# Boomerang Attack on Step-Reduced SHA-512

Hongbo Yu*, Dongxia Bai

Department of Computer Science and Technology,
Tsinghua University, Beijing 100084, China
yuhongbo@mail.tsinghua.edu.cn
baidx10@mails.tsinghua.edu.cn

**Abstract.** SHA-2 (SHA-224, SHA-256, SHA-384 and SHA-512) is hash function family issued by the National Institute of Standards and Technology (NIST) in 2002 and is widely used all over the world. In this work, we analyze the security of SHA-512 with respect to boomerang attack. Boomerang distinguisher on SHA-512 compression function reduced to 48 steps is proposed, with a practical complexity of $2^{51}$. A practical example of the distinguisher for 48-step SHA-512 is also given. As far as we know, it is the best practical attack on step-reduced SHA-512.

**Key words:** SHA-512, hash functions, boomerang attack.

## 1 Introduction

Cryptographic hash functions play an important role in modern cryptology. In 2005, many notable hash functions, including MD5 and SHA-1, were broken by Wang *et al.* [32,33]. Since these breakthrough results, many cryptographers have been convinced that these widely used hash functions can no longer be considered secure. Hash functions have been the target in lots of cryptanalytic attacks and cryptanalysis against hash functions has been improved significantly. People not only evaluate the three classical security requirements (preimage resistance, 2nd preimage resistance and collision resistance), but also consider all properties different from the expectation of a random oracle, such as (semi-) free-start collisions, near-collisions, boomerang distinguishers, etc. This is an important progress of the cryptanalysis for hash functions, since the security margin can be measured.

In recent years, the SHA-3 competition [23] organized by NIST has attracted more attention from the cryptographic community. However, as commonly used algorithms in many applications, SHA-2 still deserves

* Author is supported by 973 program (No. 2013CB834205), the National Natural Science Foundation of China (Nos. 61133013 and 61373142), the Tsinghua University Initiative Scientific Research Program (No. 20111080970).

much detailed analysis to get a good view on its security. In this paper, we present boomerang attack on the reduced-step SHA-512.

**Related Work.** In the last few years, the security of SHA-256/512 against several attacks has been discussed in many papers. In [12] Isobe and Shibutani presented preimage attacks on SHA-256 and SHA-512 reduced to 24 steps. It was improved by Aoki *et al.* to 43-step SHA-256 and 46-step SHA-512 in [1]. Then Guo *et al.* gave advanced meet-in-the-middle preimage attacks on 42-step SHA-256/512 [10]. Later Khovratovich *et al.* applied biclique to preimages and extended attacks to 45 steps on SHA-256 and 50 steps on SHA-512[15]. Note that all these attacks only slightly faster than generic attack complexity $2^{256}$.

With respect to collision resistance, Mendel *et al.* presented the first collision attack on SHA-256 reduced to 18 steps in [21]. Then in [25] Nikolić and Biryukov improved the collision techniques and constructed a practical collision for 21 steps and a semi-free-start collision for 23 steps of SHA-256. This was later extended to 24 steps on SHA-256 and SHA-512 by Sanadhya and Sarkar [26], and Indesteege *et al.* [11]. Then Mendel *et al.* improved the semi-free-start collisions on SHA-256 from 24 to 32 steps and gave a collision attack for 27 steps, which are all practical [19]. The best known collision attacks on SHA-256 so far are semi-free-start collisions for 38 and collisions for 31 out of 64 steps by Mendel *et al.* in [20]. Recently, Eichlseder *et al.* presented semi-free-start collisions for SHA-512 on up to 38 steps in [8]. Compared with the preimage attacks, all these attacks have practical complexities.

At the rump session of Eurocrypt 2008, Yu and Wang presented non-randomness of SHA-256 reduced to 39 steps [34], and gave a practical example of 33 steps. In [11], Indesteege *et al.* show nonrandom behavior of the SHA-256 compression function in the form of free-start near-collisions for up to 31 steps. In [17], Lamberger and Mendel gave a second-order differential collision on 46 steps of SHA-256 compression function. Later, Biryukov *et al.* extended the result in [17] by one round and presented a practical attack on 47 steps of SHA-256 in [7] in which the application of the attack strategy to SHA-512 was discussed, but no detailed differentials and example were given.

**Our Contribution.** In this work, the boomerang attack is used to show non-random properties for 48 (out of 80) steps of SHA-512 and an example of a confirming quartet is given. To the best of our knowledge, this is the best practical attack on reduced SHA-512. The summary of previous results and ours on SHA-512 are given in Table 1.

