The Boomerang Attacks on the Round-Reduced Skein-512*

Hongbo Yu[1], Jiazhe Chen[3,4], and Xiaoyun Wang[2,3]

[1] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
[2] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
{yuhongbo,xiaoyunwang}@mail.tsinghua.edu.cn
[3] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, School of Mathematics, Shandong University, China
[4] KU Leuven, ESAT/COSIC and IBBT, Belgium
jiazhechen@mail.sdu.edu.cn

Abstract. The hash function Skein is one of the five finalists of the NIST SHA-3 competition. It is based on the block cipher Threefish which only uses three primitive operations: modular addition, rotation and bitwise XOR (ARX). This paper studies the boomerang attacks on Skein-512. Boomerang distinguishers on the compression function reduced to 32 and 36 rounds are proposed, with time complexities $2^{104.5}$ and 2^{454} hash computations respectively. Examples of the distinguishers on 28 and 31 rounds are also given. In addition, the boomerang distinguishers are applicable to the key-recovery attacks on reduced Threefish-512. The time complexities for key-recovery attacks reduced to 32-/33-/34-round are about 2^{181}, 2^{305} and 2^{424} encryptions. Because the previous boomerang distinguishers for Threefish-512 are in fact not compatible [14], our attacks are the first valid boomerang attacks for the reduced-round Skein-512.

Keywords: Hash function, Boomerang attack, Threefish, Skein.

1 Introduction

Cryptographic hash functions, which provide integrity, authentication etc., are very important in modern cryptology. In 2007, NIST launched a hash competition for a new hash standard (SHA-3) as the most widely used hash functions MD5 and SHA-1 were broken [19,20]. Now the competition has come into the third round (the final round), and 5 finalists out of the candidates are selected. The finalist Skein [7] is a ARX-type hash function (based on modular addition, rotation and exclusive-OR). The core of the compression function of Skein is a tweakable block cipher called Threefish, which is proposed with 256-, 512-, 1024-bit block sizes and 72, 72, 80 rounds, respectively. When the algorithm entered

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

L.R. Knudsen and H. Wu (Eds.): SAC 2012, LNCS 7707, pp. 287–303, 2013.

into the second round, the authors changed the rotation constants to refine the algorithm, and after it was selected as a finalist, the constants used in the key schedule were updated to resist the rotational attack [10,11].

During the competition, Skein has been attracting the attentions of the cryptanalysts, and there are several cryptanalytic results on the security of the compression function of Skein and its based block cipher Threefish. At Asiacrypt 2009 [1], Aumasson *et al.* used the boomerang attack to launch a key recovery attack on Threefish-512 reduced to 32 rounds and the known-key distinguisher to 35 rounds under the old rotation constants. However, we find that their differential paths used in the boomerang attacks employ an inverse permutation instead of the original one. In 2010, Chen *et al.* also proposed a boomerang attack for the key recovery of Threefish-512 reduced to 33 and 34 rounds on the new rotation constants using the method of modular differential. Recently Leurent *et al.* [14] gave a boomerang distinguisher for 32-round compression function of Skein-256, and they also pointed that the differential paths in [6] are incompatible. We correct the paths in [1] with the right permutation and show that they are also incompatible under the old rotation constants due to similar contradictions as in [6]. Besides the boomerang attacks, some other attack methods also appeared for Skein. At CANS 2010 [16], Su *et al.* presented free-start near-collisions of Skein-256/-512 compression functions reduced to 20 rounds and Skein-1024 reduced to 24 rounds. At Asiacrypt 2010 [11], Khovratovich *et al.* combined the rotational attack and the rebound attack, and gave distinguishers on 53-round Skein-256 and 57-round Skein-512 respectively, and their technique depends on the constants used in the key schedule. In paper [21], Yu *et al.* gave a near-collision attack for Skein-256 using the rebound attack which was also been shown using incompatible paths [15]. In [12], Khovratovich *et al.* also gave a preimage attack on 22-round Skein-512 hash function and 37-round Skein-512 compression function by the biclique method.

Our Contribution. In this paper, we study the boomerang distinguishers on round-reduced Skein-512. Our analysis is based on two related-key differential paths of Threefish-512 with high probability. In order to solve the incompatibility pointed out in [14], we select differences for the key words and tweaks on the 59-*th* bit instead of the 64-*th* bit (the 64-*th* is the most significant bit) for the top path.

We also reveal that the four paths in the middle 8 rounds are not independent, the probability of the distinguisher in the middle 8 rounds is much higher than the average probability. Based on the differential paths, we give boomerang distinguisher on the compression function of Skein-512 reduced to 32 round with complexity $2^{104.5}$. The distinguisher can be extended to 36 rounds by adding two more rounds on the top and bottom of the differential paths respectively. Our boomerang distinguishers are applicable to the related-key key-recovery attacks on Threefish-512 reduced to 32, 33 and 34 rounds for 1/4 of the keys. Table 1 summarizes our results.

The rest of the paper is organized as follows. In Sect.2, we give a brief description of Skein-512. Sect.3 summaries the boomerang attack. Sect.4 leverages the boomerang technique to the compression functions of Skein-512. In Sec.5, we introduce the key-recovery attacks based on our boomerang distinguishers. Finally, a conclusion of the paper is given in Sect.6.

Table 1. Summary of the attacks on Skein (only the attacks independent of the constants are mentioned)

Attack	CF/KP	Rounds	Time	Ref.
Near collisions(Skein-256)	CF	20	2^{60}	[16]
Near Collisions(Skein-256)	CF	32	2^{105}	[21]*
Pseudo-preimage(Skein-512)	CF	37	$2^{511.2}$	[12]
Boomerang Dist.(Skein-256)	CF	28	2^{24}	[14]
Boomerang Dist.(Skein-256)	KP	32	2^{57}	
Boomerang Dist.(Skein-256)	CF	32	2^{114}	
Key Recovery (Threefish-512)	KP	32	2^{312}	[1]*
Boomerang Dist. (Threefish-512)	KP	35	2^{478}	
Key Recovery (Threefish-512)	KP	32	2^{189}	[6]*
Key Recovery (Threefish-512)	KP	33	$2^{324.6}$	
Key Recovery (Threefish-512)	KP	34	$2^{474.4}$	
Boomerang Dist.(Skein-512)	CF	28	$2^{40.5}$	Sec.4
Boomerang Dist.(Skein-512)	CF	31	2^{32}†	
Boomerang Dist.(Skein-512)	CF	32	$2^{56.5}$†	
Boomerang Dist.(Skein-512)	CF	32	$2^{104.5}$	
Boomerang Dist.(Skein-512)	CF	33	2^{125}†	
Boomerang Dist.(Skein-512)	CP	34	$2^{190.6}$†	
Boomerang Dist.(Skein-512)	CP	35	2^{308}†	
Boomerang Dist.(Skein-512)	CP	36	2^{454}†	
Key-recovery (Threefish-512)	KP	32	2^{181}	Sec.5
Key-recovery (Threefish-512)	KP	33	2^{305}	
Key-recovery (Threefish-512)	KP	34	2^{424}	

KP: Keyed permutation, CF: Compression Function.
*:The differential paths are incompatible.
†: The initial and final subkeys are not included.

2 Description of Skein-512

Skein is designed by Ferguson *et al.*, which is one of the SHA-3 finalists. It supports three different internal state sizes (256, 512, and 1024 bits) and each of these state sizes can support any output size. The word size which Skein operates on is 64 bits. Skein is based on the UBI (Unique Block Iteration) chaining mode that uses block cipher Threefish to build a compression function.

The compression function of Skein can be defined as $H = E(K, T, M) \oplus M$, where $E(K, T, M)$ is the block cipher Threefish, M is the plaintext, K is the master key and T is the tweak value. For Skein-512, both M and K are 512

bits, and the length of T is 128 bits. Let us denote $V_i = (a_i, b_i, c_i, d_i, e_i, f_i, g_i, h_i)$ as the output value of the i-th round, where a_i, b_i, ..., h_i are 64-bit words. Let $V_0 = M$ be the plaintext, the encryption procedure of Threefish-512 is carried out for $i = 1$ to 72 as follows.

