Improved Related-Key Boomerang Attacks on Round-Reduced Threefish-512 *

Jiazhe Chen and Keting Jia

Key Laboratory of Cryptographic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
{jiazhechen,ketingjia}@mail.sdu.edu.cn

Abstract. Hash function Skein is one of the 14 NIST SHA-3 second round candidates. Threefish is a tweakable block cipher as the core of Skein, defined with a 256-, 512-, and 1024-bit block size. The 512-bit block size is the primary proposal of the authors. Skein had been updated after it entered the second round; the only difference between the original and the new version is the rotation constants. In this paper we construct related-key boomerang distinguishers on round-reduced Threefish-512 based on the new rotation constants using the method of *modular differential*. With these distinguishers, we mount related-key boomerang key recovery attacks on Threefish-512 reduced to 32, 33 and 34 rounds. The attack on 32-round Threefish-512 has time complexity 2^{195} with memory of 2^{12} bytes. The attacks on Threefish-512 reduced to 33 and 34 rounds have time complexity of $2^{324.6}$ and $2^{474.4}$ encryptions respectively, and both with negligible memory. The best key recovery attack known before is proposed by Aumasson et al. Their attack, which bases on the old rotation constants, is also a related-key boomerang attack. For 32-round Threefish-512, their attack requires 2^{312} encryptions and 2^{71} bytes of memory.

Key words: Threefish-512, related-key boomerang attack, modular differential.

1 Introduction

Cryptographic hash functions play a very important role in cryptology. With the break of MD5 and SHA-1 [14][15], the situation of the hash functions becomes alarming. Although no flaws of SHA-2 have been found, SHA-2 still has the same structure and design principle as MD5 and SHA-1. To deal with the undesirable situation, NIST held a Hash competition for a new hash standard(SHA-3). At this time, 56 out of 64 submissions to the SHA-3 competition are publicly known and available. There are 51 submissions in the first round and 14 submissions have entered the second round. Skein [10] is one of the second-round candidates,

* Supported by 973 Program of China (Grant No.2007CB807902) and National Outstanding Young Scientist fund of China (Grant No. 60525201).

Table 1. Existing Key Recovery Attacks on Round Reduced Threefish-512

Attack	#rounds	#keys	time	memory	source
related-key key recovery*	25	2	$2^{416.6}$	–	[1]
related-key key recovery*	26	2	$2^{507.8}$	–	[1]
related-key boomerang key recovery*	32	4	2^{312}	2^{71}	[1]
related-key boomerang key recovery	32	4	2^{195}	2^{12}	Section 4
related-key boomerang key recovery	33	4	$2^{324.6}$	–	Section 5
related-key boomerang key recovery	34	4	$2^{474.4}$	–	Section 5

* results based on the old rotation constants

bases on the tweakable block cipher Threefish, which is defined with a 256-, 512-, 1024-bit block size and 72, 72, 80 rounds respectively. After getting into the second round, the authors changed the rotation constants [11]. In this paper, we will focus on Threefish-512 with the new rotation constants.

In the paper [1] accepted by Asiacrypt 2009, Aumasson et al. presented several results on Skein-512 and Threefish-512, all the results are based on the original constants. They gave a known-related-key 35-round boomerang distinguisher on threefish-512, but they had only given a key recovery attack of 32 rounds. The difference they used is the XOR difference and they used the algorithms in [9] to find the differentials of their attacks. Their attacks can be applied for the new rotations as well, with new differential trails and different probabilities.

We use another kind of difference, i.e. modular differential and use the method of Wang et al. [13,14] to construct modular differential paths. Then we use the modular differential to construct the boomerang distinguishers based on the new rotation constants. The use of modular differential is essential as the modular differential has advantages against the XOR differential for attacking Threefish. With the modular differential, we can get differential trails with much higher probability. Furthermore, we can get many trails with the same probability, so we can get boomerang distinguishers with much higher probability. The results are summarized in Table 1.

This paper is organized as follows. In Section 2.2, we give a brief description of Threefish. The related-key boomerang attack is described in section 3. Section 4 and Section 5 give our main attacks. Finally, we give the conclusion in Section 6.

2 Preliminaries and Notations

In this section, we first list some notations used in this paper, then give brief descriptions of Threefish.

2.1 Notations

– $\Delta x = x' - x$: the word difference

- $\Delta x_{j-1} = x'_{j-1} - x_{j-1} = \pm 1$: the signed bit-wise difference that is produced by changing the j-th bit of x (for $j = 1, \ldots, 64$). $x[j]$, $x[-j]$ are the resulting values by only changing the j-th bit of the word x. $x[j]$ is obtained by changing the j-th bit of x from 0 to 1, and $x[-j]$ is obtained by changing the j-th bit of x from 1 to 0.
- $x[\pm j_1, \pm j_2, \ldots, \pm j_l]$: the value by changing j_1-th, j_2-th, ..., j_l-th bits of x. The sign "+" (usually is omitted) means that the bit is changed from 0 to 1, and the sign "−" means that the bit is changed from 1 to 0. We use it to represent the signed bit-wise difference of Δx.
- $\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3, \mathcal{K}_4$: four related keys, all of them are 512 bits and composed of eight 64-bit words
- Δ_k^1, Δ_k^2: word-wise differences of the keys
- T_1, T_2, T_3, T_4: four related tweak values, all of them are 128 bits and composed of two 64-bit words
- Δ_t^1, Δ_t^2: word-wise differences of the tweaks
- $\alpha, \beta, \gamma, \zeta, \eta$: 512-bit differences, composed by eight 64-bit words
- k_d: the $(d+1)$-th word of a subkey $(0 \le d \le 7)$
- $k_{s,d}$: the $(d+1)$-th word of the $(s+1)$-th subkey$(0 \le s \le 18, 0 \le d \le 7)$
- $k_{s,d,j}$: the $(j+1)$-th bit of the $(d+1)$-th word of the $(s+1)$-th subkey $(0 \le s \le 18, 0 \le d \le 7, 0 \le j \le 63)$
- P_i: $(i = 1, 2, 3, 4)$ 512-bit plaintext, composed by eight 64-bit words
- C_i: $(i = 1, 2, 3, 4)$ 512-bit ciphertext, composed by eight 64-bit words
- $p_{i,j}$: the $(j+1)$-th word of P_i $(j = 0, \ldots, 7)$
- $c_{i,j}$: the $(j+1)$-th word of C_i $(j = 0, \ldots, 7)$
- MSB: the most significant bit

2.2 Brief Description of Threefish

The following notions are the same as those in [11]. The word size which Threefish operates on is 64 bits. Let N_w denotes the number of words in the key and the plaintext, N_r be the number of rounds. For Threefish-512, $N_w = 8$ and $N_r = 72$. Let $v_{d,i}$ be the value of the ith word of the encryption state after d rounds. The procedure of encryption is:

$$v_{0,i} = p_i \text{ for } i = 0, \ldots, N_w - 1,$$

where p_i is a 64-bit word and $(p_0, \ldots, p_{N_w-1})$ is the 512-bit plaintext.

For each round, we have:

$$e_{d,i} = \begin{cases} (v_{d,i} + k_{d/4,i}) \bmod 2^{64} & \text{if } d \bmod 4 = 0, \\ v_{d,i} & \text{otherwise.} \end{cases}$$

Where $k_{d/4,i}$ is the i-th word of the subkey added to the d-th round. For $i = 0, \ldots, N_w - 1$, $d = 0, \ldots, N_r - 1$. Then mixing and word permutations followed:

$$(f_{d,2j}, f_{d,2j+1}) := \text{MIX}_{d,j}(e_{d,2j}, e_{d,2j+1}) \text{ for } j = 0, \ldots, N_w/2 - 1,$$
$$v_{d+1,i} := f_{d,\pi(i)} \text{ for } i = 0, \ldots, N_w - 1.$$

Where $\mathrm{MIX}_{d,j}(x_0, x_1) = (x_0 + x_1, (x_1 \lll R_{d,j}) \oplus (x_0 + x_1))$, with $R_{d,j}$ a rotation constant depending on d and j. The permutation $\pi(\cdot)$ can be found in Table 3 of [11] , and the rotation constant $R_{d,j}$ can be referred to Table 4 of [11]. The original rotation constants can be found in [10].

After N_r rounds, the ciphertext is given as follows:

$$c_i := (v_{N_r,i} + k_{N_r/4,i}) \bmod 2^{64} \quad \text{for } i = 0, \ldots, N_w - 1,$$

where $(c_0, \ldots, c_{N_w-1})$ is the 512-bit ciphertext.

