On the Security of the Encryption Mode of Tiger

Ali Doğanaksoy, Onur Özen, Kerem Varıcı

Institute of Applied Mathematics,
Middle East Technical University, Ankara, Turkey,
aldoks, e127740, e127761@metu.edu.tr

Abstract. Tiger is an important type of an hash function that is proved to be secure so far as there is no known collision attack on the full Tiger. It is designed by Biham and Anderson in 1995 to be very fast on modern computers, and in particular on the 64-bit computers, while it is still not slower than other suggested hash functions on 32-bit machines. In this paper, we will investigate the security notion of reduced round Tiger against the very well known and the efficient block cipher attacks, namely related-key boomerang and the related-key rectangle attacks.

1 Introduction

Hash functions are one of the key primitives of the cryptographic algorithms that are used for many important applications such as data integrity, authentication, digital signature etc. every day. Many of the digital transactions and the e-cash applications are performed by effective hash functions. Thus, hash functions need to be secure and effective at the same time so as to meet the everyday's life needs. Moreover, the increasing attention on the security of the dedicated hash functions motivated us to work on this paper.

Several cryptanalytic articles [1] [2] were published to find collisions for very well known hash functions. Especially the attacks proposed by Wang et.al [3] [4][5] are very important attacks and many of the dedicated and widely used hash functions, such as members of MD and SHA families, were broken by the method proposed by Wang et.al.

Tiger is an important type of an hash function that is proved to be secure so far as there is no known collision attack on the full Tiger. It is designed by Biham and Anderson in 1995 to be very fast on modern computers, and in particular on the 64-bit computers, while it is still not slower than other suggested hash functions on 32-bit machines. In this paper, we will investigate the security notion of Tiger against the very well known and the efficient block cipher attacks, namely related-key boomerang and the related-key rectangle attack. We run the Tiger as a block cipher omitting the hash modes and imposing the encryption mode.

There have been several cryptanalysis papers investigating the randomness properties of the designed hash functions under the encryption mode such as [6] by Kim et.al. In that paper, related-key boomerang and related-key rectangle attacks are performed on $MD4$,$MD5$ and $HAVAL$ under 2, 4 or weak keys. Moreover, there have been very important attacks[7][8][9] on $SHACAL$ as well which is based on SHA. As in these papers, we will investigate the security of Tiger's encryption mode.

The organization of the paper is as follows. In section two, we briefly introduce the necessary parts of Tiger. In section three, the related-key boomerang and the related-key rectangle attacks are mentioned together with the boomerang attack and the rectangle attacks. In section four and five, the attack on the encryption mode of the Tiger is detailed and section six briefly concludes the paper.

2 Tiger

Tiger[10] is a hash function which is designed for 64-bit processors by Biham and Anderson. It uses 64-bit additions, subtractions, multiplications by small constants (5, 7 and 9), shifts, S-box applications and logical operations such as XOR and NOT. The main operation of Tiger is S-box application part. There exist four S-boxes in Tiger where each takes 8-bit input and gives 64-bit output operating on the even and the odd bytes of the input. The size of the hash value and the intermediate state length are 192-bit, three 64-bit words. The message block is 512-bit, eight 64-bit words.

The hashing operation of Tiger is similar to block ciphers. It has three 8-round encryption part where one constant value is used in each as multiplication value and between these parts it also uses key scheduling for the message expansion. After 24 rounds there exists also $feedforward$ part in which the updated values are combined with their initial values.

2.1 Notation

Three 64-bit words that will be used in the intermediate state are called as A, B, C. Each 64-bit message words obtained from 512-bit message block are named as X_0, X_1, …, X_7. Four 8×64 bit S-boxes are defined as t_1, t_2, t_3 and t_4. $c[i]$ denotes the ith byte of c. Addition, subtraction, multiplication signs are all used for 64-bit operations and ith round input values are denoted as A_i, B_i, C_i where $i \in \{1, \ldots, 24\}$, ith round message block is $X_{i \ mod \ 8}$ and ith round output values are A_{i+1}, B_{i+1}, C_{i+1}

2.2 The Round Function of Tiger

A, B, C are updated in this part as:

$$
\begin{aligned}
A &:= A - even(C) \\
B &:= (B + odd(C)) \ \times \ const \\
C &:= C \oplus X_i
\end{aligned}
$$

where $const \in \{5, 7, 9\}$ and after modification part, the results are shifted around and A, B, C become B, C, A. The functions *even* and *odd* are defined as:

$$even(C) := t_1(C[0]) \oplus t_2(C[2]) \oplus t_3(C[4]) \oplus t_4(C[6])$$
$$odd(C) := t_1(C[7]) \oplus t_2(C[5]) \oplus t_3(C[3]) \oplus t_4(C[1])$$

Before the beginning of the second 8-round pass, intermediate values A, B, C are updated as C_9, A_9, B_9. Before the beginning of the last 8-round pass again intermediate values are updated and they are assigned to B_{17}, C_{17}, A_{17}.

