The Boomerang Attacks on BLAKE and BLAKE2

Yonglin Hao

Department of Computer Science and Technology, Tsinghua Universtiy, Beijing 100084, China
haoyl12@mails.tsinghua.edu.cn

Abstract. In this paper, we study the security margins of hash functions BLAKE and BLAKE2 against the boomerang attack. We launch boomerang attacks on all four members of BLAKE and BLAKE2, and compare their complexities. We propose 8.5-round boomerang attacks on both BLAKE-512 and BLAKE2b with complexities 2^{464} and 2^{474} respectively. We also propose 8-round attacks on BLAKE-256 with complexity 2^{198} and 7.5-round attacks on BLAKE2s with complexity 2^{184}. We verify the correctness of our analysis by giving practical 6.5-round Type I boomerang quartets for each member of BLAKE and BLAKE2.

According to our analysis, some tweaks introduced by BLAKE2 have increased its resistance against boomerang attacks to a certain extent. But on the whole, BLAKE still has higher a secure margin than BLAKE2.

1 Introduction

Cryptographic hash functions (simply referred as hash functions) are playing a significant role in the modern cryptology. They are indispensable in achieving secure systems such as digital signatures, message authentication codes and so on. In the cryptanalysis of hash functions, one of the greatest breakthrough was made by Wang et al. in 2005 when they successfully launched collision attacks on widely used hash functions MD5 [1] and SHA-1 [2]. After that, the analytic methods against hash functions have been greatly improved which threatens the security of existing hash functions. To cope with this situation, NIST proposed the transition from SHA-1 to SHA-2. Furthermore, NIST also launched the SHA-3 competition to develop a new hash standard. After years' analysis, five proposals entered the final round of SHA-3 and the one named Keccak became the new SHA-3 standard in 2012 [3].

The BLAKE hash function [4] was one of the five finalists of the SHA-3 competition [5]. Although it was not selected as the SHA-3 standard, along with the other finalists, BLAKE is assumed to be a very strong hash function with high security margin and very good performance in software.

BLAKE2 [6] is a new family of hash functions based on BLAKE. According to [6], the main objective of BLAKE2 is to provide a number of parameters for use in applications without the need of additional constructions and modes, and also to speed-up even further the hash function to a level of compression rate close to MD5.

Ever since its proposal, BLAKE has attracted a considerable amount of cryptanalysis, such as impossible differential attack [7], differential attack[8], collision, preimage [9] etc. There is also a boomerang distinguisher on BLAKE-32 given by Biryukov et al. in [10] but some incompatible problems were pointed out by Leurent in [11]. Despite of the incompatibilities, [10] indicates that the boomerang method may have good efficiency in analyzing the BLAKE family. Recently, Bai et al. have given the first valid 7-round and 8-round boomerangs for BLAKE-256 [12].

As to BLAKE2, Guo et al. [13] have given a thorough security analysis of it. In their paper, they applied almost all the existing attacks on BLAKE to BLAKE2. According to their results, the tweaks introduced by BLAKE2, if analyzed separately, reduce the security of the version in some theoretical attacks. Some cryptanalysis methods manage to reach more rounds for BLAKE2 than BLAKE. BLAKE seems to have better resistance than BLAKE2 against various cryptanalysis methods. However, [13] did not evaluate the security margin of the two hash function families under the boomerang method and this is what we are going to do in this paper.

The original boomerang attack was introduced by Wagner in 1999 [14] as a tool for the cryptanalysis of block ciphers. It is an adaptive chosen plaintext and ciphertext attack utilizing differential cryptanalysis.

Later, Kelsey et al. [15] developed the original version into a chosen plaintext attack called the amplified boomerang attack. Developments were also made by Biham et al. in [16] and [17].

During the past few years, the idea of the boomerang attack has been applied to many hash functions. Biryukov et al. [10] and Lamberger et al. [18] independently applied the boomerang attack to BLAKE-32 and SHA-256. The SHA-256 result was later improved by Biryukov et al. in [19]. Ever after, we saw the boomerang results on many hash functions such as SIME-512 [20], HAVAL [21], RIPEMD-128/160 [22], HAS-160 [21], Skein-256/512 [23,24], SM3 [25,26] and BLAKE-256 [12]. The boomerang attack has become a common tool for analyzing various hash functions.

Our contribution. We reevaluate the boomerang attack on BLAKE-256 in [12] and apply the method to the keyed permutations of all BLAKE and BLAKE2 members namely BLAKE-256, BLAKE-512, BLAKE2s and BLAKE2b. We construct boomerang distinguishers for 8.5-round keyed permutation of BLAKE-512 and BLAKE2b (both from round 2.5 to 11). The complexity for attacking BLAKE-512 is 2^{464} and that for BLAKE2b is 2^{474}. We also present 7.5-round attack on BLAKE2s (round 2.5 to 10) with complexity 2^{184}. Besides, we lower the complexity of the 8-round BLAKE-256 result in [12] from 2^{200} to 2^{198} with slight modification of the differential characteristic. We present our boomerang results along with previous ones in Table 1. As can be seen, some tweaks introduced by BLAKE2 have surprisingly increased its resistance against boomerang attacks to a certain extent. But, since BLAKE has more rounds, the secure margin of BLAKE is still higher than that of BLAKE2.

Table 1. All existing boomerang results on BLAKE and BLAKE2.

Hash function	Target	Rounds	Time	Source
BLAKE-256	CF	6	2^{102}	[10]
	CF	6.5*	2^{184}	
	CF	7*	2^{232}	
	KP	6	$2^{11.75}$	
	KP	7*	2^{122}	
	KP	8*	2^{242}	
	KP	7	2^{37}**	[12]
	KP	8	2^{200}	
	KP	**8**	$\mathbf{2^{198}}$	**This paper**
BLAKE2s	**KP**	**7.5**	$\mathbf{2^{184}}$	**This paper**
BLAKE-512	**KP**	**8.5**	$\mathbf{2^{464}}$	**This paper**
BLAKE2b	**KP**	**8.5**	$\mathbf{2^{474}}$	**This paper**

KP: Keyed Permutation
CF: Compression Function
*: there are some incompatible problems in their attacks
**: this is the complexity for the Type III boomerang while others are of Type I.

Organization of the Paper. In Section 2, we briefly introduce the round functions of BLAKE and BLAKE2, and provide the overview of the boomerang attack. Section 3 describes the way that we deduce the differential characteristics and the process of building the boomerang distinguishers. Finally, we conclude our paper in Section 4.

2 Preliminary

In the first part of this section, we make a brief introduction of the two families of hash functions, BLAKE and BLAKE2. Since our boomerang analysis mainly focus on the keyed permutation of BLAKE and BLAKE2, which excludes the Initialization and Finalization procedures, we only introduce the round functions in this section. We refer the readers to [4] and [6] for information about initialization and finalization phases. We also give some notations that are used through this paper.

In the second part of this section, we review the procedure of the boomerang attack on hash functions and give some definitions that we use in the description of our attacks.

2.1 The Round Functions of BLAKE and BLAKE2

BLAKE and BLAKE2 share many similarities. As the successor of BLAKE, BLAKE2 has a 32-bit version (BLAKE2s) and a 64-bit version (BLAKE2b), corresponding to BLAKE-256 and BLAKE-512 of BLAKE respectively. Both BLAKE and BLAKE2 process 16-word message blocks. However, differences can be witnessed at every level including internal permutation, compression function, and hash function construction. Some notations have to be introduced first:

$\leftarrow$ variable assignment;
$+$ modular 2^{32} or 2^{64} addition (according to the word length);
$-$ modular 2^{32} or 2^{64} subtraction (according to the word length);
$\oplus$ bitwise exclusive or;
$\lll n$ cyclic shift n bits towards the most significant bit;
$\ggg n$ cyclic shift n bits towards the least significant bit;
$\wedge$ bitwise AND operation for words.

The Round functions of both BLAKE and BLAKE2 process a state of 16 64-bit or 32-bit words represented by a 4 × 4 matrix as follows:

$$V = \begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}.$$

In the remainder of this paper, we denote the 16-word intermediate state by the capital letters such as V, TV and M for message block. Single 64-bit or 32-bit words are denoted by small letters such as v, tv and m for message words. We also refer to the i-th bit of a word v ($i = 0, \cdots 31$ or 63 from the least significant to the most significant) as $v[i]$.

Once the state V is initialized, V is processed by several rounds (10, 12, 14, 16 for BLAKE2s, BLAKE2b, BLAKE-256, BLAKE512 respectively) of G functions, which means computing

$$G_0(v_0, v_4, v_8, v_{12}), G_1(v_1, v_5, v_9, v_{13}), G_2(v_2, v_6, v_{10}, v_{14}), G_3(v_3, v_7, v_{11}, v_{15})$$
$$G_4(v_0, v_5, v_{10}, v_{15}), G_5(v_1, v_6, v_{11}, v_{12}), G_6(v_2, v_7, v_8, v_{13}), G_7(v_3, v_4, v_9, v_{14})$$

where $G_i(a, b, c, d), i = 0, \cdots, 7$ differ among BLAKE2s, BLAKE2b, BLAKE-256, BLAKE512 and are all listed in Table 2. The σ_r in Step 1 and 5 of the G_i function in Table 2 belongs to the set of permutations as defined in Table 3. At round $r > 9$, the permutation used is $\sigma_{r \mod 10}$ (for example, if $r = 11$, the permutation $\sigma_{11 \mod 10} = \sigma_1$ is used).

Table 2. The G_i Functions of BLAKE-256, BLAKE2s, BLAKE-512, BLAKE2b

Step	BLAKE-256	BLAKE2s	BLAKE-512	BLAKE2b
1	$a = a + b + (m_{\sigma_r(2i)} \oplus c_{\sigma_r(2i+1)})$	$a = a + b + m_{\sigma_r(2i)}$	$a = a + b + (m_{\sigma_r(2i)} \oplus c_{\sigma_r(2i+1)})$	$a = a + b + m_{\sigma_r(2i)}$
2	$d = (d \oplus a) \ggg 16$	$d = (d \oplus a) \ggg 16$	$d = (d \oplus a) \ggg 32$	$d = (d \oplus a) \ggg 32$
3	$c = c + d$	$c = c + d$	$c = c + d$	$c = c + d$
4	$b = (b \oplus c) \ggg 12$	$b = (b \oplus c) \ggg 12$	$b = (b \oplus c) \ggg 25$	$b = (b \oplus c) \ggg 24$
5	$a = a + b + (m_{\sigma_r(2i+1)} \oplus c_{\sigma_r(2i)})$	$a = a + b + m_{\sigma_r(2i+1)}$	$a = a + b + (m_{\sigma_r(2i+1)} \oplus c_{\sigma_r(2i)})$	$a = a + b + m_{\sigma_r(2i+1)}$
6	$d = (d \oplus a) \ggg 8$	$d = (d \oplus a) \ggg 8$	$d = (d \oplus a) \ggg 16$	$d = (d \oplus a) \ggg 16$
7	$c = c + d$	$c = c + d$	$c = c + d$	$c = c + d$
8	$b = (b \oplus c) \ggg 7$	$b = (b \oplus c) \ggg 7$	$b = (b \oplus c) \ggg 11$	$b = (b \oplus c) \ggg 63$

Since we need detailed analysis of the intermediate states, we further breakdown the round functions. We denote the state after r rounds of iterations by V^r ($r = 0, 1, \cdots$). Then, TV^r is acquired after the first 4 steps of $G_{0,\cdots,3}$ and $V^{r+0.5}$ is computed after $G_{0,\cdots,3}$ are completed. Similarly, we can compute $TV^{r+0.5}$ from $V^{r+0.5}$ by applying steps 1,2,3,4 of $G_{4,\cdots,7}$ and further compute V^{r+1} by finishing $G_{4,\cdots,7}$. This representation is illustrated as (1) and (2).

$$G_{0,\cdots,3} : V^r \xrightarrow{\text{Steps } 1,\cdots,4} TV^r \xrightarrow{\text{Steps } 5,\cdots,8} V^{r+0.5} \tag{1}$$

$$G_{4,\cdots,7} : V^{r+0.5} \xrightarrow{\text{Steps } 1,\cdots,4} TV^{r+0.5} \xrightarrow{\text{Steps } 5,\cdots,8} V^{r+1} \tag{2}$$

In this way, we can refer to any intermediate state word of any round easily.

