Saturation Attack on the Block Cipher HIGHT

Peng Zhang[1], Bing Sun[1], and Chao Li[1,2]

[1] Department of Mathematics and System Science, Science College of National University of Defence Technology, Changsha, 410073, China
[2] State Key Laboratory of Information Security, Institute of Software of Chinese Academy of Sciences, Beijing, 100190, China
cheetahzhp@163.com

Abstract. HIGHT is a block cipher with 64-bit block length and 128-bit key length, which was proposed by Hong et al. in CHES 2006 for extremely constrained environments such as RFID tags and sensor networks. In this paper, a new saturation attack on HIGHT is discussed. We first point out and correct an error in the 12-round saturation distinguishers given by the HIGHT proposers. And then two new 17-round saturation distinguishers are described. Finally, we present a 22-round saturation attack on HIGHT including full whitening keys with $2^{62.04}$ chosen plaintexts and $2^{118.71}$ 22-round encryptions.

Keywords: Block cipher, HIGHT, Distinguisher, Saturation attack.

1 Introduction

With the establishment of the AES[18], the need for new block ciphers has been greatly diminished. The AES is an excellent and preferred choice for almost all block cipher applications. However, despite recent implementation advances, the AES is not suitable for extremely constrained environments such as RFID(Radio Frequency Identification) tags and sensor networks which are low-cost with limited resources. So some block ciphers suitable for these environments have been designed, such as TEA[25], HIGHT[10], SEA[22], CGEN[20], mCrypton[13], PRESENT[5] and so on.

HIGHT[10] is a block cipher with 64-bit block length and 128-bit key length, which is suitable for low-cost, low-power and ultra-light implementations, such as RFID systems. It has a 32-round iterative structure which is a variant of generalized Feistel network. Due to the simple operations such as XOR, addition mod 2^8 and left bitwise rotation, HIGHT is especially efficient in hardware implementations.

Square attack, proposed by Daemen et al. in[6], is a dedicated attack on the block cipher SQUARE. And it has been applied to some other block ciphers based on the SPN structure. In order to apply square attack to the Feistel structure, Lucks introduced the saturation attack on the Twofish cipher in FSE 2001[16], which is a variation of square attack. Then in[4], Biryukov et al. proposed the multiset attack by which we can break a 4-round SPN cipher even

J.A. Garay, A. Miyaji, and A. Otsuka (Eds.): CANS 2009, LNCS 5888, pp. 76–86, 2009.

if the S-box is unknown. And in[12], a more generalized attack, named integral attack, was proposed by Knudsen et al.. Furthermore, Z'aba et al. presented the bit-pattern based integral attack against bit-based block ciphers in[28], which is a new type of integral attack. Consequently, some famous ciphers have been analyzed based on the idea of the attacks shown above, such as Rijndael[8], FOX[26], Camellia[7,9,27], SMS4[14], CLEFIA[21,23] and so on.

In[10], the HIGHT proposers had analyzed its security against some existing cryptanalytic attacks, they described a differential attack[3], a linear attack[17] and a boomerang attack[24] on 13-round HIGHT, a truncated differential attack[11] and a saturation attack[16] on 16-round HIGHT, an impossible differential attack[1] on 18-round HIGHT, and finally a related-key boomerang attack[2] on 19-round HIGHT. Subsequently, Lu gave an impossible differential attack on 25-round HIGHT, a related-key rectangle attack on 26-round HIGHT, and a related-key impossible differential attack on 28-round HIGHT[15]. Furthermore, Özen et al. presented an impossible differential attack on 26-round HIGHT and a related-key impossible differential attack on 31-round HIGHT[19].

Particularly in [10], the proposers gave some 12-round saturation distinguishers which were applied to the attack on 16-round HIGHT with 2^{42} chosen plaintexts and 2^{51} 16-round encryptions. In this paper, we first point out and correct an error in the 12-round saturation distinguishers shown in[10]. Then two new 17-round saturation distinguishers are described. Finally, we present a 22-round saturation attack on HIGHT including full whitening keys with $2^{62.04}$ chosen plaintexts and $2^{118.71}$ 22-round encryptions.

The paper is organized as follows. In Section 2, we briefly describe some notations and the HIGHT block cipher. Section 3 corrects an error in the 12-round distinguishers shown in[10] and gives two new 17-round saturation distinguishers. Then the attacks are discussed in section 4. Finally, we conclude this paper and summarize our findings in Section 5.

