Boomerang Attacks on BLAKE-32

Alex Biryukov and Ivica Nikolić* and Arnab Roy

University of Luxembourg
{alex.biryukov,ivica.nikolic,arnab.roy}uni.lu

Abstract. We present high probability differential trails on 2 and 3 rounds of BLAKE-32. Using the trails we are able to launch boomerang attacks on up to 8 round-reduced keyed permutation of BLAKE-32. Also, we show that boomerangs can be used as distinguishers for hash/compression functions and present such distinguishers for the compression function of BLAKE-32 reduced to 7 rounds. Since our distinguishers on up to 6 round-reduced keyed permutation of BLAKE-32 are practical (complexity of only 2^{12} encryptions), we are able to find boomerang quartets on a PC.

Keywords: SHA-3 competition, hash function, BLAKE, boomerang attack, cryptanalysis.

1 Introduction

The SHA-3 competition [6] will soon enter the third and final phase, by selecting 5 out of 14 second round candidates. The hash function BLAKE [2] is among these 14 candidates, and it is one of the few functions that has not been tweaked from the initial submission in 2008. Being an addition-rotation-xor (ARX) design, BLAKE is one of the fastest functions on various platforms in software. Indeed, among the fastest candidates, BLAKE has the highest published security level, i.e. the best published attacks work only on a small fraction of the total number of rounds. Few attacks, however, were published on the round-reduced compression function and keyed permutation of BLAKE-32 (which has 10 rounds). In [3] Ji and Liangyu present collision and preimage attacks on 2.5 rounds of the compression function of BLAKE-32. Su et al. [7] give near collisions on 4 rounds with a complexity of 2^{21} compression function calls. However, one can argue that the message modification they use, requires an additional effort of 2^{64} (see Sec. 5). Aumasson et al. in [1], among other, present near collisions on 4 rounds of the compression function with 2^{56} complexity, and impossible differentials on 5 rounds of the keyed permutation.

* This author is supported by the Fonds National de la Recherche Luxembourg grant TR-PHD-BFR07-031.

Our Contribution. We show various boomerang distinguishers on round-reduced BLAKE-32. Our analysis is based on the fact that BLAKE-32, being a keyed permutation, has some high probability differential trails on two and three rounds (2^{-1} on two and 2^{-7} on three rounds). Moreover, we can extend the three round trail to four rounds. First, we use these trails to build boomerang distinguishers for the round-reduced keyed permutation of BLAKE-32 on up to 8 rounds. Then we extend the concept of boomerang distinguishers to hash functions. As far as we know, this is the first application of the standard boomerangs to hash function. An amplified boomerang attack applied to hash functions was presented in [4], however it was used in addition to a collision attack. Our boomerang attacks, on the other hand, are standalone distinguishers, and work in the same way as for block ciphers – by producing the quartet of plaintexts and ciphertexts (input chaining values and output chaining values). We also show how to obtain simpler zero-sum distinguisher from the boomerang and present such distinguishers for 4, 5, 6 rounds of BLAKE-32. Our final result is a boomerang distinguisher for 7 rounds of the compression function of BLAKE-32. The summary of our results is given in Tbl. 1.

Although in this paper we focus on BLAKE-32, our attacks can be easily extended to the other versions of BLAKE (with similar complexities and number of attacked rounds). The attacks do not contradict any security claims of BLAKE.

Table 1. Summary of the attacks on the compression function (CF) and the keyed permutation (KP) of BLAKE-32.

Attack	CF/KP	Rounds	CF/KP calls	Reference
Free-start collisions	CF	2.5	2^{112}	[3]
Near collisions[a]	CF	4	2^{21}	[7]
Near collisions	CF	4	2^{56}	[1]
Impossible diffs.	KP	5	-	[1]
Boomerang dist.	CF	4	2^{67}	Sec. 5
Boomerang dist.	CF	5	$2^{71.2}$	Sec. 5
Boomerang dist.	CF	6	2^{102}	Sec. 5
Boomerang dist.	CF	6.5	2^{184}	Sec. 5
Boomerang dist.	CF	7	2^{232}	Sec. 5
Boomerang dist.	KP	4	2^{3}	Sec. 6
Boomerang dist.	KP	5	$2^{7.2}$	Sec. 6
Boomerang dist.	KP	6	$2^{11.75}$	Sec. 6
Boomerang dist.	KP	7	2^{122}	Sec. 6
Boomerang dist.	KP	8	2^{242}	Sec. 6

[a] The attack assumes that message modification can be used anywhere in the trail.

2 Description of BLAKE32

The compression function of BLAKE-32 processes a state of 16 32-bit words represented as 4×4 matrix. Each word in BLAKE-32 has 32 bits. In the *Initialization* procedure, the state is loaded with a chaining value $h_0, \ldots, h_7$, a salt $s_0, \ldots, s_3$, constants $c_0, \ldots, c_7$, a counter t_0, t_1 as follows:

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

After the *Initialization*, the compression function takes 16 message words $m_0, \ldots, m_{15}$

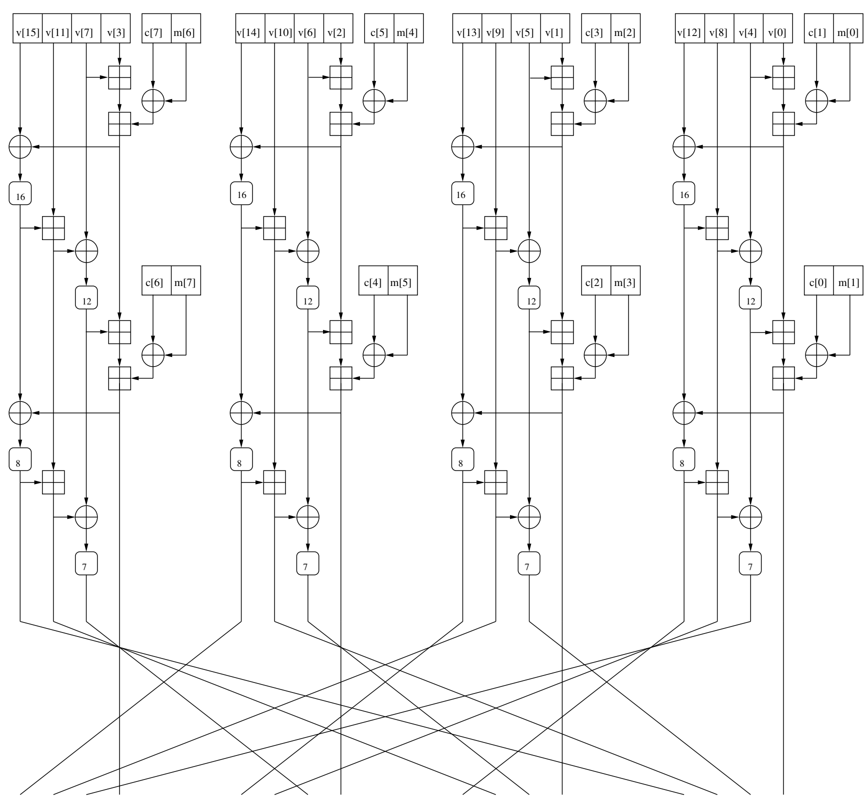

Fig. 1. Column step of round-0.