The key schedule starts with the key $K_0, \ldots, K_{N_w-1}$ and the tweak t_0, t_1. First we compute:

$$K_{N_w} := \lfloor 2^{64}/3 \rfloor \oplus \bigoplus_{i=0}^{N_w-1} K_i \quad \text{and} \quad t_2 := t_0 \oplus t_1.$$

Then the subkeys are derived:

$$\begin{array}{ll}
k_{s,i} := K_{(s+i) \bmod (N_w+1)} & \text{for } i = 0, \ldots, N_w - 4 \\
k_{s,i} := K_{(s+i) \bmod (N_w+1)} + t_{s \bmod 3} & \text{for } i = N_w - 3 \\
k_{s,i} := K_{(s+i) \bmod (N_w+1)} + t_{(s+1) \bmod 3} & \text{for } i = N_w - 2 \\
k_{s,i} := K_{(s+i) \bmod (N_w+1)} + s & \text{for } i = N_w - 1
\end{array}$$

3 Related-key Boomerang Attack

The boomerang attack was first introduced by Wagner[12]. It is an adaptive chosen plaintext and ciphertext attack. And it was further developed by Kelsey et al.[8] into a chosen plaintext attack called the amplified boomerang attack, then Biham et al. further developed it into the rectangle attack [3]. The related-key boomerang attack was first published in [4]. Both of the attacks in this paper and in [1] are related-key boomerang ones. One can extend the attacks to amplified boomerang attacks, with more data and time complexity. In the following, we only introduce the 4-related-key, adaptive chosen plaintext and ciphertext scenario. We use the modular differential, in the rest of the paper the addition and subtraction are modular addition and subtraction.

The boomerang attack bases on the differential attack [2], the idea is joining two short differential characteristics with high probabilities in a quartet instead of a long differential to get a distinguisher with more rounds and higher probability. Let E be a block cipher with block size of n, it is considered as a cascade of two sub-ciphers: $E = E^1 \circ E^0$. For the sub-cipher E^0 there is a related-key differential trail $\alpha \to \beta$ with probability p, and for E^1 there is a related-key differential trail $\gamma \to \zeta$ with probability q. $E^{-1}, {E^0}^{-1}, {E^1}^{-1}$ stand for the inverse of E, E^0, E^1 respectively. The related-key boomerang distinguisher can be constructed as follows:

- Randomly choose a pair of plaintexts (P_1, P_2) such that $P_2 - P_1 = \alpha$.
- Encrypt P_1, P_2 with two related keys $\mathcal{K}_1$ and $\mathcal{K}_2$ respectively to get $C_1 = E_{\mathcal{K}_1}(P_1)$, $C_2 = E_{\mathcal{K}_2}(P_2)$.

- Compute $C_3 = C_1 + \zeta$, $C_4 = C_2 + \zeta$. Decrypt C_3, C_4 with $\mathcal{K}_3$ and $\mathcal{K}_4$ respectively to get $P_3 = E_{\mathcal{K}_3}^{-1}(C_3)$, $P_4 = E_{\mathcal{K}_4}^{-1}(C_4)$.
- Check whether $P_4 - P_3 = \alpha$.

We call a quartet (P_1, P_2, P_3, P_4), whose corresponding ciphertexts (C_1, C_2, C_3, C_4), which passes the boomerang distinguisher a right quartet if it satisfies the following conditions besides $P_2 - P_1 = \alpha$ and $P_4 - P_3 = \alpha$,

$$E_{\mathcal{K}_2}^0(P_2) - E_{\mathcal{K}_1}^0(P_1) = \beta \tag{1}$$

$$E_{\mathcal{K}_3}^{1\ -1}(C_3) - E_{\mathcal{K}_1}^{1\ -1}(C_1) = E_{\mathcal{K}_4}^{1\ -1}(C_4) - E_{\mathcal{K}_2}^{1\ -1}(C_2) = \gamma \tag{2}$$

If a quartet satisfies the two equations above, we have $E_{\mathcal{K}_4}^{1\ -1}(C_4) - E_{\mathcal{K}_3}^{1\ -1}(C_3) = \beta$. Since we have a differential $\alpha \to \beta$ in E^0 and $P_2 - P_1 = \alpha$, the probability of equation 1 is p. Similarly, the probability of equation 2 is q^2, as the probabilities of $\gamma \to \zeta$ and $\gamma \leftarrow \zeta$ are the same. Finally, there is another probability of p to get $P_4 - P_3 = \alpha$ from $E_{\mathcal{K}_4}^{1\ -1}(C_4) - E_{\mathcal{K}_3}^{1\ -1}(C_3)$. As a result, the probability to get a right quartet is p^2q^2. The quartets that pass the distinguisher but don't satisfy equations (1) (2) are called false quartets. It's known that for a random permutation, $P_4 - P_3 = \alpha$ with probability 2^{-n}. Therefore, $pq > 2^{-n/2}$ must hold for the boomerang distinguisher to work.

Furthermore, the attack can be mounted for all possible β's and γ's simultaneously, so a right quartet can be gotten with probability $(\hat{p}\hat{q})^2$, where:

$$\hat{p} = \sqrt{\sum_{\beta} \Pr^2(\alpha \to \beta)} \quad \text{and} \quad \hat{q} = \sqrt{\sum_{\gamma} \Pr^2(\gamma \to \zeta)}$$

In our attacks, we get boomerang distinguishers with many possible β's and γ's.

More details about boomerang attack can be found in [12,3].

4 Improved Related-key Boomerang Key Recovery Attack on 32-round Threefish-512

In this section, we describe the related-key boomerang distinguisher on Threesfish-512 reduced to 32 rounds, which can be used to recovery the key of 32-round Threesfish-512. In the rest of this paper, the least significant bit is the 1-st bit, and the most significant bit is the 64-th bit.

4.1 The Modular Differential

Wang et al. [13,14] introduced the technique of modular differential, which can be used to to find efficiently collisions on the main hash functions from the MD4 family. They considered the relationship among the modular differences, XOR differences and the signed bit-wise differences. With the technique, we find a good differential characteristic for 16-round Threesfish-512.

Here we introduce two theorems from [7] that are useful in our attack,

Theorem 1 *(from [7]) If $x[\pm j_1, \pm j_2, \ldots, \pm j]$ is fixed, then the difference Δx and the XOR-difference are uniquely determined.*

Theorem 2 *(from [7]) $x \in \mathbb{Z}_n$ chosen uniformly at random. If $\Delta x = 2^k$, $0 \leq l \leq n-k-1$, then $Pr(x[k+l, -(k+l-1), \ldots, -k]) = 2^{-(l+1)}$, $Pr(x[-(n-1), \ldots, -(k)]) = 2^{-(n-k)}$. If $\Delta x = -2^k$, $0 \leq l \leq n-k-1$, then $Pr(x[-(k+l), k+l-1, \ldots, k]) = 2^{-(l+1)}$, $Pr(x[n-1, \ldots, k]) = 2^{-(n-k)}$.*

The proofs of the two theorems are refered to [7]. The two theorems play an important role in our attacks. As we know, there are only three operations in Threefish: modular addition, XOR, and rotational shift. The operation between the subkeys and intermediate states is modular addition. So we choose modular subtraction as the measure of difference in the plaintext and the ciphertext. Among the differential path, we fix the signed bit-wise differences of the two operators before the XOR operation by means of Theorem 2. Then we can get a signed bit-wise difference after the XOR operation with certain probability.

For example, in the MIX function, suppose we have $y_0[-11, 16]$ and $x_1[2, 4, 7]$. After left shift of, say, 9 bits, x_1 becomes $(x_1 \lll 9)[11, 13, 16]$. So for $y_1 = (x_1 \lll 9) \oplus y_0$, the bit differences in bit 11 and 16 disappear with probability 1. $y_1[13]$ if the 13-th bit of y_0 is 0 and $y_1[-13]$ if the 13-th bit of y_0 is 1, both of them appear with probability 1/2. We call it that there is a bit condition on the 13-th bit of y_0.

4.2 The 32-round Boomerang Distinguisher with 4 Related Keys

The four related keys have the relationship below.

$$\mathcal{K}_2 = \mathcal{K}_1 + \Delta_k^1, \mathcal{K}_3 = \mathcal{K}_1 + \Delta_k^2, \mathcal{K}_4 = \mathcal{K}_1 + \Delta_k^1 + \Delta_k^2.$$

The four related tweaks have the similar relationship:

$$T_2 = T_1 + \Delta_t^1, T_3 = T_1 + \Delta_t^2, T_4 = T_1 + \Delta_t^1 + \Delta_t^2.$$

Then one can deduce

$$\mathcal{K}_4 = \mathcal{K}_2 + \Delta_k^2, \mathcal{K}_4 = \mathcal{K}_3 + \Delta_k^1, T_4 = T_2 + \Delta_t^2, T_4 = T_3 + \Delta_t^1.$$

In this attack, we make use of two 16-round differential trails, each one of them is extended from a 8-round local collision by adding four addition rounds on the top and the bottom. Set $\delta = 2^{63}$, $\Delta_k^1 = (0,0,0,0,0,0,0,\delta)$, $\Delta_k^2 = (0,0,\delta,\delta,0,0,0,0)$, $\Delta_t^1 = (\delta, 0)$, $\Delta_t^2 = (\delta, \delta)$.

