Wuhan University
Journal of Natural Sciences

2012, Vol.17 No.5, 414-420

Article ID 1007-1202(2012)05-0414-07
DOI 10.1007/s11859-012-0863-y

A Related-Key Boomerang Distinguishing Attack of Threefish-256

□ **LIU Shusheng, WANG Libin, GONG Zheng**[†]

School of Computer Science, South China Normal University, Guangzhou 510631, Guangdong, China

Abstract: The block cipher Threefish is the main component of Skein, which is based on ARX. Based on the efficient algorithms for calculating the differential of modular addition, we extend local collisions of Threefish-256 to more round by using related-key differential of addition in this paper. A related-key boomerang distinguish attack is proposed on 31-round Threefish-256 with a time complexity of 2^{234} .

Key words: Skein; differential analysis; related-key analysis; Boomerang attack
CLC number: TN 918.4

0 Introduction

In cryptology, hash functions are designed to protect the data integrity by producing a fixed-length digest from an arbitrary-length message. Based on Wang *et al*'s breakthrough in hash cryptanalysis, the widely used hash functions (MD5, SHA-1, etc.) have been seriously attacked in Refs. [1-4]. If SHA-256 and SHA-512 were to be broken, the industry does not have any generally accepted hash functions. As a response to this undesirable consequence, a public competition was held by the National Institute of Standards and Technology to collect the new designs for a secure and applicable hash function. After 2-round competitions, five algorithms[5] have been selected as the final round candidates. One of the five proposals will be chosen as the SHA-3 standard in 2012.

The hash function Skein[6], which was designed by Ferguson *et al*, has been selected as the one of the five final-round candidates for the SHA-3 competition. The design rationale of Skein combines speed, security, and simplicity. Its conservative design provides a large security margin for the resistance of cryptanalysis. In the Skein proposal, the compression function of Skein is constructed from a family of tweakable block ciphers, which is called Threefish. The family supports three different variants called Threefish-256, -512, and -1024, which implies to Skein-256, -512, and -1024, respectively. The algorithms within Threefish are fully based on addition, exclusive-or (XOR), and constant rotation (which are called ARX operations) on 64-bit words.

In Refs. [7-10], many cryptanalyses have been proposed on the compression function of Skein and the un-

Received date: 2012-02-23
Foundation item: Supported by the National Natural Science Foundation of China (61100201) and the Foundation for Distinguished Young Talents in Higher Education of Guangdong (LYM11053)

Biography: LIU Shusheng, male, Master candidate, research direction: symmetric cryptography. E-mail: liushusheng914@gmail.com
† To whom correspondence should be addressed. E-mail: cis.gong@gmail.com

derlying block cipher Threefish. Aumasson *et al.* presented a related-key boomerang distinguishing attack on 34-round Threefish-512 with the old rotation constant[7]. Su *et al*[8] proposed a 24-round near-collision of Skein-256/512 compression functions by using linear-differential analysis. Yu *et al*[9] presented a semi-free start near-collision attack on 32-round Skein-256 compression functions based on the rebound attack, whereas Khovratovich *et al* proposed a distinguishing attack of 53-round Skein-256 and 57-round Skein-512 by using the rotational rebound attack[10].

In this article, we present a related-key boomerang attack on 31-round Threefish-256. Our cryptanalysis is different from the cryptanalysis in Ref. [9]. It is only valid for the compression function of Skein-256 that near-collision is obtained by using rebound attack. Our attack analyzes the related-key boomerang property of the block cipher Threefish-256. Our attack is based on an efficient algorithm for computing the differential of modular addition. The strategy behind our attack is to extend local collisions to more rounds by using related-key differential of the addition. In order to avoid fast increasing complexity of attack, we deal with it using boomerang attack. We obtain a related-key boomerang distinguishing attack of 31-round Threefish-256 with a time complexity of 2^{234}.

The remainder of this article is organized as follows: Section 1 describes the preliminaries for our attack. Section 2 first introduces two short related-key differentials; then, our related-key boomerang distinguishing attack of 31-round Threefish-256 is presented. Finally, a conclusion is given in Section 3.

1 Preliminaries

In this section, we first define the notations used throughout this paper and then briefly describe the related-key boomerang attack, the algorithm for computing differential of addition. Finally, we recall the specification of Threefish-256.