as inputs and iterates 10 rounds. Each round is composed of eight applications of $\mathtt{G}$ function. A column step:

$$\mathtt{G}_0(v_0, v_4, v_8, v_{12}), \mathtt{G}_1(v_1, v_5, v_9, v_{13}), \mathtt{G}_2(v_2, v_6, v_{10}, v_{14}), \mathtt{G}_3(v_3, v_7, v_{11}, v_{15})$$

followed by the diagonal step:

$$\mathtt{G}_4(v_0, v_5, v_{10}, v_{15}), \mathtt{G}_5(v_1, v_6, v_{11}, v_{12}), \mathtt{G}_6(v_2, v_7, v_8, v_{13}), \mathtt{G}_7(v_3, v_4, v_9, v_{14})$$

where $\mathtt{G}_i(i \in \{0, \ldots, 7\})$ depend on their indices, message words $m_0, \ldots, m_{15}$, constants $c_0, \ldots, c_{15}$ and round index r. At round r, $\mathtt{G}_i(a, b, c, d)$ is described with following steps:

$$\begin{aligned}
&1: a \leftarrow a + b + (m_{\sigma_r(2i)} \oplus c_{\sigma_r(2i+1)})\\
&2: d \leftarrow (d \oplus a) \ggg 16\\
&3: c \leftarrow c + d\\
&4: b \leftarrow (b \oplus c) \ggg 12\\
&5: a \leftarrow a + b + (m_{\sigma_r(2i+1)} \oplus c_{\sigma_r(2i)})\\
&6: d \leftarrow (d \oplus a) \ggg 8\\
&7: c \leftarrow c + d\\
&8: b \leftarrow (b \oplus c) \ggg 7
\end{aligned}$$

where σ_r belongs to the set of permutations as specified in [2]. The *Finalization* procedure in BLAKE-32 is depicted as:

$$\begin{aligned}
h_0^{'} &\leftarrow h_0 \oplus s_0 \oplus v_0 \oplus v_8\\
h_1^{'} &\leftarrow h_1 \oplus s_1 \oplus v_1 \oplus v_9\\
h_2^{'} &\leftarrow h_2 \oplus s_2 \oplus v_2 \oplus v_{10}\\
h_3^{'} &\leftarrow h_3 \oplus s_3 \oplus v_3 \oplus v_{11}\\
h_4^{'} &\leftarrow h_4 \oplus s_0 \oplus v_4 \oplus v_{12}\\
h_5^{'} &\leftarrow h_5 \oplus s_1 \oplus v_5 \oplus v_{13}\\
h_6^{'} &\leftarrow h_6 \oplus s_2 \oplus v_6 \oplus v_{14}\\
h_7^{'} &\leftarrow h_7 \oplus s_3 \oplus v_7 \oplus v_{15}
\end{aligned}$$

where $h_0, \ldots, h_7$ is the initial chaining value and $v_0, \ldots, v_{15}$ is the state value after the ten rounds, and $h_0', \ldots, h_7'$ are the words of the new chaining value.

3 Boomerang Attacks on Block Ciphers and Compression Functions

The boomerang attack [8] is a differential-type attack that exploits high probability differential trails in each half of a cipher E. When successful, it outputs a quartet of plaintexts and corresponding ciphertexts with some fixed particular differences between some of the pairs. This property can be used to distinguish the cipher from a random permutation, and in some cases, to recover the key.

Let us decompose the initial cipher E into two ciphers E_0, E_1, i.e. $E = E_1 \circ E_0$. Let $\Delta \rightarrow \Delta^*$ be some differential trail for E_0 that holds with probability p and $\nabla \rightarrow \nabla^*$ be a trail for E_1 with probability q. We start with a pair of plaintexts $(P_1, P_2) = (P_1, P_1 \oplus \Delta)$ and produce a pair of corresponding ciphertexts $(C_1, C_2) = (E(P_1), E(P_2))$. Then we produce a new pair of ciphertext $(C_3, C_4) = (C_1 \oplus \nabla^*, C_2 \oplus \nabla^*)$, decrypt this pair, and get the corresponding pair of plaintexts $(P_3, P_4) = (E^{-1}(C_3), E^{-1}(C_4))$. The difference $P_3 \oplus P_4$ is Δ with probability at least p^2q^2: 1)the difference $E_0(P_1) \oplus E_0(P_2)$ is Δ^* with probability p; 2) the differences $E_1^{-1}(C_1) \oplus E_1^{-1}(C_3)$, $E_1^{-1}(C_2) \oplus E_1^{-1}(C_4)$ are both ∇ with probability q^2; 3)when 1), 2) hold, then the difference $E_1^{-1}(C_3) \oplus E_1^{-1}(C_4)$ is Δ^* (with probability pq^2) and $E^{-1}(C_3) \oplus E^{-1}(C_4)$ is Δ with probability p^2q^2.

We would like to address a couple of issues. First, the boomerang distinguisher can be used even in the case when it returns a pair (P_3, P_4) with a difference $P_3 \oplus P_4$ specified only in certain bits (instead of the full plaintext). When the difference is specified in t bits ($t < n$), then the probability of the boomerang (in order to be used as a distinguisher) should be higher than 2^{-t}, i.e. $p^2q^2 > 2^{-t}$. Second, the real probability of the boomerang is $\hat{p}^2\hat{q}^2$, where $\hat{p}, \hat{q}$ are so-called amplified probabilities, defined as:

$$\hat{p} = \sqrt{\sum_{\Delta^*} P[\Delta \to \Delta^*]^2}, \hat{q} = \sqrt{\sum_{\nabla} P[\nabla \to \nabla^*]^2} \tag{1}$$

Since finding these values is hard, in some cases, we try to get experimental results for the probability of the boomerang. We run a computer simulation, start the boomerang with a number of pairs with some prefixed difference Δ, and count the number of returned pairs that have the same difference Δ. Obviously the ratio of the returned pairs to the launched pairs is the probability of the boomerang.

The main obstacle for applying the boomerang attack to compression functions, is that in general, the compression functions are non-invertible. Hence, after obtaining the pairs (C_3, C_4) from (C_1, C_2), one cannot go backwards and obtain the pair (P_3, P_4). One way to deal with this is to switch to amplified boomerang attacks [5]. However, this type of boomerangs usually has lower probability, and more importantly, since it requires internal collisions, in the case when the underlying compression functions are double pipes, the attack complexity becomes higher than in a trivial attack.