2 Preliminaries

2.1 Notations

In order to clearly illustrate the following encryption and attack, some notations and symbols are defined as follows:

$\oplus$: XOR (exclusive OR);

$\boxplus$: addtion modulo 2^8;

$A^{<<<s}$: s-bit left rotation of an 8-bit value A;

$P = (P_7, P_6, \cdots, P_0)$: the plaintext;

$C = (C_7, C_6, \cdots, C_0)$: the ciphertext;

$X_i = (X_{i,7}, X_{i,6}, \cdots, X_{i,0})$: the output of the i-th round$(1 \le i \le 32)$;

$X_{i-1} = (X_{i-1,7}, X_{i-1,6}, \cdots, X_{i-1,0})$: the input of the i-th round$(1 \le i \le 32)$;

$X_{i,j}^{(k)} (0 \le k \le 7)$: the k-th bit of $X_{i,j}$;

$MK = (MK_{15}, MK_{14}, \cdots, MK_0)$: the master key;

$MK_{i,j} (0 \le j \le 7)$: the j-th bit of MK_i;

$WK_i (0 \le i \le 7)$: the whitening keys;

$WK_{i,j} (0 \le j \le 7)$: the j-th bit of WK_i;

$SK_i (0 \le i \le 127)$: the round keys;

$SK_{i,j} (0 \le j \le 7)$: the j-th bit of SK_i.

2.2 The HIGHT Block Cipher

The encryption procedure can be described as follows:

Step1. Perform the Initial Transformation, which transforms a plaintext P to the input of the first round X_0 by using the four whitening keys, WK_0, WK_1, WK_2 and WK_3.

$$X_{0,0} = P_0 \boxplus WK_0; X_{0,1} = P_1; X_{0,2} = P_2 \oplus WK_1; X_{0,3} = P_3;$$
$$X_{0,4} = P_4 \boxplus WK_2; X_{0,5} = P_5; X_{0,6} = P_6 \oplus WK_3; X_{0,7} = P_7.$$

Step2. For $i = 1, 2, \cdots, 32$, Round Function transforms X_{i-1} to X_i as follows, which is shown in Fig.1.

$$\begin{aligned}
X_{i,0} &= X_{i-1,7} \oplus (F_0(X_{i-1,6}) \boxplus SK_{4i-1});\\
X_{i,1} &= X_{i-1,0};\\
X_{i,2} &= X_{i-1,1} \boxplus (F_1(X_{i-1,0}) \oplus SK_{4i-2});\\
X_{i,3} &= X_{i-1,2};\\
X_{i,4} &= X_{i-1,3} \oplus (F_0(X_{i-1,2}) \boxplus SK_{4i-3});\\
X_{i,5} &= X_{i-1,4};\\
X_{i,6} &= X_{i-1,5} \boxplus (F_1(X_{i-1,4}) \oplus SK_{4i-4});\\
X_{i,7} &= X_{i-1,6}.
\end{aligned}$$

And the functions F_0 and F_1 are defined as:

$$F_0(x) = (x^{<<<1}) \oplus (x^{<<<2}) \oplus (x^{<<<7}),$$
$$F_1(x) = (x^{<<<3}) \oplus (x^{<<<4}) \oplus (x^{<<<6}).$$

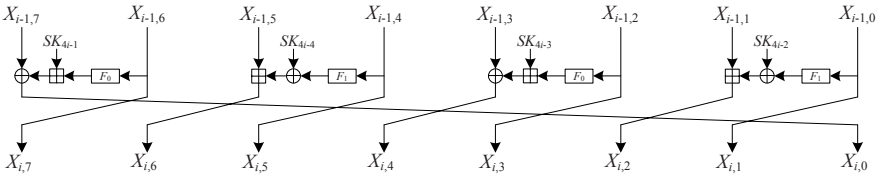

Fig. 1. The i-th Round Function of HIGHT for $i = 1, 2, \cdots, 32$

Step3. Perform the Final Transformation, which untwists the swap of the last round function and transforms X_{32} to the ciphertext C by using the four whitening keys, WK_4, WK_5, WK_6 and WK_7.

$$C_0 = X_{32,1} \boxplus WK_4; C_1 = X_{32,2}; C_2 = X_{32,3} \oplus WK_5; C_3 = X_{32,4};$$
$$C_4 = X_{32,5} \boxplus WK_6; C_5 = X_{32,6}; C_6 = X_{32,7} \oplus WK_7; C_7 = X_{32,0}.$$

