SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

May 2016, Vol. 59 052110:1–052110:14
doi: 10.1007/s11432-015-5389-4

Evaluate the security margins of SHA-512, SHA-256 and DHA-256 against the boomerang attack

Hongbo YU*, Yonglin HAO & Dongxia BAI

Department of Computer Science and Technology, Tsinghua Universtiy, Beijing 100084*, China*

Received October 14, 2015; accepted December 19, 2015; published online March 10, 2016

Abstract For an n-bit random permutation, there are three types of boomerang distinguishers, denoted as Type I, II and III, with generic complexities 2^n, $2^{n/3}$ and $2^{n/2}$ respectively. In this paper, we try to evaluate the security margins of three hash functions namely SHA-512, SHA-256 and DHA-256 against the boomerang attack. Firstly, we give a boomerang attack on 48-step SHA-512 with a practical complexity of 2^{51}. The correctness of this attack is verified by providing a Type III boomerang quartet. Then, we extend the existing differential characteristics of the three hash functions to more rounds. We deduce the sufficient conditions and give thorough evaluations to the security margins as follows: Type I boomerang method can attack 54-step SHA-512, 51-step SHA-256 and 46-step DHA-256 with complexities 2^{480}, 2^{218} and 2^{236} respectively. Type II boomerang method can attack 51-step SHA-512, 49-step SHA-256 and 43-step DHA-256 with complexities $2^{158.50}$, $2^{72.91}$ and $2^{74.50}$ respectively. Type III boomerang method can attack 52-step SHA-512, 50-step SHA-256 and 44-step DHA-256 with complexities $2^{223.80}$, $2^{123.63}$ and $2^{99.85}$ respectively.

Keywords SHA-512, SHA-256, DHA-256, hash functions, boomerang attack

Citation Yu H B, Hao Y L, Bai D X. Evaluate the security margins of SHA-512, SHA-256 and DHA-256 against the boomerang attack. Sci China Inf Sci, 2016, 59(5): 052110, doi: 10.1007/s11432-015-5389-4

1 Introduction

Cryptographic hash functions play a significant role in the modern cryptology. They are indispensable in achieving secure systems such as digital signatures, message authentication codes and so on. In 2005, many famous hash functions, including MD5 and SHA-1, are broken due to the great breakthrough made by Wang et al. [1, 2]. The cryptanalysis of MD5 and SHA-1 has convinced many cryptographers that these widely deployed hash functions can no longer be considered secure. Therefore, the National Institute of Standards and Technology (NIST) proposed the transition from SHA-1 to the SHA-2 family. Furthermore, NIST also launched the SHA-3 competition [3] to develop a new hash standard.

Since NIST's proposal, the security margins of SHA-2 have been extensively studied. The two primary members of SHA-2 family, SHA-512 and SHA-256, are analyzed with different attacking methods such as preimage attack [4–6] and collision attack [7–12]. Besides, in order to enhance the security of SHA-256, a new 256-bit hash function called DHA-256 was also proposed at the Cryptography Hash Workshop hosted by NIST in November 2005 [13].

* Corresponding author (email: yuhongbo@mail.tsinghua.edu.cn)

Table 1 Boomerang results for SHA-512, SHA-256 and DHA-256

Name	Type	Target	Steps	Time	Bound	Source
SHA-512	**III**	**CF**[a)]	**48**	$\mathbf{2^{51}}$	$\mathbf{2^{256}}$	**Section 4**
	II	**CF**	**51**	$\mathbf{2^{158.50}}$	$\mathbf{2^{170.67}}$	
	III	**CF**	**53**	$\mathbf{2^{223.80}}$	$\mathbf{2^{256}}$	**Section 5**
	I	**KP**[b)]	**54**	$\mathbf{2^{480}}$	$\mathbf{2^{512}}$	
SHA-256	III	CF	46	2^{40}	2^{128}	[19]
	III	CF	47	2^{46}	2^{128}	[20]
	II	**CF**	**48**	$\mathbf{2^{72.91}}$	$\mathbf{2^{85.33}}$	
	III	**CF**	**50**	$\mathbf{2^{123.63}}$	$\mathbf{2^{128}}$	**Section 5**
	I	**KP**	**51**	$\mathbf{2^{218}}$	$\mathbf{2^{256}}$	
DHA-256	III	CF	42	2^{46}	2^{128}	[29]
	II	**CF**	**43**	$\mathbf{2^{74.50}}$	$\mathbf{2^{85.33}}$	
	III	**CF**	**44**	$\mathbf{2^{99.85}}$	$\mathbf{2^{128}}$	**Section 5**
	I	**KP**	**46**	$\mathbf{2^{236}}$	$\mathbf{2^{256}}$	

a) Compression function.
b) Keyed permutation.

On the other hand, the SHA-3 competition has attracted much attention from the cryptographic community. In fact, ever after the SHA-3 competition began, the cryptanalysis of the SHA-3 candidates were paid even more attention than SHA-2. After years' analysis, five proposals entered the final round of SHA-3 and among these Keccak became the new SHA-3 standard. During the campaign, many cryptanalytic attacks have been applied to hash functions and the cryptanalysis of hash functions has improved significantly. Researchers no longer limit their interests within the three classical security requirements namely preimage, second preimage and collision resistance. When analyzing hash functions, they now consider all non-random properties such as (semi-) free-start collisions, near-collisions, boomerang attacks and so on. Among these analytic methods, the boomerang method was introduced into the realm of hash function cryptanalysis quite late but has turned out to be fairly fruitful.

The original boomerang attack was introduced by Wagner in 1999 [14] as a tool for the cryptanalysis of block ciphers. It is an adaptive chosen plaintext and ciphertext attack utilizing differential cryptanalysis. Later, Kelsey et al. [15] developed the original version into a chosen plaintext attack called the amplified boomerang attack. Developments were also made by Biham et al. in [16] and [17].

During the past few years, the idea of the boomerang attack has been applied to many hash functions. Biryukov et al. [18] and Lamberger et al. [19] independently applied the boomerang attack to BLAKE-32 and SHA-256. The SHA-256 result was later improved by Biryukov et al. in [20]. Since then, we have seen boomerang results for many hash functions such as SIMD-512 [21], RIPEMD-128/160 [22], HAS-160 [23], Skein-256/512 [24,25], SM3 [26,27], BLAKE-256 [28] and DHA-256 [29]. The boomerang attack has become a common tool for analyzing various hash functions.

Related work. Biryukov et al. launched a boomerang attack on the 47-step SHA-256 with complexity 2^{46} in [20]. For DHA-256, there is also a boomerang result on the version reduced to 42 steps with a practical complexity 2^{46}. According to [24, 25], for an n-bit random permutation, there are three types of boomerang distinguishers, denoted as Type I, II and III, with generic complexities 2^n, $2^{n/3}$ and $2^{n/2}$ respectively. Obviously, the complexities of the existing results are far below the generic secure bounds.

Our contribution. We aim to determine how many rounds the boomerang distinguisher can mount without exceeding the generic secure bounds. We construct differential characteristics and give the first boomerang result on SHA-512 reduced to 48 steps with a practical complexity 2^{51}. Then, for SHA-512, SHA-256 and DHA-256, we extend the existing characteristics backward and forward. We deduce the sufficient conditions and evaluate the security margins of the three hash functions against boomerang attacks. Our analysis yields the following evaluations:

• Type I boomerang method can attack the keyed permutations of 54-step SHA-512, 51-step SHA-256 and 46-step DHA-256 with complexities 2^{480}, 2^{218} and 2^{236} respectively.

• Type II boomerang method can attack the compression functions of 51-step SHA-512, 49-step SHA-256 and 43-step DHA-256 with complexities $2^{158.50}$, $2^{72.91}$ and $2^{74.50}$ respectively.

• Type III boomerang method can attack the compression functions of 52-step SHA-512, 50-step SHA-256 and 44-step DHA-256 with complexities $2^{223.80}$, $2^{123.63}$ and $2^{99.85}$ respectively.

We list existing boomerang results along with ours in Table 1.

Organization of the paper. In Section 2, we briefly introduce the round functions of SHA-512, SHA-256 and DHA-256. Section 3 summaries the boomerang attack on hash functions. We describe our boomerang attack on 48-step SHA-512 in Section 4. In Section 5, we extend the differential characteristics and evaluate the security margins of the three hash functions against the boomerang attack. Finally, we conclude our paper in Section 6.

2 Preliminary

In this part, we briefly introduce our targeted hash functions. All three hash functions adopt the Merkel-Damgård structure [30] and they share many other structural similarities as well. Since our boomerang analysis mainly focuses on the keyed permutations, which excludes the Initialization and Finalization procedures, we only introduce the round functions in this section. We refer the readers to [31] for detailed descriptions of SHA-512 and SHA-256, and the complete specification of DHA-256 can be found in [13]. Before our descriptions, some notations have to be introduced in advance:

$+$ modular 2^{32} or 2^{64} addition (according to the word size);

$\oplus$ bitwise exclusive or;

$\ll^n$ shift n bits towards the most significant bit (padded by 0s);

$\gg^n$ shift n bits towards the least significant bit (padded by 0s);

$\lll^n$ cyclic shift n bits towards the most significant bit;

$\ggg^n$ cyclic shift n bits towards the least significant bit;

Besides, the commonly used bitwise boolean functions IF and MAJ are defined as

$$\begin{aligned}\mathrm{IF}(x,y,z) &= xy \oplus xz \oplus z,\\ \mathrm{MAJ}(x,y,z) &= xy \oplus xz \oplus yz.\end{aligned}$$

2.1 Description of SHA-512

SHA-512 processes 1024-bit input message blocks and produces a 512-bit hash value. The compression function of SHA-512 consists of a message expansion function and a state update transformation.