If $(i-1) \mod 4 = 0$, first compute

$$\begin{aligned}
\hat{a}_{i-1} &= a_{i-1} + K_{(i-1)/4,a},\ \hat{b}_{i-1} = b_{i-1} + K_{(i-1)/4,b},\\
\hat{c}_{i-1} &= c_{i-1} + K_{(i-1)/4,c},\ \hat{d}_{i-1} = d_{i-1} + K_{(i-1)/4,d},\\
\hat{e}_{i-1} &= e_{i-1} + K_{(i-1)/4,e},\ \hat{f}_{i-1} = f_{i-1} + K_{(i-1)/4,f},\\
\hat{g}_{i-1} &= g_{i-1} + K_{(i-1)/4,g},\ \hat{h}_{i-1} = h_{i-1} + K_{(i-1)/4,h},
\end{aligned}$$

where $K_{(i-1)/4,a}$, $K_{(i-1)/4,b}$, ..., $K_{(i-1)/4,h}$ are round subkeys which are involved in every four rounds. Then carry out:

$$\begin{aligned}
a_i &= \hat{c}_{i-1} + \hat{d}_{i-1},\ h_i = a_i \oplus (\hat{d}_{i-1} \lll R_{i,1}),\\
c_i &= \hat{e}_{i-1} + \hat{f}_{i-1},\ f_i = c_i \oplus (\hat{f}_{i-1} \lll R_{i,2}),\\
e_i &= \hat{g}_{i-1} + \hat{h}_{i-1},\ d_i = e_i \oplus (\hat{h}_{i-1} \lll R_{i,3}),\\
g_i &= \hat{a}_{i-1} + \hat{b}_{i-1},\ b_i = g_i \oplus (\hat{b}_{i-1} \lll R_{i,0}),
\end{aligned}$$

where $R_{i,1}$ and $R_{i,2}$ are rotation constants which can be found in [7]. For the sake of convenience, we denote $\hat{V}_{i-1} = (\hat{a}_{i-1}, \hat{b}_{i-1}, \hat{c}_{i-1}, \hat{d}_{i-1}, \hat{e}_{i-1}, \hat{f}_{i-1}, \hat{g}_{i-1}, \hat{h}_{i-1})$.

If $(i-1) \mod 4 \neq 0$, compute

$$\begin{aligned}
a_i &= c_{i-1} + d_{i-1},\ h_i = a_i \oplus (d_{i-1} \lll R_{i,1}),\\
c_i &= e_{i-1} + f_{i-1},\ f_i = c_i \oplus (f_{i-1} \lll R_{i,2}),\\
e_i &= g_{i-1} + h_{i-1},\ d_i = e_i \oplus (h_{i-1} \lll R_{i,3}),\\
g_i &= a_{i-1} + b_{i-1},\ b_i = g_i \oplus (b_{i-1} \lll R_{i,0}).
\end{aligned}$$

After the last round, the ciphertext is computed as $\hat{V}_{72} = (\hat{a}_{72}, \hat{b}_{72}, ..., \hat{h}_{72})$.

The key schedule starts with the master key $K = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$ and the tweak value $T = (t_0, t_1)$. First we compute

$$k_8 := 0x1bd11bdaa9fc1a22 \oplus \bigoplus_{i=0}^{7} k_i \qquad \text{and} \qquad t_2 := t_0 \oplus t_1.$$

Then the subkeys are derived for $s = 0$ to 18:

$$\begin{aligned}
K_{s,a} &:= k_{(s+0) \bmod 9}\\
K_{s,b} &:= k_{(s+1) \bmod 9}\\
K_{s,c} &:= k_{(s+2) \bmod 9}\\
K_{s,d} &:= k_{(s+3) \bmod 9}\\
K_{s,e} &:= k_{(s+4) \bmod 9}\\
K_{s,f} &:= k_{(s+5) \bmod 9} + t_{s \bmod 3}\\
K_{s,g} &:= k_{(s+6) \bmod 9} + t_{(s+1) \bmod 3}\\
K_{s,h} &:= k_{(s+7) \bmod 9} + s
\end{aligned}$$

3 The Boomerang Attack

The boomerang attack was introduced by Wagner [17] and first applied to block ciphers; it is an adaptive chosen plaintext and ciphertext attack. Later it was further developed by Kelsey et al. into a chosen plaintext attack called the amplified boomerang attack [13], then Biham *et al.* further developed it into the rectangle attack [3]. The basic idea of the boomerang attack is joining two short differential paths with high probabilities in a quartet. The related-key boomerang attack is proposed in [4] and it uses the related-key differentials instead of the single-key differentials. Let E be a block cipher with block size n bits, and it can be decomposed into two sub-ciphers: $E = E_1 \circ E_0$. For the sub-cipher E_0, there is a differential path $(\alpha, \alpha_k) \rightarrow \beta$ with probability p. And for the sub-cipher E_1, there is a differential path $(\gamma, \gamma_k) \rightarrow \delta$ with probability q. Then the related-key boomerang attack can be constructed:

- Randomly choose a pair of plaintexts (P_1, P_2) such that $P_2 - P_1 = \alpha$.
- Compute $\mathcal{K}_2 = \mathcal{K}_1 + \alpha_k$, $\mathcal{K}_3 = \mathcal{K}_1 + \gamma_k$ and $\mathcal{K}_4 = \mathcal{K}_1 + \alpha_k + \gamma_k$. Encrypt P_1, P_2 with the related keys $\mathcal{K}_1$ and $\mathcal{K}_2$ to get $C_1 = E_{\mathcal{K}_1}(P_1)$, $C_2 = E_{\mathcal{K}_2}(P_2)$.
- Compute $C_3 = C_1 + \delta$, $C_4 = C_2 + \delta$. Decrypt C_3, C_4 with the related keys $\mathcal{K}_3$ and $\mathcal{K}_4$ to get $P_3 = E^{-1}_{\mathcal{K}_3}(C_3)$, $P_4 = E^{-1}_{\mathcal{K}_4}(C_4)$.
- Check whether $P_4 - P_3 = \alpha$.

It is known that for an n-bit random permutation, $P_4 - P_3 = \alpha$ with probability 2^{-n}. Therefore, the attack is valid if $p^2q^2 > 2^{-n}$.

In the known-key setting, a (related-key) boomerang attack can be used to distinguish a given permutation from a random oracle; it is called known-related-key boomerang attack in [5]. Applying the known-related-key boomerang attack to the compression function in the MMO mode, i.e, $CF(K, M) = E_K(M) + M$, it is possible to start from the middle rounds because the message M and the key K can be selected randomly (refer to [5] and [14]). The (known-related-key) boomerang attack is particularly efficient for the ARX-type hash functions because their compression functions have strong diffusion after several steps, only short differential paths with high probabilities can be found. See Fig. 1 for the schematic view of the boomerang distinguisher for hash functions. The known-related-key boomerang attack for a permutation (or a compression function in the MMO structure) can be summarized as follows.

- Choose a random value X_1 and $\mathcal{K}_1$, compute $X_2 = X_1 + \beta$, $X_3 = X_1 + \gamma$, $X_4 = X_3 + \beta$ and $\mathcal{K}_2 = \mathcal{K}_1 + \beta_k$, $\mathcal{K}_3 = \mathcal{K}_1 + \gamma_k$, $\mathcal{K}_4 = \mathcal{K}_3 + \beta_k$.
- Compute backward from quartets $(X_i, \mathcal{K}_i)_{i=1}^4$ using E_0^{-1} to obtain P_1, P_2, P_3 and P_4.
- Compute forward from quartets $(X_i, \mathcal{K}_i)_{i=1}^4$ using E_1 to obtain C_1, C_2, C_3 and C_4.
- Check whether $P_2 - P_1 = P_4 - P_3 = \alpha$ and $C_3 - C_1 = C_4 - C_2 = \delta$ are fulfilled.

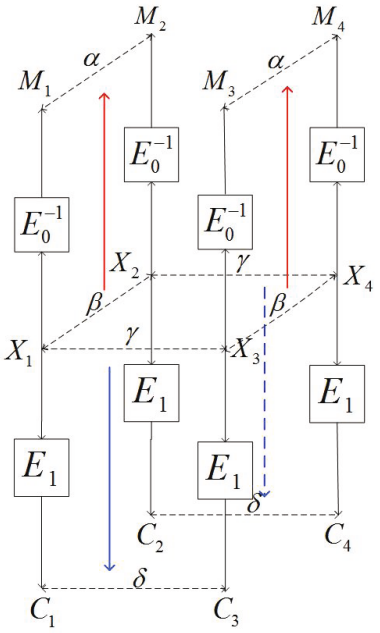

Fig. 1. The boomerang attack

Summary up the previous work [5,14], the boomerang distinguisher falls into three types according to the input and output differences for an n-bit fixed permutation.

