# Related-key Impossible Differential Cryptanalysis of Full-round HIGHT


Saeed Rostami[1], Sadegh Bamohabbat Chafjiri[2] and Seyed Amir Hossein Tabatabaei[3]

[1]*R&D Department, Tehran, Iran*

[2]*Information Systems and Security Lab, Sharif University of Technology, Tehran, Iran*

[3]*Chair for Data Communications Systems, University of Siegen, Siegen, Germany*

*sae.rostami@gmail.com, bamohabbat@ieee.org, amir.tabatabaei@uni-siegen.de*



Keywords: HIGHT, Lightweight Block Cipher, Related-key, Impossible Differential, Cryptanalysis.



Abstract: The HIGHT algorithm is a 64-bit block cipher with 128-bit key length, at CHES'06 as a lightweight cryptographic algorithm. In this paper, a new related-key impossible differential attack on the full-round algorithm is introduced. Our cryptanalysis requires time complexity of $2^{127.276}$ HIGHT evaluations which is slightly faster than exhaustive search attack. This is the first related-key impossible differential cryptanalysis on the full-round HIGHT block cipher.


## 1 INTRODUCTION

Nowadays using cryptographic primitives engaging lightweight technology is in the point of interest for the sake of efficiency. The most important applications lie in smart cards, sensors and, RFIDs where the processing and memory resources are limited. By using lightweight technology, it is tried to remove the problems which are arising from conditions imposed on the available resources by using low-cost complexity operations. On the other hand, when computational efficiency is increased security issues should be taken into account. So, considering a concrete security analysis is important in the design process of a lightweight cryptographic primitive to avoid endangering the desired security level.

The Block cipher HIGHT (high security and light weight) with 64-block length and 128-key length has been proposed by Hong *et al.* for low-cost, low-power, and, ultra-light implementation (Hong and et al., 2006). It is an iterative 32-round block cipher in the shape of generalized Feistel network which is used as a standard block cipher in South Korea. Several attacks on the HIGHT have shown some potential weaknesses of the reduced-round algorithm. The security strength of the algorithm against linear attack (Matsui, 1994) and differential cryptanalysis (Biham and Shamir, 1991) has been considered by its designers (Hong and et al., 2006). In (Ozen et al., 2009) the saturation attack (Lucks, 2002) on 16-round algorithm using 12-round characteristic was presented which has been improved in (Zhang et al., 2009) to target 22-round HIGHT. Impossible differential and related-key impossible differential attacks (Biham et al., 2005; Biham et al., 1999) on the HIGHT are covering more rounds (Hong and et al., 2006; Lu, 2007; Ozen et al., 2009). Till now with the best knowledge of the authors, the only attacks which target the full-round HIGHT are related-key rectangle attack (Hong et al., 2011) and biclique cryptanalysis (Hong et al., 2012). Although their time complexity (Hong et al., 2011) is almost the the same as complexity of our attack, our attack is the first related-key impossible differential attack on the full round HIGHT so far. In this paper, we propose a related-key impossible differential cryptanalysis on the full-round HIGHT with the complexity less than exhaustive search attack. A comparison between the result of our proposed attack and previously introduced related-key impossible differential attacks is provided in Table 1.

We mount our attack on the full-round algorithm by using a 24-round impossible differential characteristic. The main advantage of our approach in comparison with attacks proposed in (Lu, 2007) and (Ozen et al., 2009) is to use different differential characteristics which enables us to attack on the algorithm with one more round. The rest of this paper is organized as follows. In Section 2, the block cipher HIGHT is described. Extracting a new 24-round impossible differential characteristic will be given in Section 3. In Section 4, the full-round attack scenario and the complexity discussion will be given which concludes the paper.


