Collisions Of SHA-0 and Reduced SHA-1

Eli Biham, Rafi Chen

Antoine Joux,

Patrick Carribault, Christophe Lemuet, and William Jalby

Presnted by: Nael Masalha

OUTLINE

- Neutral bits
- Multi-block technique
- Multi-block collisions of SHA-0
- A collision of 34-Round SHA-1
- A collision of 36-Round SHA-1
- Strength of Reduced Versions SHA-1 with More Rounds

NEUTRAL BITS

- This attack is based on the attack of Chabaud and Joux with enhancements that increase the probability of finding collisions and near collisions.
- The main idea is to start the attack from some intermediate round, thus eliminating the probabilistic behavior of prior rounds.
- In order to start the collision search from round r, we build a pair of messages M and M^* with a difference $M \oplus M^* = \Delta$, and with two additional properties.

NEUTRAL BITS

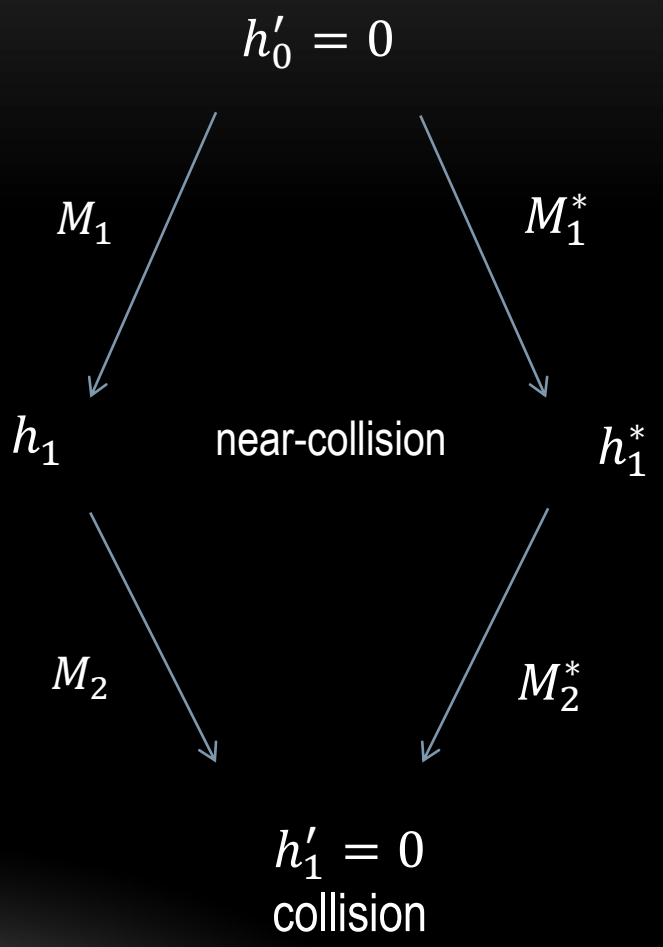
- **Definition 1.** Given the difference $\triangle$ of two messages, the attack of Chabaud and Joux defines the expected differences δ of the values of register A in each round. We say that a pair of messages *conforms to* δ_r if $A_i \oplus A_i^* = \delta_i$ for every $i \in \{1, \ldots, r\}$.
- **Definition 2.** Let M and M^* be a pair of messages that conforms to δ_r for some $r \geq 16$. We say that the *i'th* bit of the messages ($i \in \{0..511\}$) is a *neutral bit* with respect to M and M^* if the pair of messages received by complementing the *i'th* bits of M and M^* also conforms to δ_r.

THE MULTI-BLOCK TOOL

- Previous works on hash functions, and in particular on SHA, use only one block for the attack.
- This technique uses iterative process of SHA to find collisions.
- The idea of the technique is to start with a pair of blocks M_1 and M_1^* that create near collision h_1' and continue with a construction of second block.
- In the first block we base the message on a characteristic that has a zero input difference h_0' and a non-zero output difference h_1', with some message difference M_1'.
- In the second block we use a characteristic with a non-zero input difference h_1' and a zero output difference h_2'.

