On the Security of the Encryption Mode of Tiger

Onur Özen, Kerem Varıcı

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

***Abstract*—Tiger is an important type of an hash function producing 192-bit hash value from 512-bit message block and is proved to be secure so far as there is no known collision attack on the full (24 rounds) 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. Recently some weaknesses have been found for Tiger-hash function. First, in FSE $'06$ Kelsey and Lucks found a collision for 16-17 rounds of Tiger and a pseudo-near-collision for 20 rounds. Then Mendel et.al extended this attack to 19-round collision and 22-round pseudo-near-collision. Finally in 2007 Mendel and Rijmen found a pseudo-collision for the full Tiger. In this paper, we will investigate the security notion of reduced round Tiger in the encryption mode against the very well known and efficient block cipher attacks, namely related-key boomerang and the related-key rectangle attacks. Moreover, we will present a trivial related-key boomerang and rectangle distinguishers of 20 and 22 rounds.**

I. Introduction

Hash functions are one of the key elements of the cryptographic primitives which are being used for many important applications such as data integrity, authentication, digital signature etc. in everyday life. Many of the digital transactions and the e-cash applications are performed by using hash functions. Thus, the security and the effectiveness of the dedicated hash functions are of great interest nowadays.

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 which is another important type of an hash function and 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. Recently some weaknesses have been found for Tiger-hash function. First, in FSE $'06$ [6] Kelsey and Lucks found a collision for 16-17 rounds of Tiger and a pseudo-near-collision for 20 rounds. Then Mendel et.al [7] extended this attack to 19-round collision and 22-round pseudo-near-collision. Finally in 2007 Mendel and Rijmen [8] found a pseudo-collision for the full Tiger.

There have been several cryptanalysis papers investigating the randomness properties of the designed hash functions under the encryption modes such as [9] by Kim et.al. In that paper, related-key boomerang and related-key rectangle attacks are performed on `MD4,MD5` and `HAVAL` under $2, 4$ related-keys or weak keys. Moreover, there have been very important attacks [10], [11], [12] on `SHACAL` as well which is based on the hash function `SHA`. In this paper, we will investigate the security notion of reduced round Tiger in the encryption mode against the very well known and the efficient block cipher attacks, namely related-key boomerang and the related-key rectangle attacks. Moreover, we will present a trivial related-key boomerang and rectangle distinguishers of 20 and 22 rounds.

The rest of the paper is structured as follows. In section two, we briefly introduce the hash function Tiger. In section three, the related-key boomerang and the related-key rectangle attacks are introduced. In section four and five, the attack on the encryption mode of the Tiger is detailed and section six concludes the paper.

II. Tiger

A. The Overview of Tiger

Tiger[13] is a cryptographic, iterative hash function which is designed for 64-bit processors by Biham and Anderson. It uses 64-bit operations such as addition, subtraction, multiplications by small constants (5, 7 and 9) and logical operations in message expansion. The main operation of Tiger is the use of *even* and *odd* functions operating on even and odd bytes of the step variables by the use of S-boxes. There exist four S-boxes in Tiger where each takes 8-bit input and produces 64-bit output. The size of the hash value and the intermediate state length are 192-bit (three 64-bit words) and the message block is 512-bit(eight 64-bit words). We will follow the notation given in Table 1.

B. The Round Function of Tiger

In Tiger, each 8-round part uses different constant values for multiplication and in each round a new expanded mesage word is used. 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 denoted by t_1, t_2, t_3 and t_4 where $C[i]$ denotes the ith byte of C ($0 \leq i \leq 7$). The ith round input values are shown as A_i, B_i, C_i (3-64-bit words) where $i \in \{0, \ldots, 24\}$, ith round message block is X_i and ith round output values are A_{i+1}, B_{i+1}, C_{i+1}. In the round function A, B, C state variables are updated as:

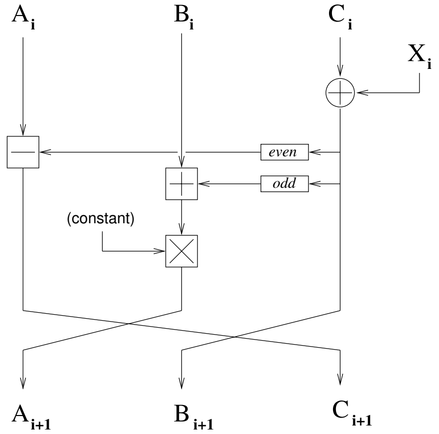


Fig. 1: The i^{th} Round of Tiger

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

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

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

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}[13]. After the last round of the state update transformation, the initial values A_0, B_0, C_0 and A_{24}, B_{24}, C_{24} are combined resulting to the hash value or the initial value of the next step

$$A_{25} = A_0 \oplus A_{24}, B_{25} = B_0 \boxminus B_{24}, C_{25} = C_0 \boxplus C_{24}$$

The block cipher mode of Tiger is straightforward. 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. Moreover, from now on, the message expansion is called the key schedule of Tiger.