1.1 Notations

The notations used in our cryptanalysis are described as follows. Let + denote addition modulo 2^{64}. <<< and >>> are cyclic left and right rotations, respectively. << and >> are shift to left and right, respectively. Moreover, let $\oplus$, $\vee$, $\wedge$, and $\neg$ be "XOR", "OR", "AND", and "NOT" operation, respectively. Let K denote the master key of Threefish-256, whereas K_i is the *i*th word of *K*. sk_i denotes the *i*th round subkey. Moreover, $\mathrm{sk}_{i,j}$ is the *j*th word of sk_i. Let *T* denote the tweak of Threefish-256, whereas T_i is the *i*th word of tweak *T*. Furthermore, let R_i denote the *i*th round of Threefish and Δx denote the XOR difference of *x* and x', whereas ΔK_i denotes the XOR difference of the *i*th word of *K* and K'. $\Delta \mathrm{sk}_{i,j}$ represents the XOR difference of the *j*th word of sk_i.

1.2 Related-Key Boomerang Attack

The related-key attack was first introduced by Biham[11]. The attack allows the accesses to encrypt plaintexts and decrypt ciphertexts under multiple unknown keys, but the relation between the unknown key is known to (or even chosen by) the adversary. The boomerang attack was introduced by Wagner[12]. By extending the boomerang attack in the related-key model, Biham *et al.* proposed the related-key boomerang attack[13]. As shown in Fig. 1, the related-key boomerang attack views a cipher *E* as a decomposition into two subciphers, such that $E = E_\alpha \circ E_\beta$. In each of two subciphers, there exists a high probability related-key differential for constructing a boomerang attack.

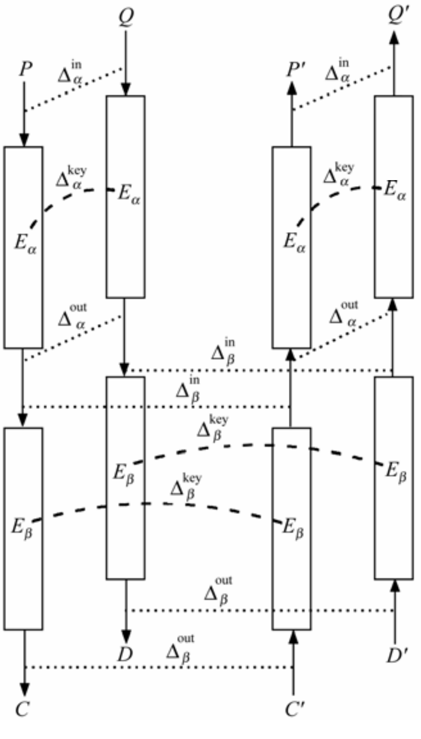

Fig. 1 A schematic of related-key boomerang attack

······ a difference of plaintexts or ciphertexts

– – – a related-key difference

If the probability of the E_α differential $(\Delta_\alpha^{in}, \Delta_\alpha^{out}, \Delta_\alpha^{key})$ is *p* and the probability of the E_β differential $(\Delta_\chi^{in}, \Delta_\beta^{out}, \Delta_\beta^{key})$ is *q*, it was proven that the probability of the corresponding related-key boomerang attack is close to $(p \bullet q)^2$.

1.3 Algorithm for Computing Differential of Addition

For integer addition, the efficient algorithms for computing the probability of any differential and finding the optimal differential were analyzed[14]. For S-function, a general framework is presented later[15], which is used to calculate the probability that, given input differences lead to given output differences, as well as to count the number of output differences with non-zero probability. Because the results of algorithm in Ref. [14] and algorithm in Ref. [15] for computing the probability of integer addition are equal, and we need to find the optimal differential of integer addition in this paper, we use efficient algorithms in Ref. [14]. They are described as follows.

Without losing the generality, the differential of addition modulo 2^n often denotes as a triplet of two input and one output differences such that $(\alpha,\beta \mapsto \gamma)$, $\alpha,\beta,\gamma \in \{0,1\}^n$. The differential probability of modular addition is defined as follows:

$$\mathrm{DP}^{+}(\alpha,\beta \mapsto \gamma) := \Pr[(x+y)\oplus((x\oplus\alpha)+(y\oplus\beta))=\gamma \mid x,y\in\{0,1\}^n]$$

The maximum differential probability of modular addition is defined in the following equation:

$$\mathrm{DP}^{+}_{\max}(\alpha,\beta) := \max_{\gamma}(\mathrm{DP}^{+}(\alpha,\beta \mapsto \gamma))$$

The all-one parity of an n-bit number x is another n-bit number y=aop(x), and aop(x) is calculated by Algorithm 1. Algorithm 2, which was introduced by Lipmaa and Moriai[14], finds all output differences γ that satisfy $\mathrm{DP}^{+}(\alpha,\beta \mapsto \gamma)$ is equal to $\mathrm{DP}^{+}_{\max}(\alpha,\beta)$. Lipmaa and Moriai also presented the definition of several functions[14], which are used in Algorithm 2. The common alternation parity of two n-bit numbers x and y is a function $C(x, y)$, such that $C(x,y) := \mathrm{aop}(\neg(x\oplus y) >> 1)\wedge(x\oplus(x>>1)))$.