Message Expansion. The message expansion of SHA-512 splits the 1024-bit message block into 16 64-bit words namely $m_0, \ldots, m_{15}$, and expands them to 64 message words w_i as

$$w_i = \begin{cases} m_i, & 0 \leqslant i < 16,\\ \sigma_1(w_{i-2}) + w_{i-7} + \sigma_0(w_{i-15}) + w_{i-16}, & 16 \leqslant i < 80.\end{cases}$$

The function $\sigma_0(x)$ and $\sigma_1(x)$ are given as

$$\begin{aligned}\sigma_0(x) &= x^{\ggg 1} \oplus x^{\ggg 8} \oplus x^{\gg 7},\\ \sigma_1(x) &= x^{\ggg 19} \oplus x^{\ggg 61} \oplus x^{\gg 6}.\end{aligned}$$

State update transformation. The state update transformation starts from an initial value of 8 64-bit words $a_{-3}, \ldots, a_0$, $e_{-3}, \ldots, e_0$ and updates them in 80 steps. For the ith ($1 \leqslant i \leqslant 80$) step, the expanded message word w_i is used and two state variables e_i, a_i are updated as:

$$e_i = a_{i-4} + e_{i-4} + \Sigma_1(e_{i-1}) + \mathrm{IF}(e_{i-1}, e_{i-2}, e_{i-3}) + k_{i-1} + w_{i-1}, \tag{1}$$

$$a_i = e_i - a_{i-4} + \Sigma_0(a_{i-1}) + \mathrm{MAJ}(a_{i-1}, a_{i-2}, a_{i-3}), \tag{2}$$

where k_i is the step constant defined in [31]. The linear functions Σ_0 and Σ_1 are defined as:

$$\Sigma_0(x) = x^{\ggg 28} \oplus x^{\ggg 34} \oplus x^{\ggg 39},$$
$$\Sigma_1(x) = x^{\ggg 14} \oplus x^{\ggg 18} \oplus x^{\ggg 41}.$$

2.2 Description of SHA-256

SHA-256 operates on 32-bit words. Therefore, SHA-256 processes 512-bit input message blocks and produces a 256-bit hash value, half of that for SHA-512. The message expansion and state update function are similar to those of SHA-512.

Message expansion. The message expansion of SHA-256 splits the 512-bit message block into 16 32-bit words namely $m_0, \ldots, m_{15}$, and expands them to 64 message words w_i as

$$w_i = \begin{cases} m_i, & 0 \leqslant i < 16, \\ \sigma_1(w_{i-2}) + w_{i-7} + \sigma_0(w_{i-15}) + w_{i-16}, & 16 \leqslant i < 64. \end{cases}$$

The function $\sigma_0(x)$ and $\sigma_1(x)$ are given as

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

State update transformation. The state update transformation starts from an initial value of 8 32-bit words $a_{-3}, \ldots, a_0$, $e_{-3}, \ldots, e_0$ and updates them in 64 steps. For $1 \leqslant i \leqslant 64$, the update functions of e_i and a_i are the same as those in (1) and (2) respectively, except for the definitions of Σ_0 and Σ_1:

$$\Sigma_0(x) = x^{\ggg 2} \oplus x^{\ggg 13} \oplus x^{\ggg 22},$$
$$\Sigma_1(x) = x^{\ggg 6} \oplus x^{\ggg 11} \oplus x^{\ggg 25}.$$

2.3 Description of DHA-256

Same with SHA-256, DHA-256 operates on 32-bit words. It processes 512-bit input message blocks and produces a 256-bit hash value.

Message expansion. DHA-256 splits the 512-bit message block into 16 32-bit words namely $m_0, \ldots, m_{15}$, and expands them to 64 message words W_i as

$$w_i = \begin{cases} m_i, & 0 \leqslant i < 16, \\ \sigma_1(w_{i-1}) + w_{i-9} + \sigma_2(w_{i-15}) + w_{i-16}, & 16 \leqslant i < 64, \end{cases}$$

where $\sigma_0(x)$ and $\sigma_1(x)$ are defined as

$$\sigma_1(x) = x \oplus x^{\lll 7} \oplus x^{\ll 22},$$
$$\sigma_2(x) = x \oplus x^{\lll 13} \oplus x^{\ll 27}.$$

State update transformation. The state update transformation starts from an initial value of 8 32-bit words $d_{-3}, \ldots, d_0$, $h_{-3}, \ldots, h_0$ and updates them in 64 steps. For $1 \leqslant i \leqslant 64$, the update function of d_i and h_i are defined as:

$$h_i = d_{i-4}^{\lll 17} + SS_1(d_{i-1}) + \mathrm{IF}(d_{i-3}^{\lll 17}, d_{i-2}, d_{i-1}) + w_{i-1} + k_{i-1},$$
$$d_i = h_{i-4}^{\lll 2} + SS_2(h_{i-1}) + \mathrm{MAJ}(h_{i-3}^{\lll 2}, h_{i-2}, h_{i-1}) + w_{i-1} + k_{i-1},$$

where k_i is the step constant defined in [13] and the linear transformations SS_1 and SS_2 are defined by

$$SS_1(x) = x \oplus x^{\lll 11} \oplus x^{\lll 25},$$

$$SS_2(x) = x \oplus x^{\lll 19} \oplus x^{\lll 29}.$$

Note: In the remainder of this paper, the chaining variables in the rth step are denoted by V_r. For SHA-512 and SHA-256, V_r (where $r \in [0, 80]$ for SHA-512 and $r \in [0, 64]$ for SHA-256) is defined as

$$V_r = (a_r, a_{r-1}, a_{r-2}, a_{r-3}, e_r, e_{r-1}, e_{r-2}, e_{r-3}).$$

And for DHA-256, V_r ($r \in [0, 64]$) is defined as

$$V_r = (d_{r-3}, d_{r-2}, d_{r-1}, d_r, h_{r-3}, h_{r-2}, h_{r-1}, h_r).$$

3 The boomerang attack on hash functions

About the boomerang attack on hash functions, we mainly review the known-related-key boomerang method given in [20]. For MD structural SHA-512, SHA-256 and DHA-256, their compression function, denoted by CF, can be represented as

$$\mathrm{CF}(M, K) = E(M, K) + M, \tag{3}$$

where the input chaining variable M is fed forward to the output of a keyed permutation E. CF can be decomposed into two sub-functions as $\mathrm{CF} = \mathrm{CF}_1 \circ \mathrm{CF}_0$. In this manner, we can start from the middle steps since M and the key K can be chosen randomly [20,24]. Then we have a backward (top) differential characteristic $(\beta, \beta_k) \to \alpha$ with probability p for CF_0^{-1}, and a forward (bottom) differential characteristic $(\gamma, \gamma_k) \to \delta$ with probability q for CF_1. Finally, we can launch the known-related-key boomerang attack with these two differential characteristics as follows:

1. Randomly choose an intermediate state (X_1, K_1) and compute $(X_i, K_i), i = 2, 3, 4$ by $X_3 = X_1 + \beta$, $X_2 = X_1 + \gamma$, $X_4 = X_3 + \gamma$, and $K_3 = K_1 + \beta_k$, $K_2 = K_1 + \gamma_k$, $K_4 = K_3 + \gamma_k$.
2. Compute backward from (X_i, K_i) and obtain P_i by $P_i = \mathrm{CF}_0^{-1}(X_i, K_i)$ $(i = 1, 2, 3, 4)$.
3. Compute forward from (X_i, K_i) and obtain C_i by $C_i = \mathrm{CF}_1(X_i, K_i)$ $(i = 1, 2, 3, 4)$.
4. Check whether $P_3 - P_1 = P_4 - P_2 = \alpha$ and $C_2 - C_1 = C_4 - C_3 = \delta$.

It can be deduced that $P_3 - P_1 = P_4 - P_2 = \alpha$ and $C_2 - C_1 = C_4 - C_3 = \delta$ hold with probability at least p^2 in the backward direction and q^2 in the forward direction. Therefore, the attack succeeds with probability p^2q^2 when assuming that the differential characteristics are independent.

According to Yu et al. in [25], for an n-bit random permutation, there are three types of boomerang distinguishers:

- Type I: A quartet satifies $P_3 - P_1 = P_4 - P_2 = \alpha$ and $C_2 - C_1 = C_4 - C_3 = \delta$ for fixed differences α and δ. In this case, the generic complexity is 2^n.
- Type II: Only $C_2 - C_1 = C_4 - C_3$ is satisfied (This property is also called zero-sum or second-order differential collision). In this case, the complexity for obtaining such a quartet is $2^{n/3}$ [32].
- Type III: A quartet satisfied $P_3 - P_1 = P_4 - P_2$ and $C_2 - C_1 = C_4 - C_3$. In this case, the best known generic attack still takes time $2^{n/2}$.