C. The Key Schedule of Tiger

The non-linear the key schedule of Tiger uses some logical operators together with the XOR, addition, subtraction, and shift operations. In the first 8 round, the original message words $X_0, ..., X_7$ are used and for the next 8 rounds the key scheduling is applied and the message words $X_8, ..., X_{15}$

Notation	Meaning
$A \boxplus B$	Addition of A and B mod 2^{64}
$A \boxminus B$	Subtraction of A and B mod 2^{64}
$A \boxtimes B$	Multiplication of A and B mod 2^{64}
$A \oplus B$	Bitwise XOR-operation of A and B mod 2^{64}
$\neg A$	Bitwise NOT-operation of A
$A << n$	Bitwise shift of A to the left
$A >> n$	Bitwise shift of A to the right
X_i	Message word i
X_i**[even]**	Even bytes of X_i
X_i**[odd]**	Odd bytes of X_i

TABLE I: Notation

are formed. For the remaining 8 rounds the key scheduling is performed to the message words $X_8, ..., X_{15}$ to gather $X_{16}, ..., X_{23}$. 512-bit key is expanded by the operations shown in Table 2 :

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

The Key Schedule of Tiger

There are some useful differentials for the message expansion of Tiger which will be given in the following sections, some of which are used to attack the hash mode of Tiger in [6], [7] and [8]. By useful differentials we mean to have probability one propagation of message differences used in the step functions.

III. 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 [10] and Dunkelman et.al [14]. Nowadays, they are the most effective and powerful block cipher attacks that are applied to many known ciphers [15], [16], [17]. In the following subsections, we will briefly introduce these attacks together with their primitives, namely the pure boomerang and the rectangle attack.

A. The Boomerang and the Related-Key Boomerang Attack

The Boomerang Attack [18] may be seen as the refinement or the effective use of the pure differential cryptanalysis [19]. After the application of differential-linear cryptanalysis [20], the boomerang attack can also be called differential-differential cryptanalysis. In the boomerang process, instead of using one long-ineffective (low probability) differential, the attacker makes use of 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 [14]. Boomerang distinguisher treats the attacked cipher E as a cascade of two sub-ciphers E_0 and E_1, i.e. $E = E_1\ o\ E_0$. 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 boomerang distinguisher works as follows:

- 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 $P_3 \oplus P_4 = \alpha$.

The boomerang distinguisher works with probability p^2q^2. 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 [14], [18], [21].

The related-key boomerang attack, on the other hand, 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) [22], [21], [23] related keys can be 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 same as in the boomerang distinguisher but they are converted to the related-key model for the related-key boomerang distinguisher.

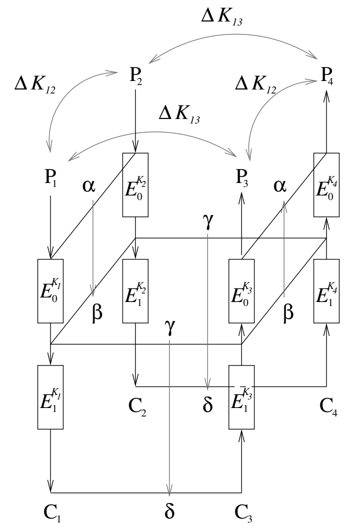
B. The Rectangle and the Related-Key Rectangle Attack

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[24] and used to attack to many known ciphers[15], [22]. Instead of using both encryption and the decryption boxes, the rectangle attack only uses the encryption box.

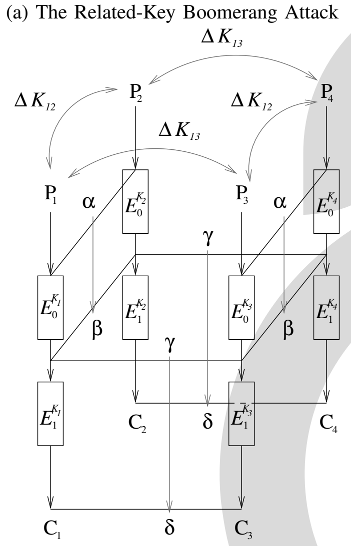
In boomerang distinguisher, the γ difference after E_0 and before E_1 is gathered through the decryption process. However, in rectangle distinguisher, the pairs (P_1, P_2) and (P_3, P_4) conforms to the differential $\alpha \to \beta$ and since (P_1, P_3) is taken as random, it is expected that the difference $E_0(P_1) \oplus E_0(P_3) = \gamma$ works with probability 2^{-n}. Once this is satisfied, the differential $\gamma \to \delta$ 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 $\alpha \to \beta'$ and all γ' values that satisfy $\gamma' \to \delta$. For the further improvements, the details are given in [14]. Using the notations given above, one can describe the rectangle distinguisher as follows.