Algorithm 1 Log-time algorithm for aop(x)

```
Input: $x \in \{0,1\}^n$.
Output: aop($x$).
    $x[1] = x \wedge (x >> 1)$;
    for $i \leftarrow 2$ to $\log_2 n$ do
        $x[i] \leftarrow x[i-1] \wedge (x[i-1] >> 2^{i-1})$;
    $y[1] \leftarrow x \wedge \neg x[1]$;
    for $i \leftarrow 2$ to $\log_2 n$ do
        $y[i] \leftarrow y[i-1] \vee (y[i-1] >> 2^{i-1}) \wedge x[i-1]$;
    return $y[\log_2 n]$;
```

Algorithm 2 Algorithm for bestdfs (α,β) that finds all γ, $\mathrm{DP}^{+}(\alpha,\beta \mapsto \gamma) = \mathrm{DP}^{+}_{\max}(\alpha,\beta)$

```
Input: $(\alpha,\beta)$.
Output: all $(\alpha,\beta)$-optimal output differences $\gamma$.
    $\gamma_0 \leftarrow \alpha_0 \oplus \beta_0$;
    $p \leftarrow C(\alpha,\beta)$;
    for $i \leftarrow 1$ to $n-1$ do
        if $\alpha_{i-1}=\beta_{i-1}=\gamma_{i-1}$, then $\gamma_i \leftarrow \alpha_i \oplus \beta_i \oplus \alpha_{i-1}$;
        else if $i=n-1$ or $\alpha_i \neq \beta_i$ or $p_i = 1$, then $\gamma_i = \{0,1\}$;
        else $\gamma_i = \alpha_i$;
    return $\gamma$;
```

1.4 Brief Description of Threefish-256

Threefish-256 works on 64-bit words using XOR, addition modulo 2^{64}, and cyclic shift. A 256-bit plaintext is parsed as four words $v_{0,0},\cdots,v_{0,3}$, and encrypted through $N_{\mathrm{r}}=72$ rounds. Round d is from 1 to 72, and the encryption procedure of Threefish-256 operates as follows:

1) If $d \equiv 1 \bmod 4$, add a subkey by setting $e_{d,i} = v_{d-1,i} + k_{d/4}$, $i=0,\cdots,3$. Else, $e_{d,i} = v_{d-1,i}$, $i=0,\cdots,3$.

2) $(f_{d,2i}, f_{d,2i+1}) \leftarrow \mathrm{MIX}_{d,i}(e_{d,2i}, e_{d,2i+1})$, for $i=0,1$. MIX function is defined by

$$\mathrm{MIX}_{d,i}(x,y) := (x+y,(x+y)\oplus(y << \mathrm{RC}_{(d-1)\bmod 8,i}))$$

where $\mathrm{RC}_{(d-1)\bmod 8,i}$ is a rotation constant in row $(d-1)\bmod 8$ column of I of the rotation constant table that can be found in Ref. [6].

3) Permute the state words:

$$v_{d,0}=f_{d,0},\ v_{d,1}=f_{d,3},\ v_{d,2}=f_{d,2},\ v_{d,3}=f_{d,1}$$

After 72 rounds, the ciphertext is

$$(v_{72,0}+k_{19,0},\cdots,v_{72,3}+k_{19,3})$$

The set of subkeys is derived from the master key $K=(K_0,K_1,K_2,K_3)$ and tweak $T=(T_0,T_1)$ as follows:

$$\mathrm{sk}_{s,0} = K_{(s+0)\bmod 5}$$

$$\mathrm{sk}_{s,1} = K_{(s+1)\bmod 5} + T_{s\bmod 3}$$

$$\mathrm{sk}_{s,2} = K_{(s+2)\bmod 5} + T_{(s+1)\bmod 3}$$

$$\mathrm{sk}_{s,3} = K_{(s+3)\bmod 5} + s$$

where $K_4 = \lfloor 2^{64}/3 \rfloor \oplus K_0 \oplus K_1 \oplus K_2 \oplus K_3$, $T_2 = T_{01} \oplus T$, and s is the value of the sth round.