According to our analysis, the results given in [20] and [29] are better than they claimed. The quartets they gave satisfy not only the requirement of Type II but that of Type III as well. Therefore, we categorize their results as Type III boomerang in Table 1.

4 The boomerang attack on 48-step SHA-512

In this section, we apply the boomerang attack to the SHA-512 compression function reduced to 48 steps. The basic idea of our attack is to connect two short differential characteristics in a quartet. The first step of our attack is to find two short differentials with high probabilities and connection part in the middle does not contain any contradictions. Secondly, we derive the sufficient conditions for the messages and chaining variables for the steps in the middle. Thirdly, we satisfy the conditions in the middle steps by

Table 2 The top differential characteristic used for boomerang attack on SHA-512

i	Δw_i	Δa_i	Δe_i
-3	-	23,25,30,36,46,50	25,30
-2	-		28,36
-1	-		
0		64	
1			23,46,50
2			
3			
4		64	64
5			
6			
7	64		
8–21			
22	56,63		
23	-	56,63	56,63

Table 3 The bottom differential characteristic used for boomerang attack on SHA-512

i	Δw_i	Δa_i	Δe_i
20	-		28,36,51,55,59,63
21	-	41	41
22	-	2,7,13,23,27,64	2,7
23	41		5,13
24			
25		41	
26			23,27,64
27			
28			
29			41
30			
31			
32	41		
33–46			
47	33,40		
48	-	33,40	33,40

modifying the chaining variables and the message words. Finally, after the message modification, we search the right quartets that pass the verification of the distinguisher.

The differential characteristics in this paper are described with the XOR difference represented in two forms as follows:

• Hex form: such as $\Delta v_r = 0$x8003 indicates that bits $v_{r,1}$, $v_{r,2}$, $v_{r,16}$ are active (having non-zero XOR difference).

• Numeric form: such as $\Delta v_r : 1, 2, 16$ is equivalent to $\Delta v_r = 0$x8003 in hex form. Besides, if $\Delta v_r = 0$x0 in hex form, we denoted by $\Delta v_r = \phi$ in numeric form.

4.1 Step-reduced differential characteristics

As shown in Table 2 and Table 3, we present the two differential characteristics used to construct the boomerang distinguisher on 48-step SHA-512, where the top differential characteristic is from step 23 to 1, and the bottom one is from step 24 to 48.

We start from the middle states of the distinguisher quartet, and the differences of the message words w_i and the chaining variables V_{23} of the top differential characteristic are selected as follows:

• $\Delta w_7 : 64, \Delta w_{22} : 56, 57, 63, \Delta w_i = \phi (0 \leqslant i \leqslant 21, i \neq 7)$, if the top characteristic has the differences in message words with this form, 18 steps (step 22 to 5) can be passed with probability 1 so that the characteristic of this type has higher probability than any other ones not following this strategy.

• $\Delta a_{23} : 56, 63$, Δe_{23}: 56, 63, these differences are decided by the choice of differences of the message words above. In order to cancel the differences of message words, we derive the differences of all these chaining variables.

Now for the bottom differential characteristic, we choose the differences as follows:

• $\Delta w_{23} : 41, \Delta w_{32} : 41, \Delta w_{47} : 33, 40, \Delta w_i = \phi$ $(24 \leqslant i \leqslant 46, i \neq 32)$, thus we can pass 14 steps (step 33 to 46) for free similarly.

• Δa_{22}: $2, 7, 13, 23, 27, 64$, Δa_{21}: 41, Δe_{23}: $5, 13$, Δe_{22}: $2, 7$, Δe_{21}: 41, $\Delta e_{20} : 28, 36, 51, 55, 59, 63$, according to the differences of message words above and also considering the compatibility with the top differential characteristic in the middle steps, the differences of chaining variables in the bottom characteristic can be derived with some sufficient conditions given in part of Table A1 and Table A2 in Appendix A.

Table 4 Message differences in steps 23 to 33

i	$\Delta w^{(1,2)}$	$\Delta w^{(1,3)}$
22	0x4180000000000000	0x0000008100000000
23	0x8000000000000000	0x0000010000000000
24	0x0502081000000002	0x0
25	0x0200100000000004	0x0
26	0x2804080001020010	0x0
27	0x1008000002000020	0x0
28	0x00825520891408a1	0x0
29	0xc184220110080140	0x0
30	0x0504804080200408	0x0
31	0x0001008000400800	0x0
32	0x2ab100a291089050	0x0000010000000000

4.2 Message differences

Let $w_i^{(1)}$ and $w_i^{(2)}$ $(0 \leqslant i \leqslant 15)$ be two 1024-bit messages whose differences are shown in Table 2. In order to carry out the message modification in the middle steps (steps 23–32), we also need to determine the specific differences $w_i^{(1)} \oplus w_i^{(2)}$ $(23 \leqslant i \leqslant 32)$.

For convenience, let $\Delta w_i^{(1,2)}$ denote the XOR difference of $w_i^{(1)}$ and $w_i^{(2)}$. According to the message expansion, we can compute the message differences $\Delta w_i^{(1,2)}$, $(22 \leqslant i \leqslant 47)$ as follows.

$$\begin{aligned}
\Delta w_{22}^{(1,2)} &= (\sigma_1(w_{20}^{(1)}) + w_{15}^{(1)} + \sigma_0(w_7^{(1)}) + w_8^{(1)}) \oplus (\sigma_1(w_{20}^{(2)}) + w_{15}^{(2)} + \sigma_0(w_7^{(2)}) + w_8^{(2)}),\\
\Delta w_{23}^{(1,2)} &= (\sigma_1(w_{21}^{(1)}) + w_{16}^{(1)} + \sigma_0(w_8^{(1)}) + w_9^{(1)}) \oplus (\sigma_1(w_{21}^{(2)}) + w_{16}^{(2)} + \sigma_0(w_8^{(2)}) + w_9^{(2)}),\\
&\cdots\\
\Delta w_{47}^{(1,2)} &= (\sigma_1(w_{45}^{(1)}) + w_{40}^{(1)} + \sigma_0(w_{32}^{(1)}) + w_{31}^{(1)}) \oplus (\sigma_1(w_{45}^{(2)}) + w_{40}^{(2)} + \sigma_0(w_{32}^{(2)}) + w_{31}^{(2)}).
\end{aligned}$$

Since $\sigma_0(w_7^{(1)}) \oplus \sigma_0(w_7^{(2)}) = \sigma_0(\Delta w_7^{(1,2)}) =$ 0x4180000000000000 and $\Delta w_{22}^{(1,2)} =$ 0x4180000000000000, the first equation holds if

$$w_{22,56}^{(1)} = w_{7,57}^{(1)} \oplus w_{7,63}^{(1)} \oplus w_{7,64}^{(1)}, \tag{4}$$

$$w_{22,57}^{(1)} = w_{7,58}^{(1)} \oplus w_{7,64}^{(1)} \oplus w_{7,1}^{(1)}, \tag{5}$$

$$w_{22,63}^{(1)} = w_{7,64}^{(1)} \oplus w_{7,9}^{(1)}. \tag{6}$$

In the same way, we set the differences $\Delta w_i^{(1,2)}$ $(23 \leqslant i \leqslant 32)$ in Table 4 and deduce the sufficient conditions on $w^{(1)}$ in Table A1 to meet the message expansion. Because we do not need to fulfill the message modifications in steps 34 to 48, the message differences $\Delta w_i^{(1,2)}$ in these steps can keep free.

For the bottom characteristic, the message differences $\Delta w_i^{(1,3)}$, $\Delta w_i^{(2,4)}$ $(22 \leqslant i \leqslant 47)$ are set in Table 3. In order to get $w_{47}^{(3)} - w_{47}^{(1)} = w_{47}^{(4)} - w_{47}^{(2)}$, according to the message expansion

$$w_{47} = w_{31} + \sigma_0(w_{32}) + w_{40} + \sigma_1(w_{45}),$$

the following three equations must be satisfied.

$$w_{32,41}^{(1)} \oplus w_{32,48}^{(1)} \oplus w_{32,47}^{(1)} = w_{32,41}^{(2)} \oplus w_{32,48}^{(2)} \oplus w_{32,47}^{(2)}, \tag{7}$$

$$w_{32,34}^{(1)} \oplus w_{32,41}^{(1)} \oplus w_{32,40}^{(1)} = w_{32,34}^{(2)} \oplus w_{32,41}^{(2)} \oplus w_{32,40}^{(2)}, \tag{8}$$

$$w_{32,35}^{(1)} \oplus w_{32,42}^{(1)} \oplus w_{32,41}^{(1)} = w_{32,35}^{(2)} \oplus w_{32,42}^{(2)} \oplus w_{32,41}^{(2)}. \tag{9}$$

The message difference $\Delta w_{32}^{(1,2)}$ we selected in Table 4 happens to meet (7)–(9). Otherwise, we can adjust it.