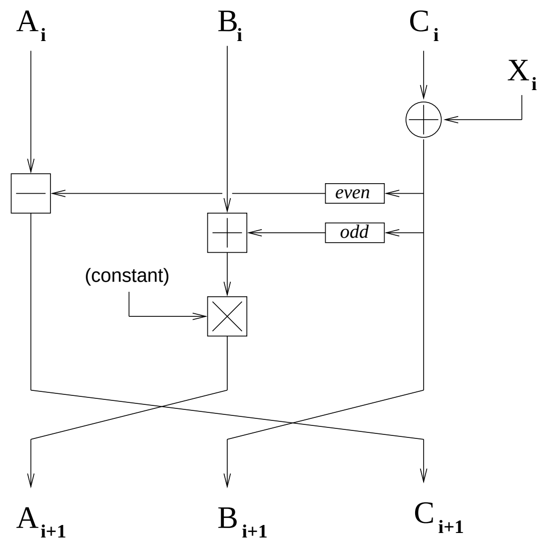

Fig. 1. The i^{th} Round of Tiger

The block cipher mode of Tiger is straightforward. First of all, the chaining operations of the intermediate values are omitted and Tiger is treated as a block cipher encrypting 192-bit plaintext into 192-bit ciphertext using 512-bit secret key. There is no need to invert the *odd* and the *even* function since their inverses do not affect the decryption mode. In the decryption mode, we just use the inverses of the binary operations that can be defined very easily except for the division $mod\ 2^{64}$. However, as we divide any number $mod\ 2^{64}$, this division operation is well defined. Thus, besides the encryption function, the decryption function is well defined.

2.3 The Key Schedule of Tiger

The key scheduling algorithm of Tiger uses some logical operators together with the XOR, addition, subtraction, and shift. 512-bit key is expanded in key schedule part as:

$$
\begin{aligned}
&X_0 := X_0 - (X_7 \oplus 0xA5A5A5A5A5A5A5A5)\\
&X_1 := X_1 \oplus X_0\\
&X_2 := X_2 + X_1\\
&X_3 := X_3 - (X_2 \oplus (\overline{X_1} << 19))\\
&X_4 := X_4 \oplus X_3\\
&X_5 := X_5 + X_4\\
&X_6 := X_6 - (X_5 \oplus (\overline{X_4} >> 23))\\
&X_7 := X_7 \oplus X_6\\
&X_0 := X_0 + X_7\\
&X_1 := X_1 - (X_0 \oplus (\overline{X_7} << 19))\\
&X_2 := X_2 \oplus X_1\\
&X_3 := X_3 + X_2\\
&X_4 := X_4 - (X_3 \oplus (\overline{X_2} >> 23))\\
&X_5 := X_5 \oplus X_4\\
&X_6 := X_6 + X_5\\
&X_7 := X_7 - (X_6 \oplus 0x0123456789ABCDEF)
\end{aligned}
$$

where $\overline{X_i}$ denotes bit-wise NOT function, $+$ and $-$ denotes modulo 2^{64} addition and subtraction and $<<$ (resp. $>>$) shows the right (resp. left) shifts operations.

3 Related-Key Boomerang and Rectangle Attacks

The related-key boomerang and the rectangle attacks are some kind of combined attacks that are introduced independently by Kim et.al[7] and Dunkelman et.al[11]. Nowadays, they are the most effective and powerful block cipher attacks that are applied to many known ciphers[12]. In the following subsections, we will briefly introduce these attacks together with their primitives, namely the pure boomerang and the rectangle attack.

3.1 The Boomerang and the Related-Key Boomerang Attack

The Boomerang Attack may be seen as the refinement or the effective use of the pure differential cryptanalysis. After the application of differential-linear cryptanalysis, the boomerang attack can also be called as differential-differential cryptanalysis. In the boomerang process, instead of using one long-ineffective (low probability) differential, the attacker may use two short-high probability differentials to increase the number of rounds attacked and the probability of the differential. The disadvantage of the boomerang attack is its adaptively chosen plaintext-ciphertext nature. Besides the encryption box of the attacked cipher, it is assumed to have the decryption box.