- Type I: A quartet satisfies $P_2 - P_1 = P_4 - P_3 = \alpha$ and $C_3 - C_1 = C_4 - C_2 = \delta$ for fixed α and δ. In this case, the generic complexity is 2^n.
- Type II: Only $C_3 - C_1 = C_4 - C_2$ are required (the property is also called zero-sum or second-order differential collision). In this case, the complexity for obtaining such a quartet is $2^{n/3}$ using Wagner's generalized birthday attack [18].
- Type III: A quartet satisfies $P_2 - P_1 = P_4 - P_3$ and $C_3 - C_1 = C_4 - C_2$. In this case, the best known attack still takes time $2^{n/2}$.

4 The Boomerang Distinguisher on Reduced Skein-512

In this section, we describe the known-related-key boomerang attack on Skein-512 reduced to 36 rounds. As mentioned above, 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 so that the switch in the middle does not contain any contradictions. Secondly, we derive the sufficient conditions for the rounds in the middle, and compute the precise probability of each condition. Thirdly, we correct the conditions in the intermediate rounds by

modifying the chaining variables, the key K and the tweak value T. Finally, after the message modification, we search the right quartet that pass the verification of the distinguisher.

4.1 Round-Reduced Differential Paths for Skein-512

The differences of the master key $K = (k_i)_{i=0}^{7}$ and tweak value $T = (t_0, t_1)$ selected for the top differential path are $\Delta k_0 = 0x0400000000000000$, $\Delta t_0 = 0x0400000000000000$ and $\Delta t_1 = 0x0400000000000000$. Suppose $k_{8,59} = t_{0,59} \oplus 1$ and $k_{0,59} = t_{1,59} \oplus 1$, then there is no difference in the fourth subkey. For the bottom path, the MSB differences are set in k_3, k_4 and t_1, and this gives no difference in the eighth subkey. According to the key schedule, the differences for the subkeys $K_i = (K_{i,a}, K_{i,b}, K_{i,c}, K_{i,d}, K_{i,e}, K_{i,f}, K_{i,g}, K_{i,h})$ $(0 \le i \le 9)$ are shown in Tables 2 and 3.

Table 2. The subkey differences of the top path

s	d	$K_{i,a}$	$K_{i,b}$	$K_{i,c}$	$K_{i,d}$	$K_{i,e}$	$K_{i,f}$	$K_{i,g}$	$K_{i,h}$
		Differences							
0	0	k_0	k_1	k_2	k_3	k_4	$k_5 + t_0$	$k_6 + t_1$	$k_7 + 0$
		$\pm 2^{58}$	0	0	0	0	$\pm 2^{58}$	$\pm 2^{58}$	0
1	4	k_1	k_2	k_3	k_4	k_5	$k_6 + t_1$	$k_7 + t_2$	$k_8 + 1$
		0	0	0	0	0	$\pm 2^{58}$	0	$\pm 2^{58}$
2	8	k_2	k_3	k_4	k_5	k_6	$k_7 + t_2$	$k_8 + t_0$	$k_0 + 2$
		0	0	0	0	0	0	0	$\pm 2^{58}$
3	12	k_3	k_4	k_5	k_6	k_7	$k_8 + t_0$	$k_0 + t_1$	$k_1 + 3$
		0	0	0	0	0	0	0	0
4	16	k_4	k_5	k_6	k_7	k_8	$k_0 + t_1$	$k_1 + t_2$	$k_2 + 4$
		0	0	0	0	$\pm 2^{58}$	0	0	0

Table 3. The subkey differences of the bottom path

s	d	$K_{i,a}$	$K_{i,b}$	$K_{i,c}$	$K_{i,d}$	$K_{i,e}$	$K_{i,f}$	$K_{i,g}$	$K_{i,h}$
		Differences							
5	20	k_5	k_6	k_7	k_8	k_0	$k_1 + t_2$	$k_2 + t_0$	$k_3 + 5$
		0	0	0	0	0	2^{63}	0	2^{63}
6	24	k_6	k_7	k_8	k_0	k_1	$k_2 + t_0$	$k_3 + t_1$	$k_4 + 6$
		0	0	0	0	0	0	0	2^{63}
7	28	k_7	k_8	k_0	k_1	k_2	$k_3 + t_1$	$k_4 + t_2$	$k_5 + 7$
		0	0	0	0	0	0	0	0
8	32	k_8	k_0	k_1	k_2	k_3	$k_4 + t_2$	$k_5 + t_0$	$k_6 + 8$
		0	0	0	0	2^{63}	0	0	0
9	36	k_0	k_1	k_2	k_3	k_4	$k_5 + t_0$	$k_6 + t_1$	$k_7 + 9$
		0	0	0	2^{63}	2^{63}	0	2^{63}	0

Table 4. The top differential path used for boomerang attacks of Skein-512

Rd	Shifts	Difference				Pr
2	17, 49	0c030025814280b4	08020024800290a0	84689060080a4234	80209020280a0224	2^{-73}
	36, 39	603a002310842201	4038002312046020	09421184e3408c32	906008062408c22	
3	44, 9	0448004020004010	0448000420000010	2002000002804221	2002000002004021	2^{-35}
	54, 56	0044110481000010	0044020401004010	0401000101401014	0001000100401004	
4		0000000000800240	0001000080000200	0000110080004000	0000010000004000	2^{-24}
		0400000001000010	0400000001000010	0000004400004000	0400000400004000	
K_1		0000000000000000	0000000000000000	0000000000000000	0000000000000000	–
		0000000000000000	0400000000000000	0000000000000000	0400000000000000	
4	39, 30	–	0001000080000200	–	0000010000004000	1
	34, 24	–	0000000001000010	–	0000000400004000	
5	13, 50	0000100080000000	0000000080000000	0400000000000000	0400000000000000	2^{-8}
	10, 17	0000004000000000	0000004000000000	0001000080800040	0000000080000040	
6	25, 29	0000000000000000	0000000000000000	0000000000000000	0000000000000000	2^{-3}
	39, 43	0001000000800000	0001000000000000	0000100000000000	0000100000000000	
7	8, 35	0000000000000000	0000000000000000	0000000000800000	0000000000800000	2^{-1}
	56,22	0000000000000000	0000000000000000	0000000000000000	0000000000000000	
8		0000000000000000	0000000000000000	0000000000000000	0000000000000000	2^{-1}
		0000000000000000	0000000000000000	0000000000000000	0400000000000000	
K_2		0000000000000000	0000000000000000	0000000000000000	0000000000000000	–
		0000000000000000	0000000000000000	0000000000000000	0400000000000000	
		no differences in rounds 9-16				
K_4		0000000000000000	0000000000000000	0000000000000000	0000000000000000	–
		0400000000000000	0000000000000000	0000000000000000	0000000000000000	
16	46, 36	0000000000000000	0000000000000000	0000000000000000	0000000000000000	1
	19, 37	–	0000000000000000	0000000000000000	0000000000000000	
17	33, 27	0000000000000000	0000000000000000	0400000000000000	0000000000000000	2^{-2}
	14, 42	0000000000000000	0400000000000000	0000000000000000	0000000000000000	
18	17, 49	0400000000000000	0000000000000000	0400000000000000	0000000000000000	2^{-5}
	36, 39	0000000000000000	0400000000000100	0000000000000000	0400000000000000	
19	44, 9	0400000000000000	0400000000000000	0400000000000100	0400000200000000	2^{-9}
	54, 56	0400000000000000	0400100040000100	0400000000000000	0400000000000000	
20		0000000200000100	0000004000000000	0000100040000100	0004000000000000	–
		0000000000000000	4001100440100100	0000000000000000	0000040200000108	

The top path we used consists of 18 rounds. Because $\Delta K_2 = (0, 0, 0, 0, 0, 0, 0, \pm 2^{58})$ and $\Delta K_3 = (0, 0, 0, 0, 0, 0, 0, 0)$, we select the intermediate difference ΔV_8 to meet $(0, 0, 0, 0, 0, 0, 0, \mp 2^{58})$. In this way, we get an 8-round path with zero-difference from rounds 9 to 16. By extending the difference ΔV_8 in the backward direction for 6 rounds and the difference $\Delta \hat{V}_{16} = \Delta K_4$ in the forward direction for 4 rounds, an 18-round differential path with high probability is obtained.