Extend the messages $w_i^{(3)}$ and $w_i^{(4)}$ $(22 \leqslant i \leqslant 47)$ in the backward direction. If we want to get $\Delta w_i^{(1,3)} = \Delta w_i^{(2,4)}$ $(0 \leqslant i \leqslant 22)$, the following three equations must be satisfied.

$$w_{22,56}^{(3)} = w_{7,57}^{(3)} \oplus w_{7,63}^{(3)} \oplus w_{7,64}^{(3)}, \tag{10}$$

$$w_{22,57}^{(3)} = w_{7,58}^{(3)} \oplus w_{7,64}^{(3)} \oplus w_{7,1}^{(3)}, \tag{11}$$

$$w_{22,63}^{(3)} = w_{7,64}^{(3)} \oplus w_{7,9}^{(3)}. \tag{12}$$

4.3 Message modification

Here message modification technique [1] can be used to modify the message words and chaining variables to satisfy the conditions of the middle steps to significantly improve the complexity of our attack.

For the middle steps (23 to 33) of the boomerang distinguisher, by modifying some certain message words and chaining variables, we can fulfill all the conditions of one side and part of the conditions of the other side of the bottom characteristic. After the message modification, the conditions of step 23 in the top differential characteristic can hold with probability 1, and the conditions of steps 24 to 33 in the bottom can hold with probability at least 2^{-40}.

4.4 Sketch of the attack

We divide our attack into two phases: the first phase is to find the right message words $w_{22}^{(1)}, \ldots, w_{32}^{(1)}$ and chaining variables $V_{23}^{(1)}$ so that the bottom characteristics of both sides in steps 23 to 33 hold; the second phase is to search $w_{17}^{(1)}, \ldots, w_{21}^{(1)}$ so that we can find a distinguisher quart. The sketch of attack is as follows.

1. Randomly select eleven 64-bit message words $w_i^{(1)}$ $(22 \leqslant i \leqslant 32)$, and a 512-bit chaining variable $V_{23}^{(1)}$. Modify the messages $w_i^{(1)}$ $(22 \leqslant i \leqslant 32)$ to meet the conditions in Table A1. Compute $V_i^{(1)}$ $(23 \leqslant i \leqslant 33)$. Modify $V_{23}^{(1)}$ and $w_i^{(1)}$ $(22 \leqslant i \leqslant 32)$ so that $V_i^{(1)}$ $(24 \leqslant i \leqslant 33)$ satisfies all the conditions in Table A2.

2. Let $w_i^{(2)} = w_i^{(1)} \oplus \Delta w_i^{(1,2)}$, $w_i^{(3)} = w_i^{(1)} \oplus \Delta w_i^{(1,3)}$, $w_i^{(4)} = w_i^{(2)} \oplus \Delta w_i^{(1,3)}$ $(22 \leqslant i \leqslant 32)$. The message differences $\Delta w_i^{(1,2)}$ and $\Delta w_i^{(1,3)}$ are defined in Table 4. Compute $V_i^{(j)}$ $(j = 2, 3, 4; 23 \leqslant i \leqslant 33)$. Check whether $V_{33}^{(1)} \oplus V_{33}^{(3)} = V_{33}^{(2)} \oplus V_{33}^{(4)} = \phi$. If yes, go to the next step. Otherwise, go back to step 1.

3. Select five 64-bit message words $w_i^{(1)}$ $(17 \leqslant i \leqslant 21)$ randomly. Let $w_i^{(2)} = w_i^{(1)} (17 \leqslant i \leqslant 21)$. Compute $w_i^{(1)}$ and $w_i^{(2)}$ $(33 \leqslant i \leqslant 47,\ 0 \leqslant i \leqslant 16)$ in forward and backward directions separately. Let $w_i^{(3)} = w_i^{(1)}$ and $w_i^{(4)} = w_i^{(2)}$ when $33 \leqslant i \leqslant 37$. Compute $w_i^{(3)}$ and $w_i^{(4)}$ when $38 \leqslant i \leqslant 47$ and $0 \leqslant i \leqslant 21$ by the message expansion.

4. Compute $V_{22}^{(j)}$, $V_{21}^{(j)}, \ldots, V_0^{(j)}$ $(j = 1, 2, 3, 4)$ in backward direction and $V_{34}^{(j)}$, $V_{35}^{(j)}, \ldots, V_{48}^{(j)}$ $(j = 1, 2, 3, 4)$ in forward direction. Check whether $V_0^{(2)} - V_0^{(1)} = V_0^{(4)} - V_0^{(3)}$ and $V_{48}^{(2)} - V_{48}^{(1)} = V_{48}^{(4)} - V_{48}^{(3)}$. If yes, output message block $M^{(j)} = (w_0^{(j)}, \ldots, w_{15}^{(j)})$ and initial state $V_0^{(j)}$ $(j = 1, 2, 3, 4)$. Otherwise, go to step 3.

4.5 Complexity of the attack

Based on the two differential characteristics and the message modification technique, we construct a 48-step boomerang distinguisher for SHA-512 compression function. The middle steps (23 to 33) of the boomerang distinguisher hold with probability 2^{-40}. Besides, the probability of steps 22 to 1 of the top differential characteristic is about 2^{-45} and for steps 34 to 48 of the bottom characteristic is 1. The probability of the message expansion is 2^{-6}. Hence, the complexity of the 48-step attack is $2^{40} + 2^{45} \times 2^6 \approx 2^{51}$ if we only get a zero-sum distinguisher, while the generic one is 2^{256}. An example of 48-step boomerang distinguisher for SHA-512 compression function is given in Table 5.

Table 5 Example of a quart satisfying $H(V_0^{(3)}, M^{(3)}) - H(V_0^{(1)}, M^{(1)}) - H(V_0^{(4)}, M^{(4)}) + H(V_0^{(2)}, M^{(2)}) = 0$ for 48 steps of the SHA-512 compression function

$V_0^{(1)}$	d51d68d22cd614bb	ad109f079123bc43	3e30194750de9356	b934d669f648b886
	2788083c8af206a4	f53a6844e79ca3ff	83333924f0fb45ee	aeca4ed80990f3c1
$V_0^{(2)}$	551d68d22cd614bb	ad109f079123bc43	be30194750de9356	3936f6621588b886
	a788083c8af206a4	753a4844e79ca3ff	0333591cf87b45ee	2ec84edfead0f3c1
$V_0^{(3)}$	3ca41aa7cc2ed702	d28a0787d13ece62	aaa0ccee378c5884	45960268826fa783
	126c152e3ed3c3d8	90227712dcb66469	c96f7308aa86be3c	5adecf0ca7c8cff9
$V_0^{(4)}$	bca41aa7cc2ed702	d28a0787d13ece62	2aa0ccee378c5884	c5982260a1afa783
	926c152e3ed3c3d8	10225712dcb66469	496f9300b206be3c	dadccf148908cff9
$M^{(1)}$	7897cf7f1c02fa18	c0e30c69c197577d	f6016b4df4a5101b	44cf12bc7c5f7f89
	d28a43112a41160f	a481e26554edd575	8a4f5ecd8ee90f42	0c10896df299f0a3
	8bd715591505422b	82f9e09643a6f94e	8ae783224a988778	d858b794e8b95a4a
	d98d2e211f08b5e3	3185a2321c2013d0	493b7695ecb8bc63	40dde2bb03f050f7
$M^{(2)}$	7897cf7f1c02fa18	c0e30c69c197577d	f6016b4df4a5101b	44cf12bc7c5f7f89
	d28a43112a41160f	a481e26554edd575	8a4f5ecd8ee90f42	8c10896df299f0a3
	8bd715591505422b	82f9e09643a6f94e	8ae783224a988778	d858b794e8b95a4a
	d98d2e211f08b5e3	3185a2321c2013d0	493b7695ecb8bc63	40dde2bb03f050f7
$M^{(3)}$	2ec928b5e9b2bae2	da67703373f8f947	c4c2b463d9c34453	a4d359b70a54809d
	829416361d1acc84	49208682435343aa	8a4c7b5efe34b2e8	d6bcd7d0a70c5663
	ef5a6123cadba871	a134d5cebfae6e21	e32944037719f06e	81033c0b86b9f18e
	9d4d5849a78a6aa9	4634d6dd6a193ca7	783f014e5106c88e	bcd2f996a68b63f7
$M^{(4)}$	2ec928b5e9b2bae2	da67703373f8f947	c4c2b463d9c34453	a4d359b70a54809d
	829416361d1acc84	49208682435343aa	8a4c7b5efe34b2e8	56bcd7d0a70c5663
	ef5a6123cadba871	a134d5cebfae6e21	e32944037719f06e	81033c0b86b9f18e
	9d4d5849a78a6aa9	4634d6dd6a193ca7	783f014e5106c88e	bcd2f996a68b63f7

5 Evaluate the security margins

We extend the existing differential characteristics backward or forward and deduce the number of sufficient conditions. With the message modification technique, many conditions in the intersection parts can be fixed and the complexities of the boomerang attacks decrease. Considering the effect of message modification, the complexities of the boomerang attacks are determined by the number of unfixed conditions in the differential characteristics. Therefore, we separately evaluate the security margins of the three hash functions as follows.