For the sake of simplicity, we will use the same notation as in[11]. Boomerang distinguisher treats the attacked cipher E as a cascade of two sub-ciphers E_0 and E_1, i.e. $E = E_1 \ o \ E_0$. As mentioned above, two short-high probability differentials are used, one for E_0 and one for E_1, in order to increase the probability of the distinguisher. Let $\alpha \to \beta$ with probability p be the first differential used for E_0 and $\gamma \to \delta$ with probability q be the second differential used for E_1. Notice that, once the differential is chosen in one direction, the same differential holds for the opposite direction. Namely, the differentials $\beta \to \alpha$ for E_0^{-1} and $\delta \to \gamma$ for E_1^{-1} hold with probabilities p and q respectively. The key step in the boomerang distinguisher is to combine these two differentials.The boomerang distinguisher works as follows:

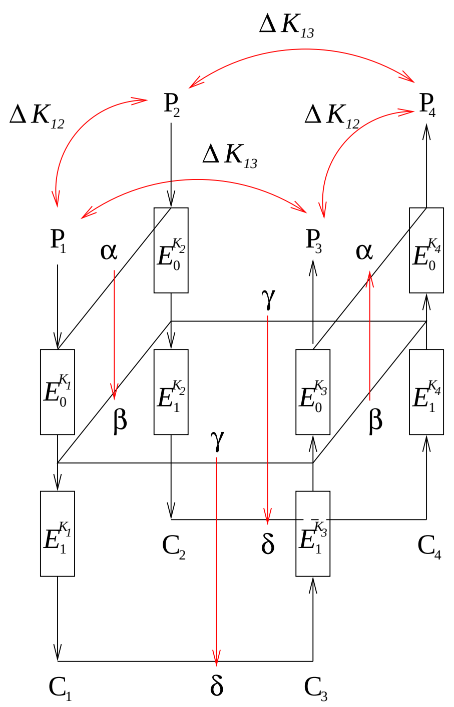

Fig. 2. Related-Key Boomerang Distinguisher Based on Four Related Keys

- Take a randomly chosen plaintext P_1 and form $P_2 = P_1 \oplus \alpha$.
- Obtain the corresponding ciphertexts $C_1 = E(P_1)$ and $C_2 = E(P_2)$ through E.
- Form the second ciphertext pair by $C_3 = C_1 \oplus \delta$ and $C_4 = C_2 \oplus \delta$.
- Obtain the corresponding plaintexts $P_3 = E^{-1}(C_3)$ and $P_4 = E^{-1}(C_4)$ through E^{-1}.
- Check $P_3 \oplus P_4 = \alpha$.

After the first step of the above algorithm, the probabilistic arguments take place. While obtaining C_1 and C_2, we assume the differential $\alpha \to \beta$ holds with probability p for E_0 once. We do not have any arguments about E_1 yet. Then, after the third step, through the decryption process we assume the differential $\delta \rightarrow \gamma$ holds with probability q for E_1^{-1} twice as we go backwards twice, once for each of the pairs (C_1, C_3) and (C_2, C_4). The crucial step of the boomerang distinguisher comes to the picture here when we are going backwards. Once we get $E_1^{-1}(C_3) \oplus E_1^{-1}(C_4) = \beta$, we are almost done as we know $E_0^{-1}(E_1^{-1}(C_3)) \oplus E_0^{-1}(E_1^{-1}(C_4)) = P_3 \oplus P_4 = \alpha$ holds with probability p. Now, it is time to explain how this is obtained.

$$
\begin{aligned}
&E_1^{-1}(C_3) \oplus E_1^{-1}(C_4) = \\
&E_1^{-1}(C_3) \oplus E_1^{-1}(C_4) \oplus E_1^{-1}(C_1) \oplus E_1^{-1}(C_1) \oplus E_1^{-1}(C_2) \oplus E_1^{-1}(C_2) = \\
&E_1^{-1}(C_1) \oplus E_1^{-1}(C_3) \oplus E_1^{-1}(C_2) \oplus E_1^{-1}(C_4) \oplus E_1^{-1}(C_1) \oplus E_1^{-1}(C_2) = \\
&\qquad \gamma \oplus \gamma \oplus E_1^{-1}(C_1) \oplus E_1^{-1}(C_2) = E_0(P_1) \oplus E_0(P_2) = \beta
\end{aligned}
$$

Therefore, the boomerang distinguisher works with probability p^2q^2. On the other hand, for a random permutation, the last step of the above argument holds with probability 2^{-n} where n is the number of the bits of each plaintext P. Thus, $pq > 2^{-n/2}$ must hold for the boomerang distinguisher. The attack can be improved by using all β and all γ values at the same time. Further details are given in[11]. This time the probabilities are denoted as $\hat{p}$ and $\hat{q}$ for E_0 and E_1 respectively, where $\hat{p} = \sqrt{\sum_\beta Pr^2(\alpha \rightarrow \beta)}$ and $\hat{q} = \sqrt{\sum_\gamma Pr^2(\gamma \rightarrow \delta)}$.

