Improved Boomerang Attacks on Round-Reduced SM3 and BLAKE-256*

Dongxia Bai[1], Hongbo Yu[1**], Gaoli Wang[2], Xiaoyun Wang[3,4,5]

[1] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

baidx10@mails.tsinghua.edu.cn, yuhongbo@mail.tsinghua.edu.cn

[2] School of Computer Science and Technology, Donghua University, Shanghai 201620, China

wanggaoli@dhu.edu.cn

[3] Institute for Advanced Study, Tsinghua University, Beijing 100084, China

[4] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China

[5] School of Mathematics, Shandong University, Jinan 250100, China

xiaoyunwang@mail.tsinghua.edu.cn

Abstract. In this paper we study the security of hash functions SM3 and BLAKE-256 against boomerang attack. SM3 is designed by X. Wang et al. and published by Chinese Commercial Cryptography Administration Office for the use of electronic certification service system in China. BLAKE is one of the five finalists of the NIST SHA-3 competition submitted by J.-P. Aumasson et al. For SM3, we present boomerang distinguishers for the compression function reduced to 34/35/36/37/38 steps out of 64 steps, with time complexities $2^{31.4}$, $2^{33.6}$, $2^{73.4}$, 2^{93} and 2^{192} respectively. Then we show some incompatible problems existed in the previous boomerang attacks on SM3. Meanwhile, we launch boomerang attacks on up to 7 and 8 rounds keyed permutation of BLAKE-256 which are the first valid 7-round and 8-round boomerangs for BLAKE-256. Especially, since our distinguishers on 34/35-step compression function of SM3 and 7-round keyed permutation of BLAKE-256 are practical, we are able to obtain boomerang quartets of these attacks. As far as we know, these are the best results against round-reduced SM3 and BLAKE-256.

Key words: SHA-3 competition, hash function, BLAKE, SM3, boomerang attack, cryptanalysis.

1 Introduction

Cryptographic hash functions play an important role in the modern cryptology. In recent years, the cryptanalysis of hash functions has become an important topic within the cryptographic community, and the significant advances of hash function research have a formative influence on the field of hash functions. Since many well-known hash functions including MD5 and SHA-1 were broken by X. Wang et al. in 2005 [1,2], NIST proposed the transition from SHA-1 to SHA-2 family, and many companies and organizations were also migrating to SHA-2. Furthermore, in 2007 NIST started a hash function competition to develop a new hash standard SHA-3 [3] to complement the older SHA-1 and SHA-2. Then five SHA-3

* Supported by 973 program (No. 2013CB834205), the National Natural Science Foundation of China (No. 61133013 and No. 61103238), the Tsinghua University Initiative Scientific Research Program (No. 20111080970), and Tsinghua National Laboratory for Information Science and Technology.

** Corresponding author.

candidate algorithms, including BLAKE, Grøstl, JH, Keccak, and Skein, were selected to advance to the final in 2010, and the competition ended in 2012 when NIST announced that Keccak would be the new SHA-3 hash algorithm. During the ongoing evaluation of these hash functions, people not only consider the three classical security requirements of hash function (preimage resistance, 2nd preimage resistance and collision resistance), but also regard near-collision, rebound distinguisher, differential distinguisher, boomerang distinguisher, etc. Whenever a hash function behaves differently from the one expected of a random function, its security is considered to be suspect. Therefore, many attack results in such framework are proposed recently. Especially, the idea of boomerang attack leads to many new and useful results on hash functions. In 2011, the boomerang attack was independently applied to hash functions BLAKE-32 by A. Biryukov et al. [4] and SHA-256 by M. Lamberger et al. [5]. Then the boomerang attack on SHA-256 was improved in [6]. Later the large potential of boomerang attack on hash functions has been demonstrated by more and more results including attacks on SIMD-512 [7], HAVAL [8], RIPEMD [9], HAS-160 [10] and Skein [11,12].

SM3 [13] is the Chinese cryptographic hash function standard which is designed by X. Wang et al., and its design builds on the Merkle-Damgård construction. It is very similar to the MD4 family of hash functions and in particular to SHA-2, but introduces some additional strengthening features, such as a more complex step function and stronger message dependency than SHA-256. BLAKE [14] is a HAIFA iteration mode hash function family submitted to the NIST hash function competition by J.-P. Aumasson et al. It is based on ChaCha stream cipher [15], but a permuted copy of the input block XORed with some round constants is added before each ChaCha round. BLAKE is chosen as one of the five finalists of the SHA-3 competition, which now mainly consists of two valid variants BLAKE-256 and BLAKE-512. In this work, we present several boomerang attacks on round-reduced SM3 and BLAKE-256.

Related Work. In the last few years, the amount of cryptanalytic results on SM3 is much lower than other hash function standards. In [16], J. Zou et al. presented the first preimage attacks on SM3 reduced to 30 steps out of 64 steps starting from step 6, and 28 steps starting from step 0. At SAC 2012, A. Kircanski et al. [17] applied the boomerang attack to SM3 compression function for 32/33/34/35 steps, and gave examples of zero-sum quartets for 32-step and 33-step distinguishers. They also exposed a side-rotational property of SM3-XOR function and gave a slide-rotational pair for SM3-XOR compression function. While incompatibility between the differential characteristics of 33/34/35-step distinguishers are found and shown later. Then G. Wang et al. [18] proposed preimage attacks on SM3 reduced to 29/30 steps and pseudo-preimage attacks reduced to 31/32 steps, with lower complexities than [16] and all from the first step (step 0), and they also converted those (pseudo) preimage attacks into pseudo-collision attacks on 29/30/31/32-step SM3 for the first time. Meanwhile, F. Mendel et al. [19] provided the first security analysis of step-reduced SM3 regarding its collision resistance, and presented a collision attack for 20 steps and a free-start collision attack for 24 steps of SM3, both with practical complexity. The above are all the previous results that we are aware of on the analysis of SM3.

As for BLAKE-256, in [20] J. Li et al. presented free-start collision and (free-start) (2nd) preimage attacks on 2.5 rounds of the compression function of BLAKE-32 (BLAKE-32 with 10 rounds submitted in 2008 is the original version of the final BLAKE-256 with 14 rounds proposed in 2010). Then L. Wang et al. [21] announced 4/4.5-round free-start preimage attacks on compression function of BLAKE-32. J.-P. Aumasson et al. [22] gave near collisions on 4-round compression function and impossible differential for 5-round keyed permutation of BLAKE-32. Then B. Su et al. [23] proposed near collision attack on 4-round compression function of BLAKE-32 with lower complexity than [22]. At FSE 2011, A. Biryukov et al. [4] presented boomerang attacks on 7 round-reduced compression function and 8 round-reduced keyed permutation of BLAKE-32, and a boomerang quartet of distinguisher on 6 round-reduced keyed permutation was also given. While there are some incompatible problems in [4] later pointed out by G. Leurent in [24]. In [25] O. Dunkelman et al. presented differential distinguisher for the keyed permutation of BLAKE-256 reduced to 6 middle rounds.

Our Contribution. In this work, we study the security of hash functions SM3 and BLAKE-256, and show the application of boomerang attack to round-reduced compression function of SM3 and keyed permutation of BLAKE-256. First, we build boomerang distinguishers for SM3 compression function on up to 34 and 35 steps with practical complexities, and examples of boomerang quartets are also given. Moreover, the distinguishers can be extended to attacks on 36, 37 and 38 steps of SM3. Then we show some incompatible problems existed in the differential characteristics used in the previous work [17]. Furthermore, we present the first valid boomerang distinguishers on up to 7 and 8 round-reduced keyed permutation of BLAKE-256. We are able to find boomerang quartets of our distinguisher on 7 round-reduced keyed permutation of BLAKE-256, which are one more round than the previous practical example [4].

With respect to the attack in the framework of boomerang distinguisher, our results of SM3 and BLAKE-256 are both the best until now. The summary of previous results and ours are given in Table 1.

Outline. The structure of the paper is as follows. In Section 2, we give a short description of hash functions SM3 and BLAKE-256. Section 3 briefly overviews the boomerang attack. In Section 4, we present the differential characteristics and build boomerang distinguishers for step-reduced SM3 compression function. The boomerang distinguishers for round-reduced keyed permutation of BLAKE-256 are proposed in Section 5. Finally, we conclude our paper in Section 6.

2 Description of Hash Functions SM3 and BLAKE-256

2.1 SM3 Hash Function

SM3 is an iterated hash function that processes 512-bit input message blocks and produces a 256-bit hash value. It basically consists of two parts: the message expansion and the state update transformation. A detailed description of SM3 hash function is given in [13].