**Table 1.** Summary of the attacks on SHA-512

| attack type | target | steps | time | source |
|---|---|---|---|---|
| preimage attack | HF | 24 | $2^{480}$ | [12] |
| | HF | 42 | $2^{501}$ | [1] |
| | HF | 46 | $2^{511.5}$ | |
| | HF | 42 | $2^{494.6}$ | [10] |
| | HF | 50 | $2^{511.5}$ | [15] |
| pseudo-preimage attack | HF | 24 | $2^{480}$ | [12] |
| | HF | 46 | $2^{509}$ | [1] |
| | HF | 57 | $2^{511}$ | [15] |
| collision | HF | 24 | $2^{53}$ | [11] |
| | HF | 24 | $2^{22.5}$ | [26] |
| semi-free-start collision | HF | 38 | $2^{40.5}$ | [8] |
| boomerang attack | CF | 48 | $2^{51}$ | Sect. 4 |

**Outline.** The structure of this paper is as follows. We give a short description of SHA-512 in Section 2. Section 3 summaries boomerang attack on hash functions. Then we present our boomerang attack on 48-step SHA-512 in Section 4. Finally, a conclusion of the paper is given in Section 5.

## 2 Description of SHA-2

The SHA-2 (SHA-224, SHA-256, SHA-384 and SHA-512) hash function family is standardized by the National Institute of Standards and Technology (NIST), and adopts the Merkle-Damgård structure [22]. This section gives a short description of SHA-512. A complete specification can be found in [24].

SHA-512 is an iterated hash function that 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 function.

The message expansion function splits the 1024-bit message block into 16 words $m_i$, $i = 0, \ldots, 15$, and expands them into 80 64-bit message words $w_i$ as follows:

$$w_i = \begin{cases} m_i, & 0 \leq i \leq 15, \\ \sigma_1(w_{i-2}) + w_{i-7} + \sigma_0(w_{i-15}) + w_{i-16}, & 16 \leq i \leq 79, \end{cases}$$

where the functions $\sigma_0(X)$ and $\sigma_1(X)$ are given by

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

The state update function updates 8 64-bit chaining values $v_i = (a_i, b_i, \ldots, h_i)$ in 80 steps using the 64-bit word $w_i$ as follows:

$$\begin{aligned}&t_1 = h_i + \Sigma_1(e_i) + F_1(e_i, f_i, g_i) + k_i + w_i,\\ &t_2 = \Sigma_0(a_i) + F_0(a_i, b_i, c_i),\\ &a_{i+1} = t_1 + t_2,\ b_{i+1} = a_i,\ c_{i+1} = b_i,\ d_{i+1} = c_i,\\ &e_{i+1} = d_i + t_1,\ f_{i+1} = e_i,\ g_{i+1} = f_i,\ h_{i+1} = g_i,\end{aligned}$$

where $k_i$ is a step constant and the function $F_0$, $F_1$, $\Sigma_0$, $\Sigma_1$ are defined as follows:

$$\begin{aligned}F_0(X, Y, Z) &= (X \wedge Y) \oplus (Y \wedge Z) \oplus (X \wedge Z),\\ F_1(X, Y, Z) &= (X \wedge Y) \oplus (\neg X \wedge Z),\\ \Sigma_0(X) &= (X \ggg 28) \oplus (X \ggg 34) \oplus (X \ggg 39),\\ \Sigma_1(X) &= (X \ggg 14) \oplus (X \ggg 18) \oplus (X \ggg 41).\end{aligned}$$

After 80 steps, the final hash value is computed by adding the output values to the initial state variables.

## 3 Boomerang Distinguishers of Hash Functions

The boomerang attack was introduced by Wagner in 1999 [31] against block ciphers. It treats the cipher as a cascade of two sub-ciphers, and uses short differentials in each sub-cipher. These differentials are combined in an adaptive chosen plaintext and ciphertext attack to exploit properties of the cipher that has high probability. Then Kelsey *et al.* [14] further developed it into a chosen plaintext attack called the amplified boomerang attack, and later it was developed by Biham *et al.* [4] into the rectangle attack. In [5], Biham *et al.* combined the boomerang (and the rectangle) attack with related-key differentials and proposed the related-key boomerang and rectangle attacks, which use the related-key differentials instead of the single-key differentials.