The related-key boomerang attack is one of the effective combined attacks on block ciphers that can be applied to many known block ciphers. For the related-key model, attacker assumes to know the relation (difference) between the keys, but not the exact values of keys. The standard differential model tries to increase $P(E_K(x) \oplus E_K(x \oplus \Delta x) = \Delta y)$. The related-key model, on the other hand, tries to increase $P(E_K(x) \oplus E_{K \oplus \Delta K}(x \oplus \Delta x) = \Delta y)$.

The adaptation of related-key model to the boomerang attack is straightforward. The usual related-key model is applied to the subciphers E_0 and E_1 separately and the normal procedure is applied for the boomerang distinguisher. However, some additional properties are adapted for the related-key boomerang distinguisher. Instead of one pair of related-keys, 4 (or more)[13] related keys can be used used and the most effective one is selected for the attack according to the structure of the cipher. For Tiger, however, we are going to give details about the related-key boomerang distinguisher based on 4 related-keys as follows:

- Take a randomly chosen plaintext P_1 and form $P_2 = P_1 \oplus \alpha$.
- Obtain the corresponding ciphertexts $C_1 = E_{K_1}(P_1)$ and $C_2 = E_{K_2}(P_2)$ through E, where $K_2 = K_1 \oplus \Delta K_{12}$.
- Form the second ciphertext pair by $C_3 = C_1 \oplus \delta$ and $C_4 = C_2 \oplus \delta$.
- Obtain the corresponding plaintexts $P_3 = E_{K_3}^{-1}(C_3)$ and $P_4 = E_{K_4}^{-1}(C_4)$ through E^{-1}, where $K_3 = K_1 \oplus \Delta K_{13}$, $K_4 = K_3 \oplus \Delta K_{12}$.
- Check $P_3 \oplus P_4 = \alpha$

The probabilistic arguments are the same as in the boomerang distinguisher but they are converted to the related-key model for the related-key boomerang distinguisher.

3.2 The Rectangle and the Related-Key Rectangle Attack

The rectangle attack converts the adaptively chosen nature of the boomerang attack into the chosen plaintext attack. In fact, it is the refinement of the amplified-boomerang attack[14] and used to attack to many known ciphers[12][13]. Instead of using both encryption and the decryption boxes, the rectangle attack only uses the encryption box.

In boomerang distinguisher, the γ difference after E_0 and before E_1 is gathered through the decryption process. However, in rectangle distinguisher, the pairs (P_1, P_2) and (P_3, P_4) make use of the differential $\alpha \rightarrow \beta$ and since (P_1, P_3) is taken as random, it is expected that the difference $E_0(P_1) \oplus E_0(P_3) = \gamma$ works with probability 2^{-n}. Once this is satisfied, the differential $\gamma \rightarrow \delta$ comes to the picture. Of course, the subciphers before and after the rectangle distinguisher works as in the boomerang distinguisher. Besides the advantage of chosen plaintext nature, it also makes use of all β' values satisfying $\alpha \rightarrow \beta'$ and all γ' values that satisfy $\gamma' \rightarrow \delta$. For the further improvements, the details are given in[11]. Using the notations given above, one can describe the rectangle distinguisher as follows.