Indeed, the standard boomerang attack can be used as a differential distinguisher for a compression function F. The idea is to start the attack in the middle of F and then go forward and backwards to obtain the quartets, thus escaping the feedforward. Let $F(H)$ be obtained from some invertible function $f(H)$ with a feedforward, for example Davies-Meyer mode $F(H) = f(H) \oplus H$. As in the attack on block ciphers, first step is to decompose f into two functions f_0, f_1 and to find two differential trails for f_0 and f_1 (further we use the same notation as in the attacks on block ciphers). We start with four states S_1, S_2, S_3, S_4 at the end of the function f_0 (beginning of f_1) such that $S_1 \oplus S_2 = S_3 \oplus S_4 = \Delta^*$ and $S_1 \oplus S_3 = S_2 \oplus S_4 = \nabla$. From these states we obtain the initial states (input chaining values) P_i and the final states (output chaining values without the feedforward) C_i, i.e. $P_i = f_0^{-1}(S_i), C_i = f_1(S_i), i = 1, \ldots, 4$. Then with probability at least p^2q^2 we have:

$$\begin{aligned} P_1 \oplus P_2 &= \Delta, & P_3 \oplus P_4 &= \Delta \\ C_1 \oplus C_3 &= \nabla^*, & C_2 \oplus C_4 &= \nabla^*. \end{aligned}$$

Extending the following attack to the whole compression function F is trivial – we just have to take into account that $C_i = f(P_i) = F(P_i) \oplus P_i$. For the boomerang quartet (P_1, P_2, P_3, P_4) we get:

$$P_1 \oplus P_2 = \Delta, \qquad P_3 \oplus P_4 = \Delta \tag{2}$$
$$[F(P_1) \oplus P_1] \oplus [F(P_3) \oplus P_3] = \nabla^*, \quad [F(P_2) \oplus P_2] \oplus [F(P_4) \oplus P_4] = \nabla^* \tag{3}$$

For a random n-bit compression function F, the complexity of finding the quartet (P_1, P_2, P_3, P_4) with the above relations (2),(3), is around[1] 2^n . Hence when $p^2q^2 > 2^{-n}$ one can launch a boomerang attack and thus obtain a distinguisher for F. The distinguisher becomes even more powerful if the attacker finds several boomerang quartets with the same differences Δ, ∇^*.

A zero-sum distinguisher, can be obtained based on the boomerangs. If in (3), we XOR the two equations, we get:

$$\begin{aligned} 0 =& [F(P_1) \oplus P_1] \oplus [F(P_3) \oplus P_3] \oplus \nabla^* \oplus [F(P_2) \oplus P_2] \oplus [F(P_4) \oplus P_4] \oplus \nabla^* = \\ =& F(P_1) \oplus F(P_2) \oplus F(P_3) \oplus F(P_4) \oplus (P_1 \oplus P_2) \oplus (P_3 \oplus P_4) = \\ =& F(P_1) \oplus F(P_2) \oplus F(P_3) \oplus F(P_4) \oplus \Delta \oplus \Delta = \\ =& F(P_1) \oplus F(P_2) \oplus F(P_3) \oplus F(P_4) \end{aligned}$$

Finding a zero-sum distinguisher for a random permutation requires $2^{n/4}$ encryptions. However, since we have the additional conditions on the plaintexts (the XORs of the pairs are fixed), the complexity rises to $2^{n/2}$.

It is important to notice that to produce the quartet (for the boomerang or the zero-sum boomerang) one has to start not necessarily from the middle states (S_1, S_2, S_3, S_4). For example, one can start from two input chaining values $(P_1, P_2) = (P_1, P_1 \oplus \Delta)$, produce the values $(S_1, S_2) = (f_0(P_1), f_0(P_2))$, then obtain the values for the two other middle states $(S_3, S_4) = (S_1 \oplus \nabla, S_2 \oplus \nabla)$, and finally get the two input chaining values $(P_3, P_4) = (f_0^{-1}(S_3), f_0^{-1}(S_4))$ and the four output chaining values $(f_1(S_1) \oplus P_1, f_1(S_2) \oplus P_2, f_1(S_3) \oplus P_3, f_1(S_4) \oplus P_4)$. Clearly, the probability of the boomerang stays the same. Starting from the beginning (or from some other particular state before the feedforward) can be beneficial in the cases when one wants to use message modification or wants to have some specific values in one of the four states (as shown further in the case of BLAKE-32).

4 Round-reduced Differential Trails in BLAKE-32

In order to obtain good differential trails in BLAKE we exploit the structure of the message word permutation. In fact we can easily obtain good 2-round differential trail. The idea is to choose a message word m_j such that

– It appears at Step 1(*Case1*) or at Step 5(*Case2*) in $\mathtt{G}_i (0 \leq i \leq 3)$ at round-r and

[1] This holds only when the difference between the messages is fixed as well. Otherwise, the complexity is only $2^{n/2}$.

– Also appears at Step 5 in $\mathtt{G}_i(4 \leq i \leq 7)$ at round-$(r+1)$.

If we choose the message word with the above mentioned strategy then with a suitable input difference we may pass 1.5 rounds for free[2] (i.e. with probability 1).

Observation 1 *A 2-round differential trail can be obtained in BLAKE-32 with probability* 2^{-1}.

Proof. Choose two rounds with a message word m_j as described previously. In

- *Case1*, we choose $\Delta m_j = \Delta a =$ `0x80000000`
- *Case2*, we choose $\Delta m_j = \Delta a = \Delta d =$ `0x80000000`

in the corresponding `G` function (see Fig. 2). After 1.5 rounds we get $\Delta v_k = 0, \forall k \in \{0, \ldots, 15\}$ with probability 1. In the next half of the second round because of our choice of message word and suitable difference, we get one active bit only at step 7 in the corresponding `G` function (see Fig. 3). Hence we get a differential trail with probability 2^{-1}.

Remark 1. In *Case1* if Δm_j and Δa have any active bits other than MSB then at round-r, probability of the trail is 2^{-t}(where t is the number of active bits in $\Delta m_j(=\Delta a)$ at round-r) and at round-$(r+1)$ the probability is 2^{-s}, where $s = 2t-1, 2t, 2t+1$(depending on the position of active bits). So in this case the probability for two rounds will be $1/2^{s+t}$. Also if m_j appears at Step 1 in $\mathtt{G}_i(4 \leq i \leq 7)$ at round-$(r+1)$ then probability of a 2-round differential trail decreases further.

Remark 2. In *Case1* if $\Delta m_j = \Delta a = \Delta$, such that Δ has two active bits at ith and $(i+16)$th position and m_j appears at step 1 in $\mathtt{G}_i(4 \leq i \leq 7)$ at round-$(r+1)$ then we have 2-round differential trail with probability $2^{-8-1}(=2^{-9})$ when ith bit is the MSB and $\geq 2^{-12-2}(=2^{-14})$ otherwise.

In order to construct 3-round trails from these 2-round differential trails we may simply add one more round at the beginning. The occurrence of the chosen message word in this one round does not affect much in terms of probability of the difference propagation.

Observation 2 *A 3-round differential trail may be obtained from the above described two round differential trail with probability* 2^{-s}*, where* $s = 6, 7$ *or* 8

Proof. After obtaining 2-round differential trail with probability 2^{-1}(*Case1*), we add one more round(say, round-$(r-1)$) at the beginning. The probability of this one round differential trail may vary depending on the position of the message word m_j. Suppose the message word occurs in $\mathtt{G}_l$ (for some index l) at round r. Then at round $r-1$:

[2] A similar technique was used in the analysis presented in [7, 1].