Message Expansion. The message expansion of SM3 splits the 512-bit message block into 16 words m_i $(0 \le i \le 15)$, and expands them into 68 expanded message words w_i $(0 \le i \le 67)$ and 64 expanded message words w'_i $(0 \le i \le 63)$ as follows:

$$w_i = \begin{cases} m_i, & 0 \le i \le 15, \\ P_1(w_{i-16} \oplus w_{i-9} \oplus (w_{i-3} \lll 15)) \oplus (w_{i-13} \lll 7) \oplus w_{i-6}, & 16 \le i \le 67, \end{cases}$$
$$w'_i = w_i \oplus w_{i+4}, 0 \le i \le 63.$$

Table 1. Summary of the attacks on SM3 and BLAKE-256

hash function	attack type	target	rounds	time	source
SM3	preimage attack	HF	28	$2^{241.5}$	[16]
	preimage attack	HF	30	2^{249}	
	preimage attack	HF	29	2^{245}	[18]
	preimage attack	HF	30	$2^{251.1}$	
	pseudo-preimage attack	HF	31	2^{245}	
	pseudo-preimage attack	HF	32	$2^{251.1}$	
	pseudo-collision	HF	29	2^{122}	
	pseudo-collision	HF	30	$2^{125.1}$	
	pseudo-collision	HF	31	2^{122}	
	pseudo-collision	HF	32	$2^{125.1}$	
	collision attack	HF	20	practical	[19]
	free-start collision	CF	24	practical	
	boomerang distinguisher	CF	32	$2^{14.4}$	[17]
	boomerang distinguisher	CF	33*	$2^{32.4}$	
	boomerang distinguisher	CF	34*	$2^{53.1}$	
	boomerang distinguisher	CF	35*	$2^{117.1}$	
	boomerang distinguisher	CF	34	$2^{31.4}$	**Sect.4**
	boomerang distinguisher	CF	35	$2^{33.6}$	
	boomerang distinguisher	CF	36	$2^{73.4}$	
	boomerang distinguisher	CF	37	2^{93}	
	boomerang distinguisher	CF	38	2^{192}	
BLAKE-256	free-start collision	CF	2.5	2^{112}	[20]
	free-start (2nd) preimage	CF	2.5	2^{224}	
	(2nd) preimage	CF	2.5	2^{241}	
	free-start preimage	CF	4	2^{224}	[21]
	free-start preimage	CF	4.5	2^{252}	
	impossible differential	KP	5	—	[22]
	near collision	CF	4	2^{56}	
	near collision	CF	4	2^{21}	[23]
	differential distinguisher	KP	6	2^{456}	[25]
	boomerang distinguisher	CF	6	2^{102}	[4]
	boomerang distinguisher	CF	6.5*	2^{184}	
	boomerang distinguisher	CF	7*	2^{232}	
	boomerang distinguisher	KP	6	$2^{11.75}$	
	boomerang distinguisher	KP	7*	2^{122}	
	boomerang distinguisher	KP	8*	2^{242}	
	boomerang distinguisher	KP	7	2^{37}	**Sect.5**
	boomerang distinguisher	KP	8	2^{200}	

$*$: the attack has some incompatible problems.

The function $P_1(X)$ is given by

$$P_1(X) = X \oplus (X \lll 15) \oplus (X \lll 23).$$

State Update Transformation. The state update transformation starts from a (fixed) initial value $IV = (A_0,\ B_0,\ C_0,\ D_0,\ E_0,\ F_0,\ G_0,\ H_0)$ of 8 32-bit words and updates them in 64 steps. In each step the two 32-bit words w_i and w'_i are used to update the state variables $A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i$ as follows:

$$\begin{aligned}
SS1_i &= ((A_i \lll 12) + E_i + (T_i \lll i)) \lll 7,\\
SS2_i &= SS1_i \oplus (A_i \lll 12),\\
TT1_i &= FF_i(A_i, B_i, C_i) + D_i + SS2_i + w'_i,\\
TT2_i &= GG_i(E_i, F_i, G_i) + H_i + SS1_i + w_i,\\
A_{i+1} &= TT1_i,\\
B_{i+1} &= A_i,\\
C_{i+1} &= B_i \lll 9,\\
D_{i+1} &= C_i,\\
E_{i+1} &= P_0(TT2_i),\\
F_{i+1} &= E_i,\\
G_{i+1} &= F_i \lll 19,\\
H_{i+1} &= G_i.
\end{aligned}$$

The step constants are $T_i = 0x79cc4519$ for $i \in \{0, \ldots, 15\}$ and $T_i = 0x7a879d8a$ for $i \in \{16, \ldots, 63\}$. The bitwise boolean functions $FF(X,Y,Z)$ and $GG(X,Y,Z)$ used in each step are defined as follows:

$$FF_i(X,Y,Z) = \begin{cases} X \oplus Y \oplus Z, & 0 \le i \le 15,\\ (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z), & 16 \le i \le 63,\end{cases}$$

$$GG_i(X,Y,Z) = \begin{cases} X \oplus Y \oplus Z, & 0 \le i \le 15,\\ (X \wedge Y) \vee (\neg X \wedge Z), & 16 \le i \le 63.\end{cases}$$

The linear function $P_0(X)$ is defined as follows:

$$P_0(X) = X \oplus (X \lll 9) \oplus (X \lll 17).$$

After the last step of the state update transformation, the initial values are added to the output values of the last step. The result is the final hash value or the initial value for the next message block.

2.2 BLAKE-256 Hash Function

The hash function BLAKE-256 operates on 32-bit words and returns a 32-byte hash value. Its compression function processes a state of 16 32-bit words represented as 4×4 matrix, and consists of three steps: Initialization, 14 iterations of Rounds and Finalization.

Initialization. In the Initialization procedure, the state is filled with a chaining value $h = h_0, \ldots, h_7$, a salt $s = s_0, \ldots, s_3$, constants $c_0, \ldots, c_7$, and a counter $t = t_0, t_1$ as follows:

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix} \leftarrow \begin{pmatrix} h_0 & h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 & h_7 \\ s_0 \oplus c_0 & s_1 \oplus c_1 & s_2 \oplus c_2 & s_3 \oplus c_3 \\ t_0 \oplus c_4 & t_0 \oplus c_5 & t_1 \oplus c_6 & t_1 \oplus c_7 \end{pmatrix}.$$

Round function. Once the state $v = (v_0, \ldots, v_{15})$ is initialized, the compression function iterates a series of 14 rounds. Each round is a transformation of the state v that computes

$$G_0(v_0, v_4, v_8, v_{12}), \quad G_1(v_1, v_5, v_9, v_{13}), \quad G_2(v_2, v_6, v_{10}, v_{14}), \quad G_3(v_3, v_7, v_{11}, v_{15}),$$

$$G_4(v_0, v_5, v_{10}, v_{15}), \quad G_5(v_1, v_6, v_{11}, v_{12}), \quad G_6(v_2, v_7, v_8, v_{13}), \quad G_7(v_3, v_4, v_9, v_{14}),$$

where $G_i(a, b, c, d)$ at round r is described with the following steps:

$$\begin{aligned}
&a = a + b + (m_{\sigma_r(2i)} \oplus c_{\sigma_r(2i+1)}), \\
&d = (d \oplus a) \ggg 16, \\
&c = c + d, \\
&b = (b \oplus c) \ggg 12, \\
&a = a + b + (m_{\sigma_r(2i+1)} \oplus c_{\sigma_r(2i)}), \\
&d = (d \oplus a) \ggg 8, \\
&c = c + d, \\
&b = (b \oplus c) \ggg 7,
\end{aligned}$$

here σ_r belongs to the set of permutations as defined in Table 2. At round $r > 9$, the permutation used is σ_{rmod10} (for example, in the last round $r = 13$, the permutation $\sigma_{13mod10} = \sigma_3$ is used).

Table 2. Permutations of $\{0, \ldots, 15\}$ used by the BLAKE functions

σ_0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
σ_1	14	10	4	8	9	15	13	6	1	12	0	2	11	7	5	3
σ_2	11	8	12	0	5	2	15	13	10	14	3	6	7	1	9	4
σ_3	7	9	3	1	13	12	11	14	2	6	5	10	4	0	15	8
σ_4	9	0	5	7	2	4	10	15	14	1	11	12	6	8	3	13
σ_5	2	12	6	10	0	11	8	3	4	13	7	5	15	14	1	9
σ_6	12	5	1	15	14	13	4	10	0	7	6	3	9	2	8	11
σ_7	13	11	7	14	12	1	3	9	5	0	15	4	8	6	2	10
σ_8	6	15	14	9	11	3	0	8	12	2	13	7	1	4	10	5
σ_9	10	2	8	4	7	6	1	5	15	11	9	14	3	12	13	0

Finalization. After the rounds sequence, the new chain value $h' = h'_0, \ldots, h'_7$ is extracted from the state $v = v_0, \ldots, v_{15}$ with the initial chain value $h = h_0, \ldots, h_7$ and the salt $s = s_0, \ldots, s_3$ as follows:

$$
\begin{aligned}
h'_0 &= h_0 \oplus s_0 \oplus v_0 \oplus v_8, \\
h'_1 &= h_1 \oplus s_1 \oplus v_1 \oplus v_9, \\
h'_2 &= h_2 \oplus s_2 \oplus v_2 \oplus v_{10}, \\
h'_3 &= h_3 \oplus s_3 \oplus v_3 \oplus v_{11}, \\
h'_4 &= h_4 \oplus s_0 \oplus v_4 \oplus v_{12}, \\
h'_5 &= h_5 \oplus s_1 \oplus v_5 \oplus v_{13}, \\
h'_6 &= h_6 \oplus s_2 \oplus v_6 \oplus v_{14}, \\
h'_7 &= h_7 \oplus s_3 \oplus v_7 \oplus v_{15}.
\end{aligned}
$$

3 The Boomerang Attack

The boomerang attack was introduced by D. Wagner in 1999 [26] as a tool for the cryptanalysis of block cipher. It is an adaptive chosen plaintext and ciphertext attack utilizing differential cryptanalysis. The cipher is treated as a cascade of two sub-ciphers, where a short differential is used in each of these sub-ciphers. These differentials are combined to exploit an adaptive chosen plaintext and ciphertext property of the cipher that has high probability. Then J. Kelsey et al. [27] further developed it into a chosen plaintext attack called the amplified boomerang attack, and later it was developed by E. Biham et al. [28] into the rectangle attack. Then E. Biham et al. [29] combined the boomerang (and the rectangle) attack with related-key differentials and proposed the related-key boomerang and rectangle attacks, which use the related-key differentials instead of the single-key differentials.