Similarly, we choose ΔV_{24} as $(0, 0, 0, 0, 0, 0, 0, 2^{63})$ to compensate the difference $\Delta K_6 = (0, 0, 0, 0, 0, 0, 0, 2^{63})$, which results in zero difference in rounds 25 to 32. As a consequence, a 18-round differential path with high probability also can be acquired by linearly expanding the difference ΔV_{24} backward for 4 rounds and the difference $\Delta \hat{V}_{32} = \Delta K_8$ forward for 6 rounds.

Table 5. The bottom differential path used for boomerang attacks of Skein-512

Rd	shifts	Difference				Pr
20		0000000010004800	0020001000004000	0002201000080000	0000200000080000	2^{-7}
		8000000020000200	8000000020000200	0000088000080000	8000008000080000	
K_5		0000000000000000	0000000000000000	0000000000000000	0000000000000000	–
		0000000000000000	8000000000000000	0000000000000000	8000000000000000	
20	39, 30	–	0020001000004000	–	0000200000080000	2^{-9}
	34, 24	–	0000000020000200	–	0000008000080000	
21	13, 50	0002001000000000	0000001000000000	8000000000000000	8000000000000000	2^{-7}
	10, 17	0000080000000000	0000080000000000	0020001010000800	0000001000000800	
22	25, 29	0000000000000000	0000000000000000	0000000000000000	0000000000000000	2^{-7}
	39, 43	0020000010000000	0020000000000000	0002000000000000	0002000000000000	
23	8, 35	0000000000000000	0000000000000000	0000000010000000	0000000010000000	2^{-3}
	56, 22	0000000000000000	0000000000000000	0000000000000000	0000000000000000	
24		0000000000000000	0000000000000000	0000000000000000	0000000000000000	2^{-1}
		0000000000000000	0000000000000000	0000000000000000	8000000000000000	
K_6		0000000000000000	0000000000000000	0000000000000000	0000000000000000	
		0000000000000000	0000000000000000	0000000000000000	8000000000000000	
		no differences in Rounds 25-32				
K_8		0000000000000000	0000000000000000	0000000000000000	0000000000000000	–
		8000000000000000	0000000000000000	0000000000000000	0000000000000000	
32	46, 36	0000000000000000	0000000000000000	0000000000000000	0000000000000000	1
	19, 37	8000000000000000	0000000000000000	0000000000000000	0000000000000000	
33	33, 27	0000000000000000	0000000000000000	8000000000000000	0000000000000000	1
	14, 42	0000000000000000	8000000000000000	0000000000000000	0000000000000000	
34	17, 49	8000000000000000	0000000000000000	8000000000000000	0000000000000000	1
	36, 39	0000000000000000	8000000000002000	0000000000000000	8000000000000000	
35	44, 9	8000000000000000	8000000000000000	8000000000002000	8000004000000000	2^{-1}
	54, 56	8000000000000000	8002000800002000	8000000000000000	8000000000000000	
36		0000004000002000	0000080000000000	0002000800002000	0080000000000000	2^{-5}
		0000000000000000	0022008802002008	0000000000000000	0000804000002100	
K_9		0000000000000000	0000000000000000	0000000000000000	8000000000000000	
		8000000000000000	0000000000000000	8000000000000000	0000000000000000	
36		0000004000002000	0000080000000000	0002000800002000	8080000000000000	2^{-18}
		8000000000000000	0022008802002008	8000000000000000	0000804000002100	
36	39, 30	–	0000080000000000	–	8080000000000000	2^{-13}
	34, 24	–	0022008802002008	–	0000804000002100	
37	13, 50	8082000800002000	0000084000042000	8022008802002008	c000806100002180	2^{-18}
	10, 17	8000804000002100	882280a802882228	0000084000002000	8082000820202000	
38		402280e902000188	818a084884040000	082200e802880328	8092480860210104	2^{-45}
		8082084820200000	8220a0e22200a108	8082084800040000	062180eb03840188	

The two differential paths are shown in Tables 4 and 5, where we use two kinds of differences: the XOR difference and the integer modular substraction difference. In the rounds after adding the subkey, we express the differences in the positions $\hat{a}_i$, $\hat{c}_i$, $\hat{e}_i$ and $\hat{g}_i$ with the integer modular substraction difference (except the final adding key round), because the XOR operations are not included when computing the next chaining value V_{i+1}; in the other positions of the differential path, we use the XOR difference.

4.2 Message Modifications for the Middle Rounds

The conditions of the middle 8 rounds can be satisfied by the message modifications. The two pair short differentials in the boomerang distinguisher from rounds 16 to 24 are shown in Fig. 2. Let D_1, D_2 denote the top two paths from rounds 20 down to 16, and D_3, D_4 be the bottom two paths from rounds 20 to 24. Then the sufficient conditions for the four paths are shown in Table 6.

If we select the chaining variables $V_{20}^{(1)}$ and the subkey $K_5^{(1)}$ randomly, then the conditions in D_1 can be fulfilled by modifying $V_{20}^{(1)}$, and those in D_3 can be satisfied by modifying $K_5^{(1)}$. But for conditions in D_2 and D_4, we cannot correct them directly because the pairs $(V_{20}^{(3)}, K_5^{(3)})$ and $(V_{20}^{(2)}, K_5^{(2)})$ are related to the pair $(V_{20}^{(1)}, K_5^{(1)})$.

Let us focus on the 39 common non-zero difference bits for D_1 and D_2 which are generated by $(V_i^{(1)}, V_i^{(2)})$ and $(V_i^{(3)}, V_i^{(4)})$ respectively $(i = 20, 19, 18, 17)$. We force the values of $V_i^{(3)}$ in these bits to be equal to the values of $V_i^{(1)}$ in the corresponding bits by the message modifications. That is, $a_{20,9}^{(3)} = a_{20,9}^{(1)}$, $a_{20,34}^{(3)} = a_{20,34}^{(1)}$, $b_{20,39}^{(3)} = b_{20,39}^{(1)}$, $\cdots$, $c_{17,59}^{(3)} = c_{17,59}^{(1)}$, $f_{17,59}^{(3)} = f_{17,59}^{(1)}$ (see Table 7). As a result, if all the sufficient conditions for the path D_1 are satisfied, then all the conditions in D_2 must be satisfied. For the fixed input difference γ of D_3, we can easily deduce that the conditions in Table 7 can be satisfied with probability $2^{-7.4}$, which is much higher than the average probability 2^{-17}. This is also verified by our experiments. All the conditions in Table 7 can be satisfied by modifying $V_{20}^{(1)}$.

Similarly, we can convert the conditions for D_4 in Table 6 to those in Table 8. These conditions hold with probability $2^{-8.4}$ when D_1 hold, which is much better than the average probability 2^{-33}. All the conditions in Table 8 can be fulfilled by modifying $K_5^{(1)}$.