5.1 SHA-512

We extend the top differential characteristics given in Section 4 backward by 4 rounds and the bottom differential characteristic forward by 2 rounds. Our new top and bottom differential characteristics are shown as Tables A3 and A4 in Appendix A (the numbers of unfixed sufficient conditions are presented in the columns specified as "Cond." hereafter). The two characteristics can cover 54 steps in total. Then, we separately evaluate SHA-512's resistance against three types of boomerang attacks.

Type I: As shown, there are 88 and 152 unfixed conditions in the top and bottom characteristics respectively. For the 54-step Type I boomerang, the complexity can be directly deduced as $2^{2\times(88+152)} = 2^{480}$, which is less than the generic bound of 2^{512}.

Note: Due to the feeding forward operation (3), this Type I boomerang can only work on the keyed permutation E rather than on the entire compression function CF. This is also true for the Type I boomerang attacks on SHA-256 and DHA-256.

Type II: With an MD structure, the feeding forward operation (3) forces us to consider both the top

and bottom characteristics even when constructing a Type II boomerang quartet. We can start from V_2 (word block start from w_2) and end at step 53. There are 68 unfixed conditions in the top differential characteristic and 38 in the bottom one. In this way, we can acquire a 51-step Type II boomerang quartet with complexity $3^{68+32} \approx 2^{158.50}$, within the generic complexity of $2^{512/3} \approx 2^{170.67}$.

Type III: If we start from the state V_1 (word block start from w_1) and end at step 53, we can acquire a 52-step Type III boomerang quartet with complexity $3^{109+32} \approx 2^{223.80}$, within the generic complexity of $2^{512/2} = 2^{256}$.

5.2 SHA-256

For SHA-256, we extend the top differential characteristic of [20] backward by 3 rounds and the bottom differential characteristic forward by 1 round. New top and bottom differential characteristics are presented in Table A5 and Table A6 of Appendix A. The two characteristics can cover 51 steps.

Type I: The top and bottom characteristics have 69 and 40 sufficient conditions respectively. Therefore, the Type I boomerang attack on 51-step SHA-256 has a complexity of $2^{2\times(69+40)} = 2^{218}$, below the bound 2^{256}.

Type II: Starting from V_2 and ending at step 50, we can acquire 48-step Type II boomerang quartet with complexity $3^{37+9} \approx 2^{72.91}$, which is within the generic complexity of $2^{256/3} \approx 2^{85.33}$.

Type III: If we end at step 50, we can acquire a 50-step Type III boomerang quartet with complexity $3^{69+9} \approx 2^{123.63}$, slightly below the bound $2^{256/2} = 2^{128}$.

5.3 DHA-256

By using the same method with SHA-512 and SHA-256, we extend the top differential characteristic of [29] backward by 3 rounds and the bottom differential characteristic forward by 1 round. New top and bottom differential characteristics for DHA-256 are presented in Table A7 and Table A8 of Appendix A. The two characteristics can cover 46 steps.

Type I: The top characteristic has 72 unfixed conditions while the bottom has 46. The Type I boomerang method can mount to 46-step DHA-256 at a complexity of $2^{2\times(72+46)} = 2^{236}$, below the bound 2^{256}.

Type II: With the same method as SHA-512 and SHA-256, we can acquire a 43-step Type II boomerang quartet with complexity $3^{38+9} \approx 2^{74.50}$ by starting from V_2 and ending at step 45.

Type III: If we start from V_1 (word block start from w_1) and end at step 45, we can acquire a 44-step Type III boomerang quartet with complexity $3^{9+54} \approx 2^{99.85}$.

6 Conclusion

In this work, we propose the first boomerang attack on 48-step SHA-512 with a practical complexity of 2^{51}. This is the best practical result on SHA-512 to date. Then we theoretically draw the secure bounds of SHA-512, SHA-256 and DHA-256 against the boomerang attack by extending the existing differential characteristics and deducing the conditions. We give thorough evaluations to the security margins of three hash functions against all three types of boomerang attacks.

Acknowledgements This work was supported by National Basic Research Program of China (973 Program) (Grant No. 2013CB834205) and National Natural Science Foundation of China (Grant Nos. 61133013, 61373142).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Wang X Y, Yu H B. How to break MD5 and other hash functions. In: Proceedings of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 19–35

2 Wang X Y, Yin Y L, Yu H B. Finding collisions in the full SHA-1. In: Proceedings of 25th Annual International Cryptology Conference, Santa Barbara, 2005. 17–36

3 Kayser R F. Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family. Federal Register, 2007, 72: 62
4 Isobe T, Shibutani K. Preimage attacks on reduced Tiger and SHA-2. In: Proceedings of 16th International Workshop on Fast Software Encryption, Leuven, 2009. 139–155
5 Guo J, Ling S, Rechberger C, et al. Advanced meet-in-the-middle preimage attacks: first results on full Tiger, and improved results on MD4 and SHA-2. In: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2010. 56–75
6 Khovratovich D, Rechberger C, Savelieva A. Bicliques for preimages: attacks on Skein-512 and the SHA-2 Family. In: Proceedings of 19th International Workshop on Fast Software Encryption, Washington, DC, 2012. 244–263
7 Mendel F, Pramstaller N, Rechberger C, et al. Analysis of step-reduced SHA-256. In: Proceedings of 13th International Workshop on Fast Software Encryption, Graz, 2006. 126–143
8 Sanadhya S K, Sarkar P. New collision attacks against up to 24-step SHA-2. In: Proceedings of 9th International Conference on Cryptology in India, Kharagpur, 2008. 91–103
9 Nikolic I, Biryukov A. Collisions for step-reduced SHA-256. In: Proceedings of 15th International Workshop on Fast Software Encryption, Lausanne, 2008. 1–15
10 Indesteege S, Mendel F, Preneel B, et al. Collisions and other non-random properties for step-reduced SHA-256. In: Proceedings of 15th International Workshop on Selected Areas in Cryptography, Sackville, 2008. 276–293
11 Mendel F, Nad T, Schläffer M. Finding SHA-2 characteristics: searching through a minefield of contradictions. In: Proceedings of 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, 2011. 288–307
12 Mendel F, Nad T, Schläffer M. Improving local collisions: new attacks on reduced SHA-256. In: Proceedings of 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, 2013. 262–278
13 Lee J, Chang D, Kim H, et al. A new 256-bit hash function DHA-256: enhancing the security of SHA-256. In: Proceedings of Cryptographic Hash Workshop Hosted by NIST, 2005. https://cse.sc.edu/~buell/csce557/NIST_SHA/ChangD_DHA256.pdf
14 Wagner D. The boomerang attack. In: Proceedings of 6th International Workshop on Fast Software Encryption, Rome, 1999. 156–170
15 Kelsey J, Kohno T, Schneier B. Amplified boomerang attacks against reduced-round MARS and Serpent. In: Proceedings of 7th International Workshop on Fast Software Encryption, New York, 2000. 75–93
16 Biham E, Dunkelman O, Keller N. The rectangle attack—rectangling the Serpent. In: Proceeding of International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, 2001. 340–357
17 Biham E, Dunkelman O, Keller N. Related-Key boomerang and rectangle attacks. In: Proceedings of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 507–525
18 Biryukov A, Nikolic I, Roy A. Boomerang attacks on BLAKE-32. In: Proceedings of 18th International Workshop on Fast Software Encryption, Lyngby, 2011. 218–237
19 Lamberger M, Mendel F. Higher-order differential attack on reduced SHA-256. IACR Cryptology ePrint Archive. 2011. 37. https://eprint.iacr.org/2011/037.pdf
20 Biryukov A, Lamberger M, Mendel F, et al. Second-order differential collisions for reduced SHA-256. In: Proceedings of 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, 2011. 270–287
21 Mendel F, Nad T. Boomerang distinguisher for the SIMD-512 compression function. In: Proceedings of 12th International Conference on Cryptology in India, Chennai, 2011. 255–269
22 Sasaki Y, Wang L. Distinguishers beyond three rounds of the RIPEMD-128/-160 compression functions. In: Proceedings of 10th International Conference on Applied Cryptography and Network Security, Singapore, 2012. 275–292
23 Sasaki Y, Wang L, Takasaki Y, et al. Boomerang distinguishers for full HAS-160 compression function. In: Proceedings of 7th International Workshop on Security, Fukuoka, 2012. 156–169
24 Leurent G, Roy A. Boomerang attacks on hash function using auxiliary differentials. In: Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, 2012. 215–230
25 Yu H B, Chen J Z, Wang X Y. The boomerang attacks on the round-reduced Skein-512. In: Proceedings of 19th International Conference on Selected Areas in Cryptography, Windsor, 2012. 287–303
26 Kircanski A, Shen Y Z, Wang G L, et al. Boomerang and slide-rotational analysis of the SM3 hash function. In: Proceedings of 19th International Conference on Selected Areas in Cryptography, Windsor, 2012. 304–320
27 Bai D X, Yu H B, Wang G L, et al. Improved boomerang attacks on SM3. In: Proceedings of 18th Australasian Conference on Information Security and Privacy, Brisbane, 2013. 251–266
28 Bai D X, Yu H B, Wang G L, et al. Improved boomerang attacks on round-reduced SM3 and keyed permutation of BLAKE-256. IET Inf Secur, 2015, 9: 167–178
29 AlTawy R, Kircanski A, Youssef A M. Second order collision for the 42-step reduced DHA-256 hash function. Inf Process Lett, 2013, 113: 764–770
30 Menezes A, van Oorschot P C, Vanstone S A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996
31 US Department of Commerce. National Bureau of Standards, Secure Hash Algorithm, FIPS PUB 180-3. 2008
32 Wagner D. A generalized birthday problem. In: Proceedings of 22nd Annual International Cryptology Conference, Santa Barbara, 2002. 288–303