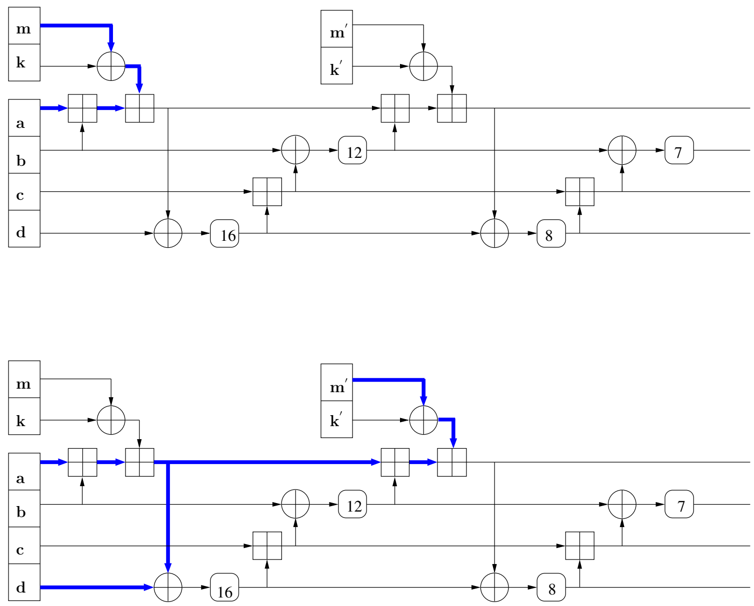

Fig. 2. Two possible differential trails for `G` at the beginning of 2-round trail. The top trail is *Case1*, while the bottom is *Case2*.

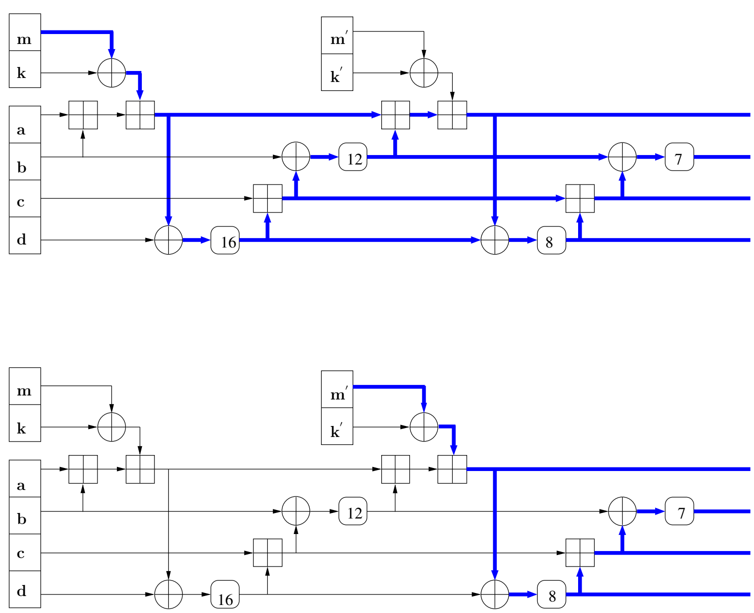

Fig. 3. Two possible differential trails for `G` at the end of 2-round trail. The top trail is when the message with the difference appears at Step 1, and the bottom at Step 5.

– If the message word is in $\mathtt{G}_i(0 \leq i \leq 3)$ or at step 1 of $\mathtt{G}_i(4 \leq i \leq 7)$, probability of this one round trail is 2^{-6}.
– If the message word occurs at step 5 of $\mathtt{G}_{l+4}$, we get differential trail with probability 2^{-5} for this one round.

For all other cases the probability of this one round differential trail is 2^{-7}. Hence we get a 3-round differential trail with probability 2^{-7},2^{-6} and 2^{-8} respectively.

Remark 3. This 3-round differential trail can be extended for half more round in the forward direction. If we add half round at the end of this three rounds and if the chosen message word does not occur there then we can get 3.5-round trail with probability $\geq 2^{-24-8}(= 2^{-32})$.

For this three round differential trail we have to inject two distinct input differences at v_{12} and v_{13} which correspond to the same counter t_0. In order to obtain a 3-round differential trail with consistent input differences at the states corresponding to the counters t_0 and t_1 we use a 2-round trail with lower probability.

Observation 3 *Let $\Delta a = \Delta c = \Delta$ such that Δ has only ith and $(i + 16)$th bits active. For a G function if there is no difference in the message words then the differential trail $(\Delta, 0, \Delta, 0) \rightarrow (\Delta, 0, 0, 0)$ occurs with probability 2^{-3} if ith bit is the MSB and with probability 2^{-6} otherwise.*

Observation 4 *A 3-round differential trail with input difference consistent with counters(t_0, t_1) may be obtained with probability 2^{-21} or at least 2^{-36}.*

Proof. Starting with $\Delta m_j = \Delta a = \Delta =$ `0x80008000` we obtain a 2-round differential trail with probability 2^{-9}(as described in *Remark 2*). Then we add one more round at the beginning. The position of the message word m_j in this one round determines which three rounds we should consider in order to obtain the 3-round trail. Such three rounds may be found if we start with round-4. Now in this one round(added at the beginning) we have two `G` functions with differences as described in *Observation 3* and one `G` function with difference $(\Delta_1, \Delta_2, \Delta, 0) \rightarrow (0, 0, \Delta, 0)$(with the message difference at step 5 in it). So probability for this one round is $2^{-6-6} = 2^{-12}$. Hence we get a 3-round trail with probability 2^{-21}. If Δ has two active bits (e.g. `0x00080008`) then probability of this one round at the beginning may be at least $2^{-12-10} = 2^{-22}$ and probability of the 2-round trail is at least 2^{-14}. Hence we get 3-round differential trail with probability at least 2^{-36}.

The choice of message word for the 3-round differential trail specified in *Observation 4* is available if we start with round-4 and the input differences for the states corresponding to the counters are $\Delta v_{12} = \Delta v_{13} = \Delta v_{14} = \Delta v_{15} = 0$.
A similar 2-round and 3-round differential trails exist for BLAKE-64.

5 Boomerang Attacks on the Compression Function of BLAKE-32

The high probability round-reduced differential trails in the permutation of BLAKE-32 can be used to attack the compression function and find boomerang distinguishers. However, due to the *Initialization* procedure, there are a few requirements on the trails. First, since the block index is copied twice, the initial differences in v_{12} and v_{13}, as well as the differences in v_{14} and v_{15}, have to be the same. Second, even in the case when the attacker has a trail with initial differences consistent to the above requirement, if he uses message modification techniques in the higher rounds of the trail, he might end up with inconsistent initial states. For example, if the attacker uses some k-round trail and starts fixing the values of the state and the messages at round k, and then goes backward, he can obtain two states with some predefined difference (as the one predicted by the trail). However, the probability that these two states are consistent with the *Initialization* procedure is 2^{-64} (if $v_{12} \oplus v_{13} = c_4 \oplus c_5$ and $v_{14} \oplus v_{15} = c_6 \oplus c_7$). Note that if one of the states is consistent, then the other one is consistent as well (if the attacker used trails with appropriate initial difference). Therefore, using message modification techniques in later steps of the trail is not trivial (without increasing the complexity of the attack). On the other hand, the modification can still be used at the beginning because the attacker starts with two states consistent with the *Initialization* procedure.