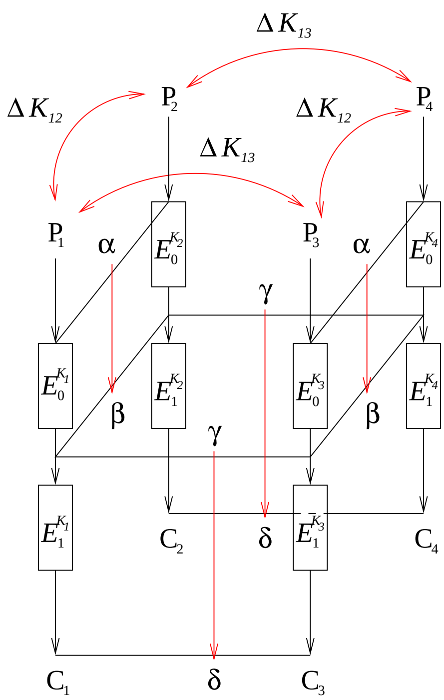

Fig. 3. Related-Key Rectangle Distinguisher Based on Four Related Keys

- Take a randomly chosen plaintext P_1 at random and obtain the corresponding ciphertext $C_1 = E_{K_1}(P_1)$.
- Form $P_2 = P_1 \oplus \alpha$ and obtain the corresponding ciphertext $C_2 = E_{K_2}(P_2)$, where $K_2 = K_1 \oplus \Delta K_{12}$.
- Pick another randomly chosen plaintext P_3 and obtain the corresponding ciphertext $C_3 = E_{K_3}(P_3)$, where $K_3 = K_1 \oplus \Delta K_{13}$.
- Form $P_4 = P_3 \oplus \alpha$ and obtain the corresponding ciphertext $C_4 = E_{K_4}(P_4)$, where $K_4 = K_3 \oplus \Delta K_{12}$.
- Check $C_1 \oplus C_3 = \delta$ and $C_2 \oplus C_4 = \delta$

The probability P of the rectangle distinguisher is given by $P = 2^{-n}\hat{p}^2\hat{q}^2$, where $\hat{p} = \sqrt{\sum_\beta P^2_{K_1,K_2}(\alpha \to \beta)}$ and $\hat{q} = \sqrt{\sum_\gamma P^2_{K_3,K_4}(\gamma \to \delta)}$. For a random cipher, the probability of the given difference is $P' = 2^{-2n}S$ where S is the cardinality of the set of differences of all δ values. Once $P \geq P'$ is satisfied, the rectangle distinguisher works.

4 The Related-Key Boomerang and Related-Key Rectangle Attacks on the Encryption Mode of Tiger

In this section, we present the related-key boomerang and the related-key rectangle attacks on the encryption mode of Tiger. We will show 19-round related-key boomerang and rectangle distinguisher by using 4 related-keys in the following subsections. This reduced round distinguishing attack covers the round $5 - 24$.

4.1 Some Notation and the Conventions

Converting additive differences into XOR difference generally works with probability 1/2. However, the most significant bit difference can be used to discard this probability. That is, if $X - Y = 2^{63}$, then $P(X - Y) = 2^{63} = 1$. For the sake of simplicity, we use the notation as in[15]. Thus, let $I = 2^{63}$. We will use the simplicity of the difference I, by not dealing with which type of difference is used. As in[15], notice that a difference I in a word W does not change when it is multiplied by a constant which is also used in the compression function of the Tiger.

4.2 The Differentials of the Key Scheduling Algorithm

In Tiger, the message expansion algorithm is not a linear function. However, some differences propagate linearly through the message expansion algorithm. One of such differential is used in[15] to find collisions to reduced round Tiger. This motivates us to search for other good differentials that propagates very efficiently. What makes it good in terms of their efficiency is quite obvious in the sense that the hamming weight of the corresponding differences should be kept small. Also, reducing carry effect by introducing the difference I we got several probability one differentials, the used ones can be seen in Table 1.

In order to make the attack efficient, we need to combine some of these differentials very effectively. Observing the propagation of these differentials, since we should make an extensive use of cancellations and probability one differentials, for the key differences we need to find low weight and near differences. By near differences, we do not mean to have huge gaps between I differences. Of course, the number of rounds attacked is also very important. In the scope of this simple tricks, in the following sections we present our attack on the encryption mode of Tiger.