- 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.



(a) The Related-Key Boomerang Attack



(b) The Related-Key Rectangle Attack

Fig. 2: The Related-Key Boomerang and Rectangle Attack Based on Four Related-Keys

IV. 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 20 and 22-round related-key boomerang and rectangle distinguishers by using 4 related-keys in the following subsections. This attack can be easily extended to a key recovery attack.

A. 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 get rid of this probability. For the sake of simplicity, we use the notation as in [6]. Thus, let $I = 2^{63}$. We will use the simplicity of the difference I, by

Rounds $0-7$	Rounds $8-15$	Rounds $16-23$
$(0,I,0,0,0,I,I,I)$	$(0,0,0,0,0,I,I,0)$	$(0,0,0,0,0,I,I,I)$
$(0,0,0,I,0,0,0,I)$	$(0,I,0,0,0,0,0,I)$	$(0,0,0,0,0,0,0,I)$
$(I,I,0,0,0,I,0,0)$	$(0,0,0,0,0,I,0,I)$	$(.,.,.,.,.,.,.,.)$
$(0,0,0,I,0,0,0,I)$	$(0,I,0,0,0,0,0,I)$	$(0,0,0,0,0,0,0,I)$

TABLE II: The Propagation of Some Key Differences with probability 1

not dealing with which type of difference is used. As in [6], notice that a difference I propagates as the zero difference through the even function since it is in the odd byte and the propagates as I after the multiplication by constants.

B. The Differentials of the Key Scheduling Algorithm

In Tiger, the message expansion algorithm is non-linear. However, some differences propagate linearly. One of such differential is used in [6] 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 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, 4 of them used in 20 and 22-round related-key rectangle and boomerang distinguishers.

In order to succeed, we need to combine some of these differentials very effectively. Observing the propagation of these differentials, we should make an extensive use of cancellations and probability one differentials. Moreover, low weight differentials and the number of rounds attacked are also very important. In the scope of this simple tricks, the following sections contain our attack on the encryption mode of Tiger.

C. 20-Round Distinguisher

The Differential for E_0 (rounds $5-13$)

In Tiger, we can find a probability 1 related-key differential for E_0. For E_0, the related-key differential $(I,I,I) \to (0,0,0)$ works with probability 1 for rounds $5-13$ under the key difference $(0,I,0,0,0,I,I,I)$ shown in Table 1. In round 5, by imposing difference $\alpha = (\Delta A_5, \Delta B_5, \Delta C_5) = (I,I,I)$, we cancel the subkey difference $\Delta X_5 = I$ with $\Delta C_5 = I$ making $(\Delta A_6, \Delta B_6, \Delta C_6) = (I,0,I)$. In round 6, as in the previous round, we cancel the subkey difference $\Delta X_6 = I$ with $\Delta C_6 = I$. Finally in round 7, we have $(\Delta A_7, \Delta B_7, \Delta C_7) = (0,0,I)$. Again, the subkey difference $\Delta X_7 = I$ and the word C_7 difference $\Delta C_7 = I$ cancel each other. From round 7 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.

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.

Round	ΔA	ΔB	ΔC	ΔK	$Probability$
5	I	I	I	I	1
6	I	0	I	I	1
7	0	0	I	I	1
8	0	0	0	0	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

TABLE III: The Propagation of Differences Through E_0

Round	ΔA	ΔB	ΔC	ΔK	$Probability$
13	0	I	0	0	1
14	I	0	0	0	1
15	0	0	I	I	1
16	0	0	0	0	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

TABLE IV: The Propagation of Differences Through E_1

The Differential for E_1 (rounds $13-22$)

For the second part of our distinguisher E_1, the related-key differential $(0, I, 0) \rightarrow (0, 0, 0)$ works with probability 1 for rounds $13-22$ 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 13 propagates to the round 15 as $(\Delta A_{15}, \Delta B_{15}, \Delta C_{15}) = (0, 0, I)$ with probability 1 and cancels the subkey difference $\Delta X_{15} = I$. From the end of the round 15 till round 22, again we use the trivial differential making $\Delta A_{22}, \Delta B_{22}, \Delta C_{22}) = (0, 0, 0)$. 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.