2 Proposed Attack

In this section, we describe how to build a related-key boomerang of Threefish-256. E_α is viewed as the subcipher of the first 17 rounds of Threefish-256, and E_β is viewed as the subcipher of the following 14 rounds (18–31) of Threefish-256. We obtain a related-key differential of E_α with a probability 2^{-99} and a related-key differential of E_β with a probability 2^{-18}. Thus, the boomerang distinguishing attack that makes use of E_α and E_β has a probability 2^{-234}. The details of the attack will be depicted in the following subsections.

2.1 Subkey Differential

Following the key schedule of Threefish-256, one can get all subkeys from an encryption key. Table 1 illustrates an overview of nine subkeys that will be used in the first 32-round Threefish-256. The number *i* denotes the round constant. The subkey differentials of E_α and E_β are searched for the related-keys boomerang distinguishing attack.

Table 1 First nine subkeys of the Threefish-256 key schedule

Subkey	Word 0	Word 1	Word 2	Word 3
sk_0	K_0	K_1+T_0	K_2+T_1	K_3+0
sk_1	K_1	K_2+T_1	K_3+T_2	K_4+1
sk_2	K_2	K_3+T_2	K_4+T_0	K_0+2
sk_3	K_3	K_4+T_0	K_0+T_1	K_1+3
sk_4	K_4	K_0+T_1	K_1+T_2	K_2+4
sk_5	K_0	K_1+T_2	K_2+T_0	K_3+5
sk_6	K_1	K_2+T_0	K_3+T_1	K_4+6
sk_7	K_2	K_3+T_1	K_4+T_2	K_0+7
sk_8	K_3	K_4+T_2	K_0+T_0	K_1+8

● **Subkeys differential of E_α.** For a pair of key and tweak, their difference patterns are chosen for the related-key differential of E_α as follows:

$$((K_0,K_1,K_2,K_3),(T_0,T_1)) \neq ((K_0',K_1',K_2',K_3'),(T_0',T_1'))$$

Hence, the difference in the sk_2 is eliminated, which implies $K_2=K_2', K_3+T_2=K_3'+T_2', K_4+T_0=K_4'+T_0', K_0+2=K_0'+2$. Let the difference δ =0x8000000000000000, where the most significant bit is isolated. One set difference of key/tweak pair can be represented as follows:

$$K_2 \oplus K_2' = 0\,,\ K_0 \oplus K_0' = 0\,,\ K_1 \oplus K_1' = 0\,,$$
$$K_3 \oplus K_3' = \delta\,,\ T_0 \oplus T_0' = \delta\,,\ T_1 \oplus T_1' = \delta$$

Under condition $\Delta_\alpha^{\mathrm{key}} = ((\Delta K_0 \Delta K_1 \Delta K_2 \Delta K_3),(\Delta T_0, \Delta T_1)) = ((0000),(\delta 0))$, the difference of the *i*th subkeys ($0 \leqslant i \leqslant 4$) is shown in Table 2.

Table 2 Subkey's differences of the Threefish-256 key

Subkey	Subkeys differential of E_α	Subkey	Subkeys differential of E_β
$\Delta\mathrm{sk}_0$	$(0,\delta,0,\delta)$	$\Delta\mathrm{sk}_5$	$(0,0,0,\delta)$
$\Delta\mathrm{sk}_1$	$(0,0,0,\delta)$	$\Delta\mathrm{sk}_6$	$(0,0,0,0)$
$\Delta\mathrm{sk}_2$	$(0,0,0,0)$	$\Delta\mathrm{sk}_7$	$(\delta,0,0,0)$
$\Delta\mathrm{sk}_3$	$(\delta,0,0,0)$	$\Delta\mathrm{sk}_8$	$(\delta,0,\delta,0)$
$\Delta\mathrm{sk}_4$	$(\delta,0,\delta,0)$		

● **Subkeys differential of E_β.** A difference of key/tweak pair is chosen for the related-key differential of E_β such that $\Delta\mathrm{sk}_6$= (0,0,0,0). This implies

$$K_1 = K_1', K_2 + T_0 = K_2' + T_0',$$
$$K_3 + T_1 = K_3' + T_1', K_4 + 6 = K_4' + 6$$

One can set $\Delta_\beta^{\mathrm{key}} = ((\Delta K_0 \Delta K_1 \Delta K_2 \Delta K_3),(\Delta T_0, \Delta T_1)) = ((00\delta\delta),(\delta\delta))$ to obtain $\Delta\mathrm{sk}_6$=(0,0,0,0). In this case, $\Delta\mathrm{sk}_5$= (0,0,0, δ). The difference of the *i*th subkeys ($5 \leqslant i \leqslant 8$) is given in Table 2.

