80b496d
	4176aa8f6b93b091	0a289a322d595460	958e7d6a665ca726	b82d422e9e59e3e3
	62188a13372b78d5	00074c63ff27970c	0810031ff62c060a	c007835890369005
hash	18061dacede7a45d	8a673215307a0c75	ad7d40871fa4d4a5	cb84a2098efd50af
	fe74b9d90faa1325	989da85d39d29187	38eef206acaca3e0	d1fdba4c54da389f

More New Results for SHA-2

1. The first valid 28-step differential trail for SHA-512.

i	ΔA_i	ΔE_i	ΔW_i
-4	==	==	
-3	==	==	
-2	==	==	
-1	==	==	
0	==	==	==
1	==	==	==
2	==	==	==
3	==	==	==
4	==	==	==
5	==	==	==
6	==	=100=10=1011101=100010011=1000101=0==0=011==110==1001100=======0	==
7	==	=001=1100010011001000101O=111101001==10101110110001100000=0=0==01	==
8	====unnnnuuuuu=n======n=nn=u=u=nuuunuu==u=u==nuu=nuu=u=n=u=====un	=unnnnn0nuuuunu1nuuuuunununununnuuu0uuuunnun00nuu10nuunnuun101110u	======u=nuuuunu====nu=uunu=nn===nu=nuun=nn===nu==nu=u=n=u======u
9	====unnnn==nnnuuuuuuuuuuuuuuuuuuuuuu=====n====nuuu=nnuu======n==	1un01unn1nnunnuun0nuuuunu0unuu111un110ununununnnnn0nn10nn1u1u01nn	1000001unnnnn0110011=nuuuu========nuuuu==========nuuuuuuuuuuuuu
10	======unnnnnn==========nu=======nuuuuunuuuuuuuuuuuuuuuuuuuuuuuu	=01000=10111u1=0111=0=101n1011000100001111=01=1111011010100l0=nuu	==
11	==	=-u0100unnn00n1n0n11010101u000u=000=1011n10u010000010u0un0111101	==
12	==	=100=-=0111n10=1=1===11=-u1==10=======u=1=01====1===01=10====00u	==
13	==	==1====11110n1=101=======10===0=======0=1==1=====1===0=11======1	========n==========u==========n==================u==n===
14	==	==========0u==========n========0===n====================n	==
15	==	==========1=========0==========0=======================0	==
16	==	==========0=========1==========1=======================1	=======unnnnn====nuuuuuuuuu=======nuuuuu==========11====nuuuuuuuuu
17	==	==	==
18	==	==	==========n==========u==========u======================u
19	==	==	==
20	==	==	==
21	==	==	==
22	==	==	==
23	==	==	==
24	==	==	==
25	==	==	==
26	==	==	==
27	==	==	==

More New Results for SHA-2

2. The first collision for 28-step SHA-512.

The colliding message pair (M, M') for 28-step SHA-512

M	1f736d69a0368ef6	7277e5081ad1c198	e953a3cdc4cbe577	bd05f6a203b2f75f
	dd18b3e39f563fca	cad0a5bb69049fcd	4d0dd2a06e2efdc0	86db19c26fc2e1cf
	0184949e92cdd314	82fb3c1420112000	e4930d9b8295ab26	5500d3a2f30a3402
	26f0aa8790cb1813	a9c09c5c5015bc0d	53892c5a64e94edb	8e60d500013a1932
M'	1f736d69a0368ef6	7277e5081ad1c198	e953a3cdc4cbe577	bd05f6a203b2f75f
	dd18b3e39f563fca	cad0a5bb69049fcd	4d0dd2a06e2efdc0	86db19c26fc2e1cf
	037a8f464c0bb995	83033bd41e111fff	e4930d9b8295ab26	5500d3a2f30a3402
	26f0aa8790cb1813	a9809e5c4015bc45	53892c5a64e94edb	8e60d500013a1932
hash	dceb3d88adf54bd2	966c4cb1ab0cf400	01e701fdf10ab603	796d6e5028a5e89a
	f29a7517b216c09f	46dbae73b1db8cce	8ea44d45041010ea	26a7a6b902f2632f

More New Results for SHA-2

3. An improved 31-step differential trail for SHA-256 with fewer uncontrolled conditions.

i	ΔA_i	ΔE_i	ΔW_i
-4	================================	================================	
-3	================================	================================	
-2	================================	================================	
-1	================================	================================	
0	================================	================================	================================
1	================================	================================	================================
2	================================	================================	================================
3	================================	==========================10====	================================
4	================================	===========0===0========01===0	================================
5	==================n=unnnnnnn=n=	00011101000111110nu=11111unnnu1	===============nuuu=======0=uu=
6	========n====================u	101011=11==0n0==u11110==1110011n	==========u=====u===u======n===u
7	===u===n==n========n========n=u	un0u1100n=01u11111001u1=n110u10n	=u=u=======n=====n=nu=n=====nun=
8	============================n==	1u01un0u0=1=1=11n=0=u0=001001u0=	=u=nn==========u===u===u==1=====
9	================================	01100001110=0=010===00=11101u0=1	===============u==========1=u==
10	===============u===========u==	=1n1uuuuu0100=1un0=10unnnnnnn010	================================
11	================================	=01u1010uu1==11100===1000001n=0=	================================
12	================================	==110001=11====1n====0011110n=0=	================================
13	================================	===0====01======1===============	================================
14	================================	===============u==========0u==	================================
15	================================	===============0===========1==	================================
16	================================	===============1===========1==	============unnnunnnnnnnnnnnn==
17	================================	================================	================================
18	================================	================================	=============1=n=0==========n==
19	================================	================================	================================
20	================================	================================	================================
21	================================	================================	================================
22	================================	================================	================================
23	================================	================================	================================
24	================================	================================	================================
25	================================	================================	================================
26	================================	================================	================================
27	================================	================================	================================
28	================================	================================	================================
29	================================	================================	================================
30	================================	================================	================================

Summary

State size	Hash size	Attack type	Steps	Time	Memory	Year
256	All	collision	28	*practical*	\	2013
			31	$2^{65.5}$	2^{34}	2013
			31	$2^{49.8}$	2^{48}	**our**
		SFS collision	38	*practical*	\	2013
			39	***practical***	\	**our**
	256	FS collision	52	$2^{127.5}$	\	2012
	224	FS collision*	39	*practical*	\	2015
		FS collision	40	2^{110}	\	2012
		FS collision*	**40**	***practical***	\	**our**
512	All	collision	27	*practical*	\	2015
			28	***practical***	\	**our**
			31	$2^{115.6}$	$2^{77.3}$	**our**
		SFS collision	38	*practical*	\	2014
			39	*practical*	\	2015
	384	FS collision	40	2^{183}	\	2012
		FS collision*	41	*practical*	\	2015
	256	FS collision*	43	*practical*	\	2015
	224	FS collision*	44	*practical*	\	2015