According to the key schedule algorithm, we can get two subkey differential trails $Trail^1$ and $Trail^2$. The differential trails are given in Table 2.

It is obvious that the probabilities of $Trail^1$ and $Trail^2$ are both 1.

We decompose the 32-round Threefish-512 into: $E = E^1 \circ E^0$, where E^0 contains the fisrt 16 rounds(including the subkey adding of 16-th round) and E_1 contains round 17-32(excluding the subkey adding of the 16-th round, including the subkey adding of the 32-th round).

Table 2. Subkey Differential Trails for 32-round Distinguisher

	$Trail^1$								$Trail^2$							
s	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7
0	0	0	0	0	0	δ	0	δ	0	0	δ	δ	0	δ	δ	0
1	0	0	0	0	0	0	0	δ	0	δ	δ	0	0	δ	0	0
2	0	0	0	0	0	0	0	0	δ	δ	0	0	0	0	δ	0
3	0	0	0	0	δ	0	0	0	δ	0	0	0	0	δ	δ	0
4	0	0	0	δ	δ	0	δ	0	0	0	0	0	0	δ	0	δ
5	0	0	δ	δ	0	δ	δ	0	0	0	0	0	0	0	0	δ
6	0	δ	δ	0	0	δ	0	0	0	0	0	0	0	0	0	0
7	δ	δ	0	0	0	0	δ	0	0	0	0	0	δ	0	0	0
8	δ	0	0	0	0	δ	δ	0	0	0	0	δ	δ	0	δ	0
9	0	0	0	0	0	δ	0	δ	0	0	δ	δ	0	δ	δ	0

Using the related-key boomerang distinguisher in Section 3, we first find related-key differential trails $\alpha \to \beta$ and $\gamma \to \zeta$. Subkey differential $Trail^1$ is compatible with $\alpha \to \beta$, and subkey differential $Trail^2$ is compatible with $\gamma \to \zeta$.

We set $\alpha = (1 + 2^8 + 2^{12} + 2^{18} + 2^{30} + 2^{36} + 2^{40} + 2^{54} + 2^{58}, -1 - 2^8 - 2^{30} - 2^{36} - 2^{58}, 2^4 + 2^{10} + 2^{15} + 2^{40} + 2^{43} + 2^{46}, -2^4 - 2^{10} - 2^{40} - 2^{43}, 2^{33} + 2^{49} + 2^{52}, -2^{33} - 2^{49} + 2^{63}, 2^4 + 2^{15} + 2^{31}, -2^{15} - 2^{31} + 2^{63})$,

$\zeta = (2^9 + 2^{42}, 2^7, 2^9 + 2^{38} + 2^{48}, 2^{21} + 2^{63}, 2^{63}, 2 + 2^9 + 2^{30} + 2^{38} + 2^{40} + 2^{48} + 2^{55}, 2^{63}, 2^9 + 2^{13} + 2^{34} + 2^{42})$.

For β and γ, we have many choices as we can choose the sign of difference.

One of the differential trails $\alpha \to \beta$ is shown in Table 4 in the Appendix, and the first column is the intermediate values. We make $v_{i,j}$, $e_{i,j}$, $f_{i,j}$ be the same meaning as in Section 2.2. $v_{i,j,k}$, $e_{i,j,k}$, $f_{i,j,k}$ are the $(k+1)$-th bits of $v_{i,j}$, $e_{i,j}$, $f_{i,j}$ $(k = 0, \ldots, 63)$. The second column gives the differences of column one. The third column means the signed bit-wise differences of column two. It means that any signed bit-wise difference with the difference in the second column is OK if we don't give a value in the third column. The sufficient conditions to make the third column hold are given in Table 7.

We can get many other β's by flipping certain bit differences of $e_{14,5}$, $e_{15,3}$, $e_{15,5}$, $e_{15,7}$, $v_{16,1}$, $v_{16,3}$, $v_{16,5}$ and $v_{16,7}$. For example, in Table 4, we choose the difference of $e_{14,5}$ to be -2^9+2^{63} instead of 2^9+2^{63} by changing the bit condition of $e_{14,5,9}$ into 1. Then the difference of $e_{15,2}$ becomes $-2^9 + 2^{63}$. We keep the other differences of e_{15} unchanged, and the difference of $v_{16,0}$ and $e_{16,0}$ becomes $-2^9 + 2^{42}$. Then we get a different β with the same probability. By similar methods, we can get 2^{18} β's. The β's can be formulated as:

β's $= (\pm 2^9 \pm 2^{42}, \pm 2^7, \pm 2^9 \pm 2^{38} \pm 2^{48}, \pm 2^{21} + 2^{63}, \pm 2^{63}, \pm 2 \pm 2^9 \pm 2^{30} \pm 2^{38} \pm 2^{40} \pm 2^{48} \pm 2^{55}, 2^{63}, \pm 2^9 \pm 2^{13} \pm 2^{34} \pm 2^{42})$,

and all the differential trails $\alpha \to \beta$ have the same probability.

Similarly, there are many γ's by flipping the differences of $e_{16,0}$, $e_{16,2}$, $e_{16,4}$ and $e_{16,6}$. Then the signs of differences of $e_{i,j}$'s $(i = 16, 17, 18, 19; j = 1, 3, 5, 7)$

should be decided to get the local collision after the 20-th round. So the γ's can be formulated as:

$\gamma = (\pm 1 \pm 2^8 \pm 2^{12} \pm 2^{18} \pm 2^{30} \pm 2^{36} \pm 2^{40} \pm 2^{54} \pm 2^{58}, \mp 1 \mp 2^8 \mp 2^{30} \mp 2^{36} \mp 2^{58}, \pm 2^4 \pm 2^{10} \pm 2^{15} \pm 2^{40} \pm 2^{43} \pm 2^{46}, \mp 2^4 \mp 2^{10} \mp 2^{40} \mp 2^{43}, \pm 2^{33} \pm 2^{49} \pm 2^{52}, \mp 2^{33} \mp 2^{49} + 2^{63}, \pm 2^4 \pm 2^{15} \pm 2^{31}, \mp 2^{15} \mp 2^{31} + 2^{63})$.

So we get 2^{21} differential trails $\gamma \rightarrow \zeta$, all with the same probability. One of the differential trails $\gamma \rightarrow \zeta$ starts from the second row of Table 4, it has the same probability as the differential $\alpha \rightarrow \beta$.

Notice that in the trail of Table 4, there is no conditions on the MSB. But it will add one bit condition in the next round if the MSB shifts to anther position and XORs with a bit that has no difference. The probabilities of the resulting bit difference to be 1 or -1 are both 1/2 no matter what the sign of MSB is.

From Table 7 we know that $Pr(\alpha \rightarrow \beta) = Pr(\gamma \rightarrow \zeta) = 2^{-57}$. So $\hat{p}\hat{q} = \sqrt{2^{18} \times 2^{2\times(-57)}}\sqrt{2^{21} \times 2^{2\times(-57)}} = 2^{94.5}$. Therefore, the probability of our related-key boomerang distinguisher is 2^{-189}.

4.3 The Key Recovery Attack on 32-round Threefish-512

We give the key recover attack on 32-round Threefish-512 exploiting the 32-round boomerang distinguisher above.

1. For $i = 1, ..., 2^{193}$
   (a) Randomly choose plaintexts P_1^i, compute $P_2^i = P_1^i + \alpha$.
   (b) Encrypt plaintext pair (P_1^i, P_2^i) with $\mathcal{K}_1, \mathcal{K}_2$ resp. to get (C_1^i, C_2^i). Compute $C_3^i = C_1^i + \zeta$, $C_4^i = C_2^i + \zeta$. Then decrypt (C_3^i, C_4^i) with $\mathcal{K}_3, \mathcal{K}_4$ resp. to get (P_3^i, P_4^i).
   (c) Check whether $P_3^i - P_4^i = \alpha$, if so, store the quartet $(C_1^i, C_2^i, C_3^i, C_4^i)$.
2. (a) Guess 192 bits of the final subkey words $k_{8,0}, k_{8,2}, k_{8,7}$ and subtract them from the corresponding words of every elements of quartets stored in Step 1. If there are at least 13 quartets, whose resulting words satisfy the signed bit-wise differential, we store this 192-bit subkey triple $(k_{8,0}, k_{8,2}, k_{8,7})$.
   (b) Then guess 192 bits of the final subkey words $k_{8,1}, k_{8,3}, k_{8,5}$ and subtract them from the corresponding words of every elements of quartets stored in Step 1. If there are at least 13 quartets, whose resulting words satisfy the signed bit-wise differential, we store this 192-bit subkey triple $(k_{8,1}, k_{8,3}, k_{8,5})$.
3. Search the remaining 128 bits of the final subkey by brute force.