THE MULTI-BLOCK TOOL

- Given messages M_1 and M_1^* that conform to the first characteristic, we receive the pair of intermediate hash values h_1 and h_1^*.
- Using these values, we search for a second block M_2, M_2^* whose input values are h_1, h_1^*, and which conforms to the second characteristic.
- Such a pair will then have $h_2' = 0$, which means a collision after the second block.

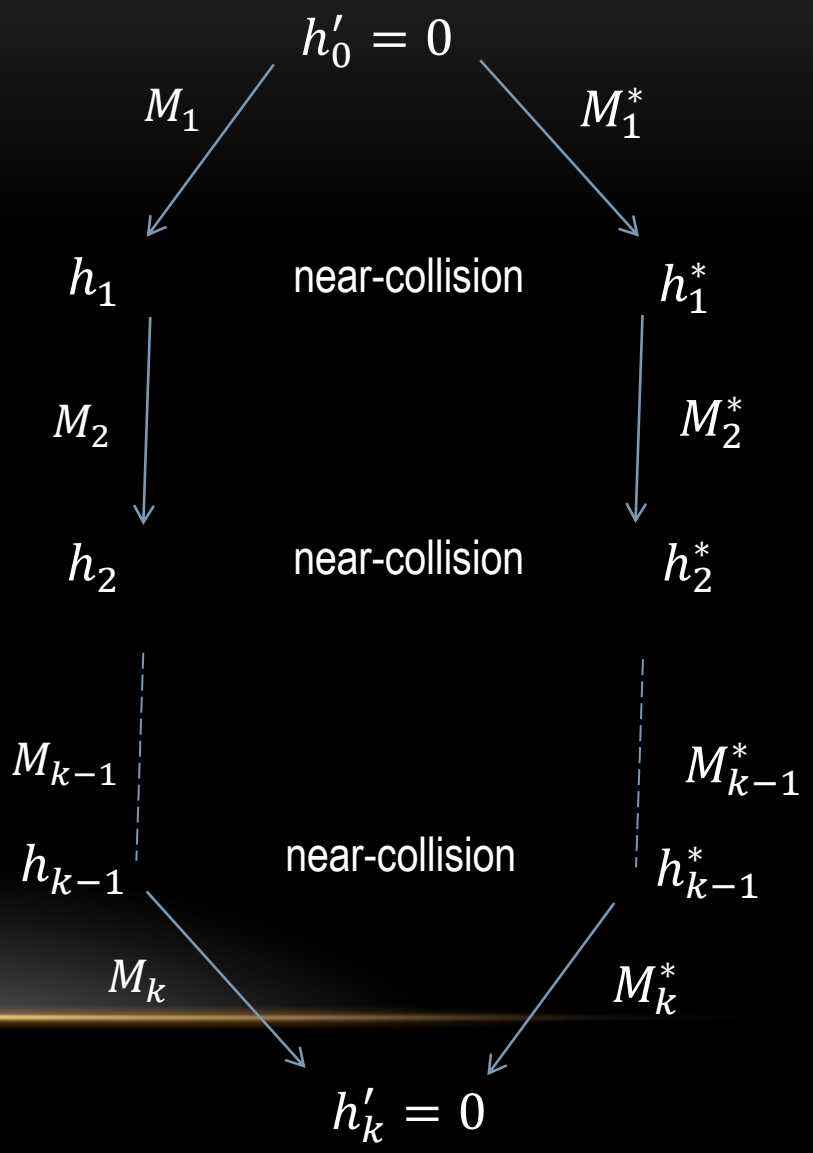


THE MULTI-BLOCK TOOL

- The multi-block tool is particularly useful when there is no characteristic that predicts a full collision in one block, and to reduce the complexity of an attack when a single-block collision is more complex.
- *Applications:* In order to illustrate the multi-block technique, we can apply to SHA-0 reduced to 50-rounds. This example is interesting, since this reduced version does not have any characteristic (i.e., any disturbance vector) that predicts a collision with a single block. However, it is very easy to find near-collisions with complexity of about 2^{17}. Using the multi-block technique, we can restart from this near-collision in order to find a longer message pair that collides after the second block. The total complexity remains about 2^{17}.