2.2 Differential of E_α

In this section, we search the related-key differential of E_α. Firstly, we assign the output difference of R_4 to $\Delta\mathrm{sk}_1 = (0,0,0,\delta)$, and then we compute the backward related-key differential from R_4 to R_1. Secondly, we investigate the forward related-key differential from R_{13} to R_{17}.

Trial of R_1 to R_4**.** In order to reach the output difference of $R_4(0,0,0,\delta)$, we need to reverse the difference of R_4 to the input difference sk_0. In Fig. 2, the numbers connected with the arrows are the Hamming weight of the differences. $\Delta\mathrm{sk}_1$ is assigned to the output difference of R_4. The input difference of sk_0 is calculated from $\Delta\mathrm{sk}_1$ in backward. The input difference of round 4 is described as follows:

$$\Delta v_{4,1} = (\Delta\mathrm{sk}_{1,0} \oplus \Delta\mathrm{sk}_{1,3}) >>> 5\,,\ \Delta v_{4,0} = \Delta v_{4,1} \oplus \Delta\mathrm{sk}_{1,0}\,,$$
$$\Delta v_{4,3} = (\Delta\mathrm{sk}_{1,2} \oplus \Delta\mathrm{sk}_{1,1}) >>> 37\,,\ \Delta v_{4,2} = \Delta v_{4,3} \oplus \Delta\mathrm{sk}_{1,2}$$

$\Delta v_{i,j}$ is the input difference of the *j*th word of the *i*th round, whereas the corresponding rotation constants (5 and 37) are used in the R_4 of Threefish-256. The input difference of $E_\alpha(v_{0,0}, v_{0,1}, v_{0,2}, v_{0,3})$ with the effect of $\Delta\mathrm{sk}_0$ is computed in the following equations.

$$\Delta v_{0,0} = \Delta\mathrm{sk}_{0,0} \oplus \Delta v_{1,0}\,,\ \Delta v_{0,1} = \Delta\mathrm{sk}_{0,1} \oplus \Delta v_{1,1}\,,$$
$$\Delta v_{0,2} = \Delta\mathrm{sk}_{0,2} \oplus \Delta v_{1,2}\,,\ \Delta v_{0,3} = \Delta\mathrm{sk}_{0,3} \oplus \Delta v_{1,3}$$

The first 4-round related-key differential of E_α is listed in Table 3.

Trial of R_5 to R_{12}. The sk_1 adds difference (0,0,0, δ) to the output difference of R_4 so that its difference is vanished. The state of difference remains (0,0,0,0) until the sk_3 is added. After the effect of sk_3, the value of the output difference is (δ ,0,0,0). Figure 2 illustrates the trail.

Trial of R_{13} to R_{17}**.** In this step, the related-key differential from R_{13} to R_{17} is calculated by equation (1) ($13 \leqslant i \leqslant 17$), where the input difference of R_{13} is (δ ,0,0,0). Figure 2 illustrates the trail, whereas its patterns are also given in Table 3.

$$\begin{cases} \Delta v_{i+1,0} = \mathrm{bestdfs}(\Delta v_{i,0}, \Delta v_{i,1}) \\ \Delta v_{i+1,2} = \mathrm{bestdfs}(\Delta v_{i,2}, \Delta v_{i,3}) \\ \Delta v_{i+1,1} = \Delta v_{i+1,2} \oplus (\Delta v_{i,3} <<< \mathrm{RC}_{(i-1)\bmod 8,1}) \\ \Delta v_{i+1,3} = \Delta v_{i+1,0} \oplus (\Delta v_{i,1} <<< \mathrm{RC}_{(i-1)\bmod 8,0}) \end{cases} \tag{1}$$