Rostami S., Bamohabbat Chafjiri S. and Amir Hossein Tabatabaei S..
Related-key Impossible Differential Cryptanalysis of Full-round HIGHT.
DOI: 10.5220/0004528805370542
In *Proceedings of the 10th International Conference on Security and Cryptography* (SECRYPT-2013), pages 537-542
ISBN: 978-989-8565-73-0

Table 1: Summarized results of previous well-known attacks and our proposed attack.

| Number of rounds | Key size (bit) | Attack | Data complexity | Time complexity |
|---|---|---|---|---|
| 28 | 128 | related-key impossible differential [8] | $2^{60}$ | $2^{125.54}$ |
| 31 | 128 | related-key impossible differential [11] | $2^{64}$ | $2^{127.28}$ |
| full round | 128 | related-key impossible differential (this paper) | $2^{64}$ | $2^{127.28}$ |

# 2 SPECIFICATION OF ALGORITHM

## 2.1 Notations

The following notations and operations are used to describe the algorithm and its cryptanalysis.

- $\oplus$: XOR
- $\boxplus$: addition mod $2^8$
- $\lll i$: $i-$bit left rotation
- $M_i$: $i^{th}$ byte of master key
- $M_i^j$: $j^{th}$ bit of $i^{th}$ byte of master key
- $X_i$: variable of round $i$
- $X_{i,j}$: the $j^{th}$byte of $X_i$
- $K_i$: the $i^{th}$subkey
- $W_i$: the $i^{th}$byte of whitening key
- $\triangle M_i$: differential in byte $i$ of master key
- $e_{i,j,k}$: indicating nonzero differential in bit positions $i$, $j$ and $k$ of a byte and zero differential for the rest
- $e_{i\sim}$: zero differential in bit positions 0 till $i-1$ and nonzero differential in bit position $i$ and unknown differential for the rest
- $z_{i\sim}$: zero differential in bit positions 0 till $i-1$ and unknown differential for the rest
- ?: an arbitrary bit or byte value

## 2.2 The Description of HIGHT

Hight is a 32-round block cipher with 64-bit block size and 128-bit master key which uses an unbalanced Feistel network as its building blocks (Hong and et al., 2006). An Initial Transformation (IT) together with input whitening keys and a Final Transformation (FT) together with output whitening keys are applied to plaintext and output of the last round respectively. The encryption process of the HIGHT consists of following steps in turn: key schedule, initial transform, round function and, final transformation. The explanation of decryption process is left out because of its similarity to encryption process.

### 2.2.1 Key Schedule

The key schedule of the HIGHT consists of two subroutines for generating 8 whitening key bytes $W_0,\dots,W_7$, and 128 subkey bytes $K_0,\dots,K_{127}$. It uses the bytes of master key based on the Table 2. The detail of the key schedule of the HIGHT is found in (Hong and et al., 2006).

### 2.2.2 Initial Transformation

In initial transformation four whitening keys $W_0,\dots,W_3$ are used to map a plaintext $P$ to the input of the first round function.

$$
\begin{array}{l}
Initial\ Transformation(P, X_0, W_3, W_2, W_1, W_0)\\
\{\\
X_{0,0} \leftarrow P_0 \boxplus W_0; X_{0,1} \leftarrow P_1; X_{0,2} \leftarrow P_2 \boxplus W_1; X_{0,3} \leftarrow P_3;\\
X_{0,4} \leftarrow P_4 \boxplus W_2; X_{0,5} \leftarrow P_5; X_{0,6} \leftarrow P_6 \boxplus W_3; X_{0,7} \leftarrow P_7\\
\}
\end{array}
$$

### 2.2.3 Round Function

One round of the HIGHT is shown in Figure 1.