Table 3. The definition of σ_r where $r = 0, \cdots, 9$.

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

2.2 The Boomerang Attack

About the boomerang attack on hash functions, we mainly review the known-related-key boomerang method given in [19]. We consider the compression function, denoted by CF, as $CF(M, K) = E(M, K) + M$ and that it can be decomposed into two sub-functions as $CF = CF_1 \circ CF_0$. In this way, we can start from the middle steps since M and the key K can be chosen randomly [19,23]. Then we have a backward (top) differential characteristic $(\beta, \beta_k) \to \alpha$ with probability p for CF_0^{-1}, and a forward (bottom) differential characteristic $(\gamma, \gamma_k) \to \delta$ with probability q for CF_1. Finally, we can launch the known-related-key boomerang attack with these two differential characteristics as follows:

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

It can be deduced that $P_1 \oplus P_3 = P_2 \oplus P_4 = \alpha$ and $C_1 \oplus C_2 = C_3 \oplus C_4 = \delta$ hold with probability at least p^2 in the backward direction and q^2 in the forward direction. Therefore, the attack succeeds with probability p^2q^2 when assuming that the differential characteristics are independent.

According H. Yu et al. in [24], for a n-bit random permutation, there are three types of boomerang distinguishers:

- Type I: A quartet satifies $P_1 \oplus P_3 = P_2 \oplus P_4 = \alpha$ and $C_1 \oplus C_2 = C_3 \oplus C_4 = \delta$ for fixed differences α and δ. In this case, the generic complexity is 2^n.
- Type II: Only $C_1 \oplus C_2 = C_3 \oplus C_4$ 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 $2^{n/3}$ [27].
- Type III: A quartet satisfied $P_1 \oplus P_3 = P_2 \oplus P_4$ and $C_1 \oplus C_2 = C_3 \oplus C_4$. In this case, the best known still takes time $2^{n/2}$.

We only study the Type I boomerang distinguisher in this paper. Besides, the complexity 2^{37} of the 7-round boomerang in [12] is actually the complexity for a Type III boomerang attack. The Type I complexity for the 7-round attack should be $2^{2\times(1+4+16+1)} = 2^{44}$ according to their methods.

3 The Boomerang Attacks on BLAKE and BLAKE2

In this section, we describe our boomerang attacks on BLAKE and BLAKE2. We only illustrate our strategies by comparing BLAKE-512 and BLAKE2b while those of BLAKE-256 and BLAKE2s can be deduced accordingly. Details are presented in Appendix A.

3.1 Construction of Differential Characteristics

The very first step for the boomerang attack is constructing two differential characteristics with high probability. Since BLAKE and BLAKE2 are ARX hash functions (only use three simple operations namely **Modular Add** "+", **Rotation** "$\ggg$" and **XOR**"$\oplus$"), we can use the XOR difference and deduce the difference linearly by considering the only nonlinear operation "+" as similar linear operation "$\oplus$".

The XOR difference in this paper is represented in two forms as follow:

- **Hex form:** such as $\Delta v = 0\text{x}8003$ indicates that bits $v[0,1,15]$ of the word v are active (having non-zero XOR difference).
- **Numeric form:** such as $\Delta v = (15,1,0)$ is equivalent to $\Delta v = 0\text{x}8003$ in hex form. Besides, if $\Delta v = 0\text{x}0$ in hex form, we denoted by $\Delta v = \phi$ in numeric form.

The numeric form is mainly used to describe the differential characteristics since it has better outlook and can save some space. But in practice, we use the hex form to linearly deduce differential characteristics. For example, in the G function of BLAKE-512, we have

$$ta = a + b + (m_i \oplus c_j)$$

where c_j is constant. Suppose we have acquired the differences Δa, Δb and Δm_i, we can dedcue Δta as

$$\Delta ta = \Delta a \oplus \Delta b \oplus \Delta m_i.$$

Once we have determined the difference of the message block ΔM and that of a intermediate state ΔV^r $(r = 0, 0.5, 1, \cdots)$, we can linearly extend the difference backward and forward.

We construct the two differential characteristics for the boomerang attack, where the top differential characteristic is from round 2.5 to 6.5 and bottom differential difference is from 6.5 to 11. We denote the difference of the top by $\Delta^t V^r$ $(r \in [2.5, 6.5])$ and that of the bottom by $\Delta^b V^r$ $(r \in [6.5, 11])$. Similarly, the difference for the message block is denoted as $\Delta^t M$ in the top characteristic and $\Delta^b M$ in the bottom characteristic. The main procedures for our characteristic construction can be summarized as follows:

Import Difference: We first import simple difference to message block $\Delta^b M$ ($\Delta^t M$) and the intermediate state $\Delta^b V^8$ ($\Delta^t V^4$).

Linear Extension: After we have determined $\Delta^b M$ ($\Delta^t M$) and $\Delta^b V^8$ ($\Delta^t V^4$), we extend the difference backward to round 6.5 (2.5) and forward to round 11 (6.5) to acquire the whole bottom (top) differential characteristic.

Construct the Bottom Differential Characteristic: In order to lower the complexity, we only import 1-bit differences to both $\Delta^b M$ and $\Delta^b V^8$. The selection of active bits is based on **Observation 1** in [10].

We found that m_{11} of the 16 message words, namely $m_0, \cdots, m_{15}$, appears at Step 1 in G_2 at round 8 and also appears at Step 5 in G_4 at round 9. So, the first step of our construction is importing 1-bit difference to m_{11} and v_2^8 as

$$\Delta^b m_{11} = \Delta^b v_2^8 = (63). \tag{3}$$

In this way, according to **Observation 1** in [10], we can pass round 8 and 9 with probability 2^{-1}. Then, we set $\Delta^b m_i = \phi$ ($i \in \{0, 1, \cdots, 15\} \setminus \{11\}$) and $\Delta^b v_j^8 = \phi$ ($j \in \{0, 1, \cdots, 15\} \setminus \{2\}$). Now that $\Delta^b M$ and $\Delta^b V^8$ are settled, we can linearly extend the difference backward to $\Delta^b V^{6.5}$ and forward to $\Delta^b V^{11}$. This method can be applied to both BLAKE-512 and BLAKE2b. We present the bottom characteristics of BLAKE-512 and BLAKE2b as Table 4 and 5 in Appendix A respectively.

For BLAKE-256 and BLAKE2s, we can also import difference to $\varDelta^b M$ and $\varDelta^b V^8$ as

$$\varDelta^b m_{11} = \varDelta^b v_2^8 = (31). \tag{4}$$

and linearly deduce the whole bottom differential characteristics. The differential characteristic for BLAKE-256 mounts to round 10.5 and BLAKE2s reaches round 10 since it only has 10 rounds in total according to [6]. Refer to Table 6 and Table 7 in Appendix A for detailed descriptions.

Construct the Top Differential Characteristic: The top differential characteristic starts from $\varDelta^t V^{2.5}$ and ends at $\varDelta^t V^{6.5}$. The strategy of constructing the top differential characteristic is similar to that of its bottom counterpart. We found that m_5 appears at Step 1 in G_1 at round 4 and also appears at Step 5 in G_5 at round 5, so we decide to import the 1-bit difference at m_5 and v_1^4. We assign that

$$\varDelta^t m_5 = \varDelta^t v_1^4 = (y), \text{ where } y \in \{0, \cdots, 63\}. \tag{5}$$

and that $\varDelta^b m_i = \phi$ ($i \in \{0, \cdots, 15\} \setminus \{5\}$) and $\varDelta^b v_j^4 = \phi$ ($j \in \{0, \cdots, 15\} \setminus \{1\}$). Then, we can linearly extend the difference backward and forward. The position of the active bit y in (5) requires careful selection. In order to avoid incompatible problems and enhance the efficiency of the attack, y must meet the following conditions:

1. When linearly extend the difference from $\varDelta^t V^4(y)$ to $\varDelta^t V^{6.5}(y)$, make sure that

   $$\varDelta^b v_i^{6.5} \wedge \varDelta^t v_i^{6.5}(y) = 0\text{x}0, \text{ for all } i \in \{0, \cdots, 15\}. \tag{6}$$

   This restriction avoid the contradictions in the intersection part of the two differential characteristics.
2. **(Only for BLAKE-512)** Make sure that the constants c_{10} and c_7 satisfies:

   $$c_{10}[y] = \neg c_7[y]. \tag{7}$$

   According to the linear extension, we have $\varDelta^t v_1^{3.5} = \phi$. It requires $(m_5 \oplus c_{10})[y] = \neg(m_5 \oplus c_7)[y]$, so (7) must be satisfied.
3. **(Only for BLAKE2b)** When linearly extend to $\varDelta^t V^{3.5}$, $\varDelta^t v_1^{3.5}$ should be set to

   $$\varDelta^t v_1^{3.5} = \varDelta^t m_5 + \varDelta^t m_5$$

   instead of 0x0. Because BLAKE2b omit the use of constant, the difference can not be eliminated at $v_1^{3.5}$.

The available ys satisfying conditions 1 and 2 compose a set $\mathbb{X}_{512}$, and those satisfying conditions 1 and 3 compose a set $\mathbb{X}_{2b}$. According to our analysis, $\mathbb{X}_{512}$ has 13 elements and $\mathbb{X}_{2b}$ has 40 elements. We present $\mathbb{X}_{512}$ and $\mathbb{X}_{2b}$ along with the corresponding top differential characteristics in Table 8 and Table 9 in Appendix A.

Using the same method, we can also acquire the available ys for BLAKE-256 ($\mathbb{X}_{256}$) and BLAKE2s ($\mathbb{X}_{2s}$). We illustrate $\mathbb{X}_{256}$ and $\mathbb{X}_{2s}$ along with their characteristics in Table 10 and Table 11 in Appendix A.

3.2 Finding the Boomerang Quartet Using Message Modification Technique

The goal of our boomerang attack is to find a quartet, denoted by $({}_aV^{2.5}, {}_bV^{2.5}, {}_cV^{2.5}, {}_dV^{2.5})$, and the message blocks $({}_aM, {}_bM, {}_cM, {}_dM)$ that satisfies

$$
\begin{aligned}
{}_aV^{2.5} \oplus {}_cV^{2.5} = {}_bV^{2.5} \oplus {}_dV^{2.5} = \varDelta^t V^{2.5} && (8)\\
{}_aM \oplus {}_cM = {}_bM \oplus {}_dM = \varDelta^t M && (9)\\
{}_aM \oplus {}_bM = {}_cM \oplus {}_dM = \varDelta^b M && (10)
\end{aligned}
$$

and, after 8.5 rounds, the corresponding quartet $({}_aV^{11}, {}_bV^{11}, {}_cV^{11}, {}_dV^{11})$ satisfies

$${}_aV^{11} \oplus {}_bV^{11} = {}_cV^{11} \oplus {}_dV^{11} = \varDelta^b V^{11}.$$

We start by searching for appropriate ${}_aV^{6.5}$ and ${}_aM$. Once ${}_aV^{6.5}$ is determined, ${}_bV^{6.5}$, ${}_cV^{6.5}$ and ${}_dV^{6.5}$ can be settled directly since

$$ {}_aV^{6.5} \oplus {}_cV^{6.5} = {}_bV^{6.5} \oplus {}_dV^{6.5} = \Delta^t V^{6.5} \tag{11}$$

$$ {}_aV^{6.5} \oplus {}_bV^{6.5} = {}_cV^{6.5} \oplus {}_dV^{6.5} = \Delta^b V^{6.5} \tag{12}$$

Once ${}_aM$ is determined, ${}_bM$, ${}_cM$ and ${}_dM$ can also be determined according to (9) and (10). The step of finding the quartet is as follows:

1. Construct an intermediate state, denoted by $V^{6.5}$, and a message block, denoted by M, by setting the values of their 16 words randomly.
2. Compute backward to TV^6 and V^6, and forward to $TV^{6.5}, V^7$. During the process, if one of bit conditions, which are deduced from the top and bottom characteristics, is violated, we can fix it by modifying the words of $V^{6.5}$ or M. This process is called the "message modification".
3. After all conditions between round 6 and 7 are satisfied, we assign that ${}_aV^{6.5} \leftarrow V^{6.5}$ and ${}_aM \leftarrow M$. We also assign corresponding values to ${}_bV^{6.5}$, ${}_cV^{6.5}$, ${}_dV^{6.5}$ according to (11) (12) and to ${}_bM$, ${}_cM$, ${}_dM$ according to (9) (10).
4. Having acquired $({}_aV^{6.5}, {}_bV^{6.5}, {}_cV^{6.5} {}_dV^{6.5})$ and $({}_aM, {}_bM, {}_cM, {}_dM)$, we compute backward to round 2.5. During the process, we check whether the differences of the intermediate states conform to the top differential characteristic. Once a contradiction is detected, go back to 1.
5. Compute forward from round 6.5 to round 11. During the computation, we check whether differences of the intermediate states conform to the bottom differential characteristic. Once a contradiction is detected, go back to 1. Otherwise, output the quartet $({}_aV^{11}, {}_bV^{11}, {}_cV^{11}, {}_dV^{11})$.