In recent years, the idea has been applied to hash functions as part of the new and useful hash function results. The first application presented in [13] used the idea of boomerang attack for the message modification technique in the collision attack for SHA-1. However, we note that this work does not build a boomerang property for a hash function to distinguish the hash functions from a random oracle, but only use the boomerang attack as a neutral bits tool for message modifications. The standard applications of boomerang attack to hash function were independently proposed by Biryukov *et al.* on BLAKE [6] and Lamberger and Mendel on the SHA-2 family [17]. In their works, the boomerang attacks are standalone distinguishers and work in the same way as for block ciphers - by producing the quartet of plaintexts and ciphertexts (input chaining values and output chaining values). Boomerang distinguishers have also been applied to SIMD-512 [18], HAVAL [27], RIPEMD [28], HAS-160 [29], Skein [9,35] and SM3 [16,3].

Let $H$ be the compression function of a hash function, $H_0$ and $H_1$ be two sub-ciphers: $H = H_1 \circ H_0$. The boomerang attack for a compression function can be summarized as follows.

- Choose a random chaining value $v^{(1)}$ and a message $w^{(1)}$, compute $v^{(2)} = v^{(1)} + \beta$, $v^{(3)} = v^{(1)} + \gamma$, $v^{(4)} = v^{(3)} + \beta$ and $w^{(2)} = w^{(1)} + \beta_w$, $w^{(3)} = w^{(1)} + \gamma_w$, $w^{(4)} = w^{(3)} + \beta_w$. We get a quartet $S = \{(v^{(i)}, w^{(i)}) | i = 1, 2, 3, 4\}$.
- Compute backward from the quartet $S$ using $H_0^{-1}$ to obtain the initial values $IV_1$, $IV_2$, $IV_3$ and $IV_4$.
- Compute forward from the quartet $S$ using $H_1$ to obtain the output values $h_1$, $h_2$, $h_3$ and $h_4$.
- Check whether $IV_2 - IV_1 = IV_4 - IV_3 = \alpha$ and $h_3 - h_1 = h_4 - h_2 = \delta$ are fulfilled.

The complexity of the boomerang attack is summarized in [9,35] as follows.

- Type I: A quartet satisfies $IV_2 - IV_1 = IV_4 - IV_3 = \alpha$ and $h_3 - h_1 = h_4 - h_2 = \delta$ for fixed $\alpha$ and $\delta$. In this case, the generic complexity is $2^n$ where $n$ is the size of hash value.
- Type II: Only $h_3 - h_1 = h_4 - h_2$ are required. This property is also called a second-order differential collision in [7]. In this case, the complexity for obtaining such a quartet is $2^{n/3}$ using Wagner's generalized birthday attack [30].
- Type III: A quartet satisfies $IV_2 - IV_1 = IV_4 - IV_3$ and $h_3 - h_1 = h_4 - h_2$. This property is also called a zero-sum distinguisher in [2]. In this case, the best known attack still takes time $2^{n/2}$.

## 4 The Boomerang Attack on Reduced 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 paths in a quartet. The first step of our attack is to find two short differentials with high probabilities and the middle 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 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.

### 4.1 Step-Reduced Differential Paths

As shown in Table 2 and Table 3, we present the two differential paths used to construct the boomerang distinguisher on 48-step SHA-512, where the top differential path is from step 23 to 1, and the bottom one is from step 24 to 48. To describe the differential paths, we utilize the XOR difference $\varDelta a = a \oplus a'$, and $\varDelta a : i(1 \leq i \leq 64)$ is used to denote that the $i$-th bit of $a$ is different from the $i$-th bit of $a'$, and the rest of the bits of $a$ and $a'$ are the same.

We start from the middle states of the distinguisher quartet $S$, and the differences of the message words $w_i$ and the chaining variables $v_{23} = (a_{23}, b_{23}, ..., h_{23})$ of the top differential path are selected as follows:

- $\varDelta w_7 : 64, \varDelta w_{22} : 56, 57, 63, \varDelta w_i = 0 (0 \leq i \leq 21, i \neq 7)$, if the top path has the differences in message words with this form, 18 steps (step 22 to 5) can be passed with probability 1 so that the path of this type has higher probability than any other ones not following this strategy.
- $\varDelta a_{23} : 56, 63$, $\varDelta e_{23}$: 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 path, we choose the differences as follows:

- $\varDelta w_{23} : 41, \varDelta w_{32} : 41, \varDelta w_{47} : 33, 40, \varDelta w_i = 0 (24 \leq i \leq 46, i \neq 32)$, thus we can pass 14 steps (step 33 to 46) for free similarly.
- $\varDelta b_{23}$: 2, 7, 13, 23, 27, 64, $\varDelta c_{23}$: 41, $\varDelta e_{23}$: 5, 13, $\varDelta f_{23}$: 2, 7, $\varDelta g_{23}$: 41, $\varDelta h_{23} = \varSigma_1(\varDelta e_{23})$, according to the differences of message words above and also considering the compatibility with the top differential path

in the middle steps, the differences of chaining variables in the bottom path can be derived with some sufficient conditions given in part of Table 6 and Table 7.