The equations of the round function are as follow.

$$
\begin{array}{l}
Round\ Function(X_i, X_{i+1}, K_{4i+3}, K_{4i+2}, K_{4i+1}, K_{4i})\\
\{\\
X_{i+1,1} \leftarrow X_{i,0}; X_{i+1,3} \leftarrow X_{i,2}; X_{i+1,5} \leftarrow X_{i,4}; X_{i+1,7} \leftarrow X_{i,6};\\
X_{i+1,0} = X_{i,7} \oplus (F_0(X_{i,6})) \boxplus K_{4i+3}\\
X_{i+1,2} = X_{i,1} \oplus (F_1(X_{i,0})) \boxplus K_{4i+2}\\
X_{i+1,4} = X_{i,3} \oplus (F_0(X_{i,2})) \boxplus K_{4i+1}\\
X_{i+1,6} = X_{i,5} \oplus (F_1(X_{i,4})) \boxplus K_{4i}\\
\}
\end{array}
$$

Round function of the HIGHT uses two building block functions $F_0$ and $F_1$:

Table 2: Relationships between master key and subkeys.

| Master key | Whitening key | Subkeys | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $M_{15}$ | $W_3$ | $K_{15}$ | $K_{24}$ | $K_{41}$ | $K_{58}$ | $K_{75}$ | $K_{92}$ | $K_{109}$ | $K_{126}$ |
| $M_{14}$ | $W_2$ | $K_{14}$ | $K_{31}$ | $K_{40}$ | $K_{57}$ | $K_{74}$ | $K_{91}$ | $K_{108}$ | $K_{125}$ |
| $M_{13}$ | $W_1$ | $K_{13}$ | $K_{30}$ | $K_{47}$ | $K_{56}$ | $K_{73}$ | $K_{90}$ | $K_{107}$ | $K_{124}$ |
| $M_{12}$ | $W_0$ | $K_{12}$ | $K_{29}$ | $K_{46}$ | $K_{63}$ | $K_{72}$ | $K_{89}$ | $K_{106}$ | $K_{123}$ |
| $M_{11}$ | - | $K_{11}$ | $K_{28}$ | $K_{45}$ | $K_{62}$ | $K_{79}$ | $K_{88}$ | $K_{105}$ | $K_{122}$ |
| $M_{10}$ | - | $K_{10}$ | $K_{27}$ | $K_{44}$ | $K_{61}$ | $K_{78}$ | $K_{95}$ | $K_{104}$ | $K_{121}$ |
| $M_9$ | - | $K_9$ | $K_{26}$ | $K_{43}$ | $K_{60}$ | $K_{77}$ | $K_{94}$ | $K_{111}$ | $K_{120}$ |
| $M_8$ | - | $K_8$ | $K_{25}$ | $K_{42}$ | $K_{59}$ | $K_{76}$ | $K_{93}$ | $K_{110}$ | $K_{127}$ |
| $M_7$ | - | $K_7$ | $K_{16}$ | $K_{33}$ | $K_{50}$ | $K_{67}$ | $K_{84}$ | $K_{101}$ | $K_{118}$ |
| $M_6$ | - | $K_6$ | $K_{23}$ | $K_{32}$ | $K_{49}$ | $K_{66}$ | $K_{83}$ | $K_{100}$ | $K_{117}$ |
| $M_5$ | - | $K_5$ | $K_{22}$ | $K_{39}$ | $K_{48}$ | $K_{65}$ | $K_{82}$ | $K_{99}$ | $K_{116}$ |
| $M_4$ | - | $K_4$ | $K_{21}$ | $K_{38}$ | $K_{55}$ | $K_{64}$ | $K_{81}$ | $K_{98}$ | $K_{115}$ |
| $M_3$ | $W_7$ | $K_3$ | $K_{20}$ | $K_{37}$ | $K_{54}$ | $K_{71}$ | $K_{80}$ | $K_{97}$ | $K_{114}$ |
| $M_2$ | $W_6$ | $K_2$ | $K_{19}$ | $K_{36}$ | $K_{53}$ | $K_{70}$ | $K_{87}$ | $K_{96}$ | $K_{113}$ |
| $M_1$ | $W_5$ | $K_1$ | $K_{18}$ | $K_{35}$ | $K_{52}$ | $K_{69}$ | $K_{86}$ | $K_{103}$ | $K_{112}$ |
| $M_0$ | $W_4$ | $K_0$ | $K_{17}$ | $K_{34}$ | $K_{51}$ | $K_{68}$ | $K_{85}$ | $K_{102}$ | $K_{119}$ |