Complexity analysis. For all 4 members of BLAKE and BLAKE2, there are 30 conditions in $\Delta^b V^6 \to \Delta^t V^{6.5}$. 29 of them can be fixed using the message modification technique. All two conditions in $\Delta^t V^6 \to \Delta^t V^{5.5}$ can be fixed as well. Similarly, all 40 conditions in $\Delta^b V^{6.5} \to \Delta^b V^7$ and 2 out of 6 conditions in $\Delta^b V^7 \to \Delta^b V^{7.5}$ can be fixed. Then, we analyze the four members separately as follows:

BLAKE-512: In the bottom characteristic, there are 4 unfixed conditions in $\Delta^b V^7 \to \Delta^b V^{7.5}$, 1 in $\Delta^b V^{9.5} \to \Delta^b V^{10}$, 24 in $\Delta^b V^{10} \to \Delta^b V^{10.5}$ and 138 in $\Delta^b V^{10.5} \to \Delta^b V^{11}$, which is 167 in total. In the top characteristics, the situation is as follows: 1 unfixed condition in $\Delta^t V^{4.5} \to \Delta^t V^4$, 2 in $\Delta^t V^4 \to \Delta^t V^{3.5}$, 11 in $\Delta^t V^{3.5} \to \Delta^t V^3$ and 51 in $\Delta^t V^3 \to \Delta^t V^{2.5}$, which is 65 in total. So, the complexity of the boomerang attack on BLAKE-512 is $2^{(167+65)\times 2} = 2^{464}$.

BLAKE2b: In the bottom characteristic, there are 4 unfixed conditions in $\Delta^b V^7 \to \Delta^b V^{7.5}$, 1 in $\Delta^b V^{9.5} \to \Delta^b V^{10}$, 24 in $\Delta^b V^{10} \to \Delta^b V^{10.5}$ and 124 in $\Delta^b V^{10.5} \to \Delta^b V^{11}$, which is 153 in total. The top differential characteristic is slightly different from BLAKE-512 after finishing the procedure $\Delta^t V^{6.5} \to \Delta^t V^4$. There are 3 unfixed conditions in $\Delta^t V^4 \to \Delta^t V^{3.5}$, 13 in $\Delta^t V^{3.5} \to \Delta^t V^3$ and 67 in $\Delta^t V^3 \to \Delta^t V^{2.5}$. So the number of unfixed conditions in the top characteristic enhances to $1+3+13+67 = 84$. The complexity of the boomerang attack on BLAKE2b is $2^{(153+84)\times 2} = 2^{474}$.

BLAKE-256: Similar to BLAKE-512, the bottom characteristic of BLAKE-256, terminated at round 10.5, has $4+1+24 = 29$ unfixed conditions ($\Delta^b V^{6.5} \to \Delta^t V^{10.5}$). For the top characteristic of BLAKE-256, if we choose the active bit position $y = 20 \in \mathbb{X}_{256}$, which is also the case of [12], there should be 71 unfixed conditions and the complexity of this 8-round boomerang attack is $2^{(29+71)\times 2} = 2^{200}$. However, if we choose $y = 28 \in \mathbb{X}_{256}$, 1 condition in $\Delta^t V^3 \to \Delta^t V^{2.5}$ can be eliminated and the complexity of the attack can lower to $2^{(29+70)\times 2} = 2^{198}$.

BLAKE2s: Similar to BLAKE2b, the bottom characteristic for BLAKE2s, terminated at round 10, has $4+1 = 5$ unfixed conditions. The top characteristic has 88 unfixed conditions. So the complexity of this 7.5-round boomerang attack for BLAKE2s is $2^{(5+88)\times 2} = 2^{186}$. Like BLAKE-256, if we choose $y = 28 \in \mathbb{X}_{2s}$, we can eliminate 1 condition in $\Delta^t V^3 \to \Delta^t V^{2.5}$ and lower the complexity by 2^2 to 2^{184}.

Practical Verifications. For each member of BLAKE and BLAKE2, we present a 6.5 round (from round 3.5 to round 10) Type I boomerang quartet based on our characteristics and present it in Appendix B. In order to show the structural difference between BLAKE and BLAKE2, we use the examples with the same message difference, which means: for BLAKE-256 and BLAKE2s, $\Delta^t m_5 = (28)$ ($y = 28 \in \mathbb{X}_{256} \bigcap \mathbb{X}_{2s}$) and $\Delta^b m_{11} = (31)$; for BLAKE-512 and BLAKE2b, $\Delta^t m_5 = (9)$ ($y = 9 \in \mathbb{X}_{512} \bigcap \mathbb{X}_{2b}$) and $\Delta^b m_{11} = (63)$.

4 Conclusion

In this paper, we compare the security margin of BLAKE and BLAKE2 under the boomerang attack model. We deduce valid differential characteristics and present boomerang attacks on keyed permutations of BLAKE-512, BLAKE2b, BLAKE-256 and BLAKE2s. According to our analysis, the boomerang method can mount to similar rounds for BLAKE and BLAKE2. For the same number of rounds, the complexities for attacking BLAKE2 are slightly higher than those for BLAKE, which indicates that some tweaks introduced by BLAKE2, aiming at enhancing efficiency and flexibility, have accidentally reinforced the resistance against the boomerang attack. However, since BLAKE has more rounds than BLAKE2, the security margin of BLAKE is still higher than that of BLAKE2. This result is in accordance with the assumptions of the designers.

Acknowledgement. This work has been supported by the National Natural Science Foundation of China (Grant No. 61133013) and by 973 Program (Grant No. 2013CB834205).

References

1. Wang, X., Yu, H.: How to break md5 and other hash functions. In: Advances in Cryptology–EUROCRYPT 2005. Springer (2005) 19–35
2. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full sha-1. In: Advances in Cryptology–CRYPTO 2005, Springer (2005) 17–36
3. Bertoni, G., Daemen, J., Peeters, M., Assche, G.: The keccak reference. Submission to NIST (Round 3) **13** (2011)
4. Aumasson, J.P., Henzen, L., Meier, W., Phan, R.C.W.: Sha-3 proposal blake. Submission to NIST (2008)
5. Chang, S.j., Perlner, R., Burr, W.E., Turan, M.S., Kelsey, J.M., Paul, S., Bassham, L.E.: Third-round report of the SHA-3 cryptographic hash algorithm competition. Citeseer (2012)
6. Aumasson, J.P., Neves, S., Wilcox-OHearn, Z., Winnerlein, C.: Blake2: simpler, smaller, fast as md5. In: Applied Cryptography and Network Security, Springer (2013) 119–135
7. Aumasson, J.P., Guo, J., Knellwolf, S., Matusiewicz, K., Meier, W.: Differential and invertibility properties of blake. In: Fast Software Encryption, Springer (2010) 318–332
8. Dunkelman, O., Khovratovich, D.: Iterative differentials, symmetries, and message modification in blake-256. In: ECRYPT2 Hash Workshop. Volume 2011. (2011)
9. Ji, L., Liangyu, X.: Attacks on round-reduced blake. Technical report, Citeseer (2009)
10. Biryukov, A., Nikolić, I., Roy, A.: Boomerang attacks on blake-32. In: Fast Software Encryption, Springer (2011) 218–237
11. Leurent, G.: Arxtools: A toolkit for arx analysis. In: The Third SHA-3 Candidate Conference. (2012)
12. Bai, D., Yu, H., Wang, G., Wang, X.: Improved boomerang attacks on round-reduced sm3 and blake-256. (2013) `http://eprint.iacr.org/`.
13. Guo, J., Karpman, P., Nikolić, I., Wang, L., Wu, S.: Analysis of blake2. In: Topics in Cryptology–CT-RSA 2014. Springer (2014) 402–423
14. Wagner, D.: The boomerang attack. In: Fast Software Encryption, Springer (1999) 156–170
15. Kelsey, J., Kohno, T., Schneier, B.: Amplified boomerang attacks against reduced-round mars and serpent. In: Fast Software Encryption, Springer (2001) 75–93
16. Biham, E., Dunkelman, O., Keller, N.: The rectangle attackrectangling the serpent. In: Advances in CryptologyEUROCRYPT 2001. Springer (2001) 340–357
17. Biham, E., Dunkelman, O., Keller, N.: Related-key boomerang and rectangle attacks. In: Advances in Cryptology–EUROCRYPT 2005. Springer (2005) 507–525
18. Lamberger, M., Mendel, F.: Higher-order differential attack on reduced sha-256. IACR Cryptology ePrint Archive **2011** (2011) 37
19. Biryukov, A., Lamberger, M., Mendel, F., Nikolić, I.: Second-order differential collisions for reduced sha-256. In: Advances in Cryptology–ASIACRYPT 2011. Springer (2011) 270–287
20. Mendel, F., Nad, T.: Boomerang distinguisher for the simd-512 compression function. In: Progress in Cryptology–INDOCRYPT 2011. Springer (2011) 255–269
21. Sasaki, Y., Wang, L., Takasaki, Y., Sakiyama, K., Ohta, K.: Boomerang distinguishers for full has-160 compression function. In: Advances in Information and Computer Security. Springer (2012) 156–169

22. Sasaki, Y., Wang, L.: Distinguishers beyond three rounds of the ripemd-128/-160 compression functions. In: Applied Cryptography and Network Security, Springer (2012) 275–292
23. Leurent, G., Roy, A.: Boomerang attacks on hash function using auxiliary differentials. In: Topics in Cryptology–CT-RSA 2012. Springer (2012) 215–230
24. Yu, H., Chen, J., Wang, X.: The boomerang attacks on the round-reduced skein-512. In: Selected Areas in Cryptography, Springer (2013) 287–303
25. Kircanski, A., Shen, Y., Wang, G., Youssef, A.M.: Boomerang and slide-rotational analysis of the sm3 hash function. In: Selected Areas in Cryptography, Springer (2013) 304–320
26. Bai, D., Yu, H., Wang, G., Wang, X.: Improved boomerang attacks on sm3. In: Information Security and Privacy, Springer (2013) 251–266
27. Wagner, D.: A generalized birthday problem. In: Advances in cryptologyCRYPTO 2002. Springer (2002) 288–304

Appendix

A The Bottom & Top Differential Characteristics for BLAKE and BLAKE2

Table 4. The bottom characteristic for BLAKE-512. $\Delta^b m_{11} = (63)$.