**Table 2.** The top differential path used for boomerang attack on SHA-512.

| step | $\Delta w_i$ | $\Delta a$ | $\Delta b$ | $\Delta c$ | $\Delta d$ | $\Delta e$ | $\Delta f$ | $\Delta g$ | $\Delta h$ |
|---|---|---|---|---|---|---|---|---|---|
| | | 64 | | | 23,25,30,36,46,50 | 0 | 0 | 28,36 | 25,30 |
| 1 | | | 64 | | | 23,46,50 | | | 28,36 |
| 2 | | | | 64 | | | 23,46,50 | | |
| 3 | | | | | 64 | | | 23,46,50 | |
| 4 | | | | | | 64 | | | 23,46,50 |
| 5 | | | | | | | 64 | | |
| 6 | | | | | | | | 64 | |
| 7 | | | | | | | | | 64 |
| 8 | 64 | | | | | | | | |
| 9-22 | | | | | | | | | |
| 23 | 56,57,63 | 56,63 | | | | 56,63 | | | |

**Table 3.** The bottom differential path used for boomerang attack on SHA-512.

| step | $\Delta w_i$ | $\Delta a$ | $\Delta b$ | $\Delta c$ | $\Delta d$ | $\Delta e$ | $\Delta f$ | $\Delta g$ | $\Delta h$ |
|---|---|---|---|---|---|---|---|---|---|
| 23 | 33,40 | | 2,7,13,23,27,64 | 41 | | 5,13 | 2,7 | 41 | $\Sigma_1(\Delta e_{23})$ |
| 24 | 41 | | | 2,7,13,23,27,64 | 41 | | 5,13 | 2,7 | 41 |
| 25 | | 41 | | | 2,7,13,23,27,64 | | | 5,13 | 2,7 |
| 26 | | | 41 | | | 23,27,64 | | | 5,13 |
| 27 | | | | 41 | | | 23,27,64 | | |
| 28 | | | | | 41 | | | 23,27,64 | |
| 29 | | | | | | 41 | | | 23,27,64 |
| 30 | | | | | | | 41 | | |
| 31 | | | | | | | | 41 | |
| 32 | | | | | | | | | 41 |
| 33 | 41 | | | | | | | | |
| 34-47 | | | | | | | | | |
| 48 | 33,40 | 33,40 | 0 | 0 | 0 | 33,40 | 0 | 0 | 0 |

### 4.2 Message Differences

Let $w_i^{(1)}$ and $w_i^{(2)}$ $(0 \leq i \leq 15)$ 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 $w_i^{(1)} \oplus w_i^{(2)}$ $(23 \leq i \leq 32)$.

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 $\Delta w_i^{(1,2)}$, $(22 \leq i \leq 47)$ as follows.

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

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

$$\begin{aligned}
w_{22,56}^{(1)} &= w_{7,57}^{(1)} \oplus w_{7,63}^{(1)} \oplus w_{7,64}^{(1)}, &(1)\\
w_{22,57}^{(1)} &= w_{7,58}^{(1)} \oplus w_{7,64}^{(1)} \oplus w_{7,1}^{(1)}, &(2)\\
w_{22,63}^{(1)} &= w_{7,64}^{(1)} \oplus w_{7,9}^{(1)}. &(3)
\end{aligned}$$

In the same way, we set the differences $\Delta w_i^{(1,2)}$ $(23 \leq i \leq 32)$ in the Table 4 and deduce the sufficient conditions on $w^{(1)}$ in Table 6 to meet the message expansion. Because we don't 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.