The key schedule of HIGHT consists of two algorithms, which generate 8 whitening key bytes $WK_i (0 \leq i \leq 7)$ and 128 subkey bytes $SK_j (0 \leq j \leq 127)$. Firstly, the 128-bit master key is considered as a concatenation of 16 bytes and denoted by $MK = (MK_{15}, MK_{14}, \cdots, MK_0)$. Then the whitening key bytes are generated as follows:

$$WK_i = MK_{i+12} (i = 0, 1, 2, 3);$$
$$WK_i = MK_{i-4} (i = 4, 5, 6, 7).$$

And the subkey bytes are generated as follows:

$$SK_{16 \cdot i+j} = MK_{j-i \bmod 8} \boxplus \delta_{16 \cdot i+j} (0 \leq i, j \leq 7),$$
$$\text{or } SK_{16 \cdot i+j+8} = MK_{(j-i \bmod 8)+8} \boxplus \delta_{16 \cdot i+j+8} (0 \leq i, j \leq 7),$$

where $\delta_{16 \cdot i+j}$ and $\delta_{16 \cdot i+j+8}$ are public constants.

3 Saturation Distinguishers

Now we will point out and correct an error in the saturation distinguishers shown in[10]. Furthermore, two new 17-round saturation distinguishers will be presented.

3.1 Distinguishers based on Byte Saturation

Let $S = \{Y_i | Y_i = (Y_{i,7}, Y_{i,6}, \cdots, Y_{i,0}) \in \{0,1\}^8, 0 \leq i < 2^8\}$ be a set of 8-bit values, where $Y_{i,k} (0 \leq k \leq 7)$ is the k-th bit of Y_i. Then we categorize the status of the set S into five groups depending on the conditions defined as follows:

(1) Const(C): if $\forall i, j, Y_i = Y_j$,

(2) All(A): if $\forall i, j, i \neq j \Longleftrightarrow Y_i \neq Y_j$,

(3) Balance(B): if $\bigoplus_{0 \leq i < 2^8} Y_i = 0$,

(4) Balance$_k$(B_k): if $\bigoplus_{0 \leq i < 2^8} Y_{i,k} = 0$,

(5) Unknown(U): unknown.

Thus, using the conditions, we can get two 11-round saturation distinguishers based on byte saturation which are shown as follows. And the details of distinguisher(I) is shown in Fig.2.

$$\text{(I)}\ \ (A, C, C, C, C, C, C, C) \xrightarrow{11r} (U, U, U, U, B_0, U, U, U),$$
$$\text{(II)}\ \ (C, C, C, C, A, C, C, C) \xrightarrow{11r} (B_0, U, U, U, U, U, U, U).$$

In[10], the HIGHT proposers had described that distinguisher(I) is a 12-round one. From the details shown in Fig.2, we can see that it is only a 11-round one. In addition, we also implement the distinguishers through the computer simulation, and we find that there are no Balance or Balance$_k$ sets in the output of the 12-round encryptions. That is to say, the distinguishers based on byte saturation are only 11-round ones.

3.2 17-Round Distinguishers

With the two 11-round distinguishers shown above, we can deduce two 17-round ones, respectively. Hereinafter, we will give the details.

Firstly, we explain how to extend to 12-round distinguishers. Let $A_{(16)}$ be an All state of 16-bit values, and it is divided into two segments as $A_{(16)} = A_{1(16)}|A_{0(16)}$. Then we can get the 12-round distinguishers as follows:

$$\text{(I)}\ \ (A_{1(16)}, A_{0(16)}, C, C, C, C, C, C) \xrightarrow{12r} (U, U, U, U, B_0, U, U, U),$$
$$\text{(II)}\ \ (C, C, C, C, A_{1(16)}, A_{0(16)}, C, C) \xrightarrow{12r} (B_0, U, U, U, U, U, U, U).$$

These distinguishers can be explained in the following way. After the first round of distinguisher(I), $(A_{1(16)}, A_{0(16)}, C, C, C, C, C, C)$ becomes $(A_{0(16)}, C, C, C, C, C, C, A'_{1(16)})$, where the concatenated segment $A'_{1(16)}|A_{0(16)}$ is also an All sate. It can be regarded as that $(A_{0(16)}, C, C, C, C, C, C, A'_{1(16)})$ contains 2^8 structures of (A, C, C, C, C, C, C, C), where the first rightmost constant takes all possible 2^8 8-bit values. Therefore, the Balance$_0$ state is kept at the output, which is presented in the above 11-round distinguishers. In addition, distinguishers(II) can also be explained using the similar method.