Table 1. The Propagation of Key Differences

Key Difference	Rounds $1-8$	Rounds $9-16$	Rounds $17-24$
$(0,0,0,0,I,I,I,I)$	$(0,0,0,0,I,I,I,I)$	$(0,I,0,I,I,0,0,I)$	$(0,0,0,I,I,I,I,0)$
(0,0,0,I,0,0,0,I)	**(0,0,0,I,0,0,0,I)**	**(0,I,0,0,0,0,0,I)**	**(0,0,0,0,0,0,0,I)**
$(0,0,0,I,I,I,I,0)$	$(0,0,0,I,I,I,I,0)$	$(0,0,0,I,I,0,0,0)$	$(0,0,0,I,I,I,I,I)$
$(0,0,I,0,0,0,I,I)$	$(0,0,I,0,0,0,I,I)$	$(I,0,0,0,0,0,I,I)$	$(0,0,0,0,0,0,I,I)$
$(0,0,I,0,I,I,0,0)$	$(0,0,I,0,I,I,0,0)$	$(I,I,0,I,I,0,I,0)$	$(0,0,0,I,I,I,0,I)$
$(0,0,I,I,0,0,I,0)$	$(0,0,I,I,0,0,I,0)$	$(I,I,0,0,0,0,I,0)$	$(0,0,0,0,0,0,I,0)$
$(0,0,I,I,I,I,0,I)$	$(0,0,I,I,I,I,0,I)$	$(I,0,0,I,I,0,I,I)$	$(0,0,0,I,I,I,0,0)$
(0,I,0,0,0,I,I,I)	**(0,I,0,0,0,I,I,I)**	**(0,0,0,0,0,I,I,0)**	**(0,0,0,0,0,I,I,I)**
$(0,I,0,0,I,0,0,0)$	$(0,I,0,0,I,0,0,0)$	$(0,I,0,I,I,I,I,I)$	$(0,0,0,I,I,0,0,I)$
$(0,I,0,I,0,I,I,0)$	$(0,I,0,I,0,I,I,0)$	$(0,I,0,0,0,I,I,I)$	$(0,0,0,0,0,I,I,0)$
$(0,I,0,I,I,0,0,I)$	$(0,I,0,I,I,0,0,I)$	$(0,0,0,I,I,I,I,0)$	$(0,0,0,I,I,0,0,0)$
$(0,I,I,0,0,I,0,0)$	$(0,I,I,0,0,I,0,0)$	$(I,0,0,0,0,I,0,I)$	$(0,0,0,0,0,I,0,0)$
$(0,I,I,0,I,0,I,I)$	$(0,I,I,0,I,0,I,I)$	$(I,I,0,I,I,I,0,0)$	$(0,0,0,I,I,0,I,0)$
$(0,I,I,I,0,I,0,I)$	$(0,I,I,I,0,I,0,I)$	$(I,I,0,0,0,I,0,0)$	$(0,0,0,0,0,I,0,I)$
$(0,I,I,I,I,0,I,0)$	$(0,I,I,I,I,0,I,0)$	$(I,0,0,I,I,I,0,I)$	$(0,0,0,I,I,0,I,I)$

4.3 The Differential for E_0 (rounds $6-13$)

In Tiger, we can find a probability 1 related-key differential for E_0. For E_0, the related-key differential $(I,I,I) \rightarrow (0,0,0)$ works with probability 1 for rounds $6-13$ under the key difference $(0,I,0,0,0,I,I,I)$. In round 6, by imposing difference $\alpha = (\Delta A_6, \Delta B_6, \Delta C_6) = (I,I,I)$, we cancel the subkey difference $\Delta K_6 = I$ with $\Delta C_6 = I$ making $(\Delta A_7, \Delta B_7, \Delta C_7) = (I,0,I)$. In round 7, as in the previous round, we cancel the subkey difference $\Delta K_7 = I$ with $\Delta C_7 = I$. Finally in round 8, we have $(\Delta A_8, \Delta B_8, \Delta C_8) = (0,0,I)$. Again, the subkey difference $\Delta K_8 = I$ and the word C_8 difference $\Delta C_8 = I$ cancel each other. From round 8 until round 13, we use the trivial differential which makes $\beta = (0,0,0)$. Notice that, we make an extensive use of the trivial propagation of the I difference through the words B_i and *even* function as it does not affect the even bytes of the corresponding words.

Table 2. The Propagation of Differences Through E_0

Round	ΔA	ΔB	ΔC	ΔK	*Probability*
6	I	I	I	I	1
7	I	0	I	I	1
8	0	0	I	I	1
9	0	0	0	0	1
10	0	0	0	0	1
11	0	0	0	0	1
12	0	0	0	0	1
13	0	0	0	0	1

Up to know, everything works with probability 1 and the differential probability p and $\hat{p}$ for the subcipher E_0 is 1. This is valid for both of the related-key rectangle and the related-key boomerang attacks.

4.4 The Differential for E_1 (rounds $14 - 23$)

For the second part of our distinguisher E_1, the related-key differential $(0, I, 0) \to (0, 0, 0)$ works with probability 1 for rounds $14 - 23$ under the key difference $(0, 0, 0, I, 0, 0, 0, I)$. Here, according to the notation given above, $\gamma = (0, I, 0)$. Again we will use the trivial propagation of the difference I through the words B_i. The difference γ in round 14 propagates to the round 16 as $(\Delta A_{16}, \Delta B_{16}, \Delta C_{16}) = (0, 0, I)$ with probability 1 and cancels the subkey difference $\Delta K_{16} = I$. From the end of the round 16 till round 23, again we use the trivial differential making $\Delta A_{23}, \Delta B_{23}, \Delta C_{23}) = (0, 0, 0)$. As in E_0, everything works with probability 1 and the differential probability q and $\hat{q}$ for the subcipher E_1 is 1. This is valid for both of the related-key rectangle and the related-key boomerang attacks.