We mainly review the known-related-key boomerang attack [6] which can be used to distinguish a given permutation from a random oracle. Applying the known-related-key boomerang attack to the compression function in the MMO mode, i.e, $CF(M, K) = E(M, K) + M$ that can be decomposed into two sub-functions with $CF = CF_1 \circ CF_0$, we can start from the middle steps since the message M and the key K can be chosen randomly (refer to [6,11]). Then we have a backward differential characteristic $(\beta, \beta_k) \rightarrow \alpha$ with probability p for CF_0^{-1}, and another forward differential characteristic

$(\gamma, \gamma_k) \to \delta$ with probability q for CF_1. Next the known-related-key boomerang attack can be constructed using these two differentials as follows:

- Choose a random value X_1 and K_1, compute $X_2 = X_1 \oplus \beta$, $X_3 = X_1 \oplus \gamma$, $X_4 = X_3 \oplus \beta$, and $K_2 = K_1 \oplus \beta_k$, $K_3 = K_1 \oplus \gamma_k$, $K_4 = K_3 \oplus \beta_k$.
- Compute backward from (X_i, K_i) using CF_0^{-1} to obtain P_i $(i = 1, 2, 3, 4)$.
- Compute forward from (X_i, K_i) using CF_1 to obtain C_i $(i = 1, 2, 3, 4)$.
- Check whether $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$ and $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$.

We can deduce that $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$ and $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$ hold with probability at least p^2 in the backward direction and q^2 in the forward direction. Hence, the attack succeeds with probability p^2q^2 when assuming that the differentials are independent.

For a n-bit random permutation, there exist three types of boomerang distinguishers according to the input and output differences which are summarized by H. Yu et al. in [12].

- Type I: A quartet satisfies $P_2 \oplus P_1 = P_4 \oplus P_3 = \alpha$ and $C_3 \oplus C_1 = C_4 \oplus C_2 = \delta$ for fixed differences α and δ. In this case, the generic complexity is 2^n.
- Type II: Only $C_3 \oplus C_1 = C_4 \oplus C_2$ is satisfied (This property is also called zero-sum or second-order differential collision). In this case, the complexity for obtaining such a quartet is $2^{n/3}$ by using D. Wagner's generalized birthday attack [30].
- Type III: A quartet satisfies $P_2 \oplus P_1 = P_4 \oplus P_3$ and $C_3 \oplus C_1 = C_4 \oplus C_2$. In this case, the best known attack still takes time $2^{n/2}$.

4 The Boomerang Attacks on SM3

In this section, we present the boomerang attacks on the SM3 compression function reduced to 34 and 35 steps with practical examples of boomerang quartets, and then extend the attacks to 36, 37 and 38 steps. Firstly, we have to find the differential characteristics used in the attack to distinguish the target compression function from random functions. Secondly, we derive the sufficient conditions in the intermediate steps, and correct these conditions by using message modification technique. Finally, we evaluate the complexities of our attacks and search right quartet examples.

4.1 Step-Reduced Differential Characteristics

We give two differential characteristics which are used to attack 34-step SM3 compression function and build boomerang distinguisher, where the top differential characteristic is from step 15 to 0, and the bottom one is from step 16 to 33. Note that we all use the XOR difference $\Delta a = a \oplus a'$, and let Δa: i for $1 \le i \le 32$ denotes that the i-th bit of a is different from the i-th bit of a', and all the other bits of a and a' are the same.

We start from the middle states of the distinguisher quartet (V_1, V_2, V_3, V_4), and for the top characteristic, the differences of the message words w_i and the chaining variables A_{16} to H_{16} are chosen as follows:

– Δw_2: 32 (the MSB difference), $\Delta w_i = 0$ ($0 \leq i \leq 15$, $i \neq 2$), if we choose the message words with such differences, we will find that 13 steps (step 13 to 1) are passed with probability 1. This is significant for us to get the high probability differential characteristic.
– ΔA_{16}: $2, 3, 10, 12, 15, 19, 23, 27, 32$, ΔB_{16}: $15, 23, 32$, ΔE_{16}: $2, 4, 10, 11, 19, 27, 28$, these differences are decided by the differences of the message words above. We can easily get the differences of the message words Δw_0–Δw_{15}, $\Delta w'_0$–$\Delta w'_{15}$ in the top characteristic from above: Δw_2: 32, $\Delta w'_2$: 32, $\Delta w'_{14}$: $15, 23, 32$, and all the other message words differences are zero. Then we directly derive the differences of the chaining variables with some sufficient conditions.

For the bottom characteristic, we select the differences as follows:

– Δw_{20}: 20 (the 20-th bit difference), $\Delta w_i = 0$ ($21 \leq i \leq 35$), so we can pass 11 steps (step 21 to 31) for free similarly.
– ΔC_{16}: $9, 16, 18, 23, 25, 26, 30, 31$, ΔD_{16}: $11, 20$, ΔG_{16}: $9, 16, 18, 24, 25, 26, 30, 32$, ΔH_{16}: $1, 3, 4, 10, 12, 19, 20, 28$, according to the differences of the message words above, also considering the compatibility with the top characteristic in the middle steps which cannot contain any contradiction, the differences of chaining variables in bottom characteristic are derived with some sufficient conditions. For example, to cancel the 9-th and 10-th bit differences of w'_{17}, we choose the difference in D_{17} only on bit 9 but not on bits 9 and 10, because if we has difference in D_{17} on bit 10, then in step 16 the condition $A_{16,10} = B_{16,10}$ (note that $C_{16} = D_{17}$) cannot be satisfied in the other side (V_2, V_4).

In Table 3 and Table 4 the differential characteristics for both forward and backward directions are shown. Furthermore, the conditions and probabilities for each step of the differential characteristics are given.

4.2 Message Modification for the Middle Steps

Here we use the message modification technique to modify the chaining values and message words to satisfy the conditions of the middle steps to improve the complexity of our attack.

In the top differential characteristic, there are 16 sufficient conditions from step 15 to 14, which can be satisfied both in two sides (V_1, V_2) and (V_3, V_4) by modifying A_{16}, B_{16} and F_{16}. Therefore, the conditions of this part (step 15 to 14) can hold with probability 1.

Similarly, 59 conditions in total from step 16 to 20 in the bottom differential characteristic need to be corrected in each side. We can make all these conditions hold in one side (V_1, V_3) by the message modification. Furthermore, part of the conditions in the other side (V_2, V_4) can be corrected, and 14 conditions including $SS1_{17,30} = A_{17,11}$, $SS1_{17,8} = E_{17,1}$, $w'_{17,8} \neq SS2_{17,8}$, $D_{17,23} = SS2_{17,23} \neq w'_{17,24}$, $D_{17,30} = SS2_{17,30} = D_{17,31}$, $w_{17,8} \neq SS1_{17,8}$, $H_{17,30} \neq SS1_{17,30}$, $A_{18,11} = C_{18,11}$, $E_{18,1} = 0$, $A_{19,20} = B_{19,20}$, $E_{19,20} = 1$, and $H_{20,20} \neq w_{20,20}$ are satisfied randomly. As a result, all the conditions of step 16 to 20 in the bottom differential characteristic hold with probability at least 2^{-14}, rather than the much lower average probability $2^{-2\times 59} = 2^{-118}$.

4.3 Complexity of the Attack

After the message modification, the boomerang distinguisher in the middle steps (14 to 20) holds with a much higher probability 2^{-14}. Meanwhile, the probability of step 0 to 13 in the top characteristic is 2^{-2}, and for step 21 to 33 in the bottom characteristic is 2^{-17}. So the complexity of the 34-step boomerang distinguisher is $2^{14} + 2^{2\times(2+17)} \approx 2^{38}$. Note that it can be further reduced to $2^{14} + 2^{2\times 3} \times 3^{2+14} \approx 2^{14} + 2^{31.4} \approx 2^{31.4}$ if we only obtain a zero-sum distinguisher.

Due to the low complexity, our distinguisher on up to 34-step compression function of SM3 is practical, and we are able to find boomerang quartets on a PC quickly. We give an example of 34-step boomerang distinguisher in Table 9.