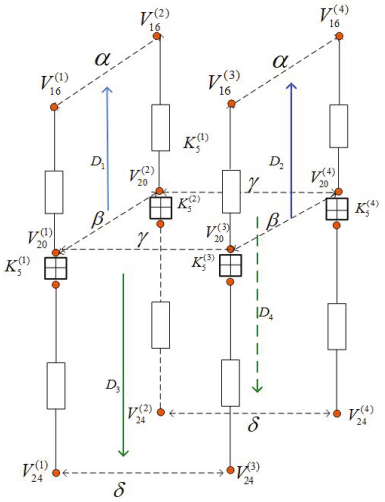

Fig. 2. The middle rounds in a boomerang distinguisher

Table 6. The conditions for differential paths D_1, D_2, D_3 and D_4

rounds	Conditions for D_1	Conditions for D_2
20	$a^{(1)}_{20,43} \oplus h^{(1)}_{20,43} = a^{(1)}_{20,34}$, $c^{(1)}_{20,63} \oplus f^{(1)}_{20,63} = c^{(1)}_{20,9}$, $c^{(1)}_{20,21} \oplus f^{(1)}_{20,21} = c^{(1)}_{20,31}$, $c^{(1)}_{20,35} \oplus f^{(1)}_{20,35} = c^{(1)}_{20,45}$	$a^{(3)}_{20,43} \oplus h^{(3)}_{20,43} = a^{(3)}_{20,34}$, $c^{(3)}_{20,63} \oplus f^{(3)}_{20,63} = c^{(3)}_{20,9}$, $c^{(3)}_{20,21} \oplus f^{(3)}_{20,21} = c^{(3)}_{20,31}$, $c^{(3)}_{20,35} \oplus f^{(3)}_{20,35} = c^{(3)}_{20,45}$
19	$a^{(1)}_{19,59} = b^{(1)}_{19,59} \oplus 1$, $c^{(1)}_{19,9} = a^{(1)}_{20,9}$, $c^{(1)}_{19,59} = d^{(1)}_{19,59} \oplus 1$, $e^{(1)}_{19,59} = f^{(1)}_{19,59} \oplus 1$, $g^{(1)}_{19,59} = h^{(1)}_{19,59} \oplus 1$, $f^{(1)}_{18,9} = c^{(1)}_{19,9}$, $f^{(1)}_{18,59} = c^{(1)}_{19,59}$, $h^{(1)}_{18,59} = e^{(1)}_{19,59}$	$a^{(3)}_{19,59} = b^{(3)}_{19,59} \oplus 1$, $c^{(3)}_{19,9} = a^{(3)}_{20,9}$, $c^{(3)}_{19,59} = d^{(3)}_{19,59} \oplus 1$, $e^{(3)}_{19,59} = f^{(3)}_{19,59} \oplus$, $g^{(3)}_{19,59} = h^{(3)}_{19,59} \oplus 1$, $f^{(3)}_{18,9} = c^{(3)}_{19,9}$, $f^{(3)}_{18,59} = c^{(3)}_{19,59}$, $h^{(3)}_{18,59} = e^{(3)}_{19,59}$
18	$a^{(1)}_{18,59} = g^{(1)}_{19,59}$, $c^{(1)}_{18,59} = a^{(1)}_{19,59}$, $f^{(1)}_{17,59} = c^{(1)}_{18,59}$	$a^{(3)}_{18,59} = g^{(3)}_{19,59}$, $c^{(3)}_{18,59} = a^{(3)}_{19,59}$, $f^{(3)}_{17,59} = c^{(3)}_{18,59}$
17	$c^{(1)}_{17,59} = a^{(1)}_{18,59}$, $k_{8,59} = c^{(1)}_{17,59}$	$c^{(3)}_{17,59} = a^{(3)}_{18,59}$, $k_{8,59} = c^{(3)}_{17,59}$
	Conditions for D_3	Conditions for D_4
20	$b^{(1)}_{20,15} = a^{(1)}_{20,15} \oplus 1$, $d^{(1)}_{20,20} = c^{(1)}_{20,20} \oplus 1$, $d^{(1)}_{20,46} = c^{(1)}_{20,46} \oplus 1$, $f^{(1)}_{20,10} = e^{(1)}_{20,10} \oplus 1$, $f^{(1)}_{20,30} = e^{(1)}_{20,30} \oplus 1$, $h^{(1)}_{20,20} = g^{(1)}_{20,20} \oplus 1$, $h^{(1)}_{20,40} = g^{(1)}_{20,40} \oplus 1$	$b^{(2)}_{20,15} = a^{(2)}_{20,15} \oplus 1$, $d^{(2)}_{20,20} = c^{(2)}_{20,20} \oplus 1$, $d^{(2)}_{20,46} = c^{(2)}_{20,46} \oplus 1$, $f^{(2)}_{20,10} = e^{(2)}_{20,10} \oplus 1$, $f^{(2)}_{20,30} = e^{(2)}_{20,30} \oplus 1$, $h^{(2)}_{20,20} = g^{(2)}_{20,20} \oplus 1$, $h^{(2)}_{20,40} = g^{(2)}_{20,40} \oplus 1$
20	$b^{(1)}_{20,15} = b^{(1)}_{20,15}$, $\hat{b}^{(1)}_{20,37} = b^{(1)}_{20,37}$, $\hat{b}^{(1)}_{20,54} = b^{(1)}_{20,54}$, $\hat{d}^{(1)}_{20,20} = d^{(1)}_{20,20}$, $\hat{d}^{(1)}_{20,46} = d^{(1)}_{20,46}$, $\hat{f}^{(1)}_{20,10} = f^{(1)}_{20,10}$, $\hat{f}^{(1)}_{20,30} = f^{(1)}_{20,30}$, $\hat{h}^{(1)}_{20,40} = h^{(1)}_{20,40}$	$\hat{b}^{(2)}_{20,15} = b^{(2)}_{20,15}$, $\hat{b}^{(2)}_{20,37} = b^{(2)}_{20,37}$, $\hat{b}^{(2)}_{20,54} = b^{(2)}_{20,54}$, $\hat{d}^{(2)}_{20,20} = d^{(2)}_{20,20}$, $\hat{d}^{(2)}_{20,46} = d^{(2)}_{20,46}$, $\hat{f}^{(2)}_{20,10} = f^{(2)}_{20,10}$, $\hat{f}^{(2)}_{20,30} = f^{(2)}_{20,30}$, $\hat{h}^{(2)}_{20,40} = h^{(2)}_{20,40}$
21	$a^{(1)}_{21,37} = c^{(1)}_{20,37}$, $a^{(1)}_{21,50} = c^{(1)}_{20,50}$, $e^{(1)}_{21,44} = g^{(1)}_{20,44}$, $g^{(1)}_{21,12} = a^{(1)}_{20,12}$, $g^{(1)}_{21,29} = a^{(1)}_{20,29}$, $g^{(1)}_{21,37} = b^{(1)}_{20,37}$, $g^{(1)}_{21,54} = b^{(1)}_{20,54}$, $b^{(1)}_{21,37} = a^{(1)}_{21,37} \oplus 1$, $f^{(1)}_{21,44} = e^{(1)}_{21,44} \oplus 1$, $h^{(1)}_{21,12} = g^{(1)}_{21,12} \oplus 1$, $h^{(1)}_{21,37} = g^{(1)}_{21,37} \oplus 1$	$a^{(2)}_{21,37} = c^{(2)}_{20,37}$, $a^{(2)}_{21,50} = c^{(2)}_{20,50}$, $e^{(2)}_{21,44} = g^{(2)}_{20,44}$, $g^{(2)}_{21,12} = a^{(2)}_{20,12}$, $g^{(2)}_{21,29} = a^{(2)}_{20,29}$, $g^{(2)}_{21,37} = b^{(2)}_{20,37}$, $g^{(2)}_{21,54} = b^{(2)}_{20,54}$, $b^{(2)}_{21,37} = a^{(2)}_{21,37} \oplus 1$, $f^{(2)}_{21,44} = e^{(2)}_{21,44} \oplus 1$, $h^{(2)}_{21,12} = g^{(2)}_{21,12} \oplus 1$, $h^{(2)}_{21,37} = g^{(2)}_{21,37} \oplus 1$
22	$e^{(1)}_{22,29} = g^{(1)}_{21,29}$, $e^{(1)}_{22,54} = g^{(1)}_{21,54}$, $f^{(1)}_{22,54} = e^{(1)}_{22,54} \oplus 1$, $g^{(1)}_{22,50} = a^{(1)}_{21,50}$, $h^{(1)}_{22,50} = g^{(1)}_{22,50} \oplus 1$	$e^{(2)}_{22,29} = g^{(2)}_{21,29}$, $e^{(2)}_{22,54} = g^{(2)}_{21,54}$, $f^{(2)}_{22,54} = e^{(2)}_{22,54} \oplus 1$, $g^{(2)}_{22,50} = a^{(2)}_{21,50}$, $h^{(2)}_{22,50} = g^{(2)}_{22,50} \oplus 1$
23	$c^{(1)}_{23,29} = e^{(1)}_{22,29}$, $d^{(1)}_{23,29} = c^{(1)}_{23,29} \oplus 1$	$c^{(2)}_{23,29} = e^{(2)}_{22,29}$, $d^{(2)}_{23,29} = c^{(2)}_{23,29} \oplus 1$

After the message modifications, the boomerang distinguisher in the middle 8 rounds hold with probability close to 1. We also observe that the differential path D_2 is heavily dependent on D_3, and the path D_4 is heavily dependent on D_1. The reason of contradictions in the previous attacks on Skein-512 is that there exist contradict conditions in D_2 or D_4 when the paths D_1 and D_3 hold.