Appendix A

Table A1 The message conditions in $w_{22}^{(1)} - w_{32}^{(1)}$

Message	Conditions
$w_{22}^{(1)}$	$w_{22,15}^{(1)} = w_{22,14}^{(1)}$, $w_{22,44}^{(1)} = w_{22,43}^{(1)} \oplus w_{22,35}^{(1)} \oplus w_{22,34}^{(1)} \oplus w_{22,15}^{(1)} \oplus w_{22,14}^{(1)}$, $w_{22,48}^{(1)} = w_{22,47}^{(1)} \oplus w_{22,14}^{(1)} \oplus w_{22,15}^{(1)} \oplus w_{22,6}^{(1)} \oplus w_{22,5}^{(1)}$, $w_{22,57}^{(1)} = w_{22,56}^{(1)} \oplus 1$
$w_{23}^{(1)}$	$w_{23,41}^{(1)} = w_{22,33}^{(1)} \oplus w_{23,34}^{(1)} \oplus w_{23,40}^{(1)}$, $w_{23,42}^{(1)} = w_{23,40}^{(1)} \oplus w_{23,35}^{(1)} \oplus w_{23,34}^{(1)} \oplus 1$, $w_{23,48}^{(1)} = w_{23,40}^{(1)} \oplus w_{23,41}^{(1)} \oplus w_{23,47}^{(1)} \oplus 1$
$w_{24}^{(1)}$	$w_{24,2}^{(1)} = w_{22,21}^{(1)} \oplus w_{22,63}^{(1)} \oplus w_{22,8}^{(1)}$, $w_{24,37}^{(1)} = w_{22,57}^{(1)} \oplus w_{22,35}^{(1)} \oplus w_{22,44}^{(1)}$, $w_{24,37}^{(1)} = w_{22,57}^{(1)} \oplus w_{22,35}^{(1)} \oplus w_{22,44}^{(1)}$, $w_{24,44}^{(1)} = w_{22,63}^{(1)} \oplus w_{22,41}^{(1)} \oplus w_{22,50}^{(1)}$, $w_{24,50}^{(1)} = w_{22,6}^{(1)} \oplus w_{22,48}^{(1)} \oplus w_{22,57}^{(1)}$, $w_{24,57}^{(1)} = w_{22,12}^{(1)} \oplus w_{22,54}^{(1)} \oplus w_{22,63}^{(1)}$, $w_{24,59}^{(1)} = w_{22,15}^{(1)} \oplus w_{22,57}^{(1)}$
$w_{25}^{(1)}$	$w_{25,3}^{(1)} = w_{23,22}^{(1)} \oplus w_{23,64}^{(1)} \oplus w_{23,9}^{(1)}$, $w_{25,45}^{(1)} = w_{23,64}^{(1)} \oplus w_{23,42}^{(1)} \oplus w_{23,51}^{(1)}$, $w_{25,58}^{(1)} = w_{23,13}^{(1)} \oplus w_{23,55}^{(1)} \oplus w_{23,64}^{(1)}$
$w_{26}^{(1)}$	$w_{26,5}^{(1)} = w_{24,24}^{(1)} \oplus w_{24,2}^{(1)} \oplus w_{24,11}^{(1)}$, $w_{26,18}^{(1)} = w_{24,37}^{(1)} \oplus w_{24,15}^{(1)} \oplus w_{24,24}^{(1)}$, $w_{26,25}^{(1)} = w_{24,44}^{(1)} \oplus w_{24,22}^{(1)} \oplus w_{24,31}^{(1)}$, $w_{26,44}^{(1)} = w_{24,63}^{(1)} \oplus w_{24,41}^{(1)} \oplus w_{24,50}^{(1)}$, $w_{26,51}^{(1)} = w_{24,6}^{(1)} \oplus w_{24,48}^{(1)} \oplus w_{24,57}^{(1)}$, $w_{26,60}^{(1)} = w_{24,15}^{(1)} \oplus w_{24,57}^{(1)}$, $w_{26,62}^{(1)} = w_{24,17}^{(1)} \oplus w_{24,59}^{(1)}$
$w_{27}^{(1)}$	$w_{27,6}^{(1)} = w_{25,25}^{(1)} \oplus w_{25,3}^{(1)} \oplus w_{25,12}^{(1)}$, $w_{27,26}^{(1)} = w_{25,45}^{(1)} \oplus w_{25,23}^{(1)} \oplus w_{25,32}^{(1)}$, $w_{27,52}^{(1)} = w_{25,7}^{(1)} \oplus w_{25,49}^{(1)} \oplus w_{25,58}^{(1)}$, $w_{27,57}^{(1)} = w_{27,19}^{(1)} \oplus w_{27,39}^{(1)} \oplus w_{27,6}^{(1)} \oplus w_{24,44}^{(1)} \oplus 1$, $w_{27,61}^{(1)} = w_{25,16}^{(1)} \oplus w_{25,58}^{(1)}$
$w_{28}^{(1)}$	$w_{28,1}^{(1)} = w_{26,20}^{(1)} \oplus w_{26,62}^{(1)} \oplus w_{26,7}^{(1)}$, $w_{28,6}^{(1)} = w_{26,25}^{(1)} \oplus w_{26,3}^{(1)} \oplus w_{26,12}^{(1)}$, $w_{28,8}^{(1)} = w_{26,27}^{(1)} \oplus w_{26,5}^{(1)} \oplus w_{26,14}^{(1)}$, $w_{28,12}^{(1)} = w_{26,31}^{(1)} \oplus w_{26,9}^{(1)} \oplus w_{26,18}^{(1)}$, $w_{28,19}^{(1)} = w_{26,38}^{(1)} \oplus w_{26,16}^{(1)} \oplus w_{26,25}^{(1)}$, $w_{28,21}^{(1)} = w_{26,40}^{(1)} \oplus w_{26,18}^{(1)} \oplus w_{26,27}^{(1)}$, $w_{28,25}^{(1)} = w_{26,44}^{(1)} \oplus w_{26,22}^{(1)} \oplus w_{26,31}^{(1)}$, $w_{28,28}^{(1)} = w_{26,47}^{(1)} \oplus w_{26,25}^{(1)} \oplus w_{26,34}^{(1)}$, $w_{28,32}^{(1)} = w_{26,51}^{(1)} \oplus w_{26,29}^{(1)} \oplus w_{26,38}^{(1)}$, $w_{28,38}^{(1)} = w_{26,57}^{(1)} \oplus w_{26,35}^{(1)} \oplus w_{26,44}^{(1)}$, $w_{28,41}^{(1)} = w_{26,60}^{(1)} \oplus w_{26,38}^{(1)} \oplus w_{26,47}^{(1)}$, $w_{28,43}^{(1)} = w_{26,62}^{(1)} \oplus w_{26,40}^{(1)} \oplus w_{26,49}^{(1)}$, $w_{28,45}^{(1)} = w_{26,64}^{(1)} \oplus w_{26,42}^{(1)} \oplus w_{26,51}^{(1)}$, $w_{28,47}^{(1)} = w_{26,2}^{(1)} \oplus w_{26,44}^{(1)} \oplus w_{26,53}^{(1)}$, $w_{28,50}^{(1)} = w_{26,5}^{(1)} \oplus w_{26,47}^{(1)} \oplus w_{26,56}^{(1)}$, $w_{28,56}^{(1)} = w_{26,11}^{(1)} \oplus w_{26,53}^{(1)} \oplus w_{26,62}^{(1)}$
$w_{29}^{(1)}$	$w_{29,7}^{(1)} = w_{27,26}^{(1)} \oplus w_{27,4}^{(1)} \oplus w_{27,13}^{(1)}$, $w_{29,9}^{(1)} = w_{27,28}^{(1)} \oplus w_{27,6}^{(1)} \oplus w_{27,15}^{(1)}$, $w_{29,14}^{(1)} = w_{22,56}^{(1)} \oplus w_{24,59}^{(1)}$, $w_{29,15}^{(1)} = w_{22,57}^{(1)} \oplus w_{27,59}^{(1)} \oplus 1$, $w_{29,20}^{(1)} = w_{27,39}^{(1)} \oplus w_{27,17}^{(1)} \oplus w_{27,26}^{(1)}$, $w_{29,21}^{(1)} = w_{22,63}^{(1)} \oplus w_{24,2}^{(1)} \oplus w_{29,8}^{(1)} \oplus 1$, $w_{29,29}^{(1)} = w_{27,48}^{(1)} \oplus w_{27,26}^{(1)} \oplus w_{27,35}^{(1)}$, $w_{29,33}^{(1)} = w_{27,52}^{(1)} \oplus w_{27,30}^{(1)} \oplus w_{27,39}^{(1)}$, $w_{29,42}^{(1)} = w_{27,61}^{(1)} \oplus