**Table 4.** Message differences in steps 23 to 33.

| $i$ | $\Delta w^{(1,2)}$ | $\Delta w^{(1,3)}$ |
|---|---|---|
| 22 | 4180000000000000 | 0000008100000000 |
| 23 | 8000000000000000 | 0000010000000000 |
| 24 | 0502081000000002 | 0 |
| 25 | 0200100000000004 | 0 |
| 26 | 2804080001020010 | 0 |
| 27 | 1008000002000020 | 0 |
| 28 | 00825520891408$a$1 | 0 |
| 29 | $c$184220110080140 | 0 |
| 30 | 0504804080200408 | 0 |
| 31 | 0001008000400800 | 0 |
| 32 | 2$ab$100$a$291089050 | 0000010000000000 |

For the bottom path, the message differences $\Delta w_i^{(1,3)}$, $\Delta w_i^{(2,4)}$ $(22 \leq i \leq 47)$ 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.

$$w_{32,41}^{(1)} \oplus w_{32,48}^{(1)} \oplus w_{32,47}^{(1)} = w_{32,41}^{(2)} \oplus w_{32,48}^{(2)} \oplus w_{32,47}^{(2)} \tag{4}$$
$$w_{32,34}^{(1)} \oplus w_{32,41}^{(1)} \oplus w_{32,40}^{(1)} = w_{32,34}^{(2)} \oplus w_{32,41}^{(2)} \oplus w_{32,40}^{(2)} \tag{5}$$
$$w_{32,35}^{(1)} \oplus w_{32,42}^{(1)} \oplus w_{32,41}^{(1)} = w_{32,35}^{(2)} \oplus w_{32,42}^{(2)} \oplus w_{32,41}^{(2)} \tag{6}$$

The message difference $\Delta w_{32}^{(1,2)}$ we selected in Table 4 happens to meet the equations (4)-(6). Otherwise, we can adjust it.

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

$$w_{22,56}^{(3)} = w_{7,57}^{(3)} \oplus w_{7,63}^{(3)} \oplus w_{7,64}^{(3)} \tag{7}$$
$$w_{22,57}^{(3)} = w_{7,58}^{(3)} \oplus w_{7,64}^{(3)} \oplus w_{7,1}^{(3)} \tag{8}$$
$$w_{22,63}^{(3)} = w_{7,64}^{(3)} \oplus w_{7,9}^{(3)} \tag{9}$$

### 4.3 Message Modification

Here message modification technique [33] 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 conditions of the other side of the bottom path. After the message modification, the conditions of step 23 in the top differential path 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 $w_{22}^{(1)}, ..., w_{32}^{(1)}$ and chaining variables $v_{23}^{(1)}$ so that the bottom paths of both sides in steps 23 to 33 hold; the second phase is to search $w_{17}^{(1)}, ..., w_{21}^{(1)}$ so that we can find a distinguisher quart. The sketch of attack is as follows.

1. Randomly select eleven 64-bit message words $w_i^{(1)}$ $(22 \le i \le 32)$, and a 512-bit chaining variables $v_{23}^{(1)} = (a_{23}^{(1)}, b_{23}^{(1)}, ..., h_{23}^{(1)})$. Modify the messages $w_i^{(1)}$ $(22 \le i \le 32)$ to meet the conditions in Table 6. Compute $v_i^{(1)}$ $(23 \le i \le 33)$. Modify $v_{23}^{(1)}$ and $w_i^{(1)}$ $(22 \le i \le 32)$ so that $v_i^{(1)}$ $(24 \le i \le 33)$ satisfy all the conditions in Table 7.
2. Let $w_i^{(2)} = w_i^{(1)} \oplus \Delta w_i^{(1,2)}$, $w_i^{(3)} = w_i^{(1)} \oplus \Delta w_i^{(1,3)}$, $w_i^{(4)} = w_i^{(2)} \oplus \Delta w_i^{(1,3)}$ $(22 \le i \le 32)$. The message differences $\Delta w_i^{(1,2)}$ and $\Delta w_i^{(1,3)}$ are defined in Table 4. Compute $v_i^{(j)}$ $(j = 2, 3, 4; 23 \le i \le 33)$. Check whether $v_{33}^{(1)} \oplus v_{33}^{(3)} = v_{33}^{(2)} \oplus v_{33}^{(4)} = 0$. If yes, goto the next step. Otherwise, go back to step 1.
3. Select five 64-bit message words $w_i^{(1)}$ $(17 \le i \le 21)$ randomly. Let $w_i^{(2)} = w_i^{(1)}(17 \le i \le 21)$. Compute $w_i^{(1)}$ and $w_i^{(2)}$ $(33 \le i \le 47, 0 \le i \le 16)$ in forward and backward directions separately. Let $w_i^{(3)} = w_i^{(1)}$ and $w_i^{(4)} = w_i^{(2)}$ when $33 \le i \le 37$. Compute $w_i^{(3)}$ and $w_i^{(4)}$ when $38 \le i \le 47$ and $0 \le i \le 21$ by the message expansion.
4. Compute $v_{22}^{(j)}$, $v_{21}^{(j)}$, ..., $v_0^{(j)}$ $(j = 1, 2, 3, 4)$ in backward direction and $v_{34}^{(j)}$, $v_{35}^{(j)}$, ..., $v_{48}^{(j)}$ $(j = 1, 2, 3, 4)$ 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 $w_i^{(j)}$ $(j = 1, 2, 3, 4;\ 0 \le i \le 15)$ and $v_1^{(j)}$ $(j = 1, 2, 3, 4)$. Otherwise, go to step 3.