THE MULTI-BLOCK

- Collisions with More than Two Blocks
  This technique can be generalized to several blocks.



A MUTLTI-BLOCK COLLISIONS OF SHA-0

- Since the multi-block technique described above is very promising, it is extremely tempting to apply it to the full 80 rounds SHA-0.
- Unfortunately, contrarily to what happens with the 50-rounds version, there is no attack of this type which behaves better than the single block attack proposed by Chabaud and Joux.
- We should note that in the early rounds of SHA-0, an IF function is used. This means, that during the early rounds, SHA-0 may in some case behave differently than the linearized model. This misbehavior might allow us to connect differentials which do not belong together in the linearized model of SHA-0.
- For that we need the following two steps.

A MUTLTI-BLOCK COLLISIONS OF SHA-0

- First, remark that in each register A to E, after a successful application of a one block differential, a difference may occur at a single, fixed, position.
- In A and B a difference may occur at bit 1, in C, D and E at bit 31.
- To describe an initial or final difference, a 5-bit number suffices. We assign the high order bit to A and the low order bit to E. Thus, a state with a single difference D will be referred to as state 2.

A MUTLTI-BLOCK COLLISIONS OF SHA-0

- The second step is to compare the expected behavior of a reference state in the linearized model with the possible behaviors of a given state when the IF function is used, i.e., in real-life SHA-0. This is done by examining how the initial difference propagates in the five first rounds.
- Example, reference state 2 is compatible with real state 3.

A MUTLTI-BLOCK COLLISIONS OF SHA-0

- The attack, assume that the current state is a and that we are given a disturbance vector $a' \rightarrow b$, i.e., a disturbance that goes from reference state a' to expected state b, then if a is compatible with a', we have a differential that goes from state a to next state $a \oplus b$ after the final addition.
- Thus, we can build a transition graph, where each possible state is a node, and each differential, with good enough probability, is an edge. In this graph, we now search for a path from state 0 to itself, with low expected complexity.
- The best path we could find has length 4, it starts from state 0, goes to 3, 25, 8 and finally comes back to zero.

A MUTLTI-BLOCK COLLISIONS OF SHA-0

Ref (DV) States		DV	Actual States	Compatible With
$0 \rightarrow 3$	00000	00010000101001000111 10010110000011100000 00000011000000110110 00000110001011011000	$0 \rightarrow 3$	**2** 3
$2 \rightarrow 26$	01000	00010000101001000111 10010110000011100000 10000000000011000000 11011000000110001011	$3 \rightarrow 25$	**17** 18 28 31
$17 \rightarrow 17$	10001	00010000101001000111 10010110000011100000 00101100100000000001 11010011101000010001	$25 \rightarrow 8$	8 **11** 13 14
$11 \rightarrow 8$	11010	00010000101001000111 10010110000011100000 11100000000000110000 00110110000001100010	$8 \rightarrow 0$	