4.4 Attacks on 35/36/37/38-Step SM3 Compression Function

35-Step Attack (Steps 0-34). Using the same top differential characteristic shown in Table 3, we add one more step as the new 16-th step in the bottom differential characteristic as illustrated in Table 5 to mount a 35-step attack. So the step where the single bit difference has been set in the message word w_i in the bottom differential characteristic should slip to step 21. Now we look at the choice of differences in bottom differential characteristic, if we still use the same bit difference on bit 20 in w_{21}, some contradictions will emerge, and through theoretical derivation and program tests we find that only the 24-th bit difference in w_{21} is applicable and compatible between the two differential characteristics. We correct all conditions in the side (V_1, V_2) and part of conditions (12 conditions) in the other side (V_3, V_4) in steps 15 to 14 of the top differential characteristic, and all conditions in the side (V_1, V_3) in steps 16 to 21 of the bottom differential characteristic. The remaining conditions in middle steps (14 to 21) have not been dealt with. So in theory the boomerang distinguisher in the middle steps holds with probability 2^{-46}. However, according to our experiments, on average, only about 32 conditions in the middle steps have not been corrected. As a result, the complexity of 35-step boomerang distinguisher is about $2^{32} + 2^{2\times 3} \times 3^{2+15} \approx 2^{32} + 2^{33} \approx 2^{33.6}$, and the practical example of 35-step boomerang distinguisher quartet can be found on a PC, see Table 10.

36-Step Attack (Steps 0-35). The 36-step attack is obtained with the same differential characteristics as 35-step attack by adding one step in the top differential characteristic as the new first step, where the top differential characteristic is from step 0 to 16 and the bottom one is from step 17 to 35. In order to keep the probability of connection part between the top and bottom differential characteristics mostly unchanged, we change the differences of the top differential characteristic slightly: $\Delta w_0 : 4, 5, 7, 12, 20, 21, 22, 28, 30$, $\Delta w_3 : 32$, $\Delta w_i = 0\ (0 \le i \le 15, i \ne 0, 3)$, $\Delta A_{17} : 2, 3, 10, 12, 19, 27$, $\Delta B_{17} : 15, 23, 32$, $\Delta E_{17} : 2, 4, 10, 11, 19, 27, 28$, see Table 6. The complexity of the 36-step attack is about $2^{32} + 2^{2\times(2+3)} \times 3^{25+15} \approx 2^{32} + 2^{73.4} \approx 2^{73.4}$.

37/38-Step Attack (Steps 0-36/37). Extending the 36-step boomerang distinguisher for one step at the end of the top differential characteristic, we get a 37-step attack with a complexity of $2^{93} + 2^{2\times(2+3)} \times 3^{25+15} \approx 2^{93} + 2^{73.4} \approx 2^{93}$ by using the message modification technique. Then with the same top differential characteristic, we add one more step after the 37-step boomerang distinguisher, and obtain a 38-step attack on SM3 with complexity $2^{93} + 2^{2\times(2+3+25+15+51)} = 2^{93} + 2^{192} \approx 2^{192}$. As illustrated in Table 6 and Table 7, we give the details of the top and bottom differential characteristics used in the boomerang attacks on 37 and 38 steps compression function of SM3.

Remark: For the 34/35/36/37-step attacks on SM3, we use the Type III boomerang distinguisher (see Sect. 3), and the complexity for the best algorithm is 2^{128}; for the 38-step attack on SM3, we use the Type I boomerang distinguisher, and the generic complexity is about 2^{256}.

4.5 The Incompatibility of Previous Boomerang Attacks on SM3

In [17], boomerang distinguisher for SM3 compression function reduced to 33 steps and the corresponding example of zero-sum quartet are given. However, we find that the proposed example of quartet is not consistent with the differential characteristics shown in that paper. According to the differences of the given example, it is supposed to be generated by adding one step after their 32-step distinguisher. Then we study the given 33-step boomerang distinguisher in [17] and find some contradictions between the two differential characteristics.

For the differences in step 20 in the bottom differential characteristic, it is easy to deduce that $D_{20,28} = C_{19,28} = B_{18,19} = A_{17,19} = TT1_{16,19} = D_{16,19}$, so the condition $D_{20,28} \neq w'_{20,28}$ in step 20 can be rewritten as $D_{16,19} \neq w'_{20,28}$. From the top differential characteristic, we get that $\Delta D_{16} = 0$ (so $\Delta D_{16,19} = 0$), $\Delta w'_{20,28} = 1$ (according to the message expansion), so the condition $D_{20,28} \neq w'_{20,28}$ in step 20 cannot be satisfied in the other side (V_2, V_4) for the bottom differential characteristic. Hence, the 33-step boomerang distinguisher in [17] cannot work in fact. Since their 34-step and 35-step distinguishers are constructed by adding one and two steps after the 33-step distinguisher, those two attacks cannot work either. We can correct the bottom differential characteristic by simply changing the single bit difference of message word w_{20} from bit 28 to 20.

5 The Boomerang Attacks on BLAKE-256

Similar to above, there are also incompatible problems in previous boomerang attacks on BLAKE-256 [4], and the detailed contradictions are shown in [24]. In this section, we give two alternative differential characteristics, and the first valid 7-round and 8-round boomerang attacks on keyed permutation of BLAKE-256 are mounted. Note that the keyed permutation of BLAKE-256 can be seen as the internal cipher of BLAKE-256, which excludes the Initialization and Finalization procedures.

7-Round Boomerang Attack on Keyed Permutation of BLAKE-256. Through comparing the probabilities of differential characteristics, we carefully choose the middle round where two differential characteristics are combined, which is round 6.5, to build the 7-round boomerang distinguisher for keyed permutation of BLAKE-256. We use two 3.5-round differential characteristics with highest probabilities than others, i.e. the top differential characteristic is from round 3 to round 6.5 and the bottom one is from round 6.5 to round 10. The differences of message words and chaining variables are selected as follows:

- Δm_5: 21 for the top characteristic,
- Δm_{11}: 32 for the bottom characteristic,
- Then set the differences of chaining variables which are basically decided by the differences of message words.

Table 8 gives the top and bottom differential characteristics used for 7-round boomerang attack on BLAKE-256.

Similar to the attacks on SM3, the message modification technique is used to correct the conditions of middle rounds to improve our attack. By modifying chaining variables v_i (i=0, ..., 15) of round 6.5 and message words m_i (i=0, ..., 15), 29 conditions in $G_0 \sim G_3$ of round 6, 40 conditions in $G_4 \sim G_7$ of round 6, 2 conditions in round 5 and 2 conditions in round 7 can be satisfied in both two sides. After message modification, the conditions of this part (rounds 5 to 7) can hold with probability at least 2^{-4} . As a result, the boomerang distinguisher on 7 rounds keyed permutation of BLAKE-256 has the complexity $2^{2\times(1+4))} \times 3^{16+1} \approx 2^{10} \times 2^{27} = 2^{37}$. Due to the practical complexity, we can obtain the boomerang quartet which is one more round than the previous best result [4]. See Table 11.

8-Round Boomerang Attack on Keyed Permutation of BLAKE-256. As shown in Table 8, we just extend the differential characteristics used in 7-round attack for additional half round both in forward and backward directions, and obtain a 8-round boomerang distinguisher for keyed permutation of BLAKE-256 with complexity $2^{2\times(54+16+1+4+1+24)} = 2^{200}$.

Remark: Similar to attacks on SM3, we use the Type III boomerang distinguisher for the 7-round attack on BLAKE-256, and Type I boomerang distinguisher for the 8-round attack on BLAKE-256.

6 Conclusion

This paper presents boomerang attacks on Chinese cryptographic hash function standard SM3 and the NIST SHA-3 finalist BLAKE-256. We propose boomerang distinguishers for the compression function of SM3 reduced to 34/35/36/37/38 steps out of 64 steps, and give examples of boomerang distinguishers on up to 34-step and 35-step SM3. Besides, we point out the incompatible problems existed in the previous attacks on SM3. Then we present boomerang distinguishers on 7 and 8 round-reduced keyed permutation of BLAKE-256 out of 14 rounds, which are the first valid boomerang results on 7-round and 8-round keyed permutation of BLAKE-256. Also, we give a boomerang quartet of the distinguisher on 7-round keyed permutation of BLAKE-256 for the first time. All these results are the best as far as we know.

References

1. Wang, X., Yin, Y.L., Yu, H.: 'Finding Collisions in the Full SHA-1', Proc. CRYPTO2005, 2005 (LNCS, 3621), pp. 17–36.
2. Wang, X., Yu, H.: 'How to Break MD5 and Other Hash Functions', Proc. EUROCRYPT2005, 2005 (LNCS, 3494), pp. 19–35.
3. SHA-3 Cryptographic Hash Algorithm Competition, http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.
4. Biryukov, A., Nikolić, I., Roy, A.: 'Boomerang Attacks on BLAKE-32', Proc. FSE2011, 2011 (LNCS, 6733), pp. 218–237.
5. Lamberger, M., Mendel, F.: 'Higher-Order Differential Attack on Reduced SHA-256', http://eprint.iacr.org/2011/037.pdf, January 2011.
6. Biryukov, A., Lamberger, M., Mendel, F., Nikolić, I.: 'Second-Order Differential Collisions for Reduced SHA-256', Proc. ASIACRYPT2011, 2011 (LNCS, 7073), pp. 270–287.
7. Mendel, F., Nad, T.: 'Boomerang Distinguisher for the SIMD-512 Compression Function', Proc. INDOCRYPT2011, 2011 (LNCS, 7107), pp. 255–269.