Variable	Difference (Numeric Form)	Cond	Variable	Difference (Numeric Form)	Cond
$\Delta^b V^{6.5}$	$\Delta^b v_0^{6.5} = (63, 42, 35, 10, 3)$ $\Delta^b v_1^{6.5} = (63, 31)$ $\Delta^b v_2^{6.5} = (63, 47, 24, 15)$ $\Delta^b v_3^{6.5} = (60, 56, 40, 31, 24, 10, 8)$ $\Delta^b v_4^{6.5} = (60, 56, 47, 40, 35, 24, 15, 8)$ $\Delta^b v_5^{6.5} = (63, 35, 24, 3)$ $\Delta^b v_7^{6.5} = (63, 47, 24, 15)$ $\Delta^b v_8^{6.5} = (63, 47, 31, 15)$ $\Delta^b v_{10}^{6.5} = (24)$ $\Delta^b v_{11}^{6.5} = (63, 31)$ $\Delta^b v_{13}^{6.5} = (63)$ $\Delta^b v_{14}^{6.5} = (35, 31, 10)$ $\Delta^b v_{15}^{6.5} = (56, 42, 31, 24, 10)$	-	$\Delta^b V^{10.5}$:	$\Delta^b v_0^{10.5} = (63, 6)$ $\Delta^b v_1^{10.5} = (43, 36, 11)$ $\Delta^b v_2^{10.5} = (22)$ $\Delta^b v_3^{10.5} = (54)$ $\Delta^b v_4^{10.5} = (59, 43, 36, 20, 4)$ $\Delta^b v_5^{10.5} = (57, 48, 41, 32, 16, 9, 0)$ $\Delta^b v_6^{10.5} = (59, 36, 11)$ $\Delta^b v_7^{10.5} = (52, 43, 27, 4)$ $\Delta^b v_8^{10.5} = (54, 47, 31, 15)$ $\Delta^b v_9^{10.5} = (59, 52, 27, 20, 4)$ $\Delta^b v_{10}^{10.5} = (47, 6)$ $\Delta^b v_{11}^{10.5} = (63, 38, 15)$ $\Delta^b v_{12}^{10.5} = (54, 47, 15)$ $\Delta^b v_{13}^{10.5} = (59, 52, 27, 20)$ $\Delta^b v_{14}^{10.5} = (6)$ $\Delta^b v_{15}^{10.5} = (63, 38)$	24
$\Delta^b V^7$	$\Delta^b v_0^7 = (63, 24)$ $\Delta^b v_1^7 = (63, 31)$ $\Delta^b v_2^7 = (63)$ $\Delta^b v_4^7 = (63, 24)$ $\Delta^b v_5^7 = (63, 31)$ $\Delta^b v_8^7 = (63)$ $\Delta^b v_9^7 = (63, 47, 31, 15)$ $\Delta^b v_{10}^7 = (63)$ $\Delta^b v_{13}^7 = (47, 15)$ $\Delta^b v_{14}^7 = (63, 31)$	40 (40 fixed)	$\Delta^b V^{11}$	$\Delta^b v_0^{11} = (63, 57, 48, 41, 22, 16, 13, 9, 6)$ $\Delta^b v_1^{11} = (63, 61, 59, 43, 38, 34, 22, 13, 11, 2)$ $\Delta^b v_2^{11} = (54, 52, 50, 27, 18, 11, 6, 4)$ $\Delta^b v_3^{11} = (61, 59, 54, 50, 36, 20, 18, 13, 4)$ $\Delta^b v_4^{11} = (59, 57, 55, 39, 34, 23, 9, 7, 2)$ $\Delta^b v_5^{11} = (59, 50, 27, 14, 2)$ $\Delta^b v_6^{11} = (55, 39, 34, 32, 23, 20, 11, 7, 2, 0)$ $\Delta^b v_7^{11} = (59, 55, 39, 36, 32, 25, 23, 20, 16, 11, 9, 7, 4)$ $\Delta^b v_8^{11} = (54, 47, 36, 34, 31, 27, 20, 15, 11, 2)$ $\Delta^b v_9^{11} = (61, 45, 43, 34, 20, 6, 4, 2)$ $\Delta^b v_{10}^{11} = (61, 38, 32, 25, 22, 6, 0)$ $\Delta^b v_{11}^{11} = (61, 50, 45, 43, 38, 31, 18)$ $\Delta^b v_{12}^{11} = (63, 61, 50, 47, 45, 43, 31, 27, 22, 18, 11)$ $\Delta^b v_{13}^{11} = (54, 52, 34, 20, 2)$ $\Delta^b v_{14}^{11} = (61, 59, 45, 43, 38, 36, 34, 22, 11, 6, 4, 2)$ $\Delta^b v_{15}^{11} = (61, 48, 47, 41, 22, 16, 9, 6)$	138
$\Delta^b V^{7.5}$	$\Delta^b v_2^{7.5} = (63)$ $\Delta^b v_8^{7.5} = (63)$ $\Delta^b v_{13}^{7.5} = (63, 31)$	6 (2 fixed)			
$\Delta^b V^8$	$\Delta^b v_2^8 = (63)$	0			
$\Delta^b V^{8.5} \cdots$ $\cdots \Delta^b V^{9.5}$	ϕ	0			
$\Delta^b V^{10}$:	$\Delta^b v_0^{10} = (63)$ $\Delta^b v_5^{10} = (36)$ $\Delta^b v_{10}^{10} = (47)$ $\Delta^b v_{15}^{10} = (47)$	1			

Table 5. The bottom characteristic for BLAKE2b. $\Delta^b m_{11} = (63)$.

Variable	Difference (Numeric Form)	Cond
$\Delta^b V^{6.5}$	$\Delta^b v_0^{6.5} = (63, 62, 54, 30, 22)$ $\Delta^b v_1^{6.5} = (63, 31)$ $\Delta^b v_2^{6.5} = (63, 47, 23, 15)$ $\Delta^b v_3^{6.5} = (62, 55, 46, 39, 31, 23, 7)$ $\Delta^b v_4^{6.5} = (55, 47, 46, 39, 23, 22, 15, 7)$ $\Delta^b v_5^{6.5} = (63, 54, 23, 22)$ $\Delta^b v_7^{6.5} = (63, 47, 23, 15)$ $\Delta^b v_8^{6.5} = (63, 47, 31, 15)$ $\Delta^b v_{10}^{6.5} = (23)$ $\Delta^b v_{11}^{6.5} = (63, 31)$ $\Delta^b v_{13}^{6.5} = (63)$ $\Delta^b v_{14}^{6.5} = (62, 31, 22)$ $\Delta^b v_{15}^{6.5} = (62, 55, 31, 30, 23)$	-
$\Delta^b V^7$	$\Delta^b v_0^7 = (63, 23)$ $\Delta^b v_1^7 = (63, 31)$ $\Delta^b v_2^7 = (63)$ $\Delta^b v_4^7 = (63, 23)$ $\Delta^b v_5^7 = (63, 31)$ $\Delta^b v_8^7 = (63)$ $\Delta^b v_9^7 = (63, 47, 31, 15)$ $\Delta^b v_{10}^7 = (63)$ $\Delta^b v_{13}^7 = (47, 15)$ $\Delta^b v_{14}^7 = (63, 31)$	40 (40 fixed)
$\Delta^b V^{7.5}$	$\Delta^b v_2^{7.5} = (63)$ $\Delta^b v_8^{7.5} = (63)$ $\Delta^b v_{13}^{7.5} = (63, 31)$	6 (2 fixed)
$\Delta^b V^8$	$\Delta^b v_2^8 = (63)$	0
$\Delta^b V^{8.5} \cdots$ $\cdots \Delta^b V^{9.5}$	ϕ	0
$\Delta^b V^{10}$:	$\Delta^b v_0^{10} = (63)$ $\Delta^b v_5^{10} = (48)$ $\Delta^b v_{10}^{10} = (47)$ $\Delta^b v_{15}^{10} = (47)$	1

Variable	Difference (Numeric Form)	Cond
$\Delta^b V^{10.5}$:	$\Delta^b v_0^{10.5} = (63, 7)$ $\Delta^b v_1^{10.5} = (56, 48, 24)$ $\Delta^b v_2^{10.5} = (23)$ $\Delta^b v_3^{10.5} = (55)$ $\Delta^b v_4^{10.5} = (56, 48, 32, 16, 8)$ $\Delta^b v_5^{10.5} = (57, 41, 33, 25, 17, 9, 1)$ $\Delta^b v_6^{10.5} = (48, 24, 8)$ $\Delta^b v_7^{10.5} = (56, 40, 16, 0)$ $\Delta^b v_8^{10.5} = (55, 47, 31, 15)$ $\Delta^b v_9^{10.5} = (40, 32, 16, 8, 0)$ $\Delta^b v_{10}^{10.5} = (47, 7)$ $\Delta^b v_{11}^{10.5} = (63, 39, 15)$ $\Delta^b v_{12}^{10.5} = (55, 47, 15)$ $\Delta^b v_{13}^{10.5} = (40, 32, 8, 0)$ $\Delta^b v_{14}^{10.5} = (7)$ $\Delta^b v_{15}^{10.5} = (63, 39)$	24
$\Delta^b V^{11}$	$\Delta^b v_0^{11} = (63, 41, 33, 23, 17, 15, 9, 7, 1)$ $\Delta^b v_1^{11} = (56, 48, 39, 24, 23, 16, 15, 8)$ $\Delta^b v_2^{11} = (55, 40, 32, 24, 16, 7)$ $\Delta^b v_3^{11} = (63, 55, 48, 16, 15, 8, 0)$ $\Delta^b v_4^{11} = (49, 48, 16, 8, 1)$ $\Delta^b v_5^{11} = (50, 40, 16, 8, 0)$ $\Delta^b v_6^{11} = (57, 49, 48, 33, 32, 25, 24, 17, 16, 1)$ $\Delta^b v_7^{11} = (57, 48, 41, 32, 24, 17, 16, 8, 1)$ $\Delta^b v_8^{11} = (55, 47, 40, 32, 31, 24, 16, 15)$ $\Delta^b v_9^{11} = (63, 56, 48, 47, 32, 7)$ $\Delta^b v_{10}^{11} = (63, 57, 49, 39, 25, 23, 7)$ $\Delta^b v_{11}^{11} = (63, 56, 47, 39, 32, 31, 0)$ $\Delta^b v_{12}^{11} = (56, 40, 32, 31, 24, 23, 0)$ $\Delta^b v_{13}^{11} = (55, 48, 32, 16, 0)$ $\Delta^b v_{14}^{11} = (63, 56, 47, 39, 24, 23, 8, 7)$ $\Delta^b v_{15}^{11} = (63, 47, 41, 33, 23, 9, 7, 1)$	124

Table 6. The bottom characteristic for BLAKE-256. $\Delta^b m_{11} = (31)$.