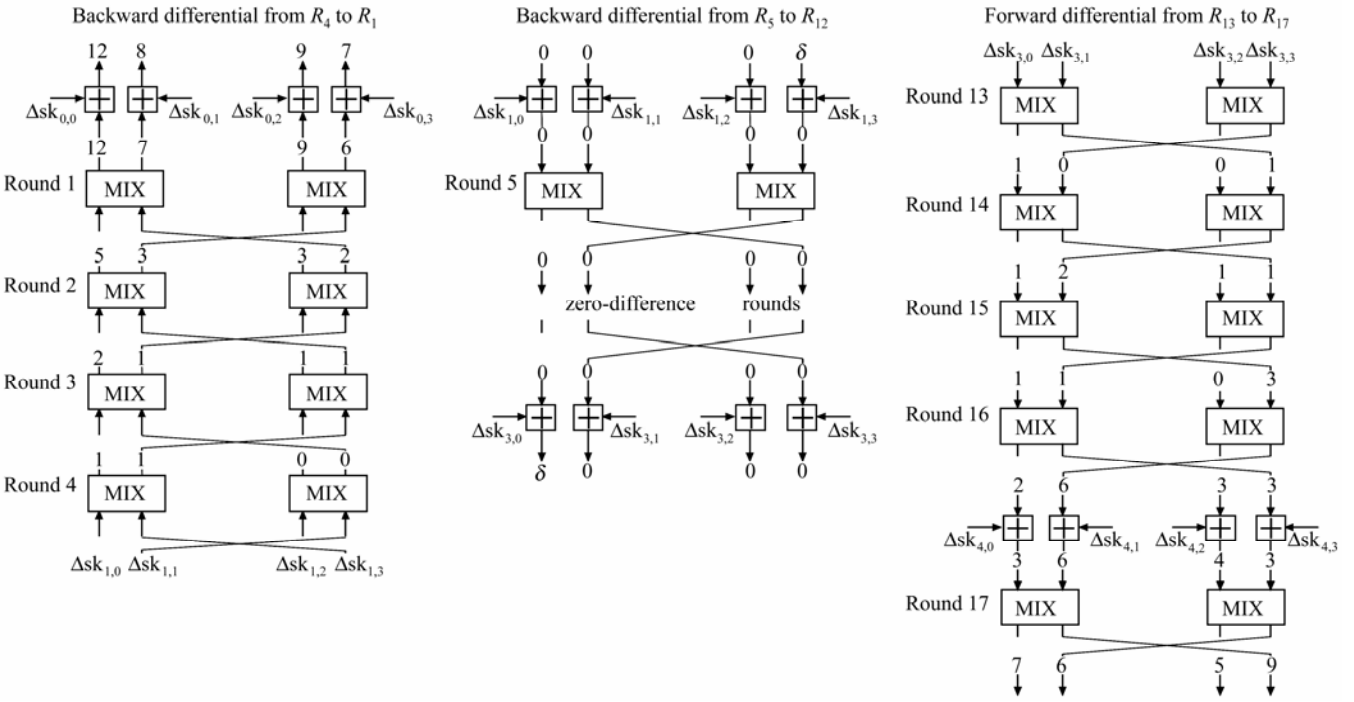
Backward differential from R_4 to R_1
12 8 9 7
$\Delta sk_{0,0}$ $\Delta sk_{0,1}$ $\Delta sk_{0,2}$ $\Delta sk_{0,3}$
12 7 9 6
Round 1
MIX
5 3 3 2
Round 2
2 1 1 1
Round 3
1 1 0 0
Round 4
$\Delta sk_{1,0}$ $\Delta sk_{1,1}$ $\Delta sk_{1,2}$ $\Delta sk_{1,3}$
Backward differential from R_5 to R_{12}
0 0 0 δ
$\Delta sk_{1,0}$ $\Delta sk_{1,1}$ $\Delta sk_{1,2}$ $\Delta sk_{1,3}$
Round 5
zero-difference rounds
$\Delta sk_{3,0}$ $\Delta sk_{3,1}$ $\Delta sk_{3,2}$ $\Delta sk_{3,3}$
δ 0 0 0
Forward differential from R_{13} to R_{17}
$\Delta sk_{3,0}$ $\Delta sk_{3,1}$ $\Delta sk_{3,2}$ $\Delta sk_{3,3}$
Round 13
1 0 0 1
Round 14
1 2 1 1
Round 15
1 1 0 3
Round 16
2 6 3 3
$\Delta sk_{4,0}$ $\Delta sk_{4,1}$ $\Delta sk_{4,2}$ $\Delta sk_{4,3}$
3 6 4 3
Round 17
7 6 5 9

Fig. 2 Related-key differential of E_α

Table 3 Differential trial of E_α

Round	Input difference	Pr
sk_0	0500900A50210840 8100100210210800 0040040086044204 8040000084004204	2^{-34}
1	0500900A50210840 0100100210210800 0040040086044204 0040000084004204	2^{-21}
2	0400800840000040 0000800040000040 0000040002040000 0000040002000000	2^{-8}
3	0400000800000000 0000000800000000 0000000000040000 0000000000040000	2^{-3}
4	0400000000000000 0400000000000000 0000000000000000 0000000000000000	2^{-1}
sk_1	0000000000000000 0000000000000000 0000000000000000 8000000000000000	1
5-12	0000000000000000 0000000000000000 0000000000000000 0000000000000000	1
13	8000000000000000 0000000000000000 0000000000000000 0000000000000000	1
14	8000000000000000 0000000000000000 0000000000000000 8000000000000000	1
15	8000000000000000 8000000000000800 8000000000000000 8000000000000000	2^{-1}
16	0000000000000800 0000000000200000 0000000000000000 0200000000000820	2^{-5}
sk_4	0000000000200800 0200082002000820 0200000000000820 0020000000200800	2^{-14}
17	8000000000200800 0200082002000820 8200000000000820 0020000000200800	2^{-12}
18	8200082002200020 8220002008200000 8220000000200020 800808A0002800A0	

2.3 Differential of E_β

Similar to the method of searching the differential of E_α, the differential of E_β is computed as follows.