8. Sasaki, Y.: 'Boomerang Distinguishers on MD4-Family: First Practical Results on Full 5-Pass HAVAL', Proc. SAC2011, 2011 (LNCS, 7118), pp. 1–18.
9. Sasaki, Y., Wang, L.: '2-Dimension Sums: Distinguishers Beyond Three Rounds of RIPEMD-128 and RIPEMD-160', http://eprint.iacr.org/2012/049.pdf, February 2012.
10. Sasaki, Y., Wang, L., Takasaki, Y., Sakiyama, K., Ohta, K.: 'Boomerang Distinguishers for Full HAS-160 Compression Function', Proc. IWSEC2012, 2012 (LNCS, 7631), pp. 156–169.
11. Leurent, G., Roy, A.: 'Boomerang Attacks on Hash Function Using Auxiliary Differentials', Proc. CT-RSA2012, 2012 (LNCS, 7178), pp. 215–230.
12. Yu, H., Chen, J., Wang, X.: 'The Boomerang Attacks on the Round-Reduced Skein-512', Proc. SAC2012, 2012 (LNCS, 7707), pp. 288–304.
13. Specification of SM3 Cryptographic Hash Function (in Chinese), http://www.oscca.gov.cn/UpFile/20101222141857786.pdf, December 2010.
14. Aumasson, J.-P., Henzen, L., Meier, W., Phan, R.C.-W.: 'SHA-3 Proposal BLAKE', http://131002.net/blake/blake.pdf, December 2010.
15. Bernstein, D.J.: 'ChaCha, a variant of Salsa20', http://cr.yp.to/chacha/chacha-20080128.pdf, January 2008.
16. Zou, J., Wu, W., Wu, S., Su, B., Dong, L.: 'Preimage Attacks on Step-Reduced SM3 Hash Function', Proc. ICISC2011, 2011 (LNCS, 7259), pp. 375–390.
17. Kircanski, A., Shen, Y., Wang, G., Youssef, A.M.: 'Boomerang and Slide-Rotational Analysis of the SM3 Hash Function', Proc. SAC2012, 2012 (LNCS, 7707), pp. 305–321.
18. Wang, G., Shen, Y.: 'Preimage and Pseudo-Collision Attacks on Step-Reduced SM3 Hash Function', Inf. Process. Lett., 2012, 113, (8), pp. 301–306.
19. Mendel, F., Nad, T., Schläffer, M.: 'Finding Collisions for Round-Reduced SM3', Proc. CT-RSA2013, 2013 (LNCS, 7779), pp. 174–188.
20. Li, J., Xu, L.: 'Attacks on Round-Reduced BLAKE', http://eprint.iacr.org/2009/238.pdf, May 2009.
21. Wang, L., Ohta, K., Sakiyama, K.: 'Free-Start Preimages of Round-Reduced BLAKE Compression Function', Rump Session on ASIACRYPT2009, 2009.
22. Aumasson, J.-P., Guo, J., Knellwolf, S., Matusiewicz, K., Meier, W.: 'Differential and Invertibility Properties of BLAKE', Proc. FSE2010, 2010 (LNCS, 6147), pp. 318–332.
23. Su, B., Wu, W., Wu, S., Dong, L.: 'Near-Collisions on the Reduced-Round Compression Functions of Skein and BLAKE', Proc. CANS2010, 2010 (LNCS, 6467), pp. 124–139.
24. Leurent, G.: 'ARXtools: A Toolkit for ARX Analysis', The Third SHA-3 Candidate Conference, 2012.
25. Dunkelman, O., Khovratovich, D.: 'Iterative Differentials, Symmetries, and Message Modification in BLAKE-256', ECRYPT II Hash Workshop, 2011.
26. Wagner, D.: 'The Boomerang Attack', Proc. FSE1999, 1999 (LNCS, 1636), pp. 156–170.
27. Kelsey, J., Kohno, T., Schneier, B.: 'Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent', Proc. FSE2000, 2001 (LNCS, 1978), pp. 75–93.
28. Biham, E., Dunkelman, O., Keller, N.: 'The Rectangle Attack – Rectangling the Serpent', Proc. EUROCRYPT2001, 2001 (LNCS, 2045), pp. 340–357.
29. Biham, E., Dunkelman, O., Keller, N.: 'Related-Key Boomerang and Rectangle Attacks', Proc. EUROCRYPT2005, 2005 (LNCS, 3494), pp. 507–525.

30. Wagner, D.: 'A Generalized Birthday Problem', Proc. CRYPTO2002, 2002 (LNCS, 2442), pp. 288–303.

A Differential Characteristics for Boomerangs of SM3 and BLAKE-256

Table 3. Differential characteristic for steps 0-15 used in the boomerang attack on 34-step CF of SM3

i	chaining variables	message	conditions	prob
0	$B_0 : 23$ $C_0 : 32$ $D_0 : 23, 32$ $F_0 : 13$ $G_0 : 32$ $H_0 : 13, 32$		$(A_0 \oplus B_0 \oplus C_0)_{23} \neq D_{0,23}$, $(E_0 \oplus F_0 \oplus G_0)_{13} \neq H_{0,13}$,	2^{-2}
1	$C_1 : 32$ $D_1 : 32$ $G_1 : 32$ $H_1 : 32$			1
2	$D_2 : 32$ $H_2 : 32$	$w_2 : 32$ $w'_2 : 32$		1
3				1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
14		$w'_{14} : 15, 23, 32$	$TT1_{14,i} = w'_{14,i} (i = 15, 23)$,	2^{-2}
15	$A_{15} : 15, 23, 32$		$SS1_{15,(2,10,19)} = A_{15,(15,23,32)}$, $TT1_{15,i} = (A_{15} \oplus B_{15} \oplus C_{15})_i (i = 15, 23)$, $TT1_{15,i} = SS2_{15,i} (i = 2, 3, 10, 12, 19, 27)$, $TT2_{15,i} = SS1_{15,i} (i = 2, 10, 19)$.	2^{-14}
16	$A_{16} : 2, 3, 10, 12, 15, 19, 23, 27, 32$ $B_{16} : 15, 23, 32$ $E_{16} : 2, 4, 10, 11, 19, 27, 28$			—

Table 4. Differential characteristic for steps 16-33 used in the boomerang attack on 34-step CF of SM3

i	chaining variables	message	conditions	prob
16	$C_{16}: 9,16,18,23,25,26,30,31$ $D_{16}: 11,20$ $G_{16}: 9,16,18,24,25,26,30,32$ $H_{16}: 1,3,4,10,12,19,20,28$	$w'_{16}: 20$	$A_{16,i} = B_{16,i}(i = 9,16,18,23,25,26,30,31)$, $D_{16,20} \neq w'_{16,20}$, $TT1_{16,11} = D_{16,11}$, $E_{16,i} = 1(i = 9,16,24,25,26,30,32)$, $E_{16,18} = 0$, $TT2_{16,i} = H_{16,i}(i = 1,3,4,10,12,19,20,28)$, $TT2_{16,18} = G_{16,18}$,	2^{-27}
17	$A_{17}: 11$ $D_{17}: 9,16,18,23,25,26,30,31$ $E_{17}: 1$ $H_{17}: 9,16,18,24,25,26,30,32$	$w_{17}: 8,9,10,16,18,24,25,27,32$ $w'_{17}: 8,9,10,16,18,24,25,27,32$	$SS1_{17,30} = A_{17,11}$, $SS1_{17,8} = E_{17,1}$, $B_{17,11} = C_{17,11}$, $w'_{17,8} \neq SS2_{17,8}$, $D_{17,9} = w'_{17,9} \neq w'_{17,10}$, $D_{17,i} \neq w'_{17,i}(i = 16,18)$, $D_{17,23} = SS2_{17,23} \neq w'_{17,24}$, $D_{17,25} = w'_{17,25} = D_{17,26} \neq w'_{17,27}$, $D_{17,30} = SS2_{17,30} = D_{17,31}$, $F_{17,1} = G_{17,1}$, $w_{17,8} \neq SS1_{17,8}$, $H_{17,9} = w_{17,9} \neq w_{17,10}$, $H_{17,i} \neq w_{17,i}(i = 16,18,24)$, $H_{17,25} = w_{17,25} = H_{17,26} \neq w_{17,27}$, $H_{17,30} \neq SS1_{17,30}$,	2^{-26}
18	$B_{18}: 11$ $F_{18}: 1$		$A_{18,11} = C_{18,11}$, $E_{18,1} = 0$,	2^{-2}
19	$C_{19}: 20$ $G_{19}: 20$		$A_{19,20} = B_{19,20}$, $E_{19,20} = 1$,	2^{-2}
20	$D_{20}: 20$ $H_{20}: 20$	$w_{20}: 20$ $w'_{20}: 20$	$D_{20,20} \neq w'_{20,20}$, $H_{20,20} \neq w_{20,20}$,	2^{-2}
21				1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
32		$w'_{32}: 3,11,20$	$TT1_{32,i} = w'_{32,i}(i = 3,11,20)$,	2^{-3}
33	$A_{33}: 3,11,20$		$SS1_{33,(22,30,7)} = A_{33,(3,11,20)}$, $B_{33,i} = C_{33,i}(i = 3,11,20)$, $TT1_{33,i} = SS2_{33,i}(i = 7,15,22,23,30)$, $TT2_{33,i} = SS1_{33,i}(i = 7,22,30)$.	2^{-14}
34	$A_{34}: 7,15,22,23,30,32$ $B_{34}: 3,11,20$ $E_{34}: 7,15,16,22,24,30,31$			—