Once we recover the subkey, the main key is known too.

Analysis of the Attack. In Step 1, we need 2^{194} encryptions and 2^{194} decryptions.

Since the probability of the related-key boomerang distinguisher is 2^{-189}, there will be $2^{193} \times 2^{-189} = 2^4$ right quartets and $2^{193} \times 2^{-512} = 2^{-319}$ false quartets left. The complexity of Step 2 is 2^{197} one round encryptions, which

equivalent to 2^{192} 32-round encryptions. So the complexity is dominated by Step 1.

In Step 2, (a) and (b) are executed independently. For (a), the probability for a ciphertext pair to satisfy the signed bit-wise differential after subtracting the round key is 2^{-9}. Therefore, the probability for a quartet to satisfy the conditions is 2^{-18}. So the probability for a false subkey triple to be stored is $2^{-18\times 13} = 2^{-234}$, and a right subkey triple will be stored with probability 1. The number of false subkey triples to be stored is $2^{192} \times 2^{-234} = 2^{-42}$. For (b), the situation is the same as (a).

The expected number of quartets passed Step 2 for a false key is $2^4 \times 2^{-18} = 2^{-14}$. Let Y be the number of the quartets passed Step 2 for a false key, using the Poisson distribution, we have $Pr(Y \geq 13) \approx 0$. The expected quartets passed Step 2 for the right key is 16. Let Z be the number of the quartets passed Step 2 for the right key, $Pr(Z \geq 13) \approx 0.81$.

From the analysis above, the only memory needed is to store the 16 quartets, about 2^{12} bytes. The time complexity is 2^{195}, the data complexity is 2^{194}, the success rate is 0.81.

5 Related-key Boomerang Key Recovery Attack on Threefish-512 reduced to 33 and 34 rounds

Obviously, to extend the attack to 33 and 34 rounds, we have to construct 33- and 34-round related-key boomerang distinguishers. We decompose the 33-round Threefish-512 into: $E' = E'^1 \circ E'^0$. E'^0 is the same as E^0 in Section 4. E'^1 is extended from E^1 by adding one more round to the bottom. After the last round, a final subkey is added. The 34-round distinguisher adds two rounds in stead of one round to the bottom of E^1, and it has different subkey differential trails. There is a main obstacle that if we want to extend the distinguisher to more than 32 rounds we have to fix four words' signed bit-wise differences before and after the 32-th round's subkey adding. But for a given unknown key it is unclear what the probability for fixing both the differences actually is.

To solve this problem, we first assume that the key is chosen uniformly at random and compute the probability for 33- and 34-round distinguishers, then use the distinguishers to recover the keys using method different from that in Section 4.

Note that we still have many β's and γ's to construct distinguishers of 33 and 34 rounds. Moreover, our differential trails from round 1 to round 16 for 33-round and 34-round distinguishers are both the same as those in the 32-round distinguisher. And differential trails from round 16 to round 31 for 33-round distinguisher are the same as those in the 32-round distinguisher. In the 34-round distinguisher, as we have different subkey differential trails, we have different trails from round 16 to round 34. The subkey differential trail for 34-round distinguisher are given in Table 3. We give the differential trail of round 32 and 33 for 33-round distinguisher in Table 5, one of the differential trails from round 16 to round 34 for 34-round distinguisher is given in Table 6. The

Table 3. Subkey Differential Trails for 34-round Distinguisher

	$Trail'^1$								$Trail'^2$							
s	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7
0	0	0	0	0	0	δ	0	δ	0	0	0	δ	0	δ	δ	0
1	0	0	0	0	0	0	0	δ	0	0	δ	0	δ	δ	δ	0
2	0	0	0	0	0	0	0	0	0	δ	0	δ	0	δ	0	0
3	0	0	0	0	δ	0	0	0	δ	0	δ	0	0	0	δ	0
4	0	0	0	δ	δ	0	δ	0	0	δ	0	0	0	δ	δ	0
5	0	0	δ	δ	0	δ	δ	0	δ	0	0	0	0	δ	0	δ
6	0	δ	δ	0	0	δ	0	0	0	0	0	0	0	0	0	0
7	δ	δ	0	0	0	0	δ	0	0	0	0	0	0	0	δ	δ
8	δ	0	0	0	0	δ	δ	0	0	0	0	0	δ	δ	δ	0
9	0	0	0	0	0	δ	0	δ	0	0	0	δ	0	δ	δ	0

columns in Table 5,6 have the same meaning as those in Table 4. The sufficient conditions for the differential in Table 5 6 are given in Table 8 9. Table 5, 6, 8, 9 are given in the Appendix.

5.1 Related-key Boomerang Key Recovery Attack on 33-round Threefish-512

We can know from Table 7 8 that the probability of the differential trails from round 16 to round 33 is 2^{-118}. So the probability of the 33-round distinguisher is $(2^{18} \times 2^{2\times(-57)}) \times (2^{21} \times 2^{2\times(-118)}) = 2^{-311}$.

We will use a method similar to that used in [5] [6] to recover the subkey bits.

When recovering keys of 33-round Threefish-512, we will use the inverse direction of the distinguisher, say we choose ciphertext pairs, decrypt them, add differences of the first round to the plaintexts then encrypt them to test whether there are quartets passing the boomerang distinguisher.

It is obvious that if the differences of a ciphertext pair after subtracting the last subkey don't satisfy the conditions of the boomerang distinguisher, then this pair can't follow the differential trails of the distinguisher. Therefore, we can control some bits of the ciphertext pair to make certain one bit condition of the last round difference depends completely on a corresponding last subkey bit. In this way, we can recover 192 last subkey bits one by one. We will recover the least significant 10 bits of $k_{9,0}$, $k_{9,1}$ and $k_{9,6}$; the least significant 35 bits of $k_{9,3}$ and $k_{9,4}$; the least significant 31 bits of $k_{9,2}$; the least significant 39 bits of $k_{9,5}$; and the least significant 22 bits of $k_{9,7}$.

We will depict how to recover the least significant 10 bits of $k_{9,6}$ as an example to illustrate the method. We make use of two of the bit conditions in $v_{33,6}$, i.e. $v_{33,6}[8, 10]$. Instead of using randomly chosen ciphertexts (C_1, C_2) only with $C_2 - C_1$ matching the desired difference, we also fix the least significant 7 bits of $c_{1,6}, c_{2,6}$ to be zero, the 8-th bit of $c_{1,6}, c_{2,6}$ to be 0, 1 resp. and the other bits of

C_1, C_2 are chosen randomly. Now there is no carry in the 8-th bit, so only when $k_{9,6,7} = 0$ can $v_{33,6}$ satisfy the bit condition of $v_{33,6}[8]$.

Then we choose sufficiently many such cipherext pairs and make them go through the boomerang distinguisher. If there are quartets passed, we know that $k_{9,6,7} = 0$. Otherwise, we conclude that $k_{9,6,7} = 1$.

Now we are leaving to estimate the probability of making a mistake that wrongly assuming $k_{9,6,7} = 1$ while in fact $k_{9,6,7} = 0$. Since our related-key boomerang distinguisher has a probability of 2^{-311}, if we make our decision after $t2^{311}$ tries, the error probability can be approximated by

$$(1 - 2^{-311})^{t2^{311}} = ((1 - 2^{-311})^{2^{311}})^t \approx (1/e)^t$$

After recovering $k_{9,6,7}$, we modify the choice of ciphertext pairs and recover key bit $k_{9,6,6}$.

- If $k_{9,6,7} = 0$, then we generate ciphertext pairs where the least significant 7 bits are 1000000. The 8-th bit of $c_{1,6}$ is set to 0, the 8-th bit of $c_{2,6}$ is set to 1. It must be $k_{9,6,6} = 0$ to satisfy the bit condition. So after $t2^{311}$ tries, if there are quartets passed, we conclude $k_{9,6,6} = 0$. Otherwise, $k_{9,6,6} = 1$.
- If $k_{9,6,7} = 1$, we generate ciphertext pairs where the the least significant 7 bits are 1000000. The 8-th bit of $c_{1,6}$ is set to 0, the 8-th bit of $c_{2,6}$ is set to 1. But in this case, we demand for a carry in the 8-th bit, so when $k_{9,6,6} = 1$ can the difference satisfy the bit condition.

Apply this procedure recursively to recover the least significant 8 bits of $k_{9,6}$. After that, a similar argument allows to recover $k_{9,6,8}$ and $k_{9,6,9}$. We use the already known key bits, choose ciphertext pairs to control the bit differences and carries. And then we make the decision. In some cases, one might have to fix several bits in the ciphertext pair in order to get one bit difference, but the idea is the same.

For the other subkey words we recover the bits with a very similar procedure. In our attack, we choose $t = 16$.