w_{27,39}^{(1)} \oplus w_{27,48}^{(1)}$, $w_{29,43}^{(1)} = w_{22,56}^{(1)} \oplus w_{24,37}^{(1)} \oplus w_{29,34}^{(1)}$, $w_{29,44}^{(1)} = w_{22,56}^{(1)} \oplus w_{29,34}^{(1)} \oplus w_{29,43}^{(1)} \oplus w_{22,57}^{(1)} \oplus w_{29,35}^{(1)} \oplus 1$, $w_{29,46}^{(1)} = w_{27,1}^{(1)} \oplus w_{27,43}^{(1)} \oplus w_{27,52}^{(1)}$, $w_{29,47}^{(1)} = w_{22,56}^{(1)} \oplus w_{24,50}^{(1)} \oplus w_{29,5}^{(1)}$, $w_{29,48}^{(1)} = w_{22,56}^{(1)} \oplus w_{29,6}^{(1)} \oplus w_{22,57}^{(1)} \oplus w_{29,5}^{(1)} \oplus w_{29,47}^{(1)}$, $w_{29,50}^{(1)} = w_{24,44}^{(1)} \oplus w_{29,41}^{(1)} \oplus w_{22,63}^{(1)}$, $w_{29,51}^{(1)} = w_{27,6}^{(1)} \oplus w_{27,48}^{(1)} \oplus w_{27,57}^{(1)}$, $w_{29,54}^{(1)} = w_{24,57}^{(1)} \oplus w_{29,12}^{(1)} \oplus w_{22,63}^{(1)}$, $w_{29,55}^{(1)} = w_{24,57}^{(1)} \oplus w_{29,13}^{(1)} \oplus w_{27,19}^{(1)} \oplus w_{27,61}^{(1)} \oplus 1$, $w_{29,56}^{(1)} = w_{22,56}^{(1)}$, $w_{29,57}^{(1)} = w_{22,57}^{(1)}$, $w_{29,58}^{(1)} = w_{29,6}^{(1)} \oplus w_{29,48}^{(1)} \oplus w_{29,57}^{(1)} \oplus w_{29,7}^{(1)} \oplus w_{29,49}^{(1)} \oplus 1$, $w_{29,63}^{(1)} = w_{22,63}^{(1)}$, $w_{29,64}^{(1)} = w_{27,19}^{(1)} \oplus w_{27,61}^{(1)}$
$w_{30}^{(1)}$	$w_{30,4}^{(1)} = w_{28,23}^{(1)} \oplus w_{28,1}^{(1)} \oplus w_{28,10}^{(1)}$, $w_{30,11}^{(1)} = w_{28,30}^{(1)} \oplus w_{28,8}^{(1)} \oplus w_{28,17}^{(1)}$, $w_{30,22}^{(1)} = w_{28,41}^{(1)} \oplus w_{28,19}^{(1)} \oplus w_{28,28}^{(1)}$, $w_{30,32}^{(1)} = w_{28,51}^{(1)} \oplus w_{28,29}^{(1)} \oplus w_{28,38}^{(1)}$, $w_{30,33}^{(1)} = w_{30,11}^{(1)} \oplus w_{30,20}^{(1)} \oplus w_{30,32}^{(1)} \oplus w_{30,10}^{(1)} \oplus w_{30,19}^{(1)} \oplus 1$, $w_{30,39}^{(1)} = w_{28,58}^{(1)} \oplus w_{28,36}^{(1)} \oplus w_{28,45}^{(1)}$, $w_{30,42}^{(1)} = w_{25,45}^{(1)} \oplus w_{25,3}^{(1)} \oplus w_{30,22}^{(1)} \oplus w_{30,9}^{(1)} \oplus w_{28,6}^{(1)} \oplus w_{28,48}^{(1)} \oplus w_{28,57}^{(1)}$, $w_{30,45}^{(1)} = w_{30,23}^{(1)} \oplus w_{30,32}^{(1)} \oplus w_{30,44}^{(1)} \oplus w_{30,22}^{(1)} \oplus w_{30,31}^{(1)} \oplus 1$, $w_{30,48}^{(1)} = w_{28,3}^{(1)} \oplus w_{28,45}^{(1)} \oplus w_{28,54}^{(1)}$, $w_{30,51}^{(1)} = w_{28,6}^{(1)} \oplus w_{28,48}^{(1)} \oplus w_{28,57}^{(1)}$, $w_{30,52}^{(1)} = w_{30,30}^{(1)} \oplus w_{30,39}^{(1)} \oplus w_{30,51}^{(1)} \oplus w_{30,29}^{(1)} \oplus w_{30,38}^{(1)}$, $w_{30,54}^{(1)} = w_{30,32}^{(1)} \oplus w_{30,41}^{(1)} \oplus w_{30,51}^{(1)} \oplus w_{30,29}^{(1)} \oplus w_{30,38}^{(1)} \oplus 1$, $w_{30,57}^{(1)} = w_{28,12}^{(1)} \oplus w_{28,54}^{(1)} \oplus w_{28,63}^{(1)}$, $w_{30,59}^{(1)} = w_{28,14}^{(1)} \oplus w_{28,56}^{(1)}$, $w_{30,64}^{(1)} = w_{25,3}^{(1)} \oplus w_{30,22}^{(1)} \oplus w_{30,9}^{(1)} \oplus 1$
$w_{31}^{(1)}$	$w_{31,12}^{(1)} = w_{29,31}^{(1)} \oplus w_{29,9}^{(1)} \oplus w_{29,18}^{(1)}$, $w_{31,23}^{(1)} = w_{29,42}^{(1)} \oplus w_{29,20}^{(1)} \oplus w_{29,29}^{(1)}$, $w_{31,40}^{(1)} = w_{29,59}^{(1)} \oplus w_{29,37}^{(1)} \oplus w_{29,46}^{(1)}$, $w_{31,49}^{(1)} = w_{29,4}^{(1)} \oplus w_{29,46}^{(1)} \oplus w_{29,55}^{(1)}$
$w_{32}^{(1)}$	$w_{32,5}^{(1)} = w_{30,24}^{(1)} \oplus w_{30,2}^{(1)} \oplus w_{30,11}^{(1)}$, $w_{32,7}^{(1)} = w_{30,26}^{(1)} \oplus w_{30,4}^{(1)} \oplus w_{30,13}^{(1)}$, $w_{32,13}^{(1)} = w_{30,33}^{(1)} \oplus w_{30,11}^{(1)} \oplus w_{30,20}^{(1)}$, $w_{32,16}^{(1)} = w_{30,35}^{(1)} \oplus w_{30,13}^{(1)} \oplus w_{30,22}^{(1)}$, $w_{32,20}^{(1)} = w_{30,39}^{(1)} \oplus w_{30,17}^{(1)} \oplus w_{30,26}^{(1)}$, $w_{32,25}^{(1)} = w_{30,45}^{(1)} \oplus w_{30,23}^{(1)} \oplus w_{30,32}^{(1)}$, $w_{32,29}^{(1)} = w_{30,48}^{(1)} \oplus w_{30,26}^{(1)} \oplus w_{30,35}^{(1)}$, $w_{32,32}^{(1)} = w_{30,51}^{(1)} \oplus w_{30,29}^{(1)} \oplus w_{30,38}^{(1)} \oplus 1$, $w_{32,34}^{(1)} = w_{30,51}^{(1)} \oplus w_{30,29}^{(1)} \oplus w_{30,38}^{(1)} \oplus 1$, $w_{32,38}^{(1)} = w_{30,57}^{(1)} \oplus w_{30,35}^{(1)} \oplus w_{30,44}^{(1)}$, $w_{32,40}^{(1)} = w_{30,59}^{(1)} \oplus w_{30,37}^{(1)} \oplus w_{30,46}^{(1)}$, $w_{32,47}^{(1)} = w_{23,47}^{(1)} \oplus 1$, $w_{32,49}^{(1)} = w_{30,4}^{(1)} \oplus w_{30,46}^{(1)} \oplus w_{30,55}^{(1)}$, $w_{32,53}^{(1)} = w_{30,8}^{(1)} \oplus w_{30,50}^{(1)} \oplus w_{30,59}^{(1)}$, $w_{32,54}^{(1)} = w_{30,9}^{(1)} \oplus w_{30,51}^{(1)} \oplus w_{30,60}^{(1)}$, $w_{32,56}^{(1)} = w_{30,11}^{(1)} \oplus w_{30,53}^{(1)} \oplus w_{30,62}^{(1)}$, $w_{32,58}^{(1)} = w_{27,58}^{(1)}$, $w_{32,60}^{(1)} = w_{30,15}^{(1)} \oplus w_{30,57}^{(1)}$, $w_{32,62}^{(1)} = w_{30,17}^{(1)} \oplus w_{30,59}^{(1)}$