Variable	Difference (Numeric Form)	Cond	Variable	Difference (Numeric Form)	Cond
$\Delta^b V^{6.5}$	$\Delta^b v_0^{6.5} = (31, 22, 18, 6, 2)$ $\Delta^b v_1^{6.5} = (31, 15)$ $\Delta^b v_2^{6.5} = (31, 23, 11, 7)$ $\Delta^b v_3^{6.5} = (30, 27, 19, 15, 11, 6, 3)$ $\Delta^b v_4^{6.5} = (30, 27, 23, 19, 18, 11, 7, 3)$ $\Delta^b v_5^{6.5} = (31, 18, 11, 2)$ $\Delta^b v_7^{6.5} = (31, 23, 11, 7)$ $\Delta^b v_8^{6.5} = (31, 23, 15, 7)$ $\Delta^b v_{10}^{6.5} = (11)$ $\Delta^b v_{11}^{6.5} = (31, 15)$ $\Delta^b v_{13}^{6.5} = (31)$ $\Delta^b v_{14}^{6.5} = (18, 15, 6)$ $\Delta^b v_{15}^{6.5} = (27, 22, 15, 11, 6)$	-	$\Delta^b V^8$	$\Delta^b v_2^8 = (31)$	0
			$\Delta^b V^{8.5} \cdots \Delta^b V^{9.5}$	ϕ	0
			$\Delta^b V^{10}$:	$\Delta^b v_0^{10} = (31)$ $\Delta^b v_5^{10} = (16)$ $\Delta^b v_{10}^{10} = (23)$ $\Delta^b v_{15}^{10} = (23)$	1
$\Delta^b V^7$	$\Delta^b v_0^7 = (31, 11)$ $\Delta^b v_1^7 = (31, 15)$ $\Delta^b v_2^7 = (31)$ $\Delta^b v_4^7 = (31, 11)$ $\Delta^b v_5^7 = (31, 15)$ $\Delta^b v_8^7 = (31)$ $\Delta^b v_9^7 = (31, 23, 15, 7)$ $\Delta^b v_{10}^7 = (31)$ $\Delta^b v_{13}^7 = (23, 7)$ $\Delta^b v_{14}^7 = (31, 15)$	40 (40 fixed)	$\Delta^b V^{10.5}$:	$\Delta^b v_0^{10.5} = (31, 3)$ $\Delta^b v_1^{10.5} = (20, 16, 4)$ $\Delta^b v_2^{10.5} = (11)$ $\Delta^b v_3^{10.5} = (27)$ $\Delta^b v_4^{10.5} = (28, 20, 16, 8, 0)$ $\Delta^b v_5^{10.5} = (29, 25, 21, 17, 13, 5, 1)$ $\Delta^b v_6^{10.5} = (28, 16, 4)$ $\Delta^b v_7^{10.5} = (24, 20, 12, 0)$ $\Delta^b v_8^{10.5} = (27, 23, 15, 7)$ $\Delta^b v_9^{10.5} = (28, 24, 12, 8, 0)$ $\Delta^b v_{10}^{10.5} = (23, 3)$ $\Delta^b v_{11}^{10.5} = (31, 19, 7)$ $\Delta^b v_{12}^{10.5} = (27, 23, 7)$ $\Delta^b v_{13}^{10.5} = (28, 24, 12, 8)$ $\Delta^b v_{14}^{10.5} = (3)$ $\Delta^b v_{15}^{10.5} = (31, 19)$	24
$\Delta^b V^{7.5}$	$\Delta^b v_2^{7.5} = (31)$ $\Delta^b v_8^{7.5} = (31)$ $\Delta^b v_{13}^{7.5} = (31, 15)$	6 (2 fixed)			

Table 7. The bottom characteristic for BLAKE2s. $\Delta^b m_{11} = (31)$.

Variable	Difference (Numeric Form)	Cond	Variable	Difference (Numeric Form)	Cond
				$\Delta^b v_0^7 = (31, 11)$ $\Delta^b v_1^7 = (31, 15)$	

7

$\Delta^b V^7$

40 (40 fixed)

$\Delta^b V^{6.5}$

-

Table 8. The top characteristic for BLAKE-512. Message difference is $\varDelta^t m_5 = (y)$ where $y \in \mathbb{X}_{512}$

	$\mathbb{X}_{512} = \{5, 9, 18, 20, 22, 29, 34, 38, 41, 45, 48, 52, 54\}$	
Variable	Difference (Numeric Form)	Cond
$\varDelta^t V^{2.5}$:	$\varDelta^t v_0^{2.5} = (y+32)$ $\varDelta^t v_1^{2.5} = (y+48, y+25, y+16)$ $\varDelta^t v_2^{2.5} = (y+41, y+25, y+11, y+9, y+61, y+57)$ $\varDelta^t v_3^{2.5} = (y+43, y+36, y+25, y+11, y+4)$ $\varDelta^t v_4^{2.5} = (y+36, y+4)$ $\varDelta^t v_5^{2.5} = (y)$ $\varDelta^t v_6^{2.5} = (y+48, y+25, y+16, y)$ $\varDelta^t v_7^{2.5} = (y+48, y+41, y+36, y+32, y+25, y+16, y+9, y, y+61, y+57)$ $\varDelta^t v_8^{2.5} = (y+48, y+32, y+16, y)$ $\varDelta^t v_9^{2.5} = (y+25)$ $\varDelta^t v_{10}^{2.5} = (y+32, y+16)$ $\varDelta^t v_{11}^{2.5} = (y+48, y+32, y+16)$ $\varDelta^t v_{12}^{2.5} = (y+32)$ $\varDelta^t v_{13}^{2.5} = (y+48, y+36, y+32, y+16, y+11, y)$ $\varDelta^t v_{14}^{2.5} = (y+43, y+25, y+11, y+57)$ $\varDelta^t v_{15}^{2.5} = (y+48)$	51
$\varDelta^t V^3$	$\varDelta^t v_0^3 = (y+32, y)$ $\varDelta^t v_3^3 = (y+25)$ $\varDelta^t v_4^3 = (y+32, y)$ $\varDelta^t v_7^3 = (y+25, y)$ $\varDelta^t v_8^3 = (y+48, y+32, y+16, y)$ $\varDelta^t v_{11}^3 = (y)$ $\varDelta^t v_{12}^3 = (y+48, y+16)$ $\varDelta^t v_{15}^3 = (y)$	11
$\varDelta^t V^{3.5}$	$\varDelta^t v_{11}^{3.5} = (y)$ $\varDelta^t v_{12}^{3.5} = (y+32, y)$	2
$\varDelta^t V^4$	$\varDelta^t v_1^4 = (y)$	1
$\varDelta^t V^{4.5} \cdots \varDelta^t V^{5.5}$	ϕ	2 (2 fixed)
$\varDelta^t V^6$	$\varDelta^t v_1^6 = (y)$ $\varDelta^t v_6^6 = (y+37)$ $\varDelta^t v_{11}^6 = (y+48)$ $\varDelta^t v_{12}^6 = (y+48)$	30 (29 fixed)
$\varDelta^t V^{6.5}$	$\varDelta^t v_0^{6.5} = (y, y+55)$ $\varDelta^t v_1^{6.5} = (y+7, y)$ $\varDelta^t v_2^{6.5} = (y+44, y+37, y+12)$ $\varDelta^t v_3^{6.5} = (y+23)$ $\varDelta^t v_4^{6.5} = (y+53, y+44, y+37, y+28, y+5)$ $\varDelta^t v_5^{6.5} = (y+44, y+37, y+21, y+5, y+60)$ $\varDelta^t v_6^{6.5} = (y+49, y+42, y+33, y+17, y+10, y+1, y+58)$ $\varDelta^t v_7^{6.5} = (y+37, y+12, y+60)$ $\varDelta^t v_8^{6.5} = (y+48, y+39, y+16, y)$ $\varDelta^t v_9^{6.5} = (y+48, y+32, y+16, y+55)$ $\varDelta^t v_{10}^{6.5} = (y+53, y+28, y+21, y+5, y+60)$ $\varDelta^t v_{11}^{6.5} = (y+48, y+7)$ $\varDelta^t v_{12}^{6.5} = (y+48, y+39, y)$ $\varDelta^t v_{13}^{6.5} = (y+48, y+16, y+55)$ $\varDelta^t v_{14}^{6.5} = (y+53, y+28, y+21, y+60)$ $\varDelta^t v_{15}^{6.5} = (y+7)$	-

Table 9. The top characteristic for BLAKE2b. Message difference is $\varDelta^t m_5 = (y)$ where $y \in \mathbb{X}_{2b}$

$\mathbb{X}_{2b} = \{0, 1, 2, 3, 4, 8, 9, 10, 11, 12, 16, 17, 18, 19, 20, 24, 25, 26, 27, 28,$ $32, 33, 34, 35, 36, 40, 41, 42, 43, 44, 48, 49, 50, 51, 52, 56, 57, 58, 59, 60\}$		
Variable	Difference (Numeric Form)	Cond
$\varDelta^t V^{2.5}$:	$\varDelta^t v_0^{2.5} = (y + 32)$ $\varDelta^t v_1^{2.5} = (y + 48, y + 24, y + 16, y + 1)$ $\varDelta^t v_2^{2.5} = (y + 47, y + 40, y + 33, y + 24, y + 8, y + 1, y + 63, y + 56)$ $\varDelta^t v_3^{2.5} = (y + 31, y + 25, y + 24, y + 23, y + 63, y + 55)$ $\varDelta^t v_4^{2.5} = (y + 25, y + 23, y + 1, y + 55)$ $\varDelta^t v_5^{2.5} = (y)$ $\varDelta^t v_6^{2.5} = (y + 48, y + 24, y + 16, y)$ $\varDelta^t v_7^{2.5} = (y + 48, y + 47, y + 40, y + 33, y + 32, y + 24, y + 23, y + 16, y + 8, y + 1, y, y + 56)$ $\varDelta^t v_8^{2.5} = (y + 49, y + 48, y + 33, y + 32, y + 17, y + 16, y + 1, y)$ $\varDelta^t v_9^{2.5} = (y + 24, y + 1)$ $\varDelta^t v_{10}^{2.5} = (y + 32, y + 16)$ $\varDelta^t v_{11}^{2.5} = (y + 48, y + 32, y + 16, y + 1)$ $\varDelta^t v_{12}^{2.5} = (y + 33, y + 32, y + 1)$ $\varDelta^t v_{13}^{2.5} = (y + 49, y + 48, y + 32, y + 23, y + 17, y + 16, y, y + 63)$ $\varDelta^t v_{14}^{2.5} = (y + 31, y + 24, y + 1, y + 63, y + 56)$ $\varDelta^t v_{15}^{2.5} = (y + 48)$	67
$\varDelta^t V^{3}$:	$\varDelta^t v_0^{3} = (y + 32, y)$ $\varDelta^t v_1^{3} = (y + 1)$ $\varDelta^t v_3^{3} = (y + 24)$ $\varDelta^t v_4^{3} = (y + 32, y)$ $\varDelta^t v_7^{3} = (y + 24, y)$ $\varDelta^t v_8^{3} = (y + 48, y + 32, y + 16, y)$ $\varDelta^t v_9^{3} = (y + 1)$ $\varDelta^t v_{11}^{3} = (y)$ $\varDelta^t v_{12}^{3} = (y + 48, y + 16)$ $\varDelta^t v_{13}^{3} = (y + 33, y + 1)$ $\varDelta^t v_{15}^{3} = (y)$	13
$\varDelta^t V^{3.5}$:	$\varDelta^t v_1^{3.5} = (y + 1)$ $\varDelta^t v_{11}^{3.5} = (y)$ $\varDelta^t v_{12}^{3.5} = (y + 32, y)$	3
$\varDelta^t V^{4}$:	$\varDelta^t v_1^{4} = (y)$	1
$\varDelta^t V^{4.5} \cdots \varDelta^t V^{5.5}$:	ϕ	2 (2 fixed)
$\varDelta^t V^{6}$:	$\varDelta^t v_1^{6} = (y)$ $\varDelta^t v_6^{6} = (y + 49)$ $\varDelta^t v_{11}^{6} = (y + 48)$ $\varDelta^t v_{12}^{6} = (y + 48)$	30 (29 fixed)
$\varDelta^t V^{6.5}$:	$\varDelta^t v_0^{6.5} = (y, y + 56)$ $\varDelta^t v_1^{6.5} = (y + 8, y)$ $\varDelta^t v_2^{6.5} = (y + 49, y + 25, y + 57)$ $\varDelta^t v_3^{6.5} = (y + 24)$ $\varDelta^t v_4^{6.5} = (y + 49, y + 41, y + 17, y + 1, y + 57)$ $\varDelta^t v_5^{6.5} = (y + 49, y + 33, y + 17, y + 9, y + 57)$ $\varDelta^t v_6^{6.5} = (y + 42, y + 34, y + 26, y + 18, y + 10, y + 2, y + 58)$ $\varDelta^t v_7^{6.5} = (y + 49, y + 25, y + 9)$ $\varDelta^t v_8^{6.5} = (y + 48, y + 40, y + 16, y)$ $\varDelta^t v_9^{6.5} = (y + 48, y + 32, y + 16, y + 56)$ $\varDelta^t v_{10}^{6.5} = (y + 41, y + 33, y + 17, y + 9, y + 1)$ $\varDelta^t v_{11}^{6.5} = (y + 48, y + 8)$ $\varDelta^t v_{12}^{6.5} = (y + 48, y + 40, y)$ $\varDelta^t v_{13}^{6.5} = (y + 48, y + 16, y + 56)$ $\varDelta^t v_{14}^{6.5} = (y + 41, y + 33, y + 9, y + 1)$ $\varDelta^t v_{15}^{6.5} = (y + 8)$	-

Table 10. The top characteristic for BLAKE-256. Message difference is $\varDelta^t m_5 = (y)$ where $y \in \mathbb{X}_{256}$.