Table 7. The conditions for Differential Path D_2 which hold with probability $2^{-7.4}$

round	conditions	pr
20	$a^{(3)}_{20,9} = a^{(1)}_{20,9}$, $a^{(3)}_{20,34} = a^{(1)}_{20,34}$, $b^{(3)}_{20,39} = b^{(1)}_{20,39}$, $c^{(3)}_{20,9} = c^{(1)}_{20,9}$, $c^{(3)}_{20,31} = c^{(1)}_{20,31}$, $c^{(3)}_{20,45} = c^{(1)}_{20,45}$, $d^{(3)}_{20,51} = d^{(1)}_{20,51}$, $f^{(3)}_{20,9} = f^{(1)}_{20,9}$, $f^{(3)}_{20,21} = f^{(1)}_{20,21}$, $f^{(3)}_{20,31} = f^{(1)}_{20,31}$, $f^{(3)}_{20,35} = f^{(1)}_{20,35}$, $f^{(3)}_{20,45} = f^{(1)}_{20,45}$, $f^{(3)}_{20,49} = f^{(1)}_{20,49}$, $f^{(3)}_{20,63} = f^{(1)}_{20,63}$, $g^{(3)}_{20,59} = g^{(1)}_{20,9}$, $h^{(3)}_{20,4} = h^{(1)}_{20,4}$, $h^{(3)}_{20,9} = h^{(1)}_{20,9}$, $h^{(3)}_{20,34} = h^{(1)}_{20,34}$, $f^{(3)}_{20,43} = f^{(1)}_{20,43}$	1
19	$b^{(3)}_{19,59} = b^{(1)}_{19,59}$, $a^{(3)}_{19,59} = a^{(1)}_{19,59}(0.75)$, $d^{(3)}_{19,34} = d^{(1)}_{19,34}$, $d^{(3)}_{19,59} = d^{(1)}_{19,59}$, $c^{(3)}_{19,9} = c^{(1)}_{19,9}(0.87)$, $c^{(3)}_{19,59} = c^{(1)}_{19,59}(0.94)$, $f^{(3)}_{19,9} = f^{(1)}_{19,9}$, $f^{(3)}_{19,31} = f^{(1)}_{19,31}$, $f^{(3)}_{19,45} = f^{(1)}_{19,45}$, $f^{(3)}_{19,59} = f^{(1)}_{19,59}$, $e^{(3)}_{19,59} = e^{(1)}_{19,59}(0.875)$, $h^{(3)}_{19,59} = h^{(1)}_{19,59}$, $g^{(3)}_{19,59} = g^{(1)}_{19,59}(0.97)$	0.52
18	$a^{(3)}_{18,59} = a^{(1)}_{18,59}(0.687)$, $c^{(3)}_{18,59} = c^{(1)}_{18,59}(0.29)$, $f^{(3)}_{18,9} = f^{(1)}_{18,9}$, $f^{(3)}_{18,59} = f^{(1)}_{18,59}(0.25)$, $h^{(3)}_{18,59} = h^{(1)}_{18,59}(0.937)$	0.047
17	$c^{(3)}_{17,59} = c^{(1)}_{17,59}(0.5)$, $f^{(3)}_{17,59} = f^{(1)}_{17,59}(0.5)$	0.25

Table 8. The conditions for Differential Path D_4 which hold with probability $2^{-8.4}$

round	conditions	pr
20	$a^{(2)}_{20,12} = a^{(1)}_{20,12}$, $a^{(2)}_{20,15} = a^{(1)}_{20,15}$, $a^{(2)}_{20,29} = a^{(1)}_{20,29}$, $b^{(2)}_{20,15} = b^{(1)}_{20,15}$, $b^{(2)}_{20,37} = b^{(1)}_{20,37}$, $b^{(2)}_{20,54} = b^{(1)}_{20,54}$, $c^{(2)}_{20,20} = c^{(1)}_{20,20}$, $c^{(2)}_{20,37} = c^{(1)}_{20,37}$, $c^{(2)}_{20,46} = c^{(1)}_{20,46}$, $c^{(2)}_{20,50} = c^{(1)}_{20,50}$, $d^{(2)}_{20,20} = d^{(1)}_{20,20}$, $d^{(2)}_{20,46} = d^{(1)}_{20,46}$, $e^{(2)}_{20,10} = e^{(1)}_{20,10}$, $e^{(2)}_{20,30} = e^{(1)}_{20,30}$, $f^{(2)}_{20,10} = f^{(1)}_{20,10}$, $f^{(2)}_{20,30} = f^{(1)}_{20,30}$, $g^{(2)}_{20,20} = g^{(1)}_{20,20}$, $g^{(2)}_{20,40} = g^{(1)}_{20,40}$, $g^{(2)}_{20,44} = g^{(1)}_{20,44}$, $h^{(2)}_{20,20} = h^{(1)}_{20,20}$, $h^{(2)}_{20,40} = h^{(1)}_{20,40}$	1
	$\hat{b}^{(2)}_{20,15} = \hat{b}^{(1)}_{20,15}$, $\hat{b}^{(2)}_{20,37} = \hat{b}^{(1)}_{20,37}$, $\hat{b}^{(2)}_{20,54} = \hat{b}^{(1)}_{20,54}$, $\hat{d}^{(2)}_{20,20} = \hat{d}^{(1)}_{20,20}$, $\hat{d}^{(2)}_{20,46} = \hat{d}^{(1)}_{20,46}$, $\hat{f}^{(2)}_{20,10} = \hat{f}^{(1)}_{20,10}(0.5)$, $\hat{f}^{(2)}_{20,30} = \hat{f}^{(1)}_{20,30}$, $\hat{h}^{(2)}_{20,40} = \hat{h}^{(1)}_{20,40}$	0.5
21	$a^{(2)}_{21,37} = a^{(1)}_{21,37}$, $a^{(2)}_{21,50} = a^{(1)}_{21,50}(0.97)$, $b^{(2)}_{21,37} = b^{(1)}_{21,37}$, $e^{(2)}_{21,44} = e^{(1)}_{21,44}(0.5)$, $f^{(2)}_{21,44} = f^{(1)}_{22,44}$, $g^{(2)}_{21,12} = g^{(1)}_{21,12}(0.875)$, $g^{(2)}_{21,29} = g^{(1)}_{21,29}$, $g^{(2)}_{21,37} = g^{(1)}_{21,37}(0.875)$, $g^{(2)}_{21,54} = g^{(1)}_{21,54}$, $h^{(2)}_{21,12} = h^{(1)}_{21,12}(0.875)$, $h^{(2)}_{21,37} = h^{(1)}_{21,37}$	0.32
22	$e^{(2)}_{22,29} = e^{(1)}_{22,29}(0.84)$, $e^{(2)}_{22,54} = e^{(1)}_{22,54}(0.75)$, $f^{(2)}_{22,54} = f^{(1)}_{22,54}(0.5)$, $g^{(2)}_{22,50} = g^{(1)}_{22,50}(0.97)$, $h^{(2)}_{22,50} = h^{(1)}_{22,50}(0.5)$	0.15
23	$c^{(2)}_{23,29} = c^{(1)}_{23,29}(0.24)$, $d^{(2)}_{23,29} = d^{(1)}_{23,29}(0.5)$	0.12

4.3 Complexity of the Attack

Using the differential paths given in Table 4 and Table 5, we can construct a boomerang distinguisher for Skein-512 reduced to 32 rounds (out of 72 rounds). The top path in the backward direction (rounds 16-4) holds with probability 2^{-37} after the message modifications. The bottom path in the forward direction (rounds 20-36) holds with probability 2^{-24} after message modifications.