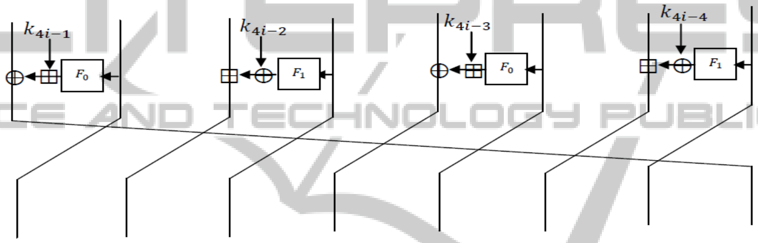


Figure 1: One encryption round of the HIGHT.

$$F_0(x) = x \lll 1 \oplus x \lll 2 \oplus x \lll 7,$$
$$F_1(x) = x \lll 3 \oplus x \lll 4 \oplus x \lll 6.$$

#### 2.2.4 Final Transformation

The final transformation applies four whitening key bytes $W_4, W_5, W_6, W_7$ and mixing operation on output of the last round to produce ciphertext.

$$Final\ Transformation(X_{32}, C, W_7, W_6, W_5, W_4)$$
$$\{$$
$$C_0 \leftarrow X_{32,1} \boxplus W_4; C_1 \leftarrow X_{32,2};$$
$$C_2 \leftarrow X_{32,2} \oplus W_5; C_3 \leftarrow X_{32,4};$$
$$C_4 \leftarrow X_{32,5} \boxplus W_6; C_5 \leftarrow X_{32,6};$$
$$C_6 \leftarrow X_{32,7} \oplus W_7; C_7 \leftarrow X_{32,0}$$
$$\}$$

# 3 CONDITIONAL ATTACK ON THE FULL-ROUND HIGHT

In this section, an improved related-key impossible differential attack on full-round algorithm is introduced. The attack is mounted on a specific 24-round differential characteristic used for filtering the wrong subkeys. The details of the mentioned differential characteristic is depicted in Tables 3 to 6.

## 3.1 24-round Characteristic

The 24-round characteristic is derived by imposing a condition on 3 key bits of $M_4$: $M_4^0 = M_4^1 = M_4^6 = 0$. Imposing this condition causes that the differentials in byte positions 1 and 7 in round 29 of Table 5 results byte differential at position 6 in round 28 in the same table with probability one (using inverse characteristic). Introducing this condition with the probability of $2^{-3}$ has no impact on the 24-round key differential characteristic which means that the 23-round impossible differential path in (Ozen et al., 2009) is increased by one round. In this case 125 key bits must be recovered and the corresponding related-key impossible differential characteristic under key differential $(\delta M_{15}, \delta M_{14}, \ldots, \delta M_8 = 80_x, \ldots \delta M_0)$ is covering rounds 6-29 of the HIGHT:

$$(0,0,0,0,80_x,0,0,0) \nrightarrow (80_x,0,0,0,0,0,0,e_{1,2,7\sim})$$

Forward and backward differential characteristic paths are shown in Tables 4 and 5 and impossible differential is occurred at the $17^{th}$ round of the algorithm.

Table 3: Forward path of plaintexts satisfying the conditions of impossible differential characteristic.