Table A2 The conditions of chaining variables in the middle steps

Message	Conditions
23	$a^{(1)}_{23,56} = w^{(1)}_{22,56} \oplus 1$, $a^{(1)}_{23,62} = w^{(1)}_{22,63} \oplus a^{(1)}_{23,3} \oplus w^{(1)}_{22,56} \oplus a^{(1)}_{23,4} \oplus a^{(1)}_{23,57}$, $a^{(1)}_{23,63} = w^{(1)}_{22,63}$
	$a^{(1)}_{22,41} = a^{(1)}_{23,41}$
	$a^{(1)}_{21,2} = a^{(1)}_{23,2}$, $a^{(1)}_{21,7} = a^{(1)}_{23,7}$, $a^{(1)}_{21,13} = a^{(1)}_{23,13}$, $a^{(1)}_{21,23} = a^{(1)}_{23,23}$, $a^{(1)}_{21,27} = a^{(1)}_{23,27}$, $a^{(1)}_{21,63} = a^{(1)}_{22,63} \oplus 1$, $a^{(1)}_{21,64} = a^{(1)}_{23,64}$
	$e^{(1)}_{23,13} = a^{(1)}_{22,13} \oplus 1$, $e^{(1)}_{23,56} = w^{(1)}_{22,56} \oplus 1$, $e^{(1)}_{23,63} = w^{(1)}_{22,63}$
	$e^{(1)}_{22,2} = a^{(1)}_{22,2} \oplus 1$, $e^{(1)}_{22,7} = a^{(1)}_{22,7} \oplus 1$
	$e^{(1)}_{21,41} = a^{(1)}_{21,41}$, $e^{(1)}_{21,63} = e^{(1)}_{22,63}$
24	$a^{(1)}_{24,2} = a^{(1)}_{23,2}$, $a^{(1)}_{24,7} = a^{(1)}_{23,7}$, $a^{(1)}_{24,13} = a^{(1)}_{23,13}$, $a^{(1)}_{24,23} = a^{(1)}_{23,23}$, $a^{(1)}_{24,27} = a^{(1)}_{23,27}$, $a^{(1)}_{24,41} = a^{(1)}_{23,41}$, $a^{(1)}_{24,63} = a^{(1)}_{23,63} \oplus 1$, $a^{(1)}_{24,64} = a^{(1)}_{23,64}$
	$e^{(1)}_{24,2} = 1$, $e^{(1)}_{24,5} = 0$, $e^{(1)}_{24,7} = 1$, $e^{(1)}_{24,13} = 0$
25	$a^{(1)}_{25,41} = e^{(1)}_{21,41}$, $a^{(1)}_{25,36} = a^{(1)}_{25,30} \oplus e^{(1)}_{21,41} \oplus e^{(1)}_{22,2} \oplus 1$, $a^{(1)}_{25,46} = a^{(1)}_{25,35} \oplus e^{(1)}_{21,41} \oplus e^{(1)}_{22,7} \oplus 1$, $a^{(1)}_{25,52} = a^{(1)}_{25,47} \oplus e^{(1)}_{21,41} \oplus a^{(1)}_{22,13}$
	$e^{(1)}_{25,5} = 1$, $e^{(1)}_{25,13} = 0$, $e^{(1)}_{25,23} = e^{(1)}_{24,23} \oplus 1$, $e^{(1)}_{25,27} = e^{(1)}_{24,27}$, $e^{(1)}_{25,64} = e^{(1)}_{24,64}$
26	$e^{(1)}_{26,23} = a^{(1)}_{22,23}$, $e^{(1)}_{26,27} = a^{(1)}_{22,27}$, $e^{(1)}_{26,41} = a^{(1)}_{24,41}$, $e^{(1)}_{26,46} = e^{(1)}_{26,23} \oplus e^{(1)}_{26,19} \oplus e^{(1)}_{23,5} \oplus 1$, $e^{(1)}_{26,54} = e^{(1)}_{26,31} \oplus e^{(1)}_{26,27} \oplus e^{(1)}_{23,13} \oplus 1$, $e^{(1)}_{26,64} = e^{(1)}_{26,37} \oplus e^{(1)}_{26,41} \oplus e^{(1)}_{26,23} \oplus e^{(1)}_{24,23} \oplus 1$
27	$e^{(1)}_{27,23} = 0$, $e^{(1)}_{27,27} = 0$, $e^{(1)}_{27,64} = 0$
	$a^{(1)}_{27,41} = a^{(1)}_{26,41}$
28	$e^{(1)}_{28,23} = 1$, $e^{(1)}_{28,27} = 1$, $e^{(1)}_{28,41} = e^{(1)}_{27,41}$, $e^{(1)}_{28,64} = 1$
29	$e^{(1)}_{29,41} = a^{(1)}_{25,41}$, $e^{(1)}_{29,45} = e^{(1)}_{29,41} \oplus e^{(1)}_{29,4} \oplus e^{(1)}_{26,27} \oplus 1$, $e^{(1)}_{29,18} = e^{(1)}_{29,14} \oplus a^{(1)}_{25,41} \oplus e^{(1)}_{26,64} \oplus 1$, $e^{(1)}_{29,64} = e^{(1)}_{29,37} \oplus a^{(1)}_{25,41} \oplus e^{(1)}_{26,23} \oplus 1$
30	$e^{(1)}_{30,41} = 0$
31	$e^{(1)}_{31,41} = 1$

Table A3 The top characteristic of SHA-512

i	Δw_i	Cond.	Δa_i	Δe_i	Cond.
-3	-		36	23,25,30, 36,46,48, 50,56,62	36
-2	-		7,11,16, 18,22,48, 50,53,59	50	41
-1	-			10,14,18, 22,51,59	18
0	48,56,62	4	64	64	11
1	56,63	3	23,25,30, 36,46,50	25,30	12
2	64	1		28,36	8
3					4
4			64		4
5				23,46,50	4
6					1
7					1
8			64	64	1
9					
10					
11	64	3			
12–25					
26	56,63	fixed			fixed
27			56,63	56,63	

Table A4 The bottom characteristic of SHA-512

i	Δw_i	Cond.	Δa_i	Δe_i	Cond.
24	-			28,36,51,55,59,63	
25	-		41	41	
26	-		2,7,13,23,27,64	2,7	
27	41			5,13	
28					
29			41		
30		fixed		23,27,64	fixed
31					
32					
33				41	
34					
35					
36	41				
37–50					
51	33,40	3			
52	41	1	33,40	33,40	5
53	14,21,27, 34,36,43	6	1,5,12, 15,19,22, 26,56,58	15,19,22, 26,56,63	23
54	-		4,12,17,21,24, 27,34,36,47, 52,55,58,61	4,12,22,26, 27,34,36, 40,43,56,61	50

Table A5 The top characteristic of SHA-256

i	Δw_i	Cond.	Δa_i	Δe_i	Cond.
-3	-			2,6,11,17, 20,24,30	18
-2	-		3	3	13
-1	-		1,10,13, 22,24,29	1,22	12
0	3	1		13,17,23	7
1					4
2			3		4
3				10,24,29	4
4					1
5					1
6				3	1
7					
8					
9	3	3			
10–23					
24	17,28	fixed			fixed
25	-		17,28	17,28	

Table A6 The bottom characteristic of SHA-256

i	Δw_i	Cond.	Δa_i	Δe_i	Cond.
22	-			1,10,14,20,24,28	
23	-		25	25	
24	-		3,12,14,19,23,32	12,23	
25	25			3,7,13	
26		fixed			fixed
27			25		
28				14,19,32	
29					
30					
31				25	
32–48					
49	7,18,22	3			
50	25	1	7,18,22	7,18,22	6
51	-		1,4,8,13,16, 19,21,24,32	4,8,17,21, 25,27,32	30

Table A7 The top characteristic of DHA-256

i	Δw_i	Cond.	Δd_i	Δh_i	Cond.
-3	-		10,15	25,30	15
-2	-		7,15,21	7,21	16
-1	-		3,6,24,31	13,29,23,32	14
0	13,27,32	3			5
1	32		13	13	6
2			9,23	15,25	7
3					2
4					2
5			15	30	2
6					
7					
8	32				
9–22					
23	17,27,32	fixed			fixed
24	-		17,27,32	17,27,32	

Table A8 The bottom characteristic of DHA-256

i	Δw_i	Cond.	Δd_i	Δh_i	Cond.
21	-				
22	-		13	13	
23	-		23,9	15,25	
24					
25		fixed			fixed
26			15	30	
27					
28					
29	32				
30–43					
44	17,27,32	3			
45	2,7,13,17, 20,22,27	8	17,27,32	17,27,32	6
46	-		2,4,7,13, 19,22,24,29	2,6,7,10, 13,22,25	29