Trial of R_{18} to R_{20}. In order to reach difference $(0,0,0,\delta)$ in the output of R_{20}, the input difference of R_{18} is computed in backward. The 3-round differential is shown in Table 4.

Trial of R_{21} to R_{28}. Because sk_5 adds the output difference of $R_{20}(0,0,0,\delta)$, the difference will be vanished until the sk_7 is added. The difference becomes (δ ,0,0,0) because the effect of sk_7.

Trial of R_{29} to R_{31}. In this step, we use Eq. (1) ($29 \leqslant i \leqslant 31$) to calculate the differential from R_{29} to R_{31}. The input difference of R_{29} is (δ ,0,0,0). Also, the patterns of the trail are shown in Table 4.

Based on the related-key differential of E_α and E_β, the value of there differences in Fig. 1 derived as follows.

$$\Delta_\alpha^{\text{in}} = \text{0500900A50210840 8100100210210800}$$
$$\text{0040040086044204 8040000084004204}$$
$$\Delta_\alpha^{\text{out}} = \text{8200082002200020 8220002008200000}$$
$$\text{8220000000200020 800808A0002800A0}$$

Table 4 Differential trial of E_β

Round	Input difference	Pr
18	0400800840000040 0000800040000040 0000040002040000 0000040002000000	2^{-8}
19	0400000800000000 0000000800000000 0000000000040000 0000000000040000	2^{-3}
20	0400000000000000 0400000000000000 0000000000000000 0000000000000000	2^{-1}
sk_5	0000000000000000 0000000000000000 0000000000000000 8000000000000000	1
21-28	0000000000000000 0000000000000000 0000000000000000 0000000000000000	1
29	8000000000000000 0000000000000000 0000000000000000 0000000000000000	1
30	8000000000000000 0000000000000000 0000000000000000 8000000000000000	1
31	8000000000000000 8000000000000800 8000000000000000 8000000000000000	2^{-1}
sk_8	0000000000000800 0000000000200000 0000000000000000 0200000000000820	2^{-5}
32	8000000000000800 0000000000200000 8000000000000000 0200000000000820	

$$\Delta_\beta^{\text{in}} = 0400800840000040\ 0000800040000040\ 0000040002040000\ 0000040002000000$$

$$\Delta_\beta^{\text{out}} = 8000000000000800\ 0000000000200000\ 8000000000000000\ 0200000000000820$$

Therefore, we obtain a differential ($\Delta_\alpha^{\text{in}}, \Delta_\alpha^{\text{out}}, \Delta_\alpha^{\text{key}}$) of E_α with the probability 2^{-99} and a differential ($\Delta_\beta^{\text{in}}, \Delta_\beta^{\text{out}}, \Delta_\beta^{\text{key}}$) of E_β with the probability 2^{-18}.

2.4 Related-Key Boomerang Distinguishing Attack and Complexity of Computation

The related-key boomerang distinguishing attack of 31-round Threefish-256 that exploits ($\Delta_\alpha^{\text{in}}, \Delta_\alpha^{\text{out}}, \Delta_\alpha^{\text{key}}$) of E_α and ($\Delta_\beta^{\text{in}}, \Delta_\beta^{\text{out}}, \Delta_\beta^{\text{key}}$) of has a probability 2^{-234}. The distinguisher works as follows:

① Choose a random message P and calculate $Q = P \oplus \Delta_\alpha^{\text{in}}$.

② Encrypt P and Q and obtain $C = E_k(p)$ and $D = E_{k\oplus\Delta_\alpha^{\text{key}}}(Q)$.

③ Set $C' = C \oplus \Delta_\beta^{\text{out}}$ and $D' = D \oplus \Delta_\beta^{\text{out}}$.

④ Decrypt C' and D' and obtain $P' = E^{-1}_{k\oplus\Delta_\beta^{\text{key}}}(C')$ and $Q' = E^{-1}_{k\oplus\Delta_\alpha^{\text{key}}\oplus\Delta_\beta^{\text{key}}}(D')$.

⑤ Check if $P' \oplus Q' = \Delta_\alpha^{\text{in}}$.