The extensions to 13,14,15,16 and 17-round distinguishers can be obtained in the similar way. Let $A_{(56)}$ be an All state of 56-bit values, which is divided into

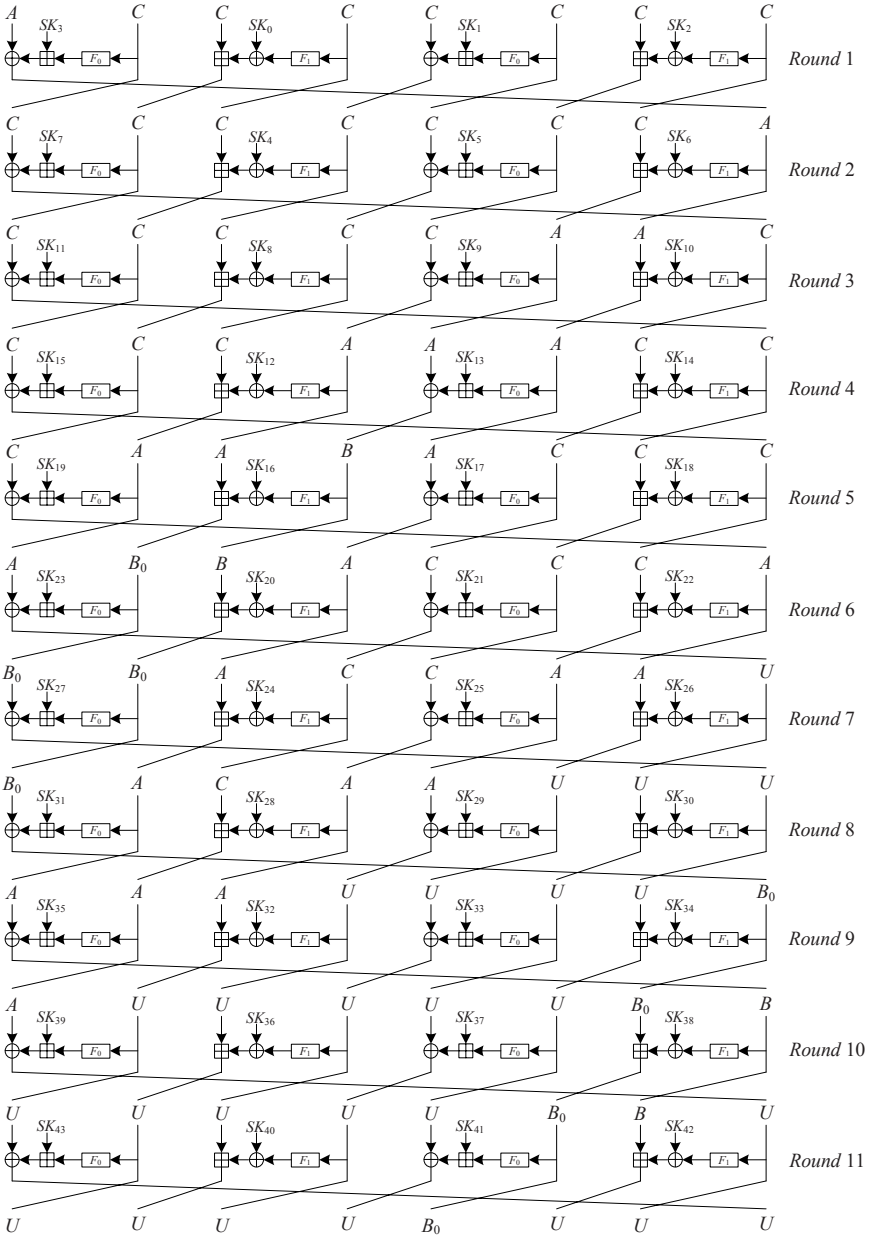

Fig. 2. 11-Round Distinguisher(I) Based on Byte Saturation

seven segments as $A_{(56)} = A_{6(56)}|A_{5(56)}|A_{4(56)}|A_{3(56)}|A_{2(56)}|A_{1(56)}|A_{0(56)}$. Then we can get the 17-round distinguishers as follows.

$$\begin{aligned}(\mathrm{I})(A_{6(56)}, A_{5(56)}, A_{4(56)}, A_{3(56)}, A_{2(56)}, A_{1(56)}, A_{0(56)}, C)\\ \xrightarrow{17r} (U, U, U, U, B_0, U, U, U),\\ (\mathrm{II})(A_{6(56)}, A_{5(56)}, A_{4(56)}, C, A_{3(56)}, A_{2(56)}, A_{1(56)}, A_{0(56)})\\ \xrightarrow{17r} (B_0, U, U, U, U, U, U, U).\end{aligned}$$

4 Saturation Attack with Full Whitening Keys

4.1 Attack Procedure

With the two 17-round distinguishers, a 22-round saturation attack on HIGHT can be obtained. As an example, we give the attack procedure based on 17-round distinguisher(I) by the following steps, which is shown in Fig.3.