D. 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 fifth round. Since $\Delta A_4 = I$ and $\Delta C_4 = I$ differences propagate directly to the next round, we just need to play with the difference ΔB_4. Remember that we have to get $\Delta A_5 = I$. Therefore, $\Delta B_4 = I \boxminus \Delta odd(I) = \alpha'$ satisfies the desired difference α. However, since we have a probability one differential, we just need to take one pair of plaintexts at the beginning of the fifth round. In fact, we can cancel the difference coming from the odd function by imposing the same difference to the internal variable B_4. That is, let $A_4 \boxminus A_4^{'} = I$ and $C_4 \boxminus C_4^{'} = I$. Now, B_4 can be chosen randomly but $B_4^{'}$ is constructed as $B_4^{'} = B_4 \boxminus I \boxplus Odd(C_4) \boxminus Odd(C_4 \boxminus I)$.

Round	ΔA	ΔB	ΔC	ΔK	$Probability$
3	0	I	0	0	1
4	I	0	0	0	1
5	0	0	I	I	1
6	0	0	0	0	1
7	0	0	0	0	1
8	0	0	0	0	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

TABLE V: The Propagation of Differences Through E_0

Since, we have one pair, there is no probabilistic arguments in that construction.

There is also a possibility to add a round after the distinguisher given above. We have $(\Delta A_{22}, \Delta B_{22}, \Delta C_{22}) = (0, 0, 0)$ and the subkey difference ΔX_{22} in the last round is I. Therefore, the propagation of this difference through the last round leads to the difference $(\Delta A_{23}, \Delta B_{23}, \Delta C_{23}) = (\delta', I, 0)$ where $A_{23} \boxminus A_{23}^{'} = Odd(B_{23}) \boxminus Odd(B_{23}^{'})$.

E. 22-Round Distinguisher

The Differential for E_0 (rounds $3-13$)

Another differential for Tiger can be used to extend the distinguisher to 22 rounds. This time the other differential in Table1 is used. In round 3, by imposing difference $\alpha = (\Delta A_3, \Delta B_3, \Delta C_3) = (0, I, 0)$, we cancel the subkey difference $\Delta X_5 = I$ with $\Delta C_5 = I$ making $(\Delta A_6, \Delta B_6, \Delta C_6) = (0, 0, 0)$. From round 6 until round 13, we use the trivial differential which makes $\beta = (0, 0, 0)$.

Again, all differential works with probability one and we make an extensive use of the propagation of I difference through round operations.

The Differential for E_1 (rounds $13-22$)

For the second part of our distinguisher E_1, the related-key differential $(0, I, 0) \rightarrow (0, 0, 0)$ works with probability 1 for rounds $13-22$ 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 13 propagates to the round 15 as $(\Delta A_{15}, \Delta B_{15}, \Delta C_{15}) = (0, 0, I)$ with probability 1 and cancels the subkey difference $\Delta X_{15} = I$. From the end of the round 15 till round 22, again we use the trivial differential making $\Delta A_{22}, \Delta B_{22}, \Delta C_{22}) = (0, 0, 0)$. 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. As in the previous distinguisher, we can extend the above distinguisher by adding one round before and after the distinguisher by imposing the necessary differences.

Round	ΔA	ΔB	ΔC	ΔK	$Probability$
13	0	I	0	0	1
14	I	0	0	0	1
15	0	0	I	I	1
16	0	0	0	0	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

TABLE VI: The Propagation of Differences Through E_1

V. The Attack

For the boomerang distinguisher, we just use the round before and after the distinguisher added to the usual related-key boomerang distinguisher that totally covers 22 rounds (20-round version is same). The related key boomerang attack to the reduced round Tiger is as follows:

- Take a randomly chosen plaintext $P_1 = (A_2, B_2, C_2)$ and form
  $P_2 = (A_2^{'}, B_2^{'}, C_2^{'})$ as above.
- Obtain the corresponding ciphertexts $C_1 = E_{K_1}(P_1)$ and $C_2 = E_{K_2}(P_2)$ through E, where $K_2 = K_1 \boxminus (I, I, 0, 0, 0, I, 0, 0)$.
- Take the second ciphertext pair as $C_3 = C_1 \boxminus (\delta^{'}, I, 0)$ and $C_4 = C_2 \boxminus (\delta^{'}, I, 0)$.
- 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 $K_3 = K_1 \boxminus (0, 0, 0, I, 0, 0, 0, I)$,
  $K_4 = K_3 \boxminus (I, I, 0, 0, 0, I, 0, 0)$.
- Check $P_3 \boxminus P_4 = P_1 \boxminus P_2$.
- If this is the case, identify the corresponding cipher as Tiger.