| Forward filter | $B_3$ | | $B_2$ | | $B_1$ | | $B_0$ | | Subkeys | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | | | | |
| IT | ? | $e_{0\sim}$ | $80_x$ | 0 | ? | ? | ? | ? | $W_3$ | $W_2$ | $W_1$ | $W_0$ |
| 0 | ? | $e_{0\sim}$ | $80_x$ | 0 | ? | ? | ? | ? | $K_3$ | $K_2$ | $K_1$ | $K_0$ |
| 1 | ? | $e_{0\sim}$ | $80_x$ | 0 | ? | ? | ? | ? | $K_7$ | $K_6$ | $K_5$ | $K_4$ |
| 2 | $80_x$ | 0 | 0 | 0 | ? | ? | ? | $z_{1\sim}$ | $K_{11}$ | $K_{10}$ | $K_9$ | $K_8$ |
| 3 | 0 | 0 | 0 | 0 | ? | ? | $z_{1\sim}$ | $80_x$ | $K_{15}$ | $K_{14}$ | $K_{13}$ | $K_{12}$ |
| 4 | 0 | 0 | 0 | 0 | ? | $e_{1\sim}$ | $80_x$ | 0 | $K_{19}$ | $K_{18}$ | $K_{17}$ | $K_{16}$ |
| 5 | 0 | 0 | 0 | 0 | $e_{1\sim}$ | $80_x$ | 0 | 0 | $K_{23}$ | $K_{22}$ | $K_{21}$ | $K_{20}$ |

Table 4: Forward path of impossible differential characteristic.

| Forward impossible differential characteristic | $B_3$ | | $B_2$ | | $B_1$ | | $B_0$ | | Subkeys | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | | | | |
| 6 | 0 | 0 | 0 | 0 | $80_x$ | 0 | 0 | 0 | $K_{27}$ | $K_{26}$ | $K_{25}$ | $K_{24}$ |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $K_{31}$ | $K_{30}$ | $K_{29}$ | $K_{28}$ |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $K_{35}$ | $K_{34}$ | $K_{33}$ | $K_{32}$ |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $K_{39}$ | $K_{38}$ | $K_{37}$ | $K_{36}$ |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $K_{43}$ | $K_{42}$ | $K_{41}$ | $K_{40}$ |
| 11 | 0 | $80_x$ | 0 | 0 | 0 | 0 | 0 | 0 | $K_{47}$ | $K_{46}$ | $K_{45}$ | $K_{44}$ |
| 12 | $80_x$ | 0 | 0 | 0 | 0 | 0 | 0 | $e_{0\sim}$ | $K_{51}$ | $K_{50}$ | $K_{49}$ | $K_{48}$ |
| 13 | 0 | 0 | 0 | 0 | 0 | ? | $e_{0\sim}$ | $80_x$ | $K_{55}$ | $K_{54}$ | $K_{53}$ | $K_{52}$ |
| 14 | 0 | 0 | 0 | ? | ? | $e_{0\sim}$ | $80_x$ | 0 | $K_{59}$ | $K_{58}$ | $K_{57}$ | $K_{56}$ |
| 15 | 0 | ? | ? | ? | $e_{0\sim}$ | $80_x$ | 0 | $80_x$ | $K_{63}$ | $K_{62}$ | $K_{61}$ | $K_{60}$ |
| 16 | ? | ? | ? | $e_{0\sim}$ | $80_x$ | $e_{0\sim}$ | $80_x$ | ? | $K_{67}$ | $K_{66}$ | $K_{65}$ | $K_{64}$ |
| 17 | ? | ? | $e_{0\sim}$ | ? | $e_{0\sim}$ | ? | ? | ? | $K_{71}$ | $K_{70}$ | $K_{69}$ | $K_{68}$ |

Table 5: Backward path of impossible differential characteristic.