A MUTLTI-BLOCK COLLISIONS OF SHA-0

- Full 4-block Collision of SHA-0

a766a602 b65cffe7 73bcf258 26b322b3 d01b1a97 2684ef53 3e3b4b7f 53fe3762

24c08e47 e959b2bc 3b519880 b9286568 247d110f 70f5c5e2 b4590ca3 f55f52fe

effd4c8f e68de835 329e603c c51e7f02 545410d1 671d108d f5a4000d cf20a439

4949d72c d14fbb03 45cf3a29 5dcda89f 998f8755 2c9a58b1 bdc38483 5e477185

f96e68be bb0025d2 d2b69edf 21724198 f688b41d eb9b4913 fbe696b5 457ab399

21e1d759 1f89de84 57e8613c 6c9e3b24 2879d4d8 783b2d9c a9935ea5 26a729c0

6edfc501 37e69330 be976012 cc5dfe1c 14c4c68b d1db3ecb 24438a59 a09b5db4

35563e0d 8bdf572f 77b53065 cef31f32 dc9dbaa0 4146261e 9994bd5c d0758e3d

A MUTLTI-BLOCK COLLISIONS OF SHA-0

a766a602 b65cffe7 73bcf258 26b322b1 d01b1ad7 2684ef51 be3b4b7f d3fe3762
a4c08e45 e959b2fc 3b519880 39286528 a47d110d 70f5c5e0 34590ce3 755f52fc

6ffd4c8d 668de875 329e603e 451e7f02 d45410d1 e71d108d f5a4000d cf20a439
4949d72c d14fbb01 45cf3a69 5dcda89d 198f8755 ac9a58b1 3dc38481 5e4771c5

796e68fe bb0025d0 52b69edd a17241d8 7688b41f 6b9b4911 7be696f5 c57ab399
a1e1d719 9f89de86 57e8613c ec9e3b26 a879d498 783b2d9e 29935ea7 a6a72980

6edfc503 37e69330 3e976010 4c5dfe5c 14c4c689 51db3ecb a4438a59 209b5db4
35563e0d 8bdf572f 77b53065 cef31f30 dc9dbae0 4146261c 1994bd5c 50758e3d

A MUTLTI-BLOCK COLLISIONS OF SHA-0

IV	67452301	EFCDAB89	98BADCFE	10325476	C3D2E1F0
Block 1	83C1CE2D	C5BF5480	C2AF2358	104B337B	9E78A1E7
Block 2	27AE025A	9D36F7B6	29FA88E7	87B70063	984119F3
Block 3	4DD120B4	D6EC801F	468628A7	0CC26464	371F36B2
Block 4	81FB4643	08FDF1F4	A3C4F3A3	6188FED3	FD2378E6
Padding	C9F16077	7D4086FE	8095FBA5	8B7E20C2	28A4006B

IV	67452301	EFCDAB89	98BADCFE	10325476	C3D2E1F0
Block 1	83C1CE2D	C5BF5480	C2AF2358	904B337B	1E78A1E7
Block 2	27AE0258	9D36F7B4	29FA88E7	87B70063	184119F3
Block 3	4DD120B4	D6EC801D	468628A7	0CC26464	371F36B2
Block 4	81FB4643	08FDF1F4	A3C4F3A3	6188FED3	FD2378E6
Padding	C9F16077	7D4086FE	8095FBA5	8B7E20C2	28A4006B

A COLLISION OF 34-ROUND SHA-1

- The attacks of SHA-0 use only bit 1 as the location of disturbances. This bit is selected to eliminate the probabilistic behavior of the carry when corrections are applied to bit 31, thus increasing the total probability of the characteristic.
- Since the expansion process in SHA-0 does not mix bits in different locations in the 32-bit word, all the disturbances in the expanded message are in bit 1, but this is not the case in SHA-1.
- Therefore, other bits can be used as disturbances. With this change in the selection, a disturbance vector in SHA-1 is not boolean, in which each entry tells whether there is a disturbance in bit 1, but instead a 32-bit word that represents all the disturbances in a round.