### 4.5 Complexity of the Attack

Based on the two differential paths 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 path is about $2^{-45}$ and for steps 34 to 48 of the bottom path 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 $2^{256}$.

The practical complexity of our attack leads to a practical boomerang distinguisher on up to 48-step compression function of SHA-512, and we are able to find its corresponding boomerang quartets. An example of 48-step boomerang distinguisher for SHA-512 compression function is given in Table 5.

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

| | | | | |
|---|---|---|---|---|
| $IV^{(1)}$ | d51d68d22cd614bb | ad109f079123bc43 | 3e30194750de9356 | b934d669f648b886 |
| | 2788083c8af206a4 | f53a6844e79ca3ff | 83333924f0fb45ee | aeca4ed80990f3c1 |
| $IV^{(2)}$ | 551d68d22cd614bb | ad109f079123bc43 | be30194750de9356 | 3936f6621588b886 |
| | a788083c8af206a4 | 753a4844e79ca3ff | 0333591cf87b45ee | 2ec84edfead0f3c1 |
| $IV^{(3)}$ | 3ca41aa7cc2ed702 | d28a0787d13ece62 | aaa0ccee378c5884 | 45960268826fa783 |
| | 126c152e3ed3c3d8 | 90227712dcb66469 | c96f7308aa86be3c | 5adecf0ca7c8cff9 |
| $IV^{(4)}$ | 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 Conclusion

In this work, we propose two step-reduced differential paths with high probabilities of SHA-512 and build a boomerang distinguisher for the compression function of SHA-512 up to 48 steps out of 80 steps with practical complexity $2^{51}$, and the example of boomerang quartet is aslo presented. Our attack is the best practical result on SHA-512 to date.

## References

1. Aoki, K., Guo, J., Matusiewicz, K., Sasaki, Y., Wang, L.: Preimages for Step-Reduced SHA-2. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 578–597.
2. Aumasson, J.-P., Meier, W.: Zero-sum Distinguishers for Reduced Keccak-f and for the Core Functions of Luffa and Hamsi, Available online, 2009. http://131002.net/data/papers/AM09.pdf.
3. Bai, D., Yu, H., Wang, G., Wang X.: Improved Boomerang Attacks on SM3. In: Boyd, C. and Simpson, L. (eds.) ACISP 2013. LNCS, vol. 7959, pp. 251–266.
4. Biham, E., Dunkelman, O., Keller, N.: The Rectangle Attack - Rectangling the Serpent. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 340–357.
5. Biham, E., Dunkelman, O., Keller, N.: Related-Key Boomerang and Rectangle Attacks. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525.
6. Biryukov, A., Nikolić, I., Roy, A.: Boomerang Attacks on BLAKE-32. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 218–237.
7. Biryukov, A., Lamberger, M., Mendel, F., Nikolić, I.: Second-Order Differential Collisions for Reduced SHA-256. In: Lee, D.H., Wang, X. (ed.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 270–287.
8. Eichlseder, A., Mendel F., Schläffer, M.: Branching Heuristics in Differential Collision Search with Applications to SHA-512. In: FSE 2014, accepted paper.
9. Gaëtan, L., Arnab R.: Boomerang Attacks on Hash Function Using Auxiliary Differentials. In: O. Dunkelman (ed.) CT-RSA 2012. LNCS, vol. 7178, pp. 215–230.
10. Guo, J., Ling, S., Rechberger, C., Wang, H.: Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 56–75.
11. Indesteege, S., Mendel, F., Preneel, B., Rechberger, C.: Collisions and Other Non-random Properties for Step-Reduced SHA-256. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 276–293.
12. Isobe, T., Shibutani, K.: Preimage Attacks on Reduced Tiger and SHA-2. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 139–155.
13. Joux, A., Peyrin, T.: Hash Functions and the (Amplified) Boomerang Attack. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 244–263.
14. Kelsey, J., Kohno, T., Schneier, B.: Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 75–93.
15. Khovratovich D., Rechberger C., Savelieva A.: Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family. In: A. Canteaut (ed.) FSE 2012. LNCS, vol. 7549, pp. 244–263.
16. Kircanski, A., Shen, Y., Wang, G., Youssef, A.M.: 'Boomerang and Slide-Rotational Analysis of the SM3 Hash Function', In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 304–320.
17. Lamberger, M., Mendel, F., Higher-Order Differential Attack on Reduced SHA-256. Cryptology ePrint Archive: Report 2011/037. (2011).
18. Mendel, F., Nad, T.: 'Boomerang Distinguisher for the SIMD-512 Compression Function'. In: Bernstein, D.J., Chatterjee, S. (eds.) INDOCRYPT 2011. LNCS, vol. 7107, pp. 255-269.
19. Mendel, F., Nad, T., Schläffer, M.: Finding SHA-2 Characteristics: Searching Through a Minefield of Contradictions. In: D.H. Lee and X. Wang (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 288–307.