For the boomerang attack on 4 rounds of the compression function of BLAKE-32 we can use two trails each on 2 rounds (see Tbl. 2). Since the probability of these trails is only 2^{-1}, the probability of the boomerang is 2^{-4}. To create a quartet of states, consistent with the *Initialization* procedure, we start with a pair of states (P_1, P_2) that have a difference Δ (note that Δ does not have a difference in the "block index" words) and consistent with the *Initialization* words $v_{12}, v_{13}, v_{14}, v_{15}$ in both of the states, then go two rounds forward and obtain the pair (S_1, S_2). Then we produce the pair $(S_3, S_4) = (S_1 \oplus \nabla, S_2 \oplus \nabla)$ and go backwards two rounds to get the pair of initial states (P_3, P_4). The probability that P_3 (and therefore P_4) is consistent with the *Initialization* is 2^{-64}. Also, from S_1, S_2, S_3, S_4 we go forward two rounds, produce the outputs and apply the *Finalization* to get the new chaining values. Note that *Finalization* is linear, hence the differential trail (with XOR difference) holds with probability 1. Therefore, we can produce the boomerang quartet with a complexity of $4 \cdot 2^{4+64} = 2^{70}$ calls to the 4-round reduced compression function of BLAKE-32.

The boomerang attack on 5 rounds is rather similar. We only need one of the trails to be on 3 rounds, instead of 2 (see Tbl. 3). Such a trail has a probability of 2^{-7}, and we use two round trail with 2^{-3}, hence the boomerang has a probability of $2^{-2 \cdot 3 - 2 \cdot 7} = 2^{-20}$ and the whole attack (taking into account the *Initialization*) has a complexity of around $4 \cdot 2^{20+64} = 2^{86}$ compression function calls.

For the boomerang attack on 6 rounds we will use two 3-round trails (see Tbl. 4). However, we cannot use the optimal trails (the ones that hold with around 2^{-7}) because the starting difference in each such trail is inconsistent with the *Initialization* procedure. Therefore, for the top trail of the boomerang we will use a trail which has lower probability 2^{-34} but has no differences in any of the "block index" words $(v_{12}, v_{13}, v_{14}, v_{15})$. For the bottom trail we can use an optimal trail. The complexity of this boomerang distinguisher on 6 rounds becomes $4 \cdot 2^{2 \cdot 34 + 2 \cdot 7 + 64} = 2^{148}$ calls.

Note, for the top trails for 5 and 6 round boomerangs (see Tbl. 3,4), we did not use the best trails with probability 2^{-1}, 2^{-21}, but instead used trails with lower probability $(2^{-3}, 2^{-34})$. We found that if we use the best trails, then the boomerang does not work, most likely because of the slow diffusion. We cannot get four states in the middle (after the third round), that have pairwise Δ^* and ∇ difference (Δ^* is the end difference of the top trail). However, if we take other trails, as the ones we have taken, the boomerang quartet can be obtained – we confirmed this experimentally, by producing a boomerang quartet.

Each of the above attacks can be improved if we take into account the amplified probabilities for the boomerang attack and if we use message modification. We can obtain the amplified probabilities (and the total probabilities) of the boomerang experimentally: we start with a number of plaintext pairs with the required difference Δ, and then check how many of the returned (by the boomerang) differences are Δ. Also, in the first round, for one side of the boomerang we use message modification, i.e. we pass this round with probability 1. Using these two approaches, we got the following results: the boomerang on 4 rounds has a probability 2^{-1}, on 5 rounds $2^{-5.2}$, and on 6 rounds 2^{-36}. Hence, the attack complexity for 4 rounds drops to $4 \cdot 2^{1+64} = 2^{67}$, for 5 rounds to $4 \cdot 2^{5.2+64} = 2^{71.2}$, and for 6 rounds to $4 \cdot 2^{36+64} = 2^{102}$ compression function calls. An example of boomerang quartet for 6 rounds, with the first pair of plaintext consistent to the *Initialization*, while only the difference in the second is consistent, and therefore obtained with around $4 \cdot 2^{36}$ compression function calls, is given in Tbl. 9. The complexities of the boomerang distinguishers for 4,5, and 6 round are bellow 2^{128}, therefore they can be used as zero-sum boomerang distinguishers, i.e. $P_1 \oplus P_2 = P_3 \oplus P_4 = \Delta$ and $F(P_1) \oplus F(P_2) \oplus F(P_3) \oplus F(P_4) = 0$.

For the boomerang on 6.5 rounds, we use a top trail on 3 rounds (from 0.5 to 3.5) with 2^{-40}, and a bottom trail on 3.5 rounds (from 3.5 to 7), with 2^{-48} (see Tbl. 5). The complexity of producing the boomerang quartet is $4 \cdot 2^{2 \cdot 40 + 2 \cdot 48 + 64} = 2^{242}$ compression function calls. The probability of the first round in the top trail is 2^{-3}, hence using message modification does not lower significantly the attack complexity. However, computing the amplified probabilities can improve the attack. Obviously, we cannot do this experimentally, as the probability of the boomerang is too low – $2^{-2 \cdot 40 - 2 \cdot 48} = 2^{-176}$. Therefore, we cannot test for the whole 6.5 rounds, but we can do it for a reduced number of rounds. We tested for only half round at the end of the first trail (round 3 to round 3.5). We start with a pair of states with a difference specified by the top trail at round 3 and go half round forward to obtain a new pair of states. Then, to each element of the pair, we XOR the same difference (the one specified by the bottom trail at round 3.5), and produce a new pair states. Finally, we go backwards a half round, and check if the difference in the pair is at the one we have started with. Note that the half round can be split into four G functions, and for each of them the amplified probabilities can be found independently. By doing so, we found that the amplified probability for this half round of the boomerang is 2^{-26} instead of twice 2^{-33}, i.e. $2^{-2\cdot 33} = 2^{-66}$. Another low probability part of the boomerang is the top half round of the second trail – round 3.5 to round 4 holds with 2^{-41}. In this part we can use message modification. We start at round 3.5 with four states that have pairwise differences Δ^* and ∇. We go half round forward and obtain four states with pairwise differences as specified by the bottom trail at round 4. To obtain such states we need $4 \cdot 2^{2\cdot 41} = 2^{84}$. Once we have this half round boomerang, we can freely change the message words that are not taken as inputs in this half round without altering the input and the output values of the half round. Hence, we have $2^{8\cdot 32} = 2^{256}$ degrees of freedom. From the middle states we can obtain the initial and final states (and the chaining values). Therefore, the total complexity of the boomerang on 6.5 rounds becomes $2^{84} + 4 \cdot 2^{2\cdot(3+1+3)+26+2\cdot(6+1)+128} = 2^{184}$ calls. Note that unlike as in the case of the boomerangs on 4 and 5 rounds, now the probability that the initial states are consistent to the *Initialization*is 2^{-128} because we use message modification in the middle rather than in the beginning. The bottom trail can easily be extended for additional half round (see Tbl. 5) with probability 2^{-24}. Therefore, the boomerang on 7 rounds requires around $2^{184+2\cdot 24} = 2^{232}$ compression function calls.