Table 3. The Propagation of Differences Through E_1

Round	ΔA	ΔB	ΔC	ΔK	*Probability*
14	0	I	0	0	1
15	I	0	0	0	1
16	0	0	I	I	1
17	0	0	0	0	1
18	0	0	0	0	1
19	0	0	0	0	1
20	0	0	0	0	1
21	0	0	0	0	1
22	0	0	0	0	1
23	0	0	0	0	1

4.5 The Round Before and After the Distinguisher

We can extend the above distinguisher by adding one round before the distinguisher by imposing α difference in the sixth round. Since $\Delta A_5 = I$ and

$\Delta C_5 = I$ differences propagate directly to the next round, we just need to play with the difference ΔB_5. Remember that we have to get $\Delta A_6 = I$. Therefore, $\Delta B_5 = I - \Delta odd(I) = \alpha'$ satisfies the desired difference α. However, we expect to have 2^{32} possible $\Delta odd(I)$ values. Moreover, by using birthday paradox techniques we can reduce this number to impose the α difference. If we take 2^{16} $\Delta odd(I)$ values at random, we expect that one of these differences cancel the difference coming from $\Delta C_5 = I$. Therefore, at the end of the round five we have I difference in the word A_6 that is enough for our distinguisher.

There is also a possibility to add a round after the distinguisher given above. We have $(\Delta A_{23}, \Delta B_{23}, \Delta C_{23}) = (0, 0, 0)$ and the subkey difference ΔX_{23} in the last round is I. Therefore, the propagation of this difference through the last round leads to the difference $(\Delta A_{24}, \Delta B_{24}, \Delta C_{24}) = (\delta', I, 0)$ where δ' is the all possible differences caused by the I difference of the *odd* function in the last round.

5 The Attack

For the boomerang distinguisher, we just use the round before the distinguisher added to the usual related-key boomerang distinguisher that totally covers the rounds $5 - 23$. The related key boomerang attack to the reduced round Tiger is as follows:

- Take a randomly chosen plaintext P_1 and form $P_2 = P_1 \oplus \alpha'$ where α' is one of the 2^{16} differences.
- Obtain the corresponding ciphertexts $C_1 = E_{K_1}(P_1)$ and $C_2 = E_{K_2}(P_2)$ through E, where $K_2 = K_1 \oplus (0, I, 0, 0, 0, I, I, I)$.
- Take the second ciphertext pair as $C_3 = C_1$ and $C_4 = C_2$.
- Obtain the corresponding plaintexts $P_3 = E^{-1}_{K_3}(C_3)$ and $P_4 = E^{-1}_{K_4}(C_4)$ through E^{-1}, where $K_3 = K_1 \oplus (0, 0, 0, I, 0, 0, 0, I)$, $K_4 = K_3 \oplus (0, I, 0, 0, 0, I, I, I)$.
- Check $P_3 \oplus P_4 = (I, I - \Delta odd(I), I)$
- If this is not the case, take another α', if this is the case identify the corresponding cipher as Tiger.

As the probability of the related-key boomerang distinguisher is 1 and there are 2^{32} possible $\Delta odd(I)$ values, identification of the Tiger will take 2^{32} trials in the worst case. Therefore, if we take a plaintext P_1 and form 2^{16} (P_1, P_2) pairs as $P_2 = P_1 \oplus \alpha'$, we expect that one of the pairs gives α' difference that we need. The required work is 2^{18} reduced round Tiger encryption and decryption which equals to $2^{14.25}$ Tiger encryption.

For the related-key rectangle distinguisher on the other hand, we use the round after the distinguisher added to the related-key rectangle distinguisher that totally covers the rounds $6 - 24$.

- Prepare 2^{97} randomly chosen plaintexts P_1 at random and obtain the corresponding ciphertext $C_1 = E_{K_1}(P_1)$.
- Form $P_2 = P_1 \oplus \alpha$ and obtain the corresponding ciphertext $C_2 = E_{K_2}(P_2)$, where $K_2 = K_1 \oplus (0, I, 0, 0, 0, I, I, I)$.