Analysis of the Attack. For each bit to be recovered, we need at most $2t2^{311} = 2^{316}$ decryptions and the same number of encryptions. So the most complexity for recovering one bit is 2^{317} encryptions. As we want to recover 192 bits, we need $192 \cdot 2^{317} \approx 2^{324.6}$ encryptions. The data complexity is $2^{323.6}$. After recovering the 192 bits, we search the rest 320 bits by brute force. So the time complexity is about $2^{324.6}$, memory complexity is negligible.

The success rate of one bit is $1 - (1/e)^{16}$, so the total success rate is $(1 - (1/e)^{16})^{192} \approx 0.99998$.

5.2 Related-key Boomerang Key Recovery Attack on 34-round Threefish-512

From Table 6 we know that one of the differential trails from round 16 to round 34 has probability 2^{-200}, and we have 2^{33} such differential trails with the same probability.

As the differential trails from round 1 to round 16 are the same as those in the 32-round distinguisher, the probability of the 34-round distinguisher is $(2^{18} \times 2^{2\times(-57)}) \times (2^{33} \times 2^{2\times(-200)})) = 2^{-463}$.

The method to attack the 34-round Threefish-512 is similar to that in Section 5.1. And this time we can use either forward or backward direction of the boomerang distinguisher, here we use the forward direction. Then we recover 42 bits of the first subkey by the means of Section 5.1. The attack needs about $2^{474.4}$ encryptions and negligible memory.

6 Conclusion

We use the modular differential instead of the XOR differential to construct boomerang distinguishers of Threefish-512. We fixed the signed bit-wise differences to get our differential trails and mount an attack on 32-round Threefish-512 with complexity that is far lower than that in [1].

Then we extend the attack to 33 and 34 rounds with 33- and 34-round related-key boomerang distinguishers, but with a different method. We fix some bits in the ciphertext(plaintext) pairs and run the distinguisher sufficiently many times to recover one key bit at a time.

Further work on the key recovery attack of Threefish-512 up to 35 rounds or more comes with unaffordable cost by means of the methods above. One may have to find some other ways to make further improvement.

Acknowledgement

We are grateful to the anonymous reviewers for their valuable comments.

References

1. Aumasson, J.-P., Calik, C., Meier, W., Ozen, O., Phan, R.C.W., Varici, K.: Improved Cryptanalysis of Skein. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 542-559. Springer, Heidelberg (2009)
2. Biham, E., Shamir, A.: Differential Cryptanalysis of The Data Encryption Standard. Springer, London (1993)
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. Borghoff, J., Knudsen, L.R., Leander G., Matusiewicz K.: Cryptanalysis of C2. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 250-266. Springer, Heidelberg (2009)
6. Contini, S., Yin, Y.L.: Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions. In: Lai, X.J. (ed.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 37-53. Springer, Heidelberg (2006)

7. Daum, M.: Cryptanalysis of Hash Fucntions of the MD4 Family, http://www.cits.rub.de/imperia/md/content/magnus/idissmd4.pdf
8. Kelsey, J., Khono, 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 (2000)
9. Lipmaa, H., Moriai, S.: Efficient Algorithms for Computing Differential Properties of Addition. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 336-350. Springer, Heidelberg (2001)
10. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The Skein Hash Function Family, http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/Skein.zip
11. 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/skein.pdf
12. Wagner, D.: The Boomerang Attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156-170. Springer, Heidelberg (1999)
13. Wang, X.Y., Lai, X.J., Feng, D.G., Chen, H., Yu, X.Y.: Cryptanalysis of the Hash Functions MD4 and RIPEMD. In: Cramer, R. (ed.) EUROCRYPT 2005, LNCS, vol. 3494, pp. 1-18. Springer, Heidelberg (2005)
14. Wang, X.Y., Yu, H.B.: How to Break MD5 and Other Hash Functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19-35. Springer, Heidelberg (2005)
15. Wang, X.Y., Yin, Y.L., Yu, H.B.: Finding Collisions in the Full SHA-1. In: Shoup V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17-36. Springer, Heidelberg (2005)

A Appendix

Table 4. One of the Differential Trails $\alpha \to \beta$

Intermediate values	**Differences**	**Signed Bit-wise Differences**
$v_{0,0}$	$1+2^8+2^{12}+2^{18}+2^{30}+2^{36}+2^{40}$ $+2^{54}+2^{58}$	
$v_{0,1}$	$-1-2^8-2^{30}-2^{36}-2^{58}$	
$v_{0,2}$	$2^4+2^{10}+2^{15}+2^{40}+2^{43}+2^{46}$	
$v_{0,3}$	$-2^4-2^{10}-2^{40}-2^{43}$	
$v_{0,4}$	$2^{33}+2^{49}+2^{52}$	
$v_{0,5}$	$-2^{33}-2^{49}+2^{63}$	
$v_{0,6}$	$2^4+2^{15}+2^{31}$	
$v_{0,7}$	$-2^{15}-2^{31}+2^{63}$	
$e_{0,0}$	$1+2^8+2^{12}+2^{18}+2^{30}+2^{36}+2^{40}$ $+2^{54}+2^{58}$	
$e_{0,1}$	$-1-2^8-2^{30}-2^{36}-2^{58}$	$e_{0,1}[-1,-9,-31,-37,-59]$
$e_{0,2}$	$2^4+2^{10}+2^{15}+2^{40}+2^{43}+2^{46}$	
$e_{0,3}$	$-2^4-2^{10}-2^{40}-2^{43}$	$e_{0,3}[-5,-11,-41,-44]$
$e_{0,4}$	$2^{33}+2^{49}+2^{52}$	
$e_{0,5}$	$-2^{33}-2^{49}$	$e_{0,5}[-34,-50]$
$e_{0,6}$	$2^4+2^{15}+2^{31}$	
$e_{0,7}$	$-2^{15}-2^{31}$	$e_{0,7}[-16,-32]$
$e_{1,0}, e_{1,1}$	$2^{15}+2^{46}, \quad -2^{46}$	$e_{1,0}[16,47], e_{1,1}[-47]$
$e_{1,2}, e_{1,3}$	$2^{52}, \quad -2^{52}$	$e_{1,2}[53], e_{1,3}[-53]$
$e_{1,4}, e_{1,5}$	$2^4, \quad -2^4$	$e_{1,4}[5], e_{1,5}[-5]$
$e_{1,6}, e_{1,7}$	$2^{12}+2^{18}+2^{40}+2^{54}, \quad -2^{12}-2^{40}$	$e_{1,6}[13,19,41,55], e_{1,7}[-13,-41]$
$e_{2,4}, e_{2,5}$	$2^{18}+2^{54}, \quad -2^{18}$	$e_{2,4}[19,55], e_{2,5}[-19]$
$e_{2,6}, e_{2,7}$	$2^{15}, \quad -2^{15}$	$e_{2,6}[16], e_{2,7}[-16]$
$e_{3,2}, e_{3,3}$	$2^{54}, \quad -2^{54}$	$e_{3,2}[55], e_{3,3}[-55]$
$v_{4,7}$	2^{63}	$v_{4,7}[*64]$
$e_4 \sim v_{12}$	0	
$e_{12,4}$	2^{63}	$e_{12,4}[*64]$
$e_{13,2}, e_{13,5}$	$2^{63}, \quad 2^{63}$	$e_{13,2}[*64], e_{13,5}[*64]$
$e_{14,0}, e_{14,2}$	$2^{63}, \quad 2^{63}$	$e_{14,0}[*64], e_{14,2}[*64]$
$e_{14,5}, e_{14,7}$	$2^9+2^{63}, \quad 2^{63}$	$e_{14,5}[10,*64], e_{14,7}[*64]$
$e_{15,0}, e_{15,1}$	$2^{63}, \quad 2^{63}$	$e_{15,0}[*64], e_{15,1}[*64]$
$e_{15,2}, e_{15,3}$	$2^9+2^{63}, \quad 2^{42}+2^{63}$	$e_{15,2}[10,*64], e_{15,3}[43,*64]$
$e_{15,4}, e_{15,5}$	$2^{63}, \quad 2^9+2^{38}+2^{48}+2^{63}$	$e_{15,4}[*64], e_{15,5}[10,39,49,*64]$
$e_{15,6}, e_{15,7}$	$2^{63}, \quad 2^{63}$	$e_{15,6}[*64], e_{15,7}[*64]$
$v_{16,0}, v_{16,1}$	$2^9+2^{42}, \quad 2^7$	$v_{16,0}[10,43], v_{16,1}[8]$
$v_{16,2}, v_{16,3}$	$2^9+2^{38}+2^{48}, \quad 2^{21}$	$v_{16,2}[10,39,49], v_{16,3}[22]$
$v_{16,4}, v_{16,5}$	$0, \ 2+2^9+2^{30}+2^{38}+2^{40}+2^{48}+2^{55}$	$v_{16,5}[2,10,31,39,41,49,56]$
$v_{16,6}, v_{16,7}$	$0, \ 2^9+2^{13}+2^{34}+2^{42}$	$v_{16,7}[10,14,35,43]$
$e_{16,0}, e_{16,1}$	$2^9+2^{42}, \quad 2^7$	
$e_{16,2}, e_{16,3}$	$2^9+2^{38}+2^{48}, \quad 2^{21}+2^{63}$	
$e_{16,4}, e_{16,5}$	$2^{63}, 2+2^9+2^{30}+2^{38}+2^{40}+2^{48}+2^{55}$	
$e_{16,6}, e_{16,7}$	$2^{63}, \ 2^9+2^{13}+2^{34}+2^{42}$	