For an ideal cipher, the final equation $P' \oplus Q' = \Delta_\alpha^{\text{in}}$ is expected to hold with probability 2^{-256}. On the other hand, the final equation is expected to hold with probability $(2^{-99} \times 2^{-18})^2 = 2^{-234}$ in the related-key boomerang distinguisher, which is apparently lower than the exhaustive search. Therefore, an adversary can distinguish between 31-round Threefish-256 and an ideal cipher by implementing our boomerang attack. The published results on reduced-round variants of Skein-256 (or Threefish-256) are summarized in Table 5. As shown in Table 5, em-dash denotes that the probability is unknown.

Table 5 Known results on Skein-256 and Threefish-256

Cipher	Rounds	Pr	Method	Attack	Ref.
Threefish-256	24	—	Related-key differential	Key recovery	[6]
UBI-256	24	2^{-60}	Linear-differential	Near-collision	[8]
UBI-256	53	2^{-224}	Rotational rebound	Distinguishing	[10]
UBI-256	32	2^{-105}	Rebound attack	Near-collision	[9]
Threefish-256	31	2^{-234}	Related-key boomerang	Distinguishing	This paper

UBI-256 denotes the compression function of Skein-256

3 Conclusion

In this paper, we have proposed the related-key boomerang distinguishing attack on a reduced-round variant of Threefish-256. By combining two short differentials that we have found, our boomerang attack can be used to distinguish 31-round Threefish with the time complexity of 2^{234}. Because Threefish is the primitive of the Skein, our analysis will be useful to the further cryptanalysis of Skein for the SHA-3 competition.

References

[1] Wang Xiaoyun, Lai Xuejia, Feng Dengguo, *et al.* Cryptanalysis of the hash functions md4 and ripemd [C]//*Advances in Cryptology-EUROCRYPT* 2005. New York: Springer-Verlag, 2005: 1-18.

[2] Wang Xiaoyun, Yin Y L, Yu Hongbo. Finding collisions in the full sha-1 [C]//*Advances in Cryptology—CRYPTO* 2005. New York: Springer-Verlag, 2005: 17-36.

[3] Wang Xiaoyun, Yu Hongbo. How to break MD5 and other

Hash function [C]//*Advances in Cryptology-EUROCRYPT* 2005. New York: Springer-Verlag, 2005: 19-35.

[4] Wang Xiaoyun, Yu Hongbo, Yin Y L. Efficient collision attack on sha-0 [C]//*Advances in Cryptology-EUROCRYPT* 2005. New York: Springer-Verlag, 2005: 1-16.

[5] National Institute of Standards and Technology. Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (sha-3) family[S/OL]. [2011-11-21]. *http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov*07*.pdf.*

[6] Ferguson N, Lucks S, Schneier B, *et al.* The skein hash function family. Submission to NIST 2008 [DB/OL]. *http://www.skein-hash.info/.*

[7] Aumasson J P, Calik C, Meier W, *et al.* Improved cryptanalysis of Skein [C]//*Advance in Cryptology —ASIACRYPT* 2009. New York: Springer-Verlag, 2009: 542-559.

[8] Su Bozhan, Wu Wenling, Wu Shuang, *et al.* Near-collisions on the reduced-round compression functions of skein and blake [C]// *Applied Cryptography and Network Security* 2010. New York: Springer-Verlag, 2010: 124-139.

[9] Yu Hongbo, Chen Jiazhe, Ketingjia, *et al.* Near-collision attack on the step-reduced compression function of skein-256[DB/OL]. [2011-11-21]. *http://eprint.iacr.org*/2011/148.

[10] Khovratovich D, Nikolic I, Rechberger C. Rotational rebound attacks on reduced skein [C]//*Advances in Cryptology-ASIACRYPT* 2010. New York: Springer-Verlag, 2006: 1-19.

[11] Biham E. New types of cryptanalytic attacks using related keys [J]. *Journal of Cryptology*, 1994, **7**(4): 229-246.

[12] Wagner D. The boomerang attack [C]//*Fast Software Encryption*. New York: Springer-Verlag, 1999: 156-170.

[13] Biham E, Dunkelman O, Keller N. Related-key boomerang and rectangle attacks [C]// *Advances in Cryptology-EUROCRYPT* 2005. New York: Springer-Verlag, 1999: 507-525.

[14] Lipmaa H, Moriai S. Effcient algorithms for computing differential properties of addition [C]// *Fast Software Encryption* 2001. New York: Springer-Verlag, 2001: 336-350.

[15] Mouha N, Velichkov V, Canni`ere C D, *et al.* The differential analysis of s-functions[C]// *Selected Areas in Cryptography*. New York: Springer-Verlag, 2010: 36-56.

□