6 Boomerang Attacks on the Keyed Permutation of BLAKE-32

Further we present boomerang attacks on the keyed permutation of BLAKE-32, assuming that the key is unknown to the attacker. These attacks can be seen as distinguishers for the internal cipher of BLAKE-32. The cipher takes 512-bit plaintexts and 512-bit key, and after 10 rounds, outputs 512-bit ciphertext (we discard the *Initialization*and *Finalization* procedures).

Switching from the boomerangs for the compression function to the boomerangs for the keyed permutation has advantages and disadvantages for the attacker. On one hand, the attacker is not concern any more about the *Initialization* procedure, and he can use any trails for the boomerang. On the other hand, since the key is unknown, he cannot use message modification techniques to improve the probability of the boomerang.

The boomerangs on 4 and 5 rounds of the keyed permutation of BLAKE-32 have the same probability as in the case of compression function: 2^{-4} for 4 rounds, and 2^{-20} for 5 rounds. For 6 rounds, we can use two high probability trails ($2^{-7}, 2^{-7}$, see Tbl. 6), and therefore, the probability of the boomerang is 2^{-28}. If we take into account the amplified probabilities, and fix the returning difference only in 128 bits (the words v_1, v_5, v_9, v_{13}) instead of in 512 bits, for the total complexity of the boomerang attack we get 2^3 encryptions for 4 rounds, $2^{7.2}$ for 5 rounds, and $2^{11.75}$ for 6 rounds. These results were confirmed on a PC and a boomerang quartet for 6 rounds is presented in Tbl. 8.

The boomerangs for 7 and 8 rounds, are rather similar: for 7 rounds we use two trails on 3.5 rounds (the first from round 2 to round 5.5, and the second from round 5.5 to round 9), and for 8 rounds, we just extend these trails for additional half round (see Tbl. 7). The complexity of the boomerangs is $4 \cdot 2^{2\cdot 31+2\cdot 52} = 2^{168}$ for 7 rounds and $4 \cdot 2^{2\cdot 73+2\cdot 82} = 2^{312}$ for 8 rounds. Again, as in the case of 6.5-round boomerang on the compression function, we can compute experimentally the lower bounds on the amplified probabilities, by testing only the probability of the first half round of the bottom trail. We get 2^{-48} instead of $2^{-2\cdot 44}$. Also, we can fix the returning difference only in 256 bits, instead of 512 bits, and thus increase the probability in the first half round of the top trail by a factor of 2^{-6} for 7 rounds, and 2^{-30} for 8 rounds. Hence, the boomerang on 7 rounds requires at most 2^{122}, and on 8 rounds at most 2^{242} encryptions.

7 Conclusions

In this paper we have shown how to apply the concept of boomerang distinguisher to compression functions, and presented such distinguishers for the compression function of BLAKE-32, as well as classical boomerang distinguishers for the keyed permutation of BLAKE-32. Our attacks work on up to 2/3 of the total number of rounds of the compression function, and on up to 4/5 (the attacks on up to 3/5 have practical complexity) of the total number of rounds of the keyed permutation of BLAKE-32. The attacks can be equally well applied to the other versions of BLAKE. Our attacks do not contradict the security claims of BLAKE.

Interestingly, tweaking the message permutation in BLAKE can reduce the number of attacked rounds only by one. Therefore, either tweaks in the function G or more advanced message expansion is required in order to significantly reduce the number of attacked rounds.

References

1. J.-P. Aumasson, J. Guo, S. Knellwolf, K. Matusiewicz, and W. Meier. Differential and invertibility properties of BLAKE. In S. Hong and T. Iwata, editors, *FSE*, volume 6147 of *Lecture Notes in Computer Science*, pages 318–332. Springer, 2010.
2. J.-P. Aumasson, L. Henzen, W. Meier, and R. C.-W. Phan. SHA-3 proposal BLAKE. Submission to NIST, 2008.
3. L. Ji and X. Liangyu. Attacks on round-reduced BLAKE. Cryptology ePrint Archive, Report 2009/238, 2009. Avalaible at `http://eprint.iacr.org/2009/238.pdf`.
4. A. Joux and T. Peyrin. Hash functions and the (amplified) boomerang attack. In A. Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 244–263. Springer, 2007.
5. J. Kelsey, T. Kohno, and B. Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In B. Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, pages 75–93. Springer, 2000.

6. National Institute of Standards and Technology. Cryptographic hash algorithm competition. `http://csrc.nist.gov/groups/ST/hash/sha-3/index.html`.
7. B. Su, W. Wu, S. Wu, and L. Dong. Near-collisions on the reduced-round compression functions of Skein and BLAKE. Cryptology ePrint Archive, Report 2010/355, 2010. Avalaible at `http://eprint.iacr.org/2010/355.pdf`.
8. D. Wagner. The boomerang attack. In L. R. Knudsen, editor, *FSE*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.

A Differential Trails for the Boomerangs

Table 2. Differential trails used in the Boomerang Attack on 4 rounds of BLAKE-32. On the left is the top trail, while on the right is the bottom trail of the boomerang. ΔM is the message difference, while ΔV_i are the differences in the state. In the left trail (top trail), ΔV_0 is the starting difference of the trail, i.e. $\Delta V_0 = \Delta$, and ΔV_2 is the ending difference, i.e. $\Delta V_2 = \Delta^*$. In the right trail (bottom trail), ΔV_2 is the starting difference of the trail, i.e. $\Delta V_2 = \nabla$, and ΔV_4 is the ending difference, i.e. $\Delta V_4 = \nabla^*$. The numbers 0,1,2, and 2,3,4, indicate the rounds covered by the boomerang – the top trail starts at round 0 and ends after round 1, while the bottom trail starts at round 2 and ends after round 3.

	Δm		Δm
	00000000 00000000 80000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		80000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
R.	ΔV_i	*R.*	ΔV_i
0	00000000 80000000 00000000 00000000	2	80000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		80000000 00000000 00000000 00000000
	1		1
1	00000000 00000000 00000000 00000000	3	00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	2^{-1}		2^{-1}
2	00000000 80000000 00000000 00000000	4	00000000 00000000 00000000 80000000
	00000000 00000000 00010000 00000000		00010000 00000000 00000000 00000000
	00000000 00000000 00000000 00800000		00000000 00800000 00000000 00000000
	00800000 00000000 00000000 00000000		00000000 00000000 00800000 00000000

Table 3. Differential trails used in the Boomerang Attack on 5 rounds of BLAKE-32.

	Δm		Δm
	00000000 00000000 40000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 80000000 00000000 00000000
R.	ΔV_i	*R.*	ΔV_i
0	00000000 40000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000	2	00000800 80008000 80000000 80000000 80000800 80008000 00000000 00000000 80000000 80808080 80000000 00000000 80000000 00800080 80008000 80000000
	2^{-1}		2^{-6}
1	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000	3	00000000 00000000 80000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	2^{-2}		1
2	00000000 40000000 00000000 00000000 00000000 00000000 00008000 00000000 00000000 00000000 00000000 00400000 00400000 00000000 00000000 00000000	4	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
			2^{-1}
		5	00000000 00000000 00000000 80000000 00010000 00000000 00000000 00000000 00000000 00800000 00000000 00000000 00000000 00000000 00800000 00000000

Table 4. Differential trails used in the Boomerang Attack on 6 rounds of CF of BLAKE-32.