Table 5. Differential characteristic for steps 16-34 used in the boomerang attack on 35-step CF of SM3

i	chaining variables	message	conditions	prob
16	$B_{16}: 4, 5, 11, 13, 18, 20, 21, 25, 26$ $C_{16}: 15, 22, 23$ $F_{16}: 1, 3, 9, 12, 15, 17, 26$ $G_{16}: 5, 7, 8, 14, 16, 23, 24, 32$		$A_{16,i} = B_{16,i}(i = 15, 22, 23)$, $A_{16,i} = C_{16,i}$ $(i = 4, 5, 11, 13, 18, 20, 21, 25, 26)$, $E_{16,i} = 0(i = 1, 3, 9, 12, 15, 17, 26)$, $E_{16,i} = 1(i = 5, 7, 8, 14, 16, 23, 24, 32)$,	2^{-27}
17	$C_{17}: 2, 3, 13, 14, 20, 22, 27, 29, 30$ $D_{17}: 15, 22, 23$ $G_{17}: 2, 4, 13, 20, 22, 28, 31$ $H_{17}: 5, 7, 8, 14, 16, 23, 24, 32$	$w'_{17}: 24$	$A_{17,i} = B_{17,i}(i = 2, 3, 13, 14, 20, 27, 29, 30)$, $A_{17,22} \neq B_{17,22}$, $TT1_{17,15} = D_{17,15}$, $C_{17,22} = D_{17,22} = D_{17,23} \neq w'_{17,24}$, $E_{17,i} = 1(i = 2, 4, 13, 20, 28, 31)$, $E_{17,22} = 0$, $TT2_{17,22} = G_{17,22}$, $TT2_{17,i} = H_{17,i}(i = 5, 7, 8, 14, 16, 23, 24)$,	2^{-28}
18	$A_{18}: 15$ $D_{18}: 2, 3, 13, 14, 20, 22, 27, 29, 30$ $E_{18}: 5$ $H_{18}: 2, 4, 13, 20, 22, 28, 31$	$w_{18}: 4, 12, 13, 14, 20, 22, 28, 29, 31$ $w'_{18}: 4, 12, 13, 14, 20, 22, 28, 29, 31$	$SS1_{18,2} = A_{18,15}$, $SS1_{18,12} = E_{18,5}$, $D_{18,2} = SS2_{18,2} = D_{18,3} \neq w'_{18,4}$, $SS2_{18,12} \neq w'_{18,12}$, $D_{18,i} \neq w'_{18,i}(i = 13, 14, 20, 22)$, $D_{18,27} = SS2_{18,27} \neq w'_{18,28}$, $D_{18,29} = w'_{18,29} = D_{18,30} \neq w'_{18,31}$, $B_{18,15} = C_{18,15}$, $SS1_{18,12} \neq w_{18,12}$, $H_{18,i} \neq w_{18,i}(i = 4, 20, 22, 31)$, $H_{18,i} = w_{18,i} \neq w_{18,i+1}(i = 13, 28)$, $H_{18,2} \neq SS1_{18,2}$, $F_{18,5} = G_{18,5}$,	2^{-27}
19	$B_{19}: 15$ $F_{19}: 5$		$A_{19,15} = C_{19,15}$, $E_{19,5} = 0$,	2^{-2}
20	$C_{20}: 24$ $G_{20}: 24$		$A_{20,24} = B_{20,24}$, $E_{20,24} = 1$,	2^{-2}
21	$D_{21}: 24$ $H_{21}: 24$	$w_{21}: 24$ $w'_{21}: 24$	$D_{21,24} \neq w'_{21,24}$, $H_{21,24} \neq w_{21,24}$,	2^{-2}
22				1
⋮	⋮	⋮	⋮	⋮
33		$w'_{33}: 7, 15, 24$	$TT1_{33,i} = w'_{33,i}(i = 7, 15, 24)$,	2^{-3}
34	$A_{34}: 7, 15, 24$		$SS1_{34,(26,2,11)} = A_{34,(7,15,24)}$, $B_{34,i} = C_{34,i}(i = 7, 15, 24)$, $TT1_{34,i} = SS2_{34,i}$ $(i = 2, 4, 11, 19, 26, 27)$, $TT2_{34,i} = SS1_{34,i}(i = 2, 11, 26)$.	2^{-15}
35	$A_{35}: 2, 4, 11, 19, 26, 27$ $B_{35}: 7, 15, 24$ $E_{35}: 2, 3, 11, 19, 20, 26, 28$			—

Table 6. Differential characteristic for steps 0-16(17) used in the boomerang attacks on 36(37/38)-step CF of SM3

i	chaining variables	message	conditions	prob
0	$A_0 : 23$ $B_0 : 23$ $C_0 : 23, 32$ $D_0 : 3, 4, 5, 7, 10, 12, 21, 22, 23, 28, 30, 32$ $E_0 : 13$ $F_0 : 13$ $G_0 : 13, 32$ $H_0 : 4, 5, 7, 10, 12, 13, 21, 22, 28, 30, 32$	$w_0 : 4, 5, 7, 12, 20, 21, 22, 28, 30$ $w'_0 : 4, 5, 7, 12, 20, 21, 22, 28, 30$	$SS1_{0,10} = A_{0,23}$, $SS1_{0,20} = E_{0,13}$, $D_{0,23} \neq (A_0 \oplus B_0 \oplus C_0)_{23}$, $D_{0,i} \neq SS2_{0,i}(i = 3, 10)$, $D_{0,i} \neq w'_{0,i}(i = 4, 5, 7, 12, 21, 22, 28, 30)$, $SS2_{0,20} \neq w'_{0,20}$, $H_{0,13} \neq (E_0 \oplus F_0 \oplus G_0)_{13}$, $H_{0,i} \neq w_{0,i}(i = 4, 5, 7, 12, 21, 22, 28, 30)$, $H_{0,10} \neq SS1_{0,10}$, $SS1_{0,20} \neq w_{0,20}$,	2^{-25}
1	$B_1 : 23$ $C_1 : 32$ $D_1 : 23, 32$ $F_1 : 13$ $G_1 : 32$ $H_1 : 13, 32$		$(A_1 \oplus B_1 \oplus C_1)_{23} \neq D_{1,23}$, $(E_1 \oplus F_1 \oplus G_1)_{13} \neq H_{1,13}$,	2^{-2}
2	$C_2 : 32$ $D_2 : 32$ $G_2 : 32$ $H_2 : 32$			1
3	$D_3 : 32$ $H_3 : 32$	$w_3 : 32$ $w'_3 : 32$		1
4				1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
15		$w'_{15} : 15, 23, 32$	$TT1_{15,i} = w'_{15,i}(i = 15, 23)$,	2^{-2}
16	$A_{16} : 15, 23, 32$		$SS1_{16,(2,10,19)} = A_{16,(15,23,32)}$, $B_{15,i} = C_{15,i}(i = 15, 23, 32)$, $TT1_{15,i} = SS2_{15,i}(i = 2, 3, 10, 12, 19, 27)$, $TT2_{16,i} = SS1_{16,i}(i = 2, 10, 19)$,	2^{-15}
17	$A_{17} : 2, 3, 10, 12, 19, 27$ $B_{17} : 15, 23, 32$ $E_{17} : 2, 4, 10, 11, 19, 27, 28$		$SS1_{17,(21,22,29,31,6,14)} = A_{17,(2,3,10,12,19,27)}$, $SS1_{17,(9,11,17,18,26,2,3)} = E_{17,(2,4,10,11,19,27,28)}$, $B_{17,i} = C_{17,i}(i = 10, 12, 19, 27)$, $B_{17,i} \neq C_{17,i}(i = 2, 3)$, $A_{17,15} \neq C_{17,15}$, $A_{17,i} = C_{17,i}(i = 23, 32)$, $SS2_{17,15} \neq B_{17,15}$, $SS2_{17,i} \neq A_{17,i}(i = 2, 3)$, $TT1_{17,i} = SS2_{17,i}$ $(i = 6, 7, 9, 11, 17, 18, 21, 24, 26, 29)$, $F_{17,i} \neq G_{17,i}(i = 2, 11)$, $F_{17,i} = G_{17,i}(i = 4, 10, 19, 27, 28)$, $SS1_{17,i} \neq ((E_{17} \wedge F_{17}) \vee (\neg E_{17} \wedge G_{17}))_i$ $(i = 2, 11)$, $TT2_{17,i} = SS1_{17,i}$ $(i = 3, 6, 9, 14, 17, 18, 21, 22, 26, 29, 31)$.	2^{-55}
18	$A_{18} : 6, 7, 9, 11, 17, 18, 21, 24, 26, 29$ $B_{18} : 2, 3, 10, 12, 19, 27$ $C_{18} : 9, 24, 32$ $E_{18} : 2, 3, 6, 7, 8, 9, 11, 12, 15, 16, 17, 20, 21, 22, 26, 27, 29, 30, 31$ $F_{18} : 2, 4, 10, 11, 19, 27, 28$			—