| Backward impossible differential characteristic | $B_3$ | | $B_2$ | | $B_1$ | | $B_0$ | | Subkeys | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | | | | |
| 17 | ? | $e_{0\sim}$ | $80_x$ | 0 | ? | ? | ? | ? | $K_{71}$ | $K_{70}$ | $K_{69}$ | $K_{68}$ |
| 18 | $e_{0\sim}$ | $80_x$ | 0 | 0 | ? | ? | ? | ? | $K_{75}$ | $K_{74}$ | $K_{73}$ | $K_{72}$ |
| 19 | $80_x$ | 0 | 0 | 0 | ? | ? | ? | $e_{0\sim}$ | $K_{79}$ | $K_{78}$ | $K_{77}$ | $K_{76}$ |
| 20 | 0 | 0 | 0 | 0 | ? | ? | $e_{0\sim}$ | $80_x$ | $K_{83}$ | $K_{82}$ | $K_{81}$ | $K_{80}$ |
| 21 | 0 | 0 | 0 | 0 | ? | $e_{0\sim}$ | $80_x$ | 0 | $K_{87}$ | $K_{86}$ | $K_{85}$ | $K_{84}$ |
| 22 | 0 | 0 | 0 | 0 | $e_{0\sim}$ | $80_x$ | 0 | 0 | $K_{91}$ | $K_{90}$ | $K_{89}$ | $K_{88}$ |
| 23 | 0 | 0 | 0 | 0 | $80_x$ | 0 | 0 | 0 | $K_{95}$ | $K_{94}$ | $K_{93}$ | $K_{22}$ |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $K_{99}$ | $K_{98}$ | $K_{97}$ | $K_{96}$ |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $K_{103}$ | $K_{102}$ | $K_{101}$ | $K_{100}$ |
| 26 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $K_{107}$ | $K_{106}$ | $K_{105}$ | $K_{104}$ |
| 27 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $K_{111}$ | $K_{110}$ | $K_{109}$ | $K_{108}$ |
| 28 | 0 | $80_x$ | 0 | 0 | 0 | 0 | 0 | 0 | $K_{115}$ | $K_{114}$ | $K_{113}$ | $K_{112}$ |
| 29 | $80_x$ | 0 | 0 | 0 | 0 | 0 | 0 | $e_{0,1,6}$ | $K_{119}$ | $K_{118}$ | $K_{117}$ | $K_{116}$ |

Table 6: Backward path of ciphertexts satisfying the conditions of impossible differential characteristic.

| Backward filter | $B_3$ | | $B_2$ | | $B_1$ | | $B_0$ | | Subkeys | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | | | | |
| 30 | 0 | 0 | 0 | 0 | 0 | $e_{1\sim}$ | $e_{0,1,6}$ | $80_x$ | $K_{123}$ | $K_{122}$ | $K_{121}$ | $K_{120}$ |
| 31 | 0 | 0 | 0 | ? | $e_{1\sim}$ | $e_{0\sim}$ | $80_x$ | 0 | $K_{127}$ | $K_{126}$ | $K_{125}$ | $K_{124}$ |
| FT | 0 | ? | ? | ? | $e_{0\sim}$ | $80_x$ | 0 | 0 | $W_7$ | $W_6$ | $W_5$ | $W_4$ |
| C | 0 | 0 | ? | ? | ? | $e_{0\sim}$ | $80_x$ | 0 | | | | |

Table 7: Key filtering process-in this table by imposing conditions on $M_4$ all subkeys will be involved together.