	Δm		Δm
	00080008 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 80000000 00000000
R.	ΔV_i	*R.*	ΔV_i
4	80088008 00000000 00080008 00000000 80088008 00000000 00000000 00000000 00080008 00000000 00080008 00000000 00000000 00000000 00000000 00000000	7	80008000 00000000 00000000 00000800 80008000 00000000 00000000 80000800 80808080 80000000 00000000 80000000 00800080 00008000 00000000 80000000
	2^{-21}		2^{-6}
5	00000000 00000000 00080008 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000	8	00000000 80000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	2^{-2}		1
6	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000	9	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	2^{-11}		2^{-1}
7	00880088 00000000 00000000 00000000 00000000 11011101 00000000 00000000 00000000 00000000 80088008 00000000 00000000 00000000 00000000 80008000		00000000 80000000 00000000 00000000 00000000 00000000 00010000 00000000 00000000 00000000 00000000 00800000 00800000 00000000 00000000 00000000

Table 5. Differential trails used in the Boomerang Attack on 6.5 and 7 rounds of CF of BLAKE-32.

	Δm		Δm
	00000000 00000000 00000000 00000000 80008000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000		00000000 00000000 80000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
$R.$	ΔV_i	$R.$	ΔV_i
0.5	00000000 80008000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 80008000 00000000 00000000 00000000 00000000	3.5	00800880 c8088848 80440044 00008000 80000000 80800880 488c0888 80040804 00000800 00008080 80808080 00000000 80048040 08408840 00800000 80000000
	2^{-3}		2^{-41}
1	00000000 80008000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000	4	80000000 00000000 80000800 80008000 00000000 00000000 80000800 80008000 80000000 00000000 80000000 80808080 80008000 00000000 80000000 00800080
	2^{-1}		2^{-6}
2	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000	5	80000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	2^{-3}		1
3	00000000 00000000 00000000 80008000 00010001 00000000 00000000 00000000 00000000 00800080 00000000 00000000 00000000 00000000 00800080 00000000	6	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	2^{-33}		2^{-1}
3.5	00010001 08000800 08000800 80088008 02000200 10111011 11111111 11101110 00010001 00880088 80888088 88008800 00000000 00080008 80088008 08000800	7	00000000 00000000 80000000 00000000 00000000 00000000 00000000 00010000 00800000 00000000 00000000 00000000 00000000 00800000 00000000 00000000
			2^{-24}
		7.5	00000800 08000000 80000008 00110010 10010010 01101001 10110101 22222022 00800008 80080080 08808080 11001101 00000008 80080000 08800080 11001100

Table 6. Differential trails used in the Boomerang Attack on 6 rounds of KP of BLAKE-32.

	Δm		Δm
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	80000000 00000000 00000000 00000000		00000000 80000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
R.	ΔV_i	*R.*	ΔV_i
0	80008000 80000000 80000000 00000800	3	80008000 00000000 00000000 00000800
	80008000 00000000 00000000 80000800		80008000 00000000 00000000 80000800
	80808080 80000000 00000000 80000000		80808080 00000000 00000000 80000000
	00800080 80008000 00000000 80000000		00800080 00000000 00000000 80000000
	2^{-6}		2^{-6}
1	00000000 80000000 00000000 00000000	4	00000000 80000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	1		1
2	00000000 00000000 00000000 00000000	5	00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	00000000 00000000 00000000 00000000		00000000 00000000 00000000 00000000
	2^{-1}		2^{-1}
3	00000000 00000000 00000000 80000000	6	00000000 80000000 00000000 00000000
	00010000 00000000 00000000 00000000		00000000 00000000 00001000 00000000
	00000000 00800000 00000000 00000000		00000000 00000000 00000000 00800000
	00000000 00000000 00800000 00000000		00800000 00000000 00000000 00000000

Table 7. Differential trails used in the Boomerang Attack on 7 and 8 rounds of KP of BLAKE-32.

	Δm		Δm
	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 80000000 00000000 00000000		00000000 00000000 00000000 00000000 00000000 00000000 00000000 80000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
R.	ΔV_i	*R.*	ΔV_i
1.5	80440044 00008000 80800880 48088848 488c0888 00040804 80000000 80800880 80808080 80000000 00000880 00008080 00800000 80000000 00040040 88c00840	5.5	80808000 80888080 c80c8008 80440044 80040804 80800000 80888000 c8880088 80000000 00000800 00808080 80000080 00800000 00048000 08408840 80800000
	2^{-42}		2^{-44}
2	00000800 80008000 80000000 80000000 80000800 80008000 00000000 00000000 80000000 80808080 80000000 00000000 80000000 00800080 80008000 80000000	6	00008000 80000000 00000000 80000800 80008000 00000000 00000000 00000800 00808080 80000000 00000000 00000080 80808080 80008000 00000000 80800000
	2^{-6}		2^{-7}
3	00000000 00000000 80000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000	7	00000000 80000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	1		1
4	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000	8	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	2^{-1}		2^{-1}
5	00000000 00000000 00000000 80000000 00010000 00000000 00000000 00000000 00000000 00800000 00000000 00000000 00000000 00000000 00800000 00000000	9	00000000 80000000 00000000 00000000 00000000 00000000 00010000 00000000 00000000 00000000 00000000 00800000 00800000 00000000 00000000 00000000
	2^{-24}		2^{-30}
5.5	00110010 00000800 08000000 80000008 22222022 10010010 01101001 10110101 11001101 00800008 80080080 08808080 11001100 00000008 80080000 08800080	9.5	08000000 80000008 80110018 00000800 01101001 10110101 32332123 10010010 80080080 08808080 19809181 00800008 80080000 08800080 19801180 00000008

B Examples of Boomerang quartets

Table 8. Example of a boomerang quartet for 6 round-reduced keyed permutation of BLAKE-32.