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 $3 - 24$.

- 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 as above and obtain the corresponding ciphertext $C_2 = E_{K_2}(P_2)$, where $K_2 = K_1 \boxminus (I, I, 0, 0, 0, I, 0, 0)$.
- Pick another randomly chosen plaintext P_3 and obtain the corresponding ciphertext $C_3 = E_{K_3}(P_3)$, where $K_3 = K_1 \boxminus ((0, 0, 0, I, 0, 0, 0, I)$.
- Form $P_4 = P_3 \oplus \alpha$ and obtain the corresponding ciphertext $C_4 = E_{K_4}(P_4)$, where $K_4 = K_3 \boxminus (I, I, 0, 0, 0, I, 0, 0)$.
- Check $C_1 \boxminus C_3 = C_2 \boxminus C_4 = \delta = (\delta^{'}, I, 0)$.
- If this is the case identify the corresponding cipher as Tiger.

VI. Conclusion

In this paper we applied the related-key boomerang and related-key rectangle attacks to the reduced round of Tiger. We constructed two related-key boomerang and rectangle distinguishers of 20 and 22 rounds. In the related-key boomerang attacks, the number of required plaintext pair is equal to 2 and the time complexity of the attack is negligible. The related-key rectangle attack works with 2^{97} chosen plaintexts and results in a time complexity of about $2^{152.8}$. The distinguishers presented above can be easily converted to a key recovery attack due to the fact that Tiger uses a 512-bit key by guessing the key values before the distinguisher. This type of analysis also can be further applied to the hash mode of Tiger to find collisions.

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 [25], 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 [25], pages 1–18.

[4] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full sha-1. In Shoup [26], pages 17–36.

[5] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. Efficient collision search attacks on sha-0. In Shoup [26], pages 1–16.

[6] John Kelsey and Stefan Lucks. Collisions and near-collisions for reduced-round tiger. In Robshaw [27], pages 111–125.

[7] Florian Mendel, Bart Preneel, Vincent Rijmen, Hirotaka Yoshida, and Dai Watanabe. Update on tiger. In Barua and Lange [28], pages 63–79.

[8] Florian Mendel and Vincent Rijmen. Cryptanalysis of tiger hash function. In *ASIACRYPT*, 2007.

[9] 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.

[10] 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.

[11] Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman. Differential and rectangle attacks on reduced-round shacal-1. In Barua and Lange [28], pages 17–31.

[12] 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.

[13] 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.

[14] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In Cramer [25], pages 507–525.

[15] 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.

[16] Jongsung Kim, Seokhie Hong, and Bart Preneel. Related-key rectangle attacks on reduced aes-192 and aes-256. In Alex Biryukov, editor, *FSE*, volume 4593 of *Lecture Notes in Computer Science*, pages 225–241. Springer, 2007.

[17] Eli Biham, Orr Dunkelman, and Nathan Keller. A related-key rectangle attack on the full kasumi. In Bimal K. Roy, editor, *ASIACRYPT*, volume 3788 of *Lecture Notes in Computer Science*, pages 443–461. Springer, 2005.

[18] David Wagner. The boomerang attack. In Lars R. Knudsen, editor, *Fast Software Encryption*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.

[19] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.

[20] Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. In Yvo Desmedt, editor, *CRYPTO*, volume 839 of *Lecture Notes in Computer Science*, pages 17–25. Springer, 1994.

[21] Orr Dunkelman. *Techniques for Cryptanalysis of Block Ciphers*. PhD thesis, Computer Science Department, Technion, 2006.

[22] Jongsung Kim, Seokhie Hong, and Bart Preneel. Related-key rectangle attacks on reduced aes-192 and aes-256. In *FSE*, 2007.

[23] Jongsung Kim. *Combined Differential, Linear and Related-Key Attacks on Block Ciphers and MAC Algorithms*. PhD thesis, Katholieke Universiteit Leuven, 2006.

[24] 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.

[25] 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.

[26] 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.

[27] Matthew J. B. Robshaw, editor. *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*. Springer, 2006.

[28] Rana Barua and Tanja Lange, editors. *Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006, Proceedings*, volume 4329 of *Lecture Notes in Computer Science*. Springer, 2006.