* both positive and negative are OK

Table 5. Differential Trail of Round 32 and 33 for 33-round Distinguisher

Intermediate values	**Differences**	**Signed Bit-wise Differences**
$v_{32,0}, v_{32,1}$	$2^9 + 2^{42}, \quad 2^7$	$v_{32,0}[10, 43], v_{32,1}[8]$
$v_{32,2}, v_{32,3}$	$2^9 + 2^{38} + 2^{48}, \quad 2^{21}$	$v_{32,2}[10, -39, 40, 49], v_{32,3}[22]$
$v_{32,4}, v_{32,5}$	$0,\ 2 + 2^9 + 2^{30} + 2^{38} + 2^{48} + 2^{55}$	$v_{32,5}[2, 10, 31, -39, -40, 41, 49, 56]$
$v_{32,6}, v_{32,7}$	$0,\ 2^9 + 2^{13} + 2^{34} + 2^{42}$	$v_{32,7}[10, 14, 35, 43]$
$e_{32,0}, e_{32,1}$	$2^9 + 2^{42}, \quad 2^7$	$e_{32,1}[8]$
$e_{32,2}, e_{32,3}$	$2^9 + 2^{38} + 2^{48}, \quad 2^{21} + 2^{63}$	$e_{32,3}[22, *64]$
$e_{32,4}, e_{32,5}$	$2^{63},\ 2 + 2^9 + 2^{30} + 2^{38} + 2^{48} + 2^{55}$	$e_{32,5}[2, 10, 31, 39, 49, 56]$
$e_{32,6}, e_{32,7}$	$2^{63},\ 2^9 + 2^{13} + 2^{34} + 2^{42}$	$e_{32,7}[10, 14, 35, 43]$
$v_{33,0}$	$2^9 + 2^{21} + 2^{38} + 2^{48} + 2^{63}$	$v_{33,0}[10, 22, 39, 49, *64]$
$v_{33,1}$	$2^7 - 2^9 + 2^{42} + 2^{53}$	$v_{33,1}[8, -10, 43, 54]$
$v_{33,2}$	$2 + 2^9 + 2^{30} + 2^{38} + 2^{48} + 2^{55} + 2^{63}$	$v_{33,2}[2, -10, 11, 31, 39, -49, 50, 56, *64]$
$v_{33,3}$	$8 - 2^9 - 2^{13} - 2^{15} - 2^{34} - 2^{42}$ $-2^{46} - 2^{50} + 2^{63}$	$v_{33,3}[8, -10, -14, -16, -35, -43,$ $-47, -51, *64]$
$v_{33,4}$	$2^9 + 2^{13} + 2^{34} + 2^{42} + 2^{63}$	$v_{33,4}[10, 14, 35, 43, *64]$
$v_{33,5}$	$2 + 2^3 - 2^9 - 2^{20} - 2^{28} - 2^{30} + 2^{38}$ $+2^{48} + 2^{55} - 2^{57} + 2^{63}$	$v_{33,5}[2, 4, -10, -21, -29, -31, 39,$ $49, 56, -58, *64]$
$v_{33,6}$	$2^7 + 2^9 + 2^{42}$	$v_{33,6}[8, 10, 43]$
$v_{33,7}$	$-2^9 + 2^{21} + 2^{35} - 2^{38} - 2^{48} + 2^{57} + 2^{63}$	$v_{33,7}[-10, 22, 36, -39, -49, 58, *64]$
$e_{33,0}$	$2^9 + 2^{21} + 2^{38} + 2^{48} + 2^{63}$	
$e_{33,1}$	$2^7 - 2^9 + 2^{42} + 2^{53}$	
$e_{33,2}$	$2 + 2^9 + 2^{30} + 2^{38} + 2^{48} + 2^{55}$	
$e_{33,3}$	$8 - 2^9 - 2^{13} - 2^{15} - 2^{34} - 2^{42}$ $-2^{46} - 2^{50}$	
$e_{33,4}$	$2^9 + 2^{13} + 2^{34} + 2^{42} + 2^{63}$	
$e_{33,5}$	$2 + 2^3 - 2^9 - 2^{20} - 2^{28} - 2^{30} + 2^{38}$ $+2^{48} + 2^{55} - 2^{57}$	
$e_{33,6}$	$2^7 + 2^9 + 2^{42} + 2^{63}$	
$e_{33,7}$	$-2^9 + 2^{21} + 2^{35} - 2^{38} - 2^{48} + 2^{57} + 2^{63}$	

* both positive and negative are OK

Table 6: One of the Differential Trails of Round 16-34 for 34-round Distinguisher

Intermediate values	**Differences**	**Signed Bit-wise Differences**
$e_{16,0}$	$2^3+2^{13}+2^{17}+2^{19}+2^{21}+2^{27}+2^{37}$ $+2^{39}+2^{45}+2^{49}+2^{55}+2^{58}+2^{59}+2^{63}$	
$e_{16,1}$	$-2^3-2^{13}-2^{17}-2^{19}-2^{39}-2^{45}$ $-2^{55}-2^{58}$	$e_{16,1}[-4,-14,-18,-20,-40,-46,$ -56,-59]
$e_{16,2}$	$2+2^4+2^9+2^{13}+2^{23}+2^{29}+2^{34}+2^{37}$ $+2^{40}+2^{49}+2^{62}$	
$e_{16,3}$	$-2^4-2^{13}-2^{23}-2^{29}-2^{37}-2^{49}-2^{62}$	$e_{16,3}[-5,-14,-24,-30,-38,-50,-63]$
$e_{16,4}$	$2^4+2^7+2^{52}+2^{58}$	
$e_{16,5}$	$-2^4-2^{52}-2^{58}$	$e_{16,5}[-5,-53,-59]$
$e_{16,6}$	$2^{13}+2^{23}+2^{34}+2^{40}+2^{50}$	
$e_{16,7}$	$-2^{34}-2^{40}-2^{50}$	$e_{16,7}[-35,-41,-51]$
$e_{17,0}, e_{17,1}$	$2+2^9+2^{34}+2^{40}, \quad -2-2^{40}$	$e_{17,0}[2,10,35,41], e_{17,1}[-2,-41]$
$e_{17,2}, e_{17,3}$	$2^7, \quad -2^7$	$e_{17,2}[8], e_{17,3}[-8]$
$e_{17,4}, e_{17,5}$	$2^{13}+2^{23}, \quad -2^{13}-2^{23}$	$e_{17,4}[14,24], e_{17,5}[-14,-24]$
$e_{17,6}$	$2^{21}+2^{27}+2^{37}+2^{49}+2^{59}+2^{63}$	$e_{17,6}[22,28,38,50,60,*64]$
$e_{17,7}$	$-2^{21}-2^{49}-2^{59}$	$e_{17,7}[-22,-50,-60]$
$e_{18,4}, e_{18,5}$	$2^{27}+2^{37}+2^{63}, \quad -2^{27}-2^{37}$	$e_{18,4}[28,38,*64], e_{18,5}[-28,-38]$
$e_{18,6}, e_{18,7}$	$2^9+2^{34}, \quad -2^{34}$	$e_{18,6}[10,35], e_{18,7}[-35]$
$e_{19,2}, e_{19,3}$	$2^{63}, \quad 0$	$e_{19,2}[*64]$
$e_{19,4}, e_{19,5}$	$2^9, \quad -2^9$	$e_{19,4}[10], e_{19,5}[-10]$
$v_{20,0}, v_{20,5}, v_{20,7}$	$2^{63}, \quad 2^{63}, \quad 2^{63}$	$v_{20,0}[*64], v_{20,5}[*64], v_{20,7}[*64]$
$e_{20} \sim v_{28}$	0	
$e_{28,6}, e_{28,7}$	$2^{63}, \quad 2^{63}$	$e_{28,6}[*64], e_{28,7}[*64]$
$e_{29,2}, e_{29,3}$	$0, \quad 2^{23}$	$e_{29,3}[24]$
$e_{30,0}, e_{30,1}$	$2^{23}, \quad 0$	$e_{30,0}[24]$
$e_{30,6}, e_{30,7}$	$0, \quad 2^9+2^{23}$	$e_{30,7}[10,24]$
$e_{31,0}, e_{31,1}$	$0, \quad 2^{23}$	$e_{31,1}[24]$
$e_{31,2}, e_{31,3}$	$0, \quad 2^2+2^9+2^{23}+2^{52}$	$e_{31,3}[3,10,24,53]$
$e_{31,4}, e_{31,5}$	$2^9+2^{23}, \quad 0$	$e_{31,4}[10,24]$
$e_{31,6}, e_{31,7}$	$2^{23}, \quad 0$	$e_{31,6}[24]$
$v_{32,0}, v_{32,1}$	$2^2+2^9+2^{23}+2^{52}, \quad -2^{23}+2^{31}$	$v_{32,0}[3,10,24,53], v_{32,1}[-24,32]$
$v_{32,2}, v_{32,3}$	$2^9+2^{23}, \quad -2^{23}$	$v_{32,2}[10,24], v_{32,3}[-24]$
$v_{32,4}, v_{32,5}$	$2^{23}, \ 2^9-2^{23}$	$v_{32,4}[24], v_{32,5}[10,-24]$
$v_{32,6}, v_{32,7}$	$2^{23}, \ 2^2+2^9+2^{37}+2^{44}+2^{52}+2^{58}$	$v_{32,6}[24], v_{32,7}[3,10,38,45,53,59]$
$e_{32,0}, e_{32,1}$	$2^2+2^9+2^{23}+2^{52}, \quad -2^{23}+2^{31}$	$e_{32,1}[-24,32]$
$e_{32,2}, e_{32,3}$	$2^9+2^{23}, \quad -2^{23}$	$e_{32,3}[-24]$
$e_{32,4}, e_{32,5}$	$2^{23}+2^{63}, \ 2^9-2^{23}+2^{63}$	$e_{32,5}[10,-24,*64]$
$e_{32,6}, e_{32,7}$	$2^{23}+2^{63}, \ 2^2+2^9+2^{37}+2^{44}+2^{52}+2^{58}$	$e_{32,7}[3,10,38,45,53,59]$
$e_{33,0}$	2^9	$e_{33,0}[10]$
$e_{33,1}$	$2^2+2^5-2^9+2^{13}+2^{31}+2^{52}$	$e_{33,1}[3,6,-10,14,32,53]$