| Step | Guess | Subkeys to be used | Bytes to be extracted | Check (bitwise) | No. of bit conditions | Remaining efforts | Time complexity |
|---|---|---|---|---|---|---|---|
| 1 | $M_{13}, M_1$ | $W_1, K_1$ | 3,4 of $X_1$ | (?, 0) | 8 | $2^{69}$ | $2^{87}$ |
| 2 | $M_0, M_{12}$ | $W_0, K_0$ | 1,2 of $X_1$ | - | - | $2^{69}$ | $2^{79}$ |
| 3 | $M_5$ | $K_5$ | 3,4 of $X_2$ | (?, 0) | 8 | $2^{61}$ | $2^{95}$ |
| 4 | $M_2, M_{15}$ | $W_6, K_{126}$ | 4, 5 of $X_{31}$ | (?, 0) | 8 | $2^{53}$ | $2^{71}$ |
| 5 | $M_{14}$ | $W_5, K_{125}$ | 2, 3 of $X_{31}$ | $(e_{0\sim}, e_{1\sim})$ | 2 | $2^{51}$ | $2^{63}$ |
| 6 | $M_{10}$ | $K_{121}$ | 2, 3 of $X_{30}$ | $(e_{0\sim}, 0)$ | 8 | $2^{43}$ | $2^{77}$ |
| 7 | $M_3$ | $W_3, K_3$ | 0, 7 of $X_1$ | - | - | - | $2^{63}$ |
| 8 | $M_4$ | $K_4$ | 1, 2 of $X_2$ | - | - | - | $2^{66}$ |
| 9 | $M_9$ | $K_9$ | 3, 4 of $X_3$ | (?, 0) | 8 | $2^{35}$ | $2^{82}$ |
| 10 | - | $W_{49}, K_{124}$ | 0, 1 of $X_{31}$ | - | - | - | $2^{47}$ |
| 11 | - | $K_{120}$ | 0, 1 of $X_{30}$ | $(80_x, e_{0,1,6})$ | 7 | $2^{28}$ | $2^{61}$ |
| 12 | - | $K_{116}$ | 0, 1 of $X_{29}$ | $(0, e_{0,1,6})$ | 6 | $2^{22}$ | $2^{70}$ |
| 13 | - | $W_2, K_2$ | 5, 6 of $X_1$ | - | - | - | $2^{32}$ |
| 14 | $M_7$ | $K_7$ | 0, 7 of $X_2$ | - | - | - | $2^{48}$ |
| 15 | $M_8$ | $K_8$ | 1, 2 of $X_3$ | - | - | - | $2^{64}$ |
| 16 | - | $K_{13}$ | 3, 4 of $X_4$ | (?, 0) | 8 | $2^{14}$ | $2^{85}$ |
| 17 | $M_6$ | $K_6$ | 2, 6 of $X_2$ | - | - | - | $2^{40}$ |
| 18 | $M_{11}$ | $K_{11}$ | 0, 7 of $X_3$ | - | - | - | $2^{56}$ |
| 19 | - | $K_{12}$ | 1, 2 of $X_4$ | - | - | - | $2^{80}$ |
| 20 | - | $K_{17}$ | 3, 4 of $X_5$ | $(e_{1\sim}, 0)$ | 8 | $2^6$ | $2^{104}$ |
| 21 | - | $K_{10}$ | 5, 6 of $X_3$ | - | - | - | $2^{48}$ |
| 22 | - | $K_{15}$ | 0, 7 of $X_4$ | - | - | - | $2^{72}$ |
| 23 | - | $K_{16}$ | 1, 2 of $X_5$ | - | - | - | $2^{96}$ |
| 24 | - | $K_{21}$ | 3, 4 of $X_6$ | $(80_X, 0)$ | 7 | - | $2^{101}$ |



## 3.2 Key Filtration

In this section, the key filtering procedure is explained. Removing impossible keys procedure is done in two steps. At first the required number of chosen plaintexts are produced to encrypt and then the wrong keys are discarded by guessing the key bits based on the texts.

The structure of required plaintext has been shown in Table 3. Required conditions are imposed on the plaintext to fulfill 24-round related-key impossible differential characteristic and the corresponding keys will be eliminated from whole key space. Similarly in Table 6 by choosing ciphertexts we discard those keys that will satisfy in the second portion of the impossible differential characteristic as well as the right keys in this process. This procedure is operated as follows.

### 3.2.1 Step 1

$2^{17}$ plaintext structures are selected where each contains $2^{47}$ texts: The fourth and fifth byte and the first bit of the sixth byte of each structure are assigned to constant values. The other bit positions get all possible values to satisfy the conditions of the first row of Table 3. Number of all possible plaintext pairs for encryption is evaluated as the following:

$$\binom{2^{47}}{2} 2^{17} \approx 2^{110} \quad (1)$$

### 3.2.2 Step 2

Encrypt all plaintexts $P_i(P'_i)$ under key $K(K'_i)$ to get ciphertexts $C_i(C'i)$ in which $K \oplus K' = (0,0,...,0,80_x,0,...,0)$ and $C \oplus C' = (0,0,*,*,*,e_{0\sim},80_x,0)$ (see differentials in row FT of Table 6). In this step 33 bits are filtered and $2^{77}$ plaintext pairs are left.