$\mathbb{X}_{256} = \{20, 28\}$		
Variable	Difference (Numeric Form)	Cond
$\varDelta^t V^{2.5}$:	$\varDelta^t v_0^{2.5} = (y+16)$ $\varDelta^t v_1^{2.5} = (y+8, y+24, y+12)$ $\varDelta^t v_2^{2.5} = (y+7, y+4, y+31, y+28, y+20, y+12)$ $\varDelta^t v_3^{2.5} = (y+7, \boldsymbol{y+3}, y+23, y+19, y+12)$ $\varDelta^t v_4^{2.5} = (\boldsymbol{y+3}, y+19)$ $\varDelta^t v_5^{2.5} = (y)$ $\varDelta^t v_6^{2.5} = (y+8, y, y+24, y+12)$ $\varDelta^t v_7^{2.5} = (y+8, y+4, y, y+31, y+28, y+24, y+20, y+19, y+16, y+12)$ $\varDelta^t v_8^{2.5} = (y+8, y, y+24, y+16)$ $\varDelta^t v_9^{2.5} = (y+12)$ $\varDelta^t v_{10}^{2.5} = (y+8, y+16)$ $\varDelta^t v_{11}^{2.5} = (y+8, y+24, y+16)$ $\varDelta^t v_{12}^{2.5} = (y+16)$ $\varDelta^t v_{13}^{2.5} = (y+8, y+7, y, y+24, y+19, y+16)$ $\varDelta^t v_{14}^{2.5} = (y+7, y+28, y+23, y+12)$ $\varDelta^t v_{15}^{2.5} = (y+24)$	54/53*
$\varDelta^t V^3$	$\varDelta^t v_0^3 = (y, y+16)$ $\varDelta^t v_3^3 = (y+12)$ $\varDelta^t v_4^3 = (y, y+16)$ $\varDelta^t v_7^3 = (y, y+12)$ $\varDelta^t v_8^3 = (y+8, y, y+24, y+16)$ $\varDelta^t v_{11}^3 = (y)$ $\varDelta^t v_{12}^3 = (y+8, y+24)$ $\varDelta^t v_{15}^3 = (y)$	14
$\varDelta^t V^{3.5}$	$\varDelta^t v_{11}^{3.5} = (y)$ $\varDelta^t v_{12}^{3.5} = (y, y+16)$	2
$\varDelta^t V^4$	$\varDelta^t v_1^4 = (y)$	1
$\varDelta^t V^{4.5} \cdots \varDelta^t V^{5.5}$	ϕ	2 (2 fixed)
$\varDelta^t V^6$	$\varDelta^t v_1^6 = (y)$ $\varDelta^t v_6^6 = (y+17)$ $\varDelta^t v_{11}^6 = (y+24)$ $\varDelta^t v_{12}^6 = (y+24)$	30 (29 fixed)
$\varDelta^t V^{6.5}$	$\varDelta^t v_0^{6.5} = (y, y+28)$ $\varDelta^t v_1^{6.5} = (y+4, y)$ $\varDelta^t v_2^{6.5} = (y+5, y+21, y+17)$ $\varDelta^t v_3^{6.5} = (y+12)$ $\varDelta^t v_4^{6.5} = (y+1, y+25, y+21, y+17, y+13)$ $\varDelta^t v_5^{6.5} = (y+9, y+1, y+29, y+21, y+17)$ $\varDelta^t v_6^{6.5} = (y+6, y+2, y+30, y+26, y+22, y+18, y+14)$ $\varDelta^t v_7^{6.5} = (y+5, y+29, y+17)$ $\varDelta^t v_8^{6.5} = (y+8, y, y+24, y+20)$ $\varDelta^t v_9^{6.5} = (y+8, y+28, y+24, y+16)$ $\varDelta^t v_{10}^{6.5} = (y+9, y+1, y+29, y+25, y+13)$ $\varDelta^t v_{11}^{6.5} = (y+4, y+24)$ $\varDelta^t v_{12}^{6.5} = (y, y+24, y+20)$ $\varDelta^t v_{13}^{6.5} = (y+8, y+28, y+24)$ $\varDelta^t v_{14}^{6.5} = (y+9, y+29, y+25, y+13)$ $\varDelta^t v_{15}^{6.5} = (y+4)$	-

*: If $y = 28$, the condition $v_3^{2.5}[y+3] = \neg v_4^{2.5}[y+3]$ in $\varDelta^t V^3 \to \varDelta^t V^{2.5}$ can be eliminated.

Table 11. The top characteristic for BLAKE2s. Message difference is $\varDelta^t m_5 = (y)$ where $y \in \mathbb{X}_{2s}$.

$\mathbb{X}_{2s} = \{0, 4, 8, 12, 16, 20, 24, 28\}$		
Variable	Difference (Numeric Form)	Cond
$\varDelta^t V^{2.5}$:	$\varDelta^t v_0^{2.5} = (y + 16)$ $\varDelta^t v_1^{2.5} = (y + 8, y + 1, y + 24, y + 12)$ $\varDelta^t v_2^{2.5} = (y + 7, y + 4, y + 1, y + 31, y + 28, y + 20, y + 17, y + 12)$ $\varDelta^t v_3^{2.5} = (y + 7, \mathbf{y + 3}, y + 23, y + 19, y + 13, y + 12)$ $\varDelta^t v_4^{2.5} = (\mathbf{y + 3}, y + 1, y + 19, y + 13)$ $\varDelta^t v_5^{2.5} = (y)$ $\varDelta^t v_6^{2.5} = (y + 8, y, y + 24, y + 12)$ $\varDelta^t v_7^{2.5} = (y + 8, y + 4, y + 1, y, y + 31, y + 28, y + 24, y + 20, y + 19, y + 17, y + 16, y + 12)$ $\varDelta^t v_8^{2.5} = (y + 9, y + 8, y + 1, y, y + 25, y + 24, y + 17, y + 16)$ $\varDelta^t v_9^{2.5} = (y + 1, y + 12)$ $\varDelta^t v_{10}^{2.5} = (y + 8, y + 16)$ $\varDelta^t v_{11}^{2.5} = (y + 8, y + 1, y + 24, y + 16)$ $\varDelta^t v_{12}^{2.5} = (y + 1, y + 17, y + 16)$ $\varDelta^t v_{13}^{2.5} = (y + 9, y + 8, y + 7, y, y + 25, y + 24, y + 19, y + 16)$ $\varDelta^t v_{14}^{2.5} = (y + 7, y + 1, y + 28, y + 23, y + 12)$ $\varDelta^t v_{15}^{2.5} = (y + 24)$	68/67*
$\varDelta^t V^{3}$:	$\varDelta^t v_0^{3} = (y, y + 16)$ $\varDelta^t v_1^{3} = (y + 1)$ $\varDelta^t v_3^{3} = (y + 12)$ $\varDelta^t v_4^{3} = (y, y + 16)$ $\varDelta^t v_7^{3} = (y, y + 12)$ $\varDelta^t v_8^{3} = (y + 8, y, y + 24, y + 16)$ $\varDelta^t v_9^{3} = (y + 1)$ $\varDelta^t v_{11}^{3} = (y)$ $\varDelta^t v_{12}^{3} = (y + 8, y + 24)$ $\varDelta^t v_{13}^{3} = (y + 1, y + 17)$ $\varDelta^t v_{15}^{3} = (y)$	16
$\varDelta^t V^{3.5}$:	$\varDelta^t v_1^{3.5} = (y + 1)$ $\varDelta^t v_{11}^{3.5} = (y)$ $\varDelta^t v_{12}^{3.5} = (y, y + 16)$	3
$\varDelta^t V^{4}$:	$\varDelta^t v_1^{4} = (y)$	1
$\varDelta^t V^{4.5} \cdots \varDelta^t V^{5.5}$:	ϕ	2 (2 fixed)
$\varDelta^t V^{6}$:	$\varDelta^t v_1^{6} = (y)$ $\varDelta^t v_6^{6} = (y + 17)$ $\varDelta^t v_{11}^{6} = (y + 24)$ $\varDelta^t v_{12}^{6} = (y + 24)$	30 (29 fixed)
$\varDelta^t V^{6.5}$:	$\varDelta^t v_0^{6.5} = (y, y + 28)$ $\varDelta^t v_1^{6.5} = (y + 4, y)$ $\varDelta^t v_2^{6.5} = (y + 5, y + 21, y + 17)$ $\varDelta^t v_3^{6.5} = (y + 12)$ $\varDelta^t v_4^{6.5} = (y + 1, y + 25, y + 21, y + 17, y + 13)$ $\varDelta^t v_5^{6.5} = (y + 9, y + 1, y + 29, y + 21, y + 17)$ $\varDelta^t v_6^{6.5} = (y + 6, y + 2, y + 30, y + 26, y + 22, y + 18, y + 14)$ $\varDelta^t v_7^{6.5} = (y + 5, y + 29, y + 17)$ $\varDelta^t v_8^{6.5} = (y + 8, y, y + 24, y + 20)$ $\varDelta^t v_9^{6.5} = (y + 8, y + 28, y + 24, y + 16)$ $\varDelta^t v_{10}^{6.5} = (y + 9, y + 1, y + 29, y + 25, y + 13)$ $\varDelta^t v_{11}^{6.5} = (y + 4, y + 24)$ $\varDelta^t v_{12}^{6.5} = (y, y + 24, y + 20)$ $\varDelta^t v_{13}^{6.5} = (y + 8, y + 28, y + 24)$ $\varDelta^t v_{14}^{6.5} = (y + 9, y + 29, y + 25, y + 13)$ $\varDelta^t v_{15}^{6.5} = (y + 4)$	-

*: If $y = 28$, the condition $v_3^{2.5}[y + 3] = \neg v_4^{2.5}[y + 3]$ in $\varDelta^t V^3 \to \varDelta^t V^{2.5}$ can be eliminated.

B 6.5-Round Examples For BLAKE and BLAKE2

The main difference between BLAKE-256 and BLAKE2s (BLAKE-512 and BLAKE2b) is at $\varDelta^t v_1^{3.5}$, where $\varDelta^t v_1^{3.5} = (29)$ for BLAKE-2s ($\varDelta^t v_1^{3.5} = (10)$ for BLAKE-2b) and ϕ for BLAKE-256 (BLAKE-512). We specifically emphasize this part with bold dark format.

Table 12. Example for 6.5-round BLAKE-256 with $y = 28 \in \mathbb{X}_{256} \bigcap \mathbb{X}_{2s}$.