So the complexity of the 32-round boomerang distinguisher is $2^{2\cdot(37+24)} = 2^{122}$ by using the differential paths in Table 4 and 5. It can be reduced to $2^{2\cdot(13+6)} \times 3^{24+18} \approx 2^{104.5}$ if we only want $\bigoplus_{i=1}^{4} P_i = 0$ and $\bigoplus_{i=1}^{4} C_i = 0$,

Table 9. A quartet that satisfies the paths for rounds 5-36 without the initial and final subkeys

Message of Round 5	
$M^{(1)}$	efeffeca89966f57 b9ede50911910872 b80346f52e40f9b2 413a42e591e3d564 b854665ac709fdc1 5b81218db8689f63 1454025d1e252a79 40086ca8b43d3382
$M^{(2)}$	efefeecb09966f57 b9ede50891910872 b40346f52e40f9b2 453a42e591e3d564 b854661ac709fdc1 5b8121cdb8689f63 1455025d9ea52a39 40086ca8343d33c2
$M^{(3)}$	5b44c68c6c74d8d8 462dcb0d8f65c514 4660e299d27ed556 1622a67e6860f1b3 8631f78ea11186d9 29bf5dee4c4708bf 54cb280ae171a9fd df5814e7668fdf95
$M^{(4)}$	5b44d68dec74d8d8 462dcb0c0f65c514 4a60e299d27ed556 1222a67e6860f1b3 8631f7cea11186d9 29bf5dae4c4708bf 54ca280a61f1a9bd df5814e7e68fdfd5
Key	
$K^{(1)}$	fd4707e3dc7b1c35 3f64c6f0bd13466a 45e7c90173366b70 dc71a6f93dbfc9d5 5c977a7bbc2dbe6d 56889bd71af7189f 8bc7bcb9d86167a1 0091f15b4d1aeaee
$K^{(2)}$	f94707e3dc7b1c35 3f64c6f0bd13466a 45e7c90173366b70 dc71a6f93dbfc9d5 5c977a7bbc2dbe6d 56889bd71af7189f 8bc7bcb9d86167a1 0091f15b4d1aeaee
$K^{(3)}$	fd4707e3dc7b1c35 3f64c6f0bd13466a 45e7c90173366b70 5c71a6f93dbfc9d5 dc977a7bbc2dbe6d 56889bd71af7189f 8bc7bcb9d86167a1 0091f15b4d1aeaee
$K^{(4)}$	f94707e3dc7b1c35 3f64c6f0bd13466a 45e7c90173366b70 5c71a6f93dbfc9d5 dc977a7bbc2dbe6d 56889bd71af7189f 8bc7bcb9d86167a1 0091f15b4d1aeaee
Tweak	
$T^{(1)}, T^{(2)}$	55422f07b9ea59be 511ad7aa13272cc9 51422f07b9ea59be 551ad7aa13272cc9
$T^{(3)}, T^{(4)}$	55422f07b9ea59be d11ad7aa13272cc9 51422f07b9ea59be d51ad7aa13272cc9

Table 10. A quartet that satisfies the paths for rounds 8-36 including the initial and final subkeys

Message of Round 8	
$M^{(1)}$	81eb65560efb565c 42171413b9dae252 ba7f35e83ceec8b7 d5dbcf318a0ecf74 5d1c176606c51b45 4f8fc8fc188100d4 45d34efc985185f5 673059aaf448427c
$M^{(2)}$	81eb65560efb565c 42171413b9dae252 ba7f35e83ceec8b7 d5dbcf318a0ecf74 5d1c176606c51b45 4f8fc8fc188100d4 45d34efc985185f5 6b3059aaf448427c
$M^{(3)}$	f96c2ea16f7aa900 7dbe4b7cc9bef8ea f94e7e6cff763332 f44decb0fcb6ecac 7f30973fad83191f 94591dff30d2e161 74c7323813fc5c42 54e6ccf74a6a1d11
$M^{(4)}$	f96c2ea16f7aa900 7dbe4b7cc9bef8ea f94e7e6cff763332 f44decb0fcb6ecac 7f30973fad83191f 94591dff30d2e161 74c7323813fc5c42 58e6ccf74a6a1d11
Key	
$K^{(1)}$	bf07320940fa73f1 64561111c05cc195 bbf500154032fa6d 8dff001fb0239bbf 5e36a0172124dd89 50e99cdbc81bab42 3ac1c8825115600a 12b40efea4188dab
$K^{(2)}$	bb07320940fa73f1 64561111c05cc195 bbf500154032fa6d 8dff001fb0239bbf 5e36a0172124dd89 50e99cdbc81bab42 3ac1c8825115600a 12b40efea4188dab
$K^{(3)}$	bf07320940fa73f1 64561111c05cc195 bbf500154032fa6d 0dff001fb0239bbf de36a0172124dd89 50e99cdbc81bab42 3ac1c8825115600a 12b40efea4188dab
$K^{(4)}$	bb07320940fa73f1 64561111c05cc195 bbf500154032fa6d 0dff001fb0239bbf de36a0172124dd89 50e99cdbc81bab42 3ac1c8825115600a 12b40efea4188dab
Tweak	
$T^{(1)}, T^{(2)}$	8fe4eab7841221ae 82aeedc8d61e677b 8be4eab7841221ae 86aeedc8d61e677b
$T^{(3)}, T^{(4)}$	8fe4eab7841221ae 02aeedc8d61e677b 8be4eab7841221ae 06aeedc8d61e677b

Table 11. The modified differential path in the middle rounds used for boomerang attacks of Skein-512 in [1]

Rd	shifts	The Difference for the top path from rounds 12-16
K_3		0000000000000000 0000000000000000 0000000000000000 0000000000000000
		8000000000000000 0000000000000000 0000000000000000 0000000000000000
12	33, 49	0000000000000000 0000000000000000 0000000000000000 0000000000000000
	8, 42	8000000000000000 0000000000000000 0000000000000000 0000000000000000
13	39, 27	0000000000000000 0000000000000000 8000000000000000 0000000000000000
	41, 14	0000000000000000 8000000000000000 0000000000000000 0000000000000000
14	29, 26	8000000000000000 0000000000000000 8000000000000000 0000000000000000
	11, 9	0000000000000000 8000010000000000 0000000000000000 8000000000000000
15	33, 51	8000000000000000 8000000000000000 8000010000000000 8000000000000100
	39, 35	8000000000000000 8008010000000400 8000000000000000 8000000000000000
16		0000010000000100 0000000100000000 0008010000000400 0000000400000000
		0000000000000000 000a014004008400 0000000000000000 0004010000000100
K_4		0000000000000000 0000000000000000 0000000000000000 8000000000000000
		8000000000000000 0000000000000000 0000000000000000 8000000000000000
16		0000010000000100 0000000100000000 0008**1**0000000**4**00 8000000400000000
		8000000000000000 000a014004008400 0000000000000000 0804010000000100
		The Difference for the bottom path from rounds 16-20
16	38, 30	4008401080102024 4000400080002004 044001**8**001000**4**00 04400080000004**4**00
	50, 53	0000000000040090 0000000000040080 0200000000008010 0000000000008010
17	48, 20	00000**1**0001000000 0000010000000000 0000000000000010 0000000000000010
	43, 31	0200000000000000 0200000000000000 0008001000100020 0000000000100020
18	34, 14	0000000000000000 0000000000000000 0000000000000000 0000000000000000
	15, 27	0008001000000000 0000001000000000 0000000001000000 0000000001000000
19	26, 12	0000000000000000 0000000000000000 0008000000000000 0008000000000000
	58, 7	0000000000000000 0000000000000000 0000000000000000 0000000000000000
20		0000000000000000 0000000000000000 0000000000000000 0000000000000000
		0000000000000000 0000000000000000 0000000000000000 8000000000000000
K_5		0000000000000000 0000000000000000 0000000000000000 0000000000000000
		0000000000000000 0000000000000000 0000000000000000 8000000000000000

because the probability for $\bigoplus_{i=1}^{4} x_j^{(i)} = 0$ is about 1/3 where $x_j^{(i)}$ denote the non-zero difference bits in rounds 4 and 36.

Extending the 32-round boomerang distinguisher for two more rounds in the backward and forward directions, we can get the 33-/34-/35-/36-round boomerang distinguisher on Skein-512 as follows:

- The complexity of 33-round distinguisher (rounds 4-37) is about $2^{2\cdot(13+6)} \times 3^{24+13+18} \approx 2^{125}$.
- The complexity of 34-round distinguisher (rounds 3-37) is about $2^{2\cdot(37+6)} \times 3^{35+13+18} \approx 2^{190.6}$.
- The complexity of 35-round distinguisher (rounds 3-38) is about $2^{2\cdot(72+82)} = 2^{308}$.
- The complexity of 36-round distinguisher (rounds 2-38) is about $2^{2\cdot(72+82+73)} = 2^{454}$.

Remark: For the 32-/33-/34-round attacks, we use the Type III boomerang distinguisher, the complexity for the best algorithm is 2^{256}; for the 35-/36-round attacks, we use the Type I boomerang distinguisher, the generic complexity is about 2^{512}. Note that the initial and final key-additions are included in our 32-round reduced Skein-512 but they are not included in the distinguishers for 33 to 36 rounds.

In the following, we give examples of the quartets to show that our technique used for 32 to 36 rounds attack is valid. Table 9 gives a zero-sum quartet for rounds 5-36 of Skein-512 (the initial and final subkeys are not included) with $\bigoplus_{i=1}^{4} V_5^{(i)} = 0$ and $\bigoplus_{i=1}^{4} V_{36}^{(i)} = 0$. The complexity of the attack is about 2^{32}. Table 10 gives a zero-sum quartet for rounds 8-36 of Skein-512 with $\bigoplus_{i=1}^{4} V_8^{(i)} = 0$ and $\bigoplus_{i=1}^{4} \hat{V}_{36}^{(i)} = 0$ (the initial and final subkeys are included). The complexity of the attack is about $2^{40.5}$.

4.4 The Incompatibility of Previous Boomerang Attacks on Threefish-512

In papers [1,2], Aumasson *et al.* first presented the boomerang distinguishers on Threefish-512 reduced to 35 rounds. We studied the differential paths used to boomerang attack in Tables 6 and 7 of [2], and found that they used an inverse permutation instead of the original one. We correct the permutation and give the middle 8-round differential paths (see Table 11) using the differences for the key words and tweaks proposed in [1] under the old rotation constants. For the top path, the MSB differences are set in k_7 and t_0. And for the bottom path, the MSB differences are set in k_2, k_3, t_0 and t_1.

From the bottom path, it is easy to deduce that $\hat{d}_{16,11}^{(1)} = \hat{c}_{16,11}^{(1)} \oplus 1$, $\hat{d}_{16,11}^{(2)} = \hat{c}_{16,11}^{(2)} \oplus 1$. From the top path, we know that $\hat{d}_{16,11}^{(1)} = \hat{d}_{16,11}^{(2)}$, so we get $\hat{c}_{16,11}^{(1)} = \hat{c}_{16,11}^{(2)}$. But from the top path, it's obvious that $\hat{c}_{16,11}^{(1)} = \hat{c}_{16,11}^{(2)} \oplus 1$. Hence a contradiction appears. Similarly, the differences on bit 41 for the top and bottom paths are also incompatible.

5 Key Recovery Attack on Reduced Threefish-512

Our boomerang distinguishers for 32 to 34 rounds Skein-512 are also applicable to (related) key recovery attack on Threefish-512. In this case, the complexity for the middle 8 rounds are added, and the initial and final subkeys are included. For the fixed input and output differences α and γ, the probabilities of the boomerang distinguishers for Threefish-512 reduced to 32(rounds 4-36), 33(rounds 4-37), 34(rounds 3-37) rounds are 2^{-177}, 2^{-301} and 2^{-419} respectively.

Consequently, we can mount key recovery attacks on reduced Threefish-512 for 1/4 of the key space, with time complexities 2^{181}, 2^{305} and 2^{424}, respectively. We give the procedure of the key recovery attack on 32-round Threefish-512 as an example.

1. For $i = 1, ..., 2^{179}$
   (a) Randomly choose plaintext P_1^i, compute $P_2^i = P_1^i \oplus \alpha$.
   (b) Encrypt plaintext pair (P_1^i, P_2^i) with $K^{(1)}, K^{(2)}$ respectively to get (C_1^i, C_2^i). Compute $C_3^i = C_1^i \oplus \delta, C_4^i = C_2^i \oplus \delta$. Then decrypt (C_3^i, C_4^i) with $K^{(3)}, K^{(4)}$ respectively to get (P_3^i, P_4^i).
   (c) Check whether $P_3^i \oplus P_4^i = \alpha$, if so, store the quartet $(C_1^i, C_2^i, C_3^i, C_4^i)$.
2. (a) Guess 128 bits of the final subkey words $K_{9,a}, K_{9,b}$ and subtract them with the corresponding words of each element of quartets stored in Step 1. If for all the quartets, whose resulting words satisfy that the XOR differences before the key addition, we store this 128-bit subkey pair $(K_{9,a}, K_{9,b})$.
   (b) Similarly, sequently guess $(K_{9,c}, K_{9,d})$ and $(K_{9,f}, K_{9,h})$ and check whether the required conditions are satisfied. If yes, store the corresponding key words.
3. Search the remaining 128 bits of the final subkey by brute force.

The complexity is dominated by Step 1, which is about 2^{181} 32-round encryptions. The expected number of quartets passed Step 2(a) for a false key is $4 \times 2^{-6} = 2^{-4}$. Let Y be the number of the quartets passed Step 2(a) for a false key, using the Poisson distribution, we have $Pr(Y \geq 4) \approx 0$. The expected quartets passed Step 2(a) for the right key is 4. Let Z be the number of the quartets passed Step 2(a) for the right key, $Pr(Z \geq 4) \approx 0.9$. The success rate of Step 2(b) is similar.

6 Conclusions

In this paper, we apply the boomerang attack to distinguish the compression function of Skein-512 reduced to 36 (out of 72) rounds from a random function. We select the key difference in the 59-*th* bit instead of the difference in the most significant bit to avoid the contradiction in the previous attack for boomerang attacks on Threefish-512. We also point out that the differential paths used in the boomerang distinguisher in the middle rounds are not independent. Our boomerang distinguishers are applicable to the key recovery attack for Threefish-512 reduced to 34 rounds. Future works on Skein-512 might apply the rebound attack [8] to Threefish, although it looks very difficult to combine two short differential paths to a long one.

References

1. Aumasson, J.-P., Çalık, Ç., Meier, W., Özen, O., Phan, R.C.-W., Varıcı, K.: Improved Cryptanalysis of Skein. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 542–559. Springer, Heidelberg (2009)
2. Aumasson, J., et al.: Improved Cryptanalysis of Skein, `http://eprint.iacr.org/2009/438.pdf`

3. Biham, E., Dunkelman, O., Keller, N.: The Rectangle Attack - Rectangling the Serpent. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 340–357. Springer, Heidelberg (2001)
4. Biham, E., Dunkelman, O., Keller, N.: Related-Key Boomerang and Rectangle Attacks. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525. Springer, Heidelberg (2005)
5. Biryukov, A., Lamberger, M., Mendel, F., Nikolić, I.: Second-Order Differential Collisions for Reduced SHA-256. In: Lee, D.H. (ed.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 270–287. Springer, Heidelberg (2011)
6. Chen, J., Jia, K.: Improved Related-Key Boomerang Attacks on Round-Reduced Threefish-512. In: Kwak, J., Deng, R.H., Won, Y., Wang, G. (eds.) ISPEC 2010. LNCS, vol. 6047, pp. 1–18. Springer, Heidelberg (2010)
7. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The Skein Hash Function Family, `http://www.schneier.com/skein1.3.pdf`
8. Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: The Rebound Attack: Cryptanalysis of Reduced Whirlpool and `Grøstl`. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 260–276. Springer, Heidelberg (2009)
9. Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: Rebound Attacks on the Reduced `Grøstl` Hash Function. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 350–365. Springer, Heidelberg (2010)
10. Khovratovich, D., Nikolić, I.: Rotational Cryptanalysis of ARX. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 333–346. Springer, Heidelberg (2010)
11. Khovratovich, D., Nikolić, I., Rechberger, C.: Rotational Rebound Attacks on Reduced Skein. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 1–19. Springer, Heidelberg (2010)
12. Khovratovich, D., Rechberger, C., Savelieva, A.: Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 244–263. Springer, Heidelberg (2012)
13. 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. Springer, Heidelberg (2001)
14. Leurent, G., Roy, A.: Boomerang Attacks on Hash Function Using Auxiliary Differentials. In: Dunkelman, O. (ed.) CT-RSA 2012. LNCS, vol. 7178, pp. 215–230. Springer, Heidelberg (2012)
15. Leurent, G.: ARXtools: A toolkit for ARX analysis. In: The 3rd SHA-3 Conference
16. Su, B.Z., Wu, W.L., Wu, S., Dong, L.: Near-Collisions on the Reduced-Round Compression Functions of Skein and BLAKE. In: Heng, S.-H., Wright, R.N., Goi, B.-M. (eds.) CANS 2010. LNCS, vol. 6467, pp. 124–139. Springer, Heidelberg (2010)
17. Wagner, D.: The Boomerang Attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)
18. Wagner, D.: A Generalized Birthday Problem. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 288–303. Springer, Heidelberg (2002)
19. Wang, X., Yu, H.: How to Break MD5 and Other Hash Functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35. Springer, Heidelberg (2005)
20. 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. Springer, Heidelberg (2005)
21. Yu, H.B., Chen, J.Z., Jia, K.T., Wang, X.Y.: Near-Collision Attack on the Step-Reduced compression Function of Skein-256. Cryptology ePrint Archive, Report 2011/148 (2011), `http://eprint.iacr.org`