### 3.2.3 Step 3

The procedure of filtering the wrong keys is shown step by step in Table 7. In step 24 from Table 7, a guessed related key is discarded if a pair satisfies the related-key impossible differential characteristic. As there is a condition on 7 bits in step 24, each plaintext pair will suggest $2^{-7}$ wrong keys and at the end $2^{125}(1-2^{-7})^{2^6} = 2^{124.276}$ keys are remained. Time and memory complexities of this scenario is about $2^{104.177}$ and $2^{101}$ respectively and it requires data complexity corresponding to block size i.e., $2^{64}$. This can be derived simply by calculating the required complexity for each of 24 steps.

## 4 EXTENSION OF THE ATTACK AND CONCLUSIONS

In 3, all of the impossible keys of the attack has been suggested based on the assumption $K_4 = (?0????00)$ which forces 3 bits of $K_4$ to be zero. Now we remove this condition and extend the attack. In the new scenario, we guess a differential $\alpha = (0, 0, \ldots, (0z0000yx), \ldots 0)$ and we assign it to two chosen keys $K$ and $K'$ with non-zero common bits (in positions 0, 1 and, 6 of $K_4$). By guessing $2^3$ bits from $\alpha$ the corresponding space of rejected keys is mapped to the one of 3 so that $K \oplus \alpha = (?, ?, \ldots, K_4 = (?0????00), \ldots, ?)$ and $(K \oplus \alpha \oplus \beta = (?, ?, \ldots, K'_4 = (?0????00), \ldots, ?)$. By trying all possible values of $\alpha$ , the 24-step process of Section 3 is repeated to discard $2^3 2^{125}(1-2^{-7})^{2^6} = 2^{127.276}$ number of keys. Regarding to the discussions in Section 3, the whole exhaustive search space of key is reduced to $2^{127.276}$ which means the reduction in the entropy by 0.724. The computational complexity of the key filtering is around $2^3 2^{104.177} = 2^{107.177}$. Also it requires data complexity around $2^{64}$ and memory complexity about $2^3 2^{101} = 2^{104}$.

## REFERENCES


Biham, E., Biryukov, A., and Shamir, A. (1999). Miss in the middle attacks on idea and khufu. In *FSE 1999, LNCS, vol. 1636*. Springer, Heidelberg.

Biham, E., Biryukov, A., and Shamir, A. (2005). Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In *Journal of Cryptology 18(4)*. Springer, Heidelberg.

Biham, E. and Shamir, A. (1991). Differential cryptanalysis of des-like cryptosystems. In *CRYPTO 1990, LNCS, vol. 537*. Springer, Heidelberg.

Hong, D. and et al. (2006). Hight: A new block cipher suitable for low-resource device. In *CHES 2006, LNCS, vol. 4249*. Springer, Heidelberg.

Hong, D., Koo, B., and kwon, D. (2011). Related-key attack on the full hight. In *ICISC 2010, LNCS 6829*. Springer, Heidelberg.

Hong, D., Koo, B., and kwon, D. (2012). Biclique attack on the full hight. In *ICISC 2011, LNCS, vol. 7259*. Springer, Heidelberg.

Lu, J. (2007). Cryptanalysis of reduced versions of the hight block cipher from ches 2006. In *ICISC 2007, LNCS, vol. 4817*. Springer, Heidelberg.

Lucks, S. (2002). The saturation attacka bait for twofish. In *FSE 2001, LNCS, vol. 2355*. Springer, Heidelberg.

Matsui, M. (1994). Linear cryptanalysis method for des cipher. In *EUROCRYPT 1993, LNCS, vol. 765*. Springer, Heidelberg.

Ozen, O., Vaici, K., Tezcan, C., and Kocair, C. (2009). Lightweight block cipher revisited: Cryptanalysis of reduced round present and hight. In *CANS 2009, LNCS, vol. 5888*. Springer, Heidelberg.

Zhang, P., Sun, B., and Li, C. (2009). Saturation attack on the block cipher hight. In *ACISP 2009, LNCS, vol. 5594*. Springer, Heidelberg.