Table 7. Differential characteristic for steps 18-36(37) used in the boomerang attacks on 37(38)-step CF of SM3

i	chaining variables	message	conditions	prob
18	$B_{18}: 4,5,11,13,18,20,21,25,26$ $C_{18}: 15,22,23$ $F_{18}: 1,3,9,12,15,17,26$ $G_{18}: 5,7,8,14,16,23,24,32$		$A_{18,i} = B_{18,i} (i = 15,22,23)$, $A_{18,i} = C_{18,i} (i = 4,5,11,13,18,20,21,25,26)$, $E_{18,i} = 0 (i = 1,3,9,12,15,17,26)$, $E_{18,i} = 1 (i = 5,7,8,14,16,23,24,32)$,	2^{-27}
19	$C_{19}: 2,3,13,14,20,22,27,29,30$ $D_{19}: 15,22,23$ $G_{19}: 2,4,13,20,22,28,31$ $H_{19}: 5,7,8,14,16,23,24,32$	$w'_{19}: 24$	$A_{19,i} = B_{19,i} (i = 2,3,13,14,20,27,29,30)$, $A_{19,22} \neq B_{19,22}$, $TT1_{19,15} = D_{19,15}$, $C_{19,22} = D_{19,22} = D_{19,23} \neq w'_{19,24}$, $E_{19,i} = 1 (i = 2,4,13,20,28,31)$, $E_{19,22} = 0$, $TT2_{19,i} = H_{19,i} (i = 5,7,8,14,16,23,24)$, $TT2_{19,22} = G_{19,22}$,	2^{-28}
20	$A_{20}: 15$ $D_{20}: 2,3,13,14,20,22,27,29,30$ $E_{20}: 5$ $H_{20}: 2,4,13,20,22,28,31$	$w_{20}: 4,12,13,$ $14,20,22,$ $28,29,31$ $w'_{20}: 4,12,13,$ $14,20,22,$ $28,29,31$	$SS1_{20,2} = A_{20,15}$, $SS1_{20,12} = E_{20,5}$, $D_{20,2} = SS2_{20,2} = D_{20,3} \neq w'_{20,4}$, $SS2_{20,12} \neq w'_{20,12}$, $D_{20,i} \neq w'_{20,i} (i = 13,14,20,22)$, $D_{20,27} = SS2_{20,27} \neq w'_{20,28}$, $D_{20,29} = w'_{20,29} = D_{20,30} \neq w'_{20,31}$, $B_{20,15} = C_{20,15}$, $SS1_{20,12} \neq w_{20,12}$, $H_{20,i} \neq w_{20,i} (i = 4,20,22,31)$, $H_{20,i} = w_{20,i} \neq w_{20,i+1} (i = 13,28)$, $H_{20,2} \neq SS1_{20,2}$, $F_{20,5} = G_{20,5}$,	2^{-27}
21	$B_{21}: 15$ $F_{21}: 5$		$A_{21,15} = C_{21,15}$, $E_{21,5} = 0$,	2^{-2}
22	$C_{22}: 24$ $G_{22}: 24$		$A_{22,24} = B_{22,24}$, $E_{22,24} = 1$,	2^{-2}
23	$D_{23}: 24$ $H_{23}: 24$	$w_{23}: 24$ $w'_{23}: 24$	$D_{23,24} \neq w'_{23,24}$, $H_{23,24} \neq w_{23,24}$,	2^{-2}
24				1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
35		$w'_{35}: 7,15,24$	$TT1_{35,i} = w'_{35,i} (i = 7,15,24)$,	2^{-3}
36	$A_{36}: 7,15,24$		$SS1_{36,(26,2,11)} = A_{36,(7,15,24)}$, $B_{36,i} = C_{36,i} (i = 7,15,24)$, $TT1_{36,i} = SS2_{36,i} (i = 2,4,11,19,26,27)$, $TT2_{36,i} = SS1_{36,i} (i = 2,11,26)$,	2^{-15}
37	$A_{37}: 2,4,11,19,26,27$ $B_{37}: 7,15,24$ $E_{37}: 2,3,11,19,20,26,28$		$SS1_{37,9} \neq E_{37,2} \neq E_{37,3}$, $SS1_{37,26} \neq E_{37,19} \neq E_{37,20}$, $SS1_{37,(18,1,3)} = E_{37,(11,26,28)}$, $SS1_{37,(21,23,30,6,13,14)} = A_{37,(2,4,11,19,26,27)}$, $C_{37,i} = B_{37,i} (i = 2,4,11,19,27)$, $C_{37,26} \neq B_{37,26}$, $C_{37,i} = A_{37,i} (i = 15,24)$, $C_{37,7} \neq A_{37,7}$, $SS2_{37,7} \neq B_{37,7}$, $SS2_{37,26} \neq A_{37,26}$, $TT1_{37,i} = SS2_{37,i} (i = 1,3,9,13,16,18,21,30,31)$, $F_{37,i} = G_{37,i} (i = 2,11,19,20,28)$, $F_{37,i} \neq G_{37,i} (i = 3,26)$, $SS1_{37,i} \neq ((E_{37} \wedge F_{37}) \vee (\neg E_{37} \wedge G_{37}))_i (i = 3,26)$, $TT2_{37,i} = SS1_{37,i} (i = 1,6,9,13,14,18,21,23,30)$.	2^{-51}
38	$A_{38}: 1,3,9,13,16,18,21,30,31$ $B_{38}: 2,4,11,19,26,27$ $C_{38}: 1,16,24$ $E_{38}: 1,3,7,8,9,10,13,14,18,21,$ $22,23,26,27,30,31,32$ $F_{38}: 2,3,11,19,20,26,28$			—

Table 8. Differential characteristics used in the boomerang attacks on 7 and 8 rounds of KP of BLAKE-256

message	$m_5 : 21$	
i	chaining variables	prob
2.5	$v_0 : 5$ $v_1 : 1, 13, 29$ $v_2 : 1, 9, 17, 20, 25, 28$ $v_3 : 1, 8, 12, 24, 28$ $v_4 : 8, 24$ $v_5 : 21$ $v_6 : 1, 13, 21, 29$ $v_7 : 1, 5, 8, 9, 13, 17, 20, 21, 25, 29$ $v_8 : 5, 13, 21, 29$ $v_9 : 1$ $v_{10} : 5, 29$ $v_{11} : 5, 13, 29$ $v_{12} : 5$ $v_{13} : 5, 8, 13, 21, 28, 29$ $v_{14} : 1, 12, 17, 28$ $v_{15} : 13$	2^{-54}
3	$v_0 : 5, 21$ $v_3 : 1$ $v_4 : 5, 21$ $v_7 : 1, 21$ $v_8 : 5, 13, 21, 29$ $v_{11} : 21$ $v_{12} : 13, 29$ $v_{15} : 21$	2^{-16}
4	$v_1 : 21$	2^{-1}
5		2^{-2}
6	$v_1 : 21$ $v_6 : 6$ $v_{11} : 13$ $v_{12} : 13$	2^{-29}
6.5	$v_0 : 17, 21$ $v_1 : 21, 25$ $v_2 : 6, 10, 26$ $v_3 : 1$ $v_4 : 2, 6, 10, 14, 22$ $v_5 : 6, 10, 18, 22, 30$ $v_6 : 3, 7, 11, 15, 19, 23, 27$ $v_7 : 6, 18, 26$ $v_8 : 9, 13, 21, 29$ $v_9 : 5, 13, 17, 29$ $v_{10} : 2, 14, 18, 22, 30$ $v_{11} : 13, 25$ $v_{12} : 9, 13, 21$ $v_{13} : 13, 17, 29$ $v_{14} : 2, 14, 18, 30$ $v_{15} : 25$	—

message	$m_{11} : 32$	
i	chaining variables	prob
6.5	$v_0 : 3, 7, 19, 23, 32$ $v_1 : 16, 32$ $v_2 : 8, 12, 24, 32$ $v_3 : 4, 7, 12, 16, 20, 28, 31$ $v_4 : 4, 8, 12, 19, 20, 24, 28, 31$ $v_5 : 3, 12, 19, 32$ $v_7 : 8, 12, 24, 32$ $v_8 : 8, 16, 24, 32$ $v_{10} : 12$ $v_{11} : 16, 32$ $v_{13} : 32$ $v_{14} : 7, 16, 19$ $v_{15} : 7, 12, 16, 23, 28$	2^{-40}
7	$v_0 : 12, 32$ $v_1 : 16, 32$ $v_2 : 32$ $v_4 : 12, 32$ $v_5 : 16, 32$ $v_8 : 32$ $v_9 : 8, 16, 24, 32$ $v_{10} : 32$ $v_{13} : 8, 24$ $v_{14} : 16, 32$	2^{-6}
8	$v_2 : 32$	1
9		2^{-1}
10	$v_0 : 32$ $v_5 : 17$ $v_{10} : 24$ $v_{15} : 24$	2^{-24}
10.5	$v_0 : 4, 32$ $v_1 : 5, 17, 21$ $v_2 : 12$ $v_3 : 28$ $v_4 : 1, 9, 17, 21, 29$ $v_5 : 2, 6, 14, 18, 22, 26, 30$ $v_6 : 5, 17, 29$ $v_7 : 1, 13, 21, 25$ $v_8 : 8, 16, 24, 28$ $v_9 : 1, 9, 13, 25, 29$ $v_{10} : 4, 24$ $v_{11} : 8, 20, 32$ $v_{12} : 8, 24, 28$ $v_{13} : 9, 13, 25, 29$ $v_{14} : 4$ $v_{15} : 20, 32$	—