P_1	7d8a1f02	206849ad	42413a50	d702fa14	facc9c67	11306e7c	eba852eb	4f31f62f
	993e3958	bc426fcc	55033261	b2ac26a9	6dfc2edd	32163c44	ef989577	2d6d6bb4
P_2	fd8a9f02	a06849ad	c2413a50	d702f214	7acc1c67	11306e7c	eba852eb	cf31fe2f
	19beb9d8	3c426fcc	55033261	32ac26a9	6d7c2e5d	b216bc44	ef989577	ad6d6bb4
P_3	de971194	ae012c6a	4422f8ea	fff2d41b	80a79b50	b1d61b36	fe8c23fe	a883faf9
	e1dab487	e4971af1	51dbf40b	6e32fb27	7c797796	19b156e9	16e0ac52	a12eefcb
P_4	5e979194	2e012c6a	c422f8ea	fff2dc1b	00a71b50	b1d61b36	fe8c23fe	2883f2f9
	615a3407	64971af1	51dbf40b	ee32fb27	7cf97716	99b1d6e9	16e0ac52	212eefcb
$P_1 \oplus P_2$	80008000	80000000	80000000	00000800	80008000	00000000	00000000	80000800
	80808080	80000000	00000000	80000000	00800080	80008000	00000000	80000000
$P_3 \oplus P_4$	80008000	80000000	80000000	00000800	80008000	00000000	00000000	80000800
	80808080	80000000	00000000	80000000	00800080	80008000	00000000	80000000
M_1	a0a28e67	1fd77849	83d86d19	4a72bc82	3704f04d	bb57c994	37612239	0f7ad68a
	df14386d	4e2e05c7	55d1a87f	187d8225	fcc527c5	96071c3e	4ae251d8	52de23f2
M_2	a0a28e67	1fd77849	83d86d19	4a72bc82	b704f04d	bb57c994	37612239	0f7ad68a
	df14386d	4e2e05c7	55d1a87f	187d8225	fcc527c5	96071c3e	4ae251d8	52de23f2
M_3	a0a28e67	1fd77849	83d86d19	4a72bc82	3704f04d	3b57c994	37612239	0f7ad68a
	df14386d	4e2e05c7	55d1a87f	187d8225	fcc527c5	96071c3e	4ae251d8	52de23f2
M_4	a0a28e67	1fd77849	83d86d19	4a72bc82	b704f04d	3b57c994	37612239	0f7ad68a
	df14386d	4e2e05c7	55d1a87f	187d8225	fcc527c5	96071c3e	4ae251d8	52de23f2
$M_1 \oplus M_2$	00000000	00000000	00000000	00000000	80000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
$M_1 \oplus M_3$	00000000	00000000	00000000	00000000	00000000	80000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
$M_2 \oplus M_4$	00000000	00000000	00000000	00000000	00000000	80000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
C_1	928c1f77	3aa097f2	4d5589bb	f307e618	c8ea4ebc	c63769df	64e2b7ba	f2c76b2b
	c909808a	672bcdf3	260608d6	7de7ba36	749c4e7d	aef2defd	b7d3318a	5080389e
C_2	9948791c	21c19a0f	8804efac	d56588e4	c6f6b101	32456224	20c423d5	df0105fe
	33ee8883	23bde21d	bedb2451	2c673c2f	bf7d194d	cfc78321	5ec259f9	a9c8786b
C_3	928c1f77	baa097f2	4d5589bb	f307e618	c8ea4ebc	c63769df	64e3b7ba	f2c76b2b
	c909808a	672bcdf3	260608d6	7d67ba36	741c4e7d	aef2defd	b7d3318a	5080389e
C_4	9948791c	a1c19a0f	8804efac	d56588e4	c6f6b101	32456224	20c523d5	df0105fe
	33ee8883	23bde21d	bedb2451	2ce73c2f	bffd194d	cfc78321	5ec259f9	a9c8786b
$C_1 \oplus C_3$	00000000	80000000	00000000	00000000	00000000	00000000	00010000	00000000
	00000000	00000000	00000000	00800000	00800000	00000000	00000000	00000000
$C_2 \oplus C_4$	00000000	80000000	00000000	00000000	00000000	00000000	00010000	00000000
	00000000	00000000	00000000	00800000	00800000	00000000	00000000	00000000

Table 9. Example of a boomerang quartet for 6 round-reduced compression function of BLAKE-32. Note that the initial states P_1, P_2 are consistent with the *Initialization*.

P_1	30841585	41abc330	447466d0	17ae8472	b94fc56d	e9cb678a	1d9d6e9e	eb558123
	66d322c2	23cbae19	52e9bb2a	dd6b8f2b	ea1cd197	678ad865	6594bdd4	81f42bc5
P_2	b08c958d	41abc330	447c66d8	17ae8472	39474565	e9cb678a	1d9d6e9e	eb558123
	66db22ca	23cbae19	52e1bb22	dd6b8f2b	ea1cd197	678ad865	6594bdd4	81f42bc5
P_3	f3383666	710fc071	1990f347	34475dd7	7d41ddc9	68e231ed	ea9bba79	a4990860
	d7ede8b5	f1c0b054	1c754989	a0e95ceb	3d259f5f	878bffae	f511b0fd	def26a26
P_4	7330b66e	710fc071	1998f34f	34475dd7	fd495dc1	68e231ed	ea9bba79	a4990860
	d7e5e8bd	f1c0b054	1c7d4981	a0e95ceb	3d259f5f	878bffae	f511b0fd	def26a26
$P_1 \oplus P_2$	80088008	00000000	00080008	00000000	80088008	00000000	00000000	00000000
	00080008	00000000	00080008	00000000	00000000	00000000	00000000	00000000
$P_3 \oplus P_4$	80088008	00000000	00080008	00000000	80088008	00000000	00000000	00000000
	00080008	00000000	00080008	00000000	00000000	00000000	00000000	00000000
M_1	7670ae70	c6539713	373c66b6	3d4522c3	b66689d0	37ee4f5d	467de620	9aabd357
	b6b3b13c	c6d41a4c	cb994b4c	b79e16fa	8a9d8079	9914ccb1	9c68b051	86d41e1e
M_2	7678ae78	c6539713	373c66b6	3d4522c3	b66689d0	37ee4f5d	467de620	9aabd357
	b6b3b13c	c6d41a4c	cb994b4c	b79e16fa	8a9d8079	9914ccb1	9c68b051	86d41e1e
M_3	7670ae70	c6539713	373c66b6	3d4522c3	b66689d0	37ee4f5d	467de620	9aabd357
	b6b3b13c	c6d41a4c	cb994b4c	b79e16fa	8a9d8079	9914ccb1	1c68b051	86d41e1e
M_4	7678ae78	c6539713	373c66b6	3d4522c3	b66689d0	37ee4f5d	467de620	9aabd357
	b6b3b13c	c6d41a4c	cb994b4c	b79e16fa	8a9d8079	9914ccb1	1c68b051	86d41e1e
$M_1 \oplus M_2$	00080008	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
$M_1 \oplus M_3$	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	80000000	00000000
$M_2 \oplus M_4$	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	80000000	00000000
C_1	3f432ef6	5f89fb80	7283d8cf	13731945	344d16f8	2203b3b5	74b3637e	52ed9169
	efcea8db	32b84ffc	57cfa772	2258156c	22696ef4	53cb7ac6	3ab6294a	ce58038c
C_2	f284e034	f866e60d	1e52775f	f6f764cb	ef09e2e8	da83b2d1	a4a869d1	f22eefb0
	821c38c2	6da245e0	7b52665c	0f8ce3ba	7ed4c20c	ef76217d	77835c6d	184a17e3
C_3	3f432ef6	df89fb80	7283d8cf	13731945	344d16f8	2203b3b5	74b2637e	52ed9169
	efcea8db	32b84ffc	57cfa772	22d8156c	22e96ef4	53cb7ac6	3ab6294a	ce58038c
C_4	f284e034	7866e60d	1e52775f	f6f764cb	ef09e2e8	da83b2d1	a4a969d1	f22eefb0
	821c38c2	6da245e0	7b52665c	0f0ce3ba	7e54c20c	ef76217d	77835c6d	184a17e3
$C_1 \oplus C_3$	00000000	80000000	00000000	00000000	00000000	00000000	00010000	00000000
	00000000	00000000	00000000	00800000	00800000	00000000	00000000	00000000
$C_2 \oplus C_4$	00000000	80000000	00000000	00000000	00000000	00000000	00010000	00000000
	00000000	00000000	00000000	00800000	00800000	00000000	00000000	00000000