A COLLISION OF 34-ROUND SHA-1

Rnd	D.Vec	D&C	Rnd	D.Vec	D&C	Rnd	D.Vec	D&C
-5	00000000		8	00000000	80000003	21	00000000	00000040
-4	00000000		9	00000002	40000002	22	00000002	00000000
-3	00000000		10	00000000	C0000040	23	00000000	80000040
-2	00000000		11	00000000	C0000002	24	00000000	80000002
-1	00000000		12	00000000	80000000	25	00000000	00000000
0	00000002	00000002	13	00000000	80000000	26	00000000	80000000
1	00000000	00000040	14	00000002	80000002	**27**	**00000000**	80000000
2	00000002	00000000	15	00000000	00000040	**28**	**00000000**	00000000
3	00000000	80000040	16	00000000	00000002	**29**	**00000000**	00000000
4	00000002	80000000	17	00000000	80000000	**30**	**00000000**	00000000
5	00000000	00000040	18	00000000	80000000	**31**	**00000000**	00000000
6	00000003	80000001	**19**	**00000000**	80000000	**32**	**00000000**	00000000
7	00000000	00000060	20	00000002	00000002	**33**	**00000000**	00000000

A COLLISION OF 34-ROUND SHA-1

Message 1:

F1641C2B 242BFDB5 EAE01E30 F4BBBA6F 18D45E8E DE68AEBA 74EC8CF9 FC204957

45AAA8BF 1CD3AE7D D845C2F3 AC737464 F25BEBBB BE5FFF1D 2ADB2818 0B1D13FB

Message 2:

F1641C29 242BFDF5 EAE01E30 74BBBA2F 98D45E8E DE68AEFA F4EC8CF8 FC204937

C5AAA8BC 5CD3AE7F 1845C2B3 6C737466 725BEBBB 3E5FFF1D AADB281A 0B1D13BB

A COLLISION OF 34-ROUND SHA-1

- Two Messages in ASCII Letters that Collide Under 34-Round SHA-1

Message 1:

IkGDqVMwISGGcBMpNHMYavPTsmUlykPTzokJOkwnrSgJSfDmIpeqsmDzWbAjmNxP

Message 2:

IkgDqRMwISGGcFEpNHEYarPTsmMlymPTzoSJOkSnrWkJSfhmIpmqsmLzWbijmJxP

- Two Examples of Partially Meaningful Messages that Collide Under 34-Round SHA-1

Message 1:

I Am OilMANgujnPay9164721363l4$USAkNOWwTkjepMFXGlmfHNGcpodElGfvL

Message 2:

I am KilMANgunfPay11607213.312$USASNOWSTknipMFtGlmnHNGkpodmlGbvL

Message 1:

OhG, not this mess,age notThat onenot U, oh noHRtBMTkKllLIIluvpB

Message 2:

Ohg, jot this$eess$aga notLhar oneVot q, kd nodRtBETkKdlLlalurpB

A COLLISION OF 36-ROUND SHA-1

- In our attack on 36-round SHA-1 we use the best characteristic that predicts a collision after one block.
- It should be noted that this characteristic cannot be used with the standard initial value of SHA-1, i.e., with: h0 = (67452301x; EFCDAB89x; 98BADCFEx; 10325476x; C3D2E1F0x) due to the observation that in round 2 there is a difference in the most significant bit of register B (B' = 80000000x), but both most significant bits of C and D are zero (where C = 67452301x << 30 and D = EFCDAB89x << 30). Thus, considering the differences of the messages (W_2' = 80000001x) in that bit, the new content of A must have a difference in this bit, in contrary to the prediction of the disturbance vector.
- After adding an additional first block, which in this case is the whole zero block (M_1 = M_1^* = 0). The resultant intermediate hash value is

  h1 = (37970DFFx; 5E912289x; C78B3705x; 923B82E9x; CC36E948x)