- Pick another randomly chosen plaintext P_3 and obtain the corresponding ciphertext $C_3 = E_{K_3}(P_3)$, where $K_3 = K_1 \oplus (0, 0, 0, I, 0, 0, 0, I)$.
- Form $P_4 = P_3 \oplus \alpha$ and obtain the corresponding ciphertext $C_4 = E_{K_4}(P_4)$, where $K_4 = K_3 \oplus (0, I, 0, 0, 0, I, I, I)$.
- Check $C_1 \oplus C_3 = \delta = (\Delta odd(I), I, 0)$ and $C_2 \oplus C_4 = \delta = (\Delta odd(I), I, 0)$.
- If this is the case identify the corresponding cipher as Tiger.

From the 2^{97} plaintext pairs we can form 2^{193} quartets. As the probability of our related-key rectangle distinguisher is 2^{-192}, the trial of 2^{97} plaintext pairs results in a success probability of $1 - (1 - (2^{-192})^{2^{-193}})$, which is approximately 0.86. We perform 2^{195} reduced round Tiger encryption and 2^{32} operation to check whether we have $(\Delta odd(I), I, 0)$ or not. So, total work will become approximately $2^{154.3}$ Tiger encryption and a negligible checking operation.

6 Conclusion

In this paper we applied the related-key boomerang and related-key rectangle attacks to the reduced round of Tiger. In the related-key boomerang attack, the number of required plaintext pair equals to 2^{16} and the time complexity of the attack is $2^{14.25}$. The related-key rectangle attack works with 2^{97} chosen plaintexts and results in a time complexity of $2^{154.3}$. This attack can be further improved by adding more rounds before and after the dstinguisher and trying to find more effective subkey differentials. Moreover, this differentials can be used to find collissions for Tiger as an hash function.

References

1. Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, and William Jalby. Collisions of sha-0 and reduced sha-1. In Cramer [16], pages 36–57.
2. Christophe De Cannière and Christian Rechberger. Finding sha-1 characteristics: General results and applications. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2006.
3. Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu. Cryptanalysis of the hash functions md4 and ripemd. In Cramer [16], pages 1–18.
4. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full sha-1. In Shoup [17], pages 17–36.
5. Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. Efficient collision search attacks on sha-0. In Shoup [17], pages 1–16.
6. Jongsung Kim, Alex Biryukov, Bart Preneel, and Sangjin Lee. On the security of encryption modes of md4, md5 and haval. In Sihan Qing, Wenbo Mao, Javier Lopez, and Guilin Wang, editors, *ICICS*, volume 3783 of *Lecture Notes in Computer Science*, pages 147–158. Springer, 2005.
7. Jongsung Kim, Guil Kim, Seokhie Hong, Sangjin Lee, and Dowon Hong. The related-key rectangle attack - application to shacal-1. In Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors, *ACISP*, volume 3108 of *Lecture Notes in Computer Science*, pages 123–136. Springer, 2004.

8. Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman. Differential and rectangle attacks on reduced-round shacal-1. In Rana Barua and Tanja Lange, editors, *INDOCRYPT*, volume 4329 of *Lecture Notes in Computer Science*, pages 17–31. Springer, 2006.
9. Jongsung Kim, Dukjae Moon, Wonil Lee, Seokhie Hong, Sangjin Lee, and Seokwon Jung. Amplified boomerang attack against reduced-round shacal. In Yuliang Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 243–253. Springer, 2002.
10. Ross J. Anderson and Eli Biham. Tiger: A fast new hash function. In Dieter Gollmann, editor, *Fast Software Encryption*, volume 1039 of *Lecture Notes in Computer Science*, pages 89–97. Springer, 1996.
11. Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In Cramer [16], pages 507–525.
12. Seokhie Hong, Jongsung Kim, Sangjin Lee, and Bart Preneel. Related-key rectangle attacks on reduced versions of shacal-1 and aes-192. In Henri Gilbert and Helena Handschuh, editors, *FSE*, volume 3557 of *Lecture Notes in Computer Science*, pages 368–383. Springer, 2005.
13. Jongsung Kim, Seokhie Hong, and Bart Preneel. Related-key rectangle attacks on reduced aes-192 and aes-256. In *FSE*, 2007.
14. John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round mars and serpent. In Bruce Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, pages 75–93. Springer, 2000.
15. John Kelsey and Stefan Lucks. Collisions and near-collisions for reduced-round tiger. In Matthew J. B. Robshaw, editor, *FSE*, volume 4047 of *Lecture Notes in Computer Science*, pages 111–125. Springer, 2006.
16. Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.
17. Victor Shoup, editor. *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*. Springer, 2005.