$\varDelta M$	$\varDelta^b m_{11} = (31)$, $\varDelta^t m_5 = (28)$							
${}_aM$	0x932a5d7f	0xa2625330	0x46a9466f	0xae3052a3	0xbf9a6338	0xd4167790	0x7bf0ef5e	0x4ef572ba
	0x308dc96d	0x23b415c3	0x6fb64798	0xa75b42e8	0x3cb6d30e	0xb56003b4	0x7a4db777	0x715b79a
${}_bM$	0x932a5d7f	0xa2625330	0x46a9466f	0xae3052a3	0xbf9a6338	0xd4167790	0x7bf0ef5e	0x4ef572ba
	0x308dc96d	0x23b415c3	0x6fb64798	0x275b42e8	0x3cb6d30e	0xb56003b4	0x7a4db777	0x715b79a
${}_cM$	0x932a5d7f	0xa2625330	0x46a9466f	0xae3052a3	0xbf9a6338	0xc4167790	0x7bf0ef5e	0x4ef572ba
	0x308dc96d	0x23b415c3	0x6fb64798	0xa75b42e8	0x3cb6d30e	0xb56003b4	0x7a4db777	0x715b79a
${}_dM$	0x932a5d7f	0xa2625330	0x46a9466f	0xae3052a3	0xbf9a6338	0xc4167790	0x7bf0ef5e	0x4ef572ba
	0x308dc96d	0x23b415c3	0x6fb64798	0x275b42e8	0x3cb6d30e	0xb56003b4	0x7a4db777	0x715b79a
$\varDelta^t V^{3.5}$	$\boldsymbol{\Delta^t v_1^{3.5} = \phi}$, $\varDelta^t v_{11}^{3.5} = (28)$, $\varDelta^t v_{12}^{3.5} = (28, 2)$							
${}_aV^{3.5}$	0x7ce3001a	0x5f257eb	0x7cb1b540	0xf5f76e6	0x62eba0a0	0x8723a3b3	0x3a617d3b	0x616c91a2
	0xf2e28cd6	0x2dd8b157	0x888f9a21	0x6074df04	0x370f729f	0xeecddee4	0x7f42197f	0x36ace0f3
${}_bV^{3.5}$	0xce7042ae	0xc394a0c1	0xbdedbda1	0xbf9d773f	0x7fdd9e46	0xdefe6c9e	0xf9985a99	0x2e67c857
	0x8903f293	0xfc2ed055	0xbcb66021	0x5ac97fd7	0xa42a029b	0x60de7589	0x637162de	0xfd1bd434
${}_cV^{3.5}$	0x7ce3001a	0x5f257eb	0x7cb1b540	0xf5f76e6	0x62eba0a0	0x8723a3b3	0x3a617d3b	0x616c91a2
	0xf2e28cd6	0x2dd8b157	0x888f9a21	0x7074df04	0x270f629f	0xeecddee4	0x7f42197f	0x36ace0f3
${}_dV^{3.5}$	0xce7042ae	0xc394a0c1	0xbdedbda1	0xbf9d773f	0x7fdd9e46	0xdefe6c9e	0xf9985a99	0x2e67c857
	0x8903f293	0xfc2ed055	0xbcb66021	0x4ac97fd7	0xb42a129b	0x60de7589	0x637162de	0xfd1bd434
$\varDelta^b V^{10}$	$\varDelta^b v_0^{10} = (31)$, $\varDelta^b v_5^{10} = (16)$, $\varDelta^b v_{10}^{10} = (23)$, $\varDelta^b v_{15}^{10} = (23)$							
${}_aV^{10}$	0x9920f4d5	0x7d8a6621	0xc7139615	0x205a3fce	0x4ded77e1	0x1ed1c43f	0x6e8efedc	0xf6f4fe72
	0x6e17623b	0x4cd8bea2	0xfe2149af	0xd2f8e09c	0x53b6139c	0x3972162e	0xd4f82167	0x4d1b2a46
${}_bV^{10}$	0x1920f4d5	0x7d8a6621	0xc7139615	0x205a3fce	0x4ded77e1	0x1ed0c43f	0x6e8efedc	0xf6f4fe72
	0x6e17623b	0x4cd8bea2	0xfea149af	0xd2f8e09c	0x53b6139c	0x3972162e	0xd4f82167	0x4d9b2a46
${}_cV^{10}$	0x5a870d65	0x8d12db5	0x537127c9	0xabdb13a9	0xcaf27105	0x17ef5f49	0x66721638	0x8f333fbf
	0xccdc1196	0x3d9aaba6	0x84ee030c	0xda86539	0x976348e3	0xfde7c240	0x1df99dc8	0x568a818c
${}_dV^{10}$	0xda870d65	0x8d12db5	0x537127c9	0xabdb13a9	0xcaf27105	0x17ee5f49	0x66721638	0x8f333fbf
	0xccdc1196	0x3d9aaba6	0x846e030c	0xda86539	0x976348e3	0xfde7c240	0x1df99dc8	0x560a818c

Table 13. Example for 6.5-round BLAKE2s with $y = 28 \in \mathbb{X}_{256} \bigcap \mathbb{X}_{2s}$.

$\varDelta M$	$\varDelta^b m_{11} = (31)$, $\varDelta^t m_5 = (28)$							
${}_aM$	0xce9f1cc6	0x7f3a9b64	0x9e9ddc55	0x4553fa8c	0xe2f4ad99	0x33a0533a	0x8b1d785c	0xc7f56492
	0xe5b2b205	0xd44f69a1	0x2d83e500	0x18b03f68	0x13d0c628	0x15fce9f2	0x9108f878	0xc477ca04
${}_bM$	0xce9f1cc6	0x7f3a9b64	0x9e9ddc55	0x4553fa8c	0xe2f4ad99	0x33a0533a	0x8b1d785c	0xc7f56492
	0xe5b2b205	0xd44f69a1	0x2d83e500	0x98b03f68	0x13d0c628	0x15fce9f2	0x9108f878	0xc477ca04
${}_cM$	0xce9f1cc6	0x7f3a9b64	0x9e9ddc55	0x4553fa8c	0xe2f4ad99	0x23a0533a	0x8b1d785c	0xc7f56492
	0xe5b2b205	0xd44f69a1	0x2d83e500	0x18b03f68	0x13d0c628	0x15fce9f2	0x9108f878	0xc477ca04
${}_dM$	0xce9f1cc6	0x7f3a9b64	0x9e9ddc55	0x4553fa8c	0xe2f4ad99	0x23a0533a	0x8b1d785c	0xc7f56492
	0xe5b2b205	0xd44f69a1	0x2d83e500	0x98b03f68	0x13d0c628	0x15fce9f2	0x9108f878	0xc477ca04
$\varDelta^t V^{3.5}$	$\mathbf{\Delta^t v_1^{3.5}} = (\mathbf{29})$, $\varDelta^t v_{11}^{3.5} = (28)$, $\varDelta^t v_{12}^{3.5} = (28, 2)$							
${}_aV^{3.5}$	0x71177c4a	0x456e63aa	0x63bc0484	0xe348f6a9	0xfa5c62fe	0x1229c0a3	0x12ea25d0	0xd7a6a55f
	0x3ca79134	0x6ccc6e48	0x2bd29e5	0xc386b1	0x86f12557	0x414c79f1	0x3fb6c33	0x4baef1a0
${}_bV^{3.5}$	0xaae6286d	0x1af8dcfe	0x70a74337	0xa293966a	0xe35d9b23	0xe74273b3	0xfb967985	0xc16500a7
	0x57a589c8	0x5edbf5ae	0x66de7b25	0x15c8f5ff	0xd730836	0x357d6100	0x3ae77969	0x54a834da
${}_cV^{3.5}$	0x71177c4a	0x656e63aa	0x63bc0484	0xe348f6a9	0xfa5c62fe	0x1229c0a3	0x12ea25d0	0xd7a6a55f
	0x3ca79134	0x6ccc6e48	0x2bd29e5	0x10c386b1	0x96f13557	0x414c79f1	0x3fb6c33	0x4baef1a0
${}_dV^{3.5}$	0xaae6286d	0x3af8dcfe	0x70a74337	0xa293966a	0xe35d9b23	0xe74273b3	0xfb967985	0xc16500a7
	0x57a589c8	0x5edbf5ae	0x66de7b25	0x5c8f5ff	0x1d731836	0x357d6100	0x3ae77969	0x54a834da
$\varDelta^b V^{10}$	$\varDelta^b v_0^{10} = (31)$, $\varDelta^b v_5^{10} = (16)$, $\varDelta^b v_{10}^{10} = (23)$, $\varDelta^b v_{15}^{10} = (23)$							
${}_aV^{10}$	0x945cf52e	0x422107ab	0x3a682330	0x2f8bd4f1	0xeead389	0x21e907ec	0x17138a07	0xae021462
	0x229a3e13	0x3c623c2c	0x64327d4a	0xf1d0e09a	0x5df5abad	0x1be8464a	0x7890983a	0x85288868
${}_bV^{10}$	0x145cf52e	0x422107ab	0x3a682330	0x2f8bd4f1	0xeead389	0x21e807ec	0x17138a07	0xae021462
	0x229a3e13	0x3c623c2c	0x64b27d4a	0xf1d0e09a	0x5df5abad	0x1be8464a	0x7890983a	0x85a88868
${}_cV^{10}$	0xc136da56	0xe91ba476	0xfa9ad265	0x6b4d2f9e	0x68ef06c8	0x9ab4757a	0xe63456e0	0x8818e9d4
	0x5da1784c	0x57ecd14b	0xcb0788b8	0xf3148edf	0xa19d7f24	0xf17b5303	0x9ec70b70	0x2f763872
${}_dV^{10}$	0x4136da56	0xe91ba476	0xfa9ad265	0x6b4d2f9e	0x68ef06c8	0x9ab5757a	0xe63456e0	0x8818e9d4
	0x5da1784c	0x57ecd14b	0xcb8788b8	0xf3148edf	0xa19d7f24	0xf17b5303	0x9ec70b70	0x2ff63872

Table 14. Example for 6.5-round BLAKE-512 with $y = 9 \in \mathbb{X}_{512} \bigcap \mathbb{X}_{2b}$.