A COLLISION OF 36-ROUND SHA-1

Rnd	D.Vec	D&C	Rnd	D.Vec	D&C	Rnd	D.Vec	D&C
-5	00000000		9	00000002	00000008	23	00000000	80000050
-4	00000000		10	00000002	00000042	24	80000003	80000001
-3	00000000		11	80000000	50000042	25	00000000	A0000070
-2	00000000		12	00000002	10000010	26	00000000	20000003
-1	00000000		13	00000000	90000040	27	00000002	40000002
0	80000000	80000000	14	00000002	20000000	28	00000000	E0000040
1	00000000	00000010	15	00000000	20000040	29	00000000	E0000002
2	00000001	80000001	16	80000003	20000001	30	00000002	80000002
3	00000000	20000020	17	00000000	00000070	31	00000000	80000040
4	00000003	20000002	18	00000000	00000003	32	00000000	80000002
5	00000002	60000062	19	00000002	60000002	33	00000000	80000000
6	00000001	40000042	20	00000000	E0000040	34	00000000	80000000
7	00000002	80000020	21	00000000	E0000002	35	**00000000**	80000000
8	40000000	00000041	22	80000002	00000002			

A COLLISION OF 36-ROUND SHA-1

- The Second Block of the Collision of 36-Round SHA-1 (in 32-bit hex words)

Common block 1: sixteen 00000000 words
Message 1, block 2: 9F29DE8D BBD58270 1F11EB22 A6637C3E 7E6FB0C0 63E9BF5E C4FF7010 073174B3 3133689A 579A753E 2D17124D 7D37E853 5B5BBB01 F0371FBB 025A725C 8FB9FE33
Message 2, block 2: 1F29DE8D BBD58260 9F11EB23 86637C1E 5E6FB0C2 03E9BF3C 84FF7052 87317493 313368DB 579A7536 2D17120F 2D37E811 4B5BBB11 60371FFB 225A725C AFB9FE73

A COLLISION OF 36-ROUND SHA-1

Round	D&C	δ_{i+1}	A'_{i+1}	B'_{i+1}	C'_{i+1}	D'_{i+1}
0	80000000	80000000	80000000	00000000	00000000	00000000
1	00000010	00000000	00000000	80000000	00000000	00000000
2	80000001	00000001	00000001	00000000	20000000	00000000
3	20000020	00000000	00000000	00000001	00000000	20000000
4	20000002	**00000003**	**00000001**	00000000	40000000	00000000
5	60000062	00000002	00000002	00000001	00000000	40000000
6	40000042	00000001	00000001	00000002	40000000	00000000
7	80000020	00000002	00000002	00000001	80000000	40000000
8	00000041	40000000	40000000	00000002	40000000	80000000
9	00000008	00000002	00000002	40000000	80000000	40000000
10	00000042	00000002	00000002	00000002	10000000	80000000
11	50000042	80000000	80000000	00000002	80000000	10000000
12	10000010	00000002	00000002	80000000	80000000	80000000
13	90000040	00000000	00000000	00000002	20000000	80000000
14	20000000	00000002	00000002	00000000	80000000	20000000
15	20000040	00000000	00000000	00000002	00000000	80000000

STRENGTH OF REDUCED VERSIONS OF SHA-1 WITH MORE RESULTS

Rounds	SHA-1			NO-IF		
	HW	2B	NC	HW	2B	NC
34	2			2		
35	7	6	3	4	5	3
36	7	3	3	5	3	3
37	11	9	3	**5**	5	3
38	12	7	4	8	6	3
39	12	11	5	8	8	4
40	19	5	5	11	5	5
41	17	14	6	12	10	6
42	17	14	7	13	11	7
43	17	15	8	17	13	7
44	19	17	9	15	15	8
45	25	16	10	15	15	10
46	25	18	10	23	13	10
47	26	23	12	24	21	11

Rounds	SHA-1			NO-IF		
	HW	2B	NC	HW	2B	NC
48	28	25	13	14	14	13
49	32	22	15	14	14	14
50	35	29	16	14	14	14
51	38	26	19	15	15	15
52	42	32	19	16	16	15
53	42	32	20	16	16	16
54	39	42	24	36	34	16
55	39	48	27	39	38	16
56	41	39	28	41	29	16
57	61	56	29	42	23	17
58	58	52	29	42	17	17
59	64	53	29	51		17
60	45	45		29		18
61	45	38		30		19