20. Mendel, F., Nad, T., Schläffer, M.: Improving Local Collisions: New Attacks on Reduced SHA-256. In: T. Johansson and P. Nguyen (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 262–278.
21. Mendel, F., Pramstaller, N., Rechberger, C., Rijmen, V.: Analysis of Step-Reduced SHA-256. In: Robshaw, M.J.B. (ed.) FSE 2006. LNCS, vol. 4047, pp. 126–143.
22. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1997).
23. National Institute of Standards and Technology: Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family. Federal Register 27(212), 62212–62220 (November 2007).
24. National Institute of Standards and Technology: FIPS PUB 180-3: Secure Hash Standard. Federal Information Processing Standards Publication 180-3, U.S. Department of Commerce (October 2008).
25. Nikolić, I., Biryukov, A.: Collisions for Step-Reduced SHA-256. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 1–15.
26. Sanadhya, S.K., Sarkar, P.: New Collision Attacks Against up to 24-Step SHA-2. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 91–103.
27. Sasaki, Y.: Boomerang Distinguishers on MD4-Based Hash Functions: First Practical Results on Full 5-Pass HAVAL. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 1–18.
28. Sasaki, Y., Wang, L.: '2-Dimension Sums: Distinguishers Beyond Three Rounds of RIPEMD-128 and RIPEMD-160', http://eprint.iacr.org/2012/049.pdf, February 2012.
29. Sasaki, Y., Wang, L., Takasaki, Y., Sakiyama, K., Ohta, K.: 'Boomerang Distinguishers for Full HAS-160 Compression Function'. In: Hanaoka, G., Yamauchi, T. (eds.) IWSEC 2012. LNCS, vol. 7631, pp. 156-169.
30. Wagner, D.: A Generalized Birthday Problem. In: M. Yung (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 288–303.
31. Wagner, D.: The Boomerang Attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170.
32. Wang, X., Yin, Y.L., Yu, H.: Finding Collisions in the Full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17–36.
33. Wang, X., Yu, H.: How to Break MD5 and Other Hash Functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35.
34. Wang, X., Yu, H.: Non-randomness of 39-step SHA-256. Presented at rump session of EUROCRYPT (2008).
35. Yu, H., Chen, J., Wang, X.: The Boomerang Attacks on the Round-Reduced Skein-512. In: Kundsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 288–304.