$e_{33,2}$	2^9	$e_{33,2}[10]$
$e_{33,3}$	$2^2+2^9-2^{10}+2^{17}+2^{23}+2^{25}+2^{31}+2^{37}$ $+2^{39}+2^{44}+2^{46}+2^{52}+2^{58}+2^{63}$	$e_{33,3}[3,10,-11,18,24,26,32,38,$ $40,45,47,53,59,*64]$
$e_{33,4}$	$2^2+2^9+2^{23}+2^{37}+2^{44}+2^{52}+2^{58}+2^{63}$	$e_{33,4}[3,10,24,38,45,53,59,*64]$
$e_{33,5}$	$-2^9+2^{18}+2^{28}+2^{42}$	$e_{33,5}[-10,19,29,43]$
$e_{33,6}$	$2^2+2^9+2^{31}+2^{52}$	$e_{33,6}[3,10,32,53]$
$e_{33,7}$	-2^9+2^{59}	$e_{33,7}[-10,60]$
$v_{34,0}$	$2^2+2^{17}+2^{23}+2^{25}+2^{31}+2^{37}+2^{39}$ $+2^{44}+2^{46}+2^{52}+2^{58}+2^{63}$	$v_{34,0}[3,18,24,26,32,38,40,$ $45,47,53,59,*64]$
$v_{34,1}$	$1+2^2+2^5+2^{13}+2^{21}+2^{31}+2^{35}+2^{38}$ $+2^{42}+2^{46}+2^{52}$	$v_{34,1}[1,3,6,14,22,32,36,39,$ $43,47,53]$
$v_{34,2}$	$2^2+2^{18}+2^{23}+2^{28}+2^{37}+2^{42}+2^{44}+2^{52}$ $+2^{58}+2^{63}$	$v_{34,2}[3,19,24,29,38,43,45,53,$ $59,*64]$
$v_{34,3}$	$2^2+2^{31}+2^{37}+2^{51}+2^{52}+2^{59}$	$v_{34,3}[3,32,38,52,53,60]$
$v_{34,4}$	$2^2+2^{31}+2^{52}+2^{59}$	$v_{34,4}[3,32,53,60]$
$v_{34,5}$	$2^2+2^{18}+2^{28}+2^{32}+2^{37}+2^{44}+2^{52}$ $+2^{56}+2^{58}+2^{63}$	$v_{34,5}[3,19,29,33,38,45,53,$ $57,59,*64]$
$v_{34,6}$	$2^2+2^5+2^{13}+2^{31}+2^{52}$	$v_{34,6}[3,6,14,32,53]$
$v_{34,7}$	$1+2^7+2^9+2^{15}+2^{17}+2^{21}+2^{23}$ $+2^{25}+2^{26}+2^{29}+2^{31}+2^{36}$ $+2^{39}+2^{46}+2^{50}+2^{63}$	$v_{34,7}[1,8,10,16,18,22,24,$ $26,27,30,32,37,$ $40,47,51,*64]$
$e_{34,0}$	$2^2+2^{17}+2^{23}+2^{25}+2^{31}+2^{37}+2^{39}$ $+2^{44}+2^{46}+2^{52}+2^{58}+2^{63}$	
$e_{34,1}$	$1+2^2+2^5+2^{13}+2^{21}+2^{31}+2^{35}+2^{38}$ $+2^{42}+2^{46}+2^{52}$	
$e_{34,2}$	$2^2+2^{18}+2^{23}+2^{28}+2^{37}+2^{42}+2^{44}+2^{52}$ $+2^{58}$	
$e_{34,3}$	$2^2+2^{31}+2^{37}+2^{51}+2^{52}+2^{59}+2^{63}$	
$e_{34,4}$	$2^2+2^{31}+2^{52}+2^{59}$	
$e_{34,5}$	$2^2+2^{18}+2^{28}+2^{32}+2^{37}+2^{44}+2^{52}$ $+2^{56}+2^{58}$	
$e_{34,6}$	$2^2+2^5+2^{13}+2^{31}+2^{52}+2^{63}$	
$e_{34,7}$	$1+2^7+2^9+2^{15}+2^{17}+2^{21}+2^{23}$ $+2^{25}+2^{26}+2^{29}+2^{31}+2^{36}$ $+2^{39}+2^{46}+2^{50}+2^{63}$	

* both positive and negative are OK

Table 7. Sufficient Conditions of the Trail in Table 4

$e_{0,5,33}=1; e_{0,5,49}=1; e_{0,3,4}=1; e_{0,3,10}=1; e_{0,3,40}=1; e_{0,3,43}=1;$ $e_{0,1,0}=1; e_{0,1,8}=1; e_{0,1,30}=1; e_{0,1,36}=1; e_{0,1,58}=1;$ $e_{0,7,15}=1; e_{0,7,31}=1$
$e_{1,4,4}=0; e_{1,2,4}=0; e_{1,2,52}=0; e_{1,0,46}=0; e_{1,0,15}=0; e_{1,6,12}=0;$ $e_{1,6,18}=0; e_{1,6,40}=0; e_{1,6,54}=0; e_{1,4,52}=0; e_{1,6,46}=0; e_{1,0,12}=0;$ $e_{1,0,40}=0$
$e_{2,4,15}=0; e_{2,4,54}=0; e_{2,6,15}=0; e_{2,2,18}=0; e_{2,0,15}=0$
$e_{3,2,54}=0; e_{3,4,54}=0$
$e_{14,5,9}=0$
$e_{15,5,38}=0; e_{15,2,46}=0; e_{14,5,48}=0; e_{15,2,9}=0; e_{15,3,42}=0$
$v_{16,0,9}=0; v_{16,0,43}=0; v_{16,2,9}=0; v_{16,2,38}=0; v_{16,2,48}=0;$ $v_{16,1,7}=0; v_{16,7,34}=0; v_{16,0,13}=0; e_{15,3,38}=0; e_{15,3,7}=0;$ $e_{15,5,1}=0; e_{15,5,30}=0; e_{15,5,40}=0; v_{16,5,55}=0; v_{16,2,1}=0;$ $v_{16,2,30}=0; v_{16,2,40}=0; v_{16,3,21}=0$