B Examples of Boomerang quartets for SM3 and BLAKE-256

Table 9. Example of a boomerang quartet for 34-step CF of SM3. P_i, C_i and M_i respectively denote the chaining variables of step 0, 33 and message words.

P_1	8e328bf1	540ba9e5	026995ca	d1271808	8afc4d19	95bddaa7	a56d9207	a2c44d1c
P_2	8e328bf1	544ba9e5	826995ca	51671808	8afc4d19	95bdcaa7	256d9207	22c43d1c
P_3	11ee1c76	ee57de46	54838689	0665bf71	df61a977	5f4c46e9	d42981b4	c15ec4f8
P_4	11ee1c76	ee17de46	d4838689	8625bf71	df61a977	5f4c56e9	542981b4	415eb4f8
M_1	d7a6bd34	66fa6efa	78ce08a1	9a585055	94c8bc0b	3b679ebd	3910da41	f0e82d8a
	d5f41b80	64f0041d	947bccb4	4344d2ed	bcc94a67	6b5f97ff	79000306	16233872
M_2	d7a6bd34	66fa6efa	f8ce08a1	9a585055	94c8bc0b	3b679ebd	3910da41	f0e82d8a
	d5f41b80	64f0041d	947bccb4	4344d2ed	bcc94a67	6b5f97ff	79000306	16233872
M_3	d7acbd36	26fbaefa	50ce00a1	1fdad3d5	94c2b90e	333fb685	3918da41	70e8ad8c
	d5f49b80	64f0041d	9570c9b3	c3c4d3ed	bcc94a67	6b5797ff	f9008304	16233872
M_4	d7acbd36	26fbaefa	d0ce00a1	1fdad3d5	94c2b90e	333fb685	3918da41	70e8ad8c
	d5f49b80	64f0041d	9570c9b3	c3c4d3ed	bcc94a67	6b5797ff	f9008304	16233872
C_1	5cc18f78	adf682b8	837bc39c	1550ef7d	5e6d092c	b95a7f10	0fdde16d	3dc6bf65
C_2	35437883	a37697ca	94fa71b5	169e842d	07d1f375	e5e58686	e97b5e86	72b07d54
C_3	bcd1cfbd	adee86bc	837bc39c	1550ef7d	fecc48ec	b95a7f10	0fdde16d	3dc6bf65
C_4	d5533846	a36e93ce	94fa71b5	169e842d	a770b2b5	e5e58686	e97b5e86	72b07d54

Table 10. Example of a boomerang quartet for 35-step CF of SM3

P_1	7f57e38d	801906df	caf2cf8c	42c58fba	9feec59b	ef5ab3fc	d261869c	892ca15c
P_2	7f57e38d	805906df	4af2cf8c	c2858fba	9feec59b	ef5aa3fc	5261869c	092cb15c
P_3	0188f80d	5d3b7666	9f941688	fc411326	3a674355	2c6075fb	85a38600	892e081b
P_4	0188f80d	5d7b7666	1f941688	7c011326	3a674355	2c6065fb	05a38600	092e181b
M_1	f5bc88b9	af543ad9	f5068596	beaebbf0	9984c067	ed6e551a	7973166d	cef6b36f
	c6978096	fdba14b7	2872ffba	2cf314e6	750499b3	4ceb9f22	bd2d99db	71cc928b
M_2	f5bc88b9	af543ad9	75068596	beaebbf0	9984c067	ed6e551a	7973166d	cef6b36f
	c6978096	fdba14b7	2872ffba	2cf314e6	750499b3	4ceb9f22	bd2d99db	71cc928b
M_3	75bc89b9	aff43af9	f51a8592	3eae3bf2	c1acf86f	edce054a	fcf195ed	ce76b36f
	c69f80fe	fdb214b7	2872ffba	3c434496	7d0489bb	4ceb9f22	bdad99db	71c492a3
M_4	75bc89b9	aff43af9	751a8592	3eae3bf2	c1acf86f	edce054a	fcf195ed	ce76b36f
	c69f80fe	fdb214b7	2872ffba	3c434496	7d0489bb	4ceb9f22	bdad99db	71c492a3
C_1	ecda4c19	39e58fb5	8fbc81e3	75eec099	655e3f8b	f4273d52	94532c77	6967f472
C_2	93ffb93f	e7e2ffb3	447c0e9f	b8ff8f6c	37a12b0a	ca38d92c	7eb36c56	899e0baf
C_3	f2de485f	3965cff5	8fbc81e3	75eec099	6f523b8d	f4273d52	94532c77	6967f472
C_4	8dfbbd79	e762bff3	447c0e9f	b8ff8f6c	3dad2f0c	ca38d92c	7eb36c56	899e0baf

Table 11. Example of a boomerang quartet for 7-round KP of BLAKE-256

P_1	3c8a4276	cfb0dcc0	ab6c46fc	da21a046	ec13b53b	cf12cee3	45fc2729	ccca4dee
	14c76a6a	40f2aada	a0933ddf	d51f0f3e	260c01f7	6beb49c8	da575eb9	a72108d8
P_2	3c9a4286	cfb0dcc0	ab6c46fc	da21a045	ec03b52b	cf12cee3	45fc2729	ccda4def
	04b75a7a	40f2aada	a0933ddf	d50f0f3e	360c11f7	6beb49c8	da575eb9	a71108d8
P_3	ac3b9572	70a2660d	6520d49f	d01074b9	71422e9e	39e0c7ab	4af9b4d4	797282e3
	86cddb58	b5c62820	5b8ff4d0	be138673	8b1e21ea	b6dd991a	36176157	ebc193f1
P_4	ac2b9582	70a2660d	6520d49f	d01074ba	71522e8e	39e0c7ab	4af9b4d4	796282e2
	96bdeb48	b5c62820	5b8ff4d0	be038673	9b1e31ea	b6dd991a	36176157	ebf193f1
M_1	cf25b88d	0b85815c	7a2c591a	6df41a94	59eb3709	ef111a43	c3f441c7	846d24e6
	950acec4	dfaa5876	05676c74	a3a2894f	a000ff75	31595bf2	61592468	79f50b81
M_2	cf25b88d	0b85815c	7a2c591a	6df41a94	59eb3709	ef011a43	c3f441c7	846d24e6
	950acec4	dfaa5876	05676c74	a3a2894f	a000ff75	31595bf2	61592468	79f50b81
M_3	cf25b88d	0b85815c	7a2c591a	6df41a94	59eb3709	ef111a43	c3f441c7	846d24e6
	950acec4	dfaa5876	05676c74	23a2894f	a000ff75	31595bf2	61592468	79f50b81
M_4	cf25b88d	0b85815c	7a2c591a	6df41a94	59eb3709	ef011a43	c3f441c7	846d24e6
	950acec4	dfaa5876	05676c74	23a2894f	a000ff75	31595bf2	61592468	79f50b81
C_1	1db2186a	ce3fe558	a96bdf5e	b0895b04	678b343b	d6dd58ea	e333eb5d	fe982f92
	52660ebe	f519fabe	d32be0de	b81731bb	185dd895	050bf35e	bc6f992c	eb0364f8
C_2	fbb8c27f	99cff7f2	ab2dabef	faa5905e	709f8d52	81f4ec99	d3b15660	d6412448
	ad141e81	bf02aa21	fd84e3fb	02a3bc0d	973c04e0	bb95e80b	5fcad084	f2f36107
C_3	9db2186a	ce3fe558	a96bdf5e	b0895b04	678b343b	d6dc58ea	e333eb5d	fe982f92
	52660ebe	f519fabe	d3abe0de	b81731bb	185dd895	050bf35e	bc6f992c	eb8364f8
C_4	7bb8c27f	99cff7f2	ab2dabef	faa5905e	709f8d52	81f5ec99	d3b15660	d6412448
	ad141e81	bf02aa21	fd04e3fb	02a3bc0d	973c04e0	bb95e80b	5fcad084	f2736107