$\varDelta M$	$\varDelta^b m_{11} = (63),\ \varDelta^t m_5 = (9)$			
${}_a M$	0x9c1860c444a6a9f4	0xc95a712fd5a29b72	0x6e5c6811448b300f	0x5c0af45531e396d3
	0x679dee5280c15ad0	0x329f5347ccb9bf64	0x297828d3ec89e9d0	0xa55ffc029ea78609
	0xef01f63ec485f87d	0x86560936e36d9dff	0xfd9674bb724d62e0	0x9c03f6f64a96659f
	0xe3666bd816053d27	0xe4669665a4a0a440	0x1cbf0c93a121eb09	0x65a6a90ac809c019
${}_b M$	0x9c1860c444a6a9f4	0xc95a712fd5a29b72	0x6e5c6811448b300f	0x5c0af45531e396d3
	0x679dee5280c15ad0	0x329f5347ccb9bf64	0x297828d3ec89e9d0	0xa55ffc029ea78609
	0xef01f63ec485f87d	0x86560936e36d9dff	0xfd9674bb724d62e0	0x1c03f6f64a96659f
	0xe3666bd816053d27	0xe4669665a4a0a440	0x1cbf0c93a121eb09	0x65a6a90ac809c019
${}_c M$	0x9c1860c444a6a9f4	0xc95a712fd5a29b72	0x6e5c6811448b300f	0x5c0af45531e396d3
	0x679dee5280c15ad0	0x329f5347ccb9bd64	0x297828d3ec89e9d0	0xa55ffc029ea78609
	0xef01f63ec485f87d	0x86560936e36d9dff	0xfd9674bb724d62e0	0x9c03f6f64a96659f
	0xe3666bd816053d27	0xe4669665a4a0a440	0x1cbf0c93a121eb09	0x65a6a90ac809c019
${}_d M$	0x9c1860c444a6a9f4	0xc95a712fd5a29b72	0x6e5c6811448b300f	0x5c0af45531e396d3
	0x679dee5280c15ad0	0x329f5347ccb9bd64	0x297828d3ec89e9d0	0xa55ffc029ea78609
	0xef01f63ec485f87d	0x86560936e36d9dff	0xfd9674bb724d62e0	0x1c03f6f64a96659f
	0xe3666bd816053d27	0xe4669665a4a0a440	0x1cbf0c93a121eb09	0x65a6a90ac809c019
$\varDelta^t V^{3.5}$	$\boldsymbol{\Delta^t v_1^{3.5}} = \boldsymbol{\phi},\ \varDelta^t v_{11}^{3.5} = (9),\ \varDelta^t v_{12}^{3.5} = (41, 9)$			
${}_a V^{3.5}$	0xc87af7255a6ec986	0xc59be5b07a4418d7	0x5295eb179fee042c	0x4f87d569d171c685
	0xc1c24f85f094b263	0xbc711b20878eb4ea	0x1cda016fcf08ee93	0x878f439bd1398fec
	0x982d7a384b8549bb	0x29cd6958f1a234c3	0xb81579ed9e3eff45	0xbfba600ee495e360
	0x4d5e10f24eba6506	0x4f8a20a0c7164ef8	0x4156d917e0e33e7b	0x8f204cb6dc806747
${}_b V^{3.5}$	0x57926274c228f656	0x5ac46fa843cda867	0x936f1f621381dad4	0xbd0f73ec836d47bc
	0xbac8918094537e74	0x1edec058ea817875	0xc5bf41aeadf39382	0x4149082191041e60
	0x9fd575b7fe10ace3	0x8fed3642acc17d51	0x1ded33ae6ee468ba	0x5365299759c0a42
	0x89f06ef09e1612ee	0xe597ede91683a2d8	0x389825cb39587e4f	0xff48c413164455c3
${}_c V^{3.5}$	0xc87af7255a6ec986	0xc59be5b07a4418d7	0x5295eb179fee042c	0x4f87d569d171c685
	0xc1c24f85f094b263	0xbc711b20878eb4ea	0x1cda016fcf08ee93	0x878f439bd1398fec
	0x982d7a384b8549bb	0x29cd6958f1a234c3	0xb81579ed9e3eff45	0xbfba600ee495e160
	0x4d5e12f24eba6706	0x4f8a20a0c7164ef8	0x4156d917e0e33e7b	0x8f204cb6dc806747
${}_d V^{3.5}$	0x57926274c228f656	0x5ac46fa843cda867	0x936f1f621381dad4	0xbd0f73ec836d47bc
	0xbac8918094537e74	0x1edec058ea817875	0xc5bf41aeadf39382	0x4149082191041e60
	0x9fd575b7fe10ace3	0x8fed3642acc17d51	0x1ded33ae6ee468ba	0x5365299759c0842
	0x89f06cf09e1610ee	0xe597ede91683a2d8	0x389825cb39587e4f	0xff48c413164455c3
$\varDelta^b V^{10}$	$\varDelta^b v_0^{10} = (63),\ \varDelta^b v_5^{10} = (36),\ \varDelta^b v_{10}^{10} = (47),\ \varDelta^b v_{15}^{10} = (47)$			
${}_a V^{10}$	0x1b404ab31fbe9343	0xc01ae4355f49855f	0xf52deb99e6d25dee	0xba1e74d813d9e09c
	0x1d4142ceee078181	0x8c7261a65899559	0x780312586191c134	0x86c7c29f8161a9ac
	0x77f4ec97a373e3dd	0x7068ac849086f0c3	0xfc3c0163cdc3f7b9	0x52d68b2940599cfa
	0x59ad1c82831be8f7	0x74d99e11568eb396	0x3552275c6ddcf7a3	0x8dfe0979b5e83dbd
${}_b V^{10}$	0x9b404ab31fbe9343	0xc01ae4355f49855f	0xf52deb99e6d25dee	0xba1e74d813d9e09c
	0x1d4142ceee078181	0x8c7260a65899559	0x780312586191c134	0x86c7c29f8161a9ac
	0x77f4ec97a373e3dd	0x7068ac849086f0c3	0xfc3c8163cdc3f7b9	0x52d68b2940599cfa
	0x59ad1c82831be8f7	0x74d99e11568eb396	0x3552275c6ddcf7a3	0x8dfe8979b5e83dbd
${}_c V^{10}$	0xcc0a78ca6c133737	0xa6a12a75a2ab0a78	0xaaff3e032bf0964f	0x6a833f52c06326f8
	0x1571fbe8468d6869	0x224b394014f172d8	0x72a0866c8eb1dfcc	0x4af2b98060eea9bb
	0xe7f5b1b201006785	0xa57c9190f805d201	0xdea0ecffe0219e24	0xbbec25c771762bfb
	0xd312a8ab8e4df740	0xd9a366032739ede2	0xb8d5bfa962e8d684	0xb122b4542c543d9d
${}_d V^{10}$	0x4c0a78ca6c133737	0xa6a12a75a2ab0a78	0xaaff3e032bf0964f	0x6a833f52c06326f8
	0x1571fbe8468d6869	0x224b395014f172d8	0x72a0866c8eb1dfcc	0x4af2b98060eea9bb
	0xe7f5b1b201006785	0xa57c9190f805d201	0xdea06cffe0219e24	0xbbec25c771762bfb
	0xd312a8ab8e4df740	0xd9a366032739ede2	0xb8d5bfa962e8d684	0xb12234542c543d9d

Table 15. Example for 6.5-round BLAKE2b with $y = 9 \in \mathbb{X}_{512} \bigcap \mathbb{X}_{2b}$.

ΔM	$\Delta^b m_{11} = (63)$, $\Delta^t m_5 = (9)$			
${}_aM$	0x3cec6965bf357a5	0x3efa6687e114e70d	0x6fe9d72277e832e4	0x60574e830fad0b27
	0x1bad3b4b1257079e	0x43b8e8ebf1bc4557	0xc553a639b52984b0	0x95bd9c03c94695e5
	0xc4e9f58d840c74c9	0x2186128d765d51b0	0x10bc4fee175e6c82	0x18ddcb4d4ac938ee
	0x5cf2d8b6cf1ea3ce	0x3ec5aa659dacedf5	0xadf91c482e6b4506	0xa34876d149007c7b
${}_bM$	0x3cec6965bf357a5	0x3efa6687e114e70d	0x6fe9d72277e832e4	0x60574e830fad0b27
	0x1bad3b4b1257079e	0x43b8e8ebf1bc4557	0xc553a639b52984b0	0x95bd9c03c94695e5
	0xc4e9f58d840c74c9	0x2186128d765d51b0	0x10bc4fee175e6c82	0x98ddcb4d4ac938ee
	0x5cf2d8b6cf1ea3ce	0x3ec5aa659dacedf5	0xadf91c482e6b4506	0xa34876d149007c7b
${}_cM$	0x3cec6965bf357a5	0x3efa6687e114e70d	0x6fe9d72277e832e4	0x60574e830fad0b27
	0x1bad3b4b1257079e	0x43b8e8ebf1bc4757	0xc553a639b52984b0	0x95bd9c03c94695e5
	0xc4e9f58d840c74c9	0x2186128d765d51b0	0x10bc4fee175e6c82	0x18ddcb4d4ac938ee
	0x5cf2d8b6cf1ea3ce	0x3ec5aa659dacedf5	0xadf91c482e6b4506	0xa34876d149007c7b
${}_dM$	0x3cec6965bf357a5	0x3efa6687e114e70d	0x6fe9d72277e832e4	0x60574e830fad0b27
	0x1bad3b4b1257079e	0x43b8e8ebf1bc4757	0xc553a639b52984b0	0x95bd9c03c94695e5
	0xc4e9f58d840c74c9	0x2186128d765d51b0	0x10bc4fee175e6c82	0x98ddcb4d4ac938ee
	0x5cf2d8b6cf1ea3ce	0x3ec5aa659dacedf5	0xadf91c482e6b4506	0xa34876d149007c7b
$\Delta^t V^{3.5}$	$\boldsymbol{\Delta^t v_1^{3.5} = (10)}$, $\Delta^t v_{11}^{3.5} = (9)$, $\Delta^t v_{12}^{3.5} = (41, 9)$			
${}_aV^{3.5}$	0xa8f431bca7166664	0x2bce47208c2b479d	0x2554f082eb89d530	0x12b06bc7f71ebe12
	0x5d733d5fa41457fc	0xae2b3d68d8adfe2f	0xe03c7fa88285b93d	0xe134f22af656a9d9
	0x8bcd47a74a5e35a2	0x21098bd0acfbc078	0x9d0ddd6c2403d2ab	0xf0dbb0c6a9a392c5
	0xd72aa227f3c2a651	0x406e07f8eec1929f	0x863da54a0653fe1f	0xefb750af7de2c392
${}_bV^{3.5}$	0x63b1930b9a252aff	0xd754470ae2a5de96	0x1b39d8f987ec3762	0x201afad51a642cb1
	0x1d5c8e5fb50c1c68	0x709103f9ba538f43	0xb847dad7a1bf8a56	0xa59f9b63902edb4
	0x40d96db5d9d3b546	0x332aed26d86aceaa	0x424eaab611c9c6f	0x802b683db9ac54b9
	0x110cd82fdac384dd	0xa93fe8a10201b57b	0x49eed3d94b17685a	0xcdf2a00fd5300651
${}_cV^{3.5}$	0xa8f431bca7166664	0x2bce47208c2b439d	0x2554f082eb89d530	0x12b06bc7f71ebe12
	0x5d733d5fa41457fc	0xae2b3d68d8adfe2f	0xe03c7fa88285b93d	0xe134f22af656a9d9
	0x8bcd47a74a5e35a2	0x21098bd0acfbc078	0x9d0ddd6c2403d2ab	0xf0dbb0c6a9a390c5
	0xd72aa027f3c2a451	0x406e07f8eec1929f	0x863da54a0653fe1f	0xefb750af7de2c392
${}_dV^{3.5}$	0x63b1930b9a252aff	0xd754470ae2a5da96	0x1b39d8f987ec3762	0x201afad51a642cb1
	0x1d5c8e5fb50c1c68	0x709103f9ba538f43	0xb847dad7a1bf8a56	0xa59f9b63902edb4
	0x40d96db5d9d3b546	0x332aed26d86aceaa	0x424eaab611c9c6f	0x802b683db9ac56b9
	0x110cda2fdac386dd	0xa93fe8a10201b57b	0x49eed3d94b17685a	0xcdf2a00fd5300651
$\Delta^b V^{10}$	$\Delta^b v_0^{10} = (63)$, $\Delta^b v_5^{10} = (48)$, $\Delta^b v_{10}^{10} = (47)$, $\Delta^b v_{15}^{10} = (47)$			
${}_aV^{10}$	0x96ace3d164600933	0x6785c14493444a3d	0xadc3b5f6dbc8c992	0xada06d115f42653a
	0xcb06b797a6152dbe	0xf701f3e0f76be4cb	0xf4baf3238d75bdb6	0xb71965677688de57
	0xaa494db2c0d12db8	0x10ab8d9652485fcf	0xb97f5a3ef869239f	0x560aff2ec6a0d95f
	0x1597013f79b484d1	0x182beacffdc6ec05	0x6802644a544f6271	0x59ac761a17acecca
${}_bV^{10}$	0x16ace3d164600933	0x6785c14493444a3d	0xadc3b5f6dbc8c992	0xada06d115f42653a
	0xcb06b797a6152dbe	0xf700f3e0f76be4cb	0xf4baf3238d75bdb6	0xb71965677688de57
	0xaa494db2c0d12db8	0x10ab8d9652485fcf	0xb97fda3ef869239f	0x560aff2ec6a0d95f
	0x1597013f79b484d1	0x182beacffdc6ec05	0x6802644a544f6271	0x59acf61a17acecca
${}_cV^{10}$	0xe8d4f6a3aa68e9d6	0x1ba5272a94ed608d	0x51b3a429d5ee6873	0x50af4c1bb7b31dd2
	0x738835de6bff309d	0xc5fc88e668afef14	0x1671fea856c55b2d	0xd04b446c31b59a1b
	0x8f120d94bae51fa1	0x5be58c40a2d2c0a9	0xe9c1de5ac5992a67	0xa307fd45e31b7817
	0xbd4864acd0f2e4bc	0x4a8a43605d94a9b4	0x16e63ec7c12bc056	0x30e48769ae169de0
${}_dV^{10}$	0x68d4f6a3aa68e9d6	0x1ba5272a94ed608d	0x51b3a429d5ee6873	0x50af4c1bb7b31dd2
	0x738835de6bff309d	0xc5fd88e668afef14	0x1671fea856c55b2d	0xd04b446c31b59a1b
	0x8f120d94bae51fa1	0x5be58c40a2d2c0a9	0xe9c15e5ac5992a67	0xa307fd45e31b7817
	0xbd4864acd0f2e4bc	0x4a8a43605d94a9b4	0x16e63ec7c12bc056	0x30e40769ae169de0