## Appendix

**Table 6.** The message conditions in $w^{(1)}_{22} - w^{(1)}_{32}$.

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

**Table 7.** The conditions of chaining variables in the middle steps.

| steps | conditions |
|---|---|
| 23 | $a^{(1)}_{23,56} = w^{(1)}_{22,56} \oplus 1$, $a^{(1)}_{23,62} = w^{(1)}_{22,63} \oplus a^{(1)}_{23,3} \oplus w^{(1)}_{22,56} \oplus a^{(1)}_{23,4} \oplus a^{(1)}_{23,57}$, $a^{(1)}_{23,63} = w^{(1)}_{22,63}$ |
|  | $b^{(1)}_{23,41} = a^{(1)}_{23,41}$ |
|  | $c^{(1)}_{23,2} = a^{(1)}_{23,2}$, $c^{(1)}_{23,7} = a^{(1)}_{23,7}$, $c^{(1)}_{23,13} = a^{(1)}_{23,13}$, $c^{(1)}_{23,23} = a^{(1)}_{23,23}$, $c^{(1)}_{23,27} = a^{(1)}_{23,27}$, $c^{(1)}_{23,63} = b^{(1)}_{23,63} \oplus 1$, $c^{(1)}_{23,64} = a^{(1)}_{23,64}$ |
|  | $e^{(1)}_{23,13} = b^{(1)}_{23,13} \oplus 1$, $e^{(1)}_{23,56} = w^{(1)}_{22,56} \oplus 1$, $e^{(1)}_{23,63} = w^{(1)}_{22,63}$ |
|  | $f^{(1)}_{23,2} = b^{(1)}_{23,2} \oplus 1$, $f^{(1)}_{23,7} = b^{(1)}_{23,7} \oplus 1$ |
|  | $g^{(1)}_{23,41} = c^{(1)}_{23,41}$, $g^{(1)}_{23,63} = f^{(1)}_{23,63}$ |
| 24 | $a^{(1)}_{24,2} = b^{(1)}_{24,2}$, $a^{(1)}_{24,7} = b^{(1)}_{24,7}$, $a^{(1)}_{24,13} = b^{(1)}_{24,13}$, $a^{(1)}_{24,23} = b^{(1)}_{24,23}$, $a^{(1)}_{24,27} = b^{(1)}_{24,27}$, $a^{(1)}_{24,41} = b^{(1)}_{24,41}$, $a^{(1)}_{24,63} = a^{(1)}_{23,63} \oplus 1$, $a^{(1)}_{24,64} = b^{(1)}_{24,64}$ |
|  | $e^{(1)}_{24,2} = 1$, $e^{(1)}_{24,5} = 0$, $e^{(1)}_{24,7} = 1$, $e^{(1)}_{24,13} = 0$ |
| 25 | $a^{(1)}_{25,41} = h^{(1)}_{24,41}$, $a^{(1)}_{25,36} = a^{(1)}_{25,30} \oplus h^{(1)}_{24,41} \oplus h^{(1)}_{25,2} \oplus 1$, $a^{(1)}_{25,46} = a^{(1)}_{25,35} \oplus h^{(1)}_{24,41} \oplus h^{(1)}_{25,7} \oplus 1$, $a^{(1)}_{25,52} = a^{(1)}_{25,47} \oplus h^{(1)}_{24,41} \oplus d^{(1)}_{25,13}$ |
|  | $e^{(1)}_{25,5} = 1$, $e^{(1)}_{25,13} = 0$, $e^{(1)}_{25,23} = f^{(1)}_{25,23} \oplus 1$, $e^{(1)}_{25,27} = f^{(1)}_{25,27}$, $e^{(1)}_{25,64} = f^{(1)}_{25,64}$ |
| 26 | $e^{(1)}_{26,23} = d^{(1)}_{25,23}$, $e^{(1)}_{26,27} = d^{(1)}_{25,27}$, $e^{(1)}_{26,41} = c^{(1)}_{26,41}$, $e^{(1)}_{26,46} = e^{(1)}_{26,23} \oplus e^{(1)}_{26,19} \oplus e^{(1)}_{23,5} \oplus 1$, $e^{(1)}_{26,54} = e^{(1)}_{26,31} \oplus e^{(1)}_{26,27} \oplus e^{(1)}_{23,13} \oplus 1$, $e^{(1)}_{26,64} = e^{(1)}_{26,37} \oplus e^{(1)}_{26,41} \oplus e^{(1)}_{26,23} \oplus g^{(1)}_{26,23} \oplus 1$ |
| 27 | $e^{(1)}_{27,23} = 0$, $e^{(1)}_{27,27} = 0$, $e^{(1)}_{27,64} = 0$ |
|  | $a^{(1)}_{27,41} = b^{(1)}_{27,41}$ |
| 28 | $e^{(1)}_{28,23} = 1$, $e^{(1)}_{28,27} = 1$, $e^{(1)}_{28,41} = f^{(1)}_{28,41}$, $e^{(1)}_{28,64} = 1$ |
| 29 | $e^{(1)}_{29,41} = d^{(1)}_{28,41}$, $e^{(1)}_{29,45} = e^{(1)}_{29,41} \oplus e^{(1)}_{29,4} \oplus h^{(1)}_{29,27} \oplus 1$, $e^{(1)}_{29,18} = e^{(1)}_{29,14} \oplus d^{(1)}_{28,41} \oplus h^{(1)}_{29,64} \oplus 1$, $e^{(1)}_{29,64} = e^{(1)}_{29,37} \oplus d^{(1)}_{28,41} \oplus h^{(1)}_{29,23} \oplus 1$ |
| 30 | $e^{(1)}_{30,41} = 0$ |
| 31 | $e^{(1)}_{31,41} = 1$ |