Table 8. Sufficient Conditions of the Trail in Table 5

$v_{32,0,9}=0; v_{32,0,43}=0; v_{32,2,9}=0; v_{32,2,38}=1; v_{32,2,39}=0; v_{32,2,48}=0;$ $v_{32,1,7}=0; v_{32,7,34}=0; v_{32,0,13}=0; e_{31,3,38}=0; e_{31,3,7}=0;$ $e_{31,5,17}=0; e_{31,5,46}=0; e_{31,5,47}=1; e_{31,5,56}=0; v_{32,5,55}=0; v_{32,2,1}=0;$ $v_{32,2,30}=0; v_{32,2,40}=0; v_{32,3,21}=0$
$e_{32,1,7}=0; e_{32,7,9}=0; e_{32,7,13}=0; e_{32,7,34}=0; e_{32,7,42}=0; e_{32,5,1}=0;$ $e_{32,5,9}=0; e_{32,5,30}=0; e_{32,5,38}=0; e_{32,5,48}=0; e_{32,5,55}=0; e_{32,3,21}=0$
$v_{33,6,7}=0; v_{33,6,9}=0; v_{33,6,42}=0; e_{32,1,25}=0; e_{32,1,27}=1; e_{32,1,60}=0; v_{32,6,53}=0;$ $v_{33,0,9}=0; v_{33,0,21}=0; v_{33,0,38}=0; v_{33,0,48}=0; e_{32,3,37}=1; v_{33,0,57}=0; v_{33,0,35}=0;$ $e_{32,3,2}=1; e_{32,3,12}=1; e_{32,3,49}=1; v_{33,2,1}=0; v_{33,2,9}=1; v_{33,2,10}=0; v_{33,2,30}=0;$ $v_{33,2,38}=0; v_{33,2,48}=1; v_{33,2,49}=0; v_{33,2,55}=0; e_{32,5,49}=1; v_{33,2,3}=0;$ $e_{32,5,54}=0; v_{33,2,20}=1; v_{33,2,28}=1; e_{32,5,11}=1; e_{32,5,19}=0; e_{32,5,29}=1;$ $e_{32,5,36}=0; v_{33,2,57}=1; v_{33,4,9}=0; v_{33,4,13}=0; v_{33,4,34}=0; v_{33,4,42}=0;$ $v_{33,4,7}=0; e_{32,7,36}=1; e_{32,7,40}=1; v_{33,4,15}=1; e_{32,7,61}=1; e_{32,7,5}=1;$ $v_{33,4,46}=1; v_{33,4,50}=1$

Table 9. Sufficient Conditions of the Trail in Table 6

$e_{16,1,3} = 1; e_{16,1,13} = 1; e_{16,1,17} = 1; e_{16,1,19} = 1; e_{16,1,39} = 1; e_{16,1,45} = 1;$ $e_{16,1,55} = 1; e_{16,1,58} = 1; e_{16,3,4} = 1; e_{16,3,13} = 1; e_{16,3,23} = 1; e_{16,3,29} = 1;$ $e_{16,3,37} = 1; e_{16,3,49} = 1; e_{16,3,62} = 1; e_{16,5,4} = 1; e_{16,5,52} = 1; e_{16,5,58} = 1;$ $e_{16,7,34} = 1; e_{16,7,40} = 1; e_{16,7,50} = 1$
$e_{17,0,1} = 0; e_{17,0,9} = 0; e_{17,0,34} = 0; e_{17,0,40} = 0; e_{17,2,7} = 0; e_{17,4,13} = 0;$ $e_{17,4,23} = 0; e_{17,6,21} = 0; e_{17,6,27} = 0; e_{17,6,37} = 0; e_{17,6,49} = 0; e_{17,6,59} = 0;$ $e_{17,6,1} = 0; e_{17,6,40} = 0; e_{17,4,7} = 0; e_{17,2,13} = 0; e_{17,2,23} = 0;$ $e_{17,0,21} = 0; e_{17,0,49} = 0; e_{17,0,59} = 0$
$e_{18,4,27} = 0; e_{18,4,37} = 0; e_{18,6,9} = 0; e_{18,6,34} = 0; e_{18,2,27} = 0;$ $e_{18,2,37} = 0; e_{18,0,34} = 0$
$e_{19,4,9} = 0; e_{19,2,9} = 0$
$e_{29,3,23} = 0$
$e_{30,0,23} = 0; e_{30,0,9} = 0; e_{29,3,37} = 0$
$e_{31,4,9} = 0; e_{31,4,23} = 0; e_{31,6,23} = 0; e_{30,1,62} = 0;$ $e_{31,4,2} = 0; e_{30,7,30} = 0; e_{30,7,44} = 0; e_{31,4,52} = 0$
$v_{32,0,2} = 0; v_{32,0,9} = 0; v_{32,0,23} = 0; v_{32,0,52} = 0; v_{32,2,9} = 0; v_{32,2,23} = 0;$ $v_{32,4,23} = 0; v_{32,6,23} = 0; e_{31,1,15} = 1; v_{32,6,31} = 0; e_{31,7,1} = 1; e_{31,5,17} = 0;$ $e_{31,5,31} = 1; e_{31,3,31} = 0; e_{31,3,38} = 0; v_{32,0,37} = 0; v_{32,0,44} = 0; e_{31,3,17} = 0;$ $v_{32,0,58} = 0$
$e_{32,1,23} = 1; e_{32,1,31} = 0; e_{32,3,23} = 1; e_{32,5,9} = 0; e_{32,5,23} = 1;$ $e_{32,7,2} = 0; e_{32,7,9} = 0; e_{32,7,37} = 0; e_{32,7,44} = 0; e_{32,7,52} = 0; e_{32,7,58} = 0;$
$e_{33,0,9} = 0; e_{33,2,9} = 0; e_{33,4,2} = 0; e_{33,4,9} = 0; e_{33,4,23} = 0; e_{33,4,37} = 0;$ $e_{33,4,44} = 0; e_{33,4,52} = 0; e_{33,4,58} = 0; e_{33,6,2} = 0; e_{33,6,9} = 0; e_{33,6,31} = 0;$ $e_{33,6,52} = 0; e_{32,1,20} = 0; e_{33,6,5} = 1; e_{32,1,27} = 1; e_{33,6,13} = 0; e_{32,1,49} = 0;$ $e_{32,1,6} = 0; e_{32,7,29} = 0; e_{32,7,36} = 0; e_{33,4,10} = 1; e_{33,4,17} = 0; e_{32,7,50} = 0;$ $e_{33,4,25} = 0; e_{33,4,31} = 0; e_{32,7,0} = 0; e_{33,4,39} = 0; e_{32,7,7} = 0; e_{33,4,46} = 0;$ $e_{32,7,15} = 0; e_{32,7,21} = 0; e_{32,5,54} = 1; e_{33,5,18} = 0; e_{33,2,28} = 0; e_{33,2,42} = 1;$ $e_{32,3,37} = 1; e_{33,0,59} = 1;$
$v_{34,0,2} = 0; v_{34,0,17} = 0; v_{34,0,23} = 0; v_{34,0,25} = 0; v_{34,0,31} = 0; v_{34,0,37} = 0;$ $v_{34,0,39} = 0; v_{34,0,44} = 0; v_{34,0,46} = 0; v_{34,0,52} = 0; v_{34,0,58} = 0; v_{34,2,2} = 0;$ $v_{34,2,18} = 0; v_{34,2,23} = 0; v_{34,2,28} = 0; v_{34,2,37} = 0; v_{34,2,42} = 0; v_{34,2,44} = 0;$ $v_{34,2,52} = 0; v_{34,2,58} = 0; v_{34,4,2} = 0; v_{34,4,31} = 0; v_{34,4,52} = 0; v_{34,4,59} = 0;$ $v_{34,6,2} = 0; v_{34,6,5} = 0; v_{34,6,13} = 0; v_{34,6,31} = 0; v_{34,6,52} = 0; v_{34,6,0} = 0;$ $e_{33,1,33} = 0; e_{33,1,36} = 0; e_{33,1,44} = 0; v_{34,6,21} = 0; e_{33,1,62} = 0; v_{34,6,35} = 0;$ $v_{34,6,38} = 0; v_{34,6,42} = 1; v_{34,6,46} = 0; e_{33,1,19} = 0; e_{33,7,24} = 0; e_{33,7,53} = 0;$ $v_{34,4,37} = 0; v_{34,4,51} = 1; e_{33,7,10} = 0; e_{33,7,17} = 0; e_{33,5,52} = 0; e_{33,5,4} = 0;$ $e_{33,5,14} = 0; v_{34,2,32} = 0; e_{33,5,23} = 0; e_{33,5,30} = 0; e_{33,5,38} = 0; v_{34,2,56} = 0;$ $e_{33,5,44} = 0; v_{34,0,0} = 0; v_{34,0,7} = 0; v_{34,0,9} = 0; v_{34,0,15} = 0; e_{33,3,54} = 0;$ $v_{34,0,21} = 0; e_{33,3,60} = 0; e_{33,3,62} = 0; v_{34,7,26} = 0; v_{34,0,29} = 0; e_{33,3,4} = 0;$ $v_{34,0,36} = 0; e_{33,3,12} = 0; e_{33,3,19} = 0; v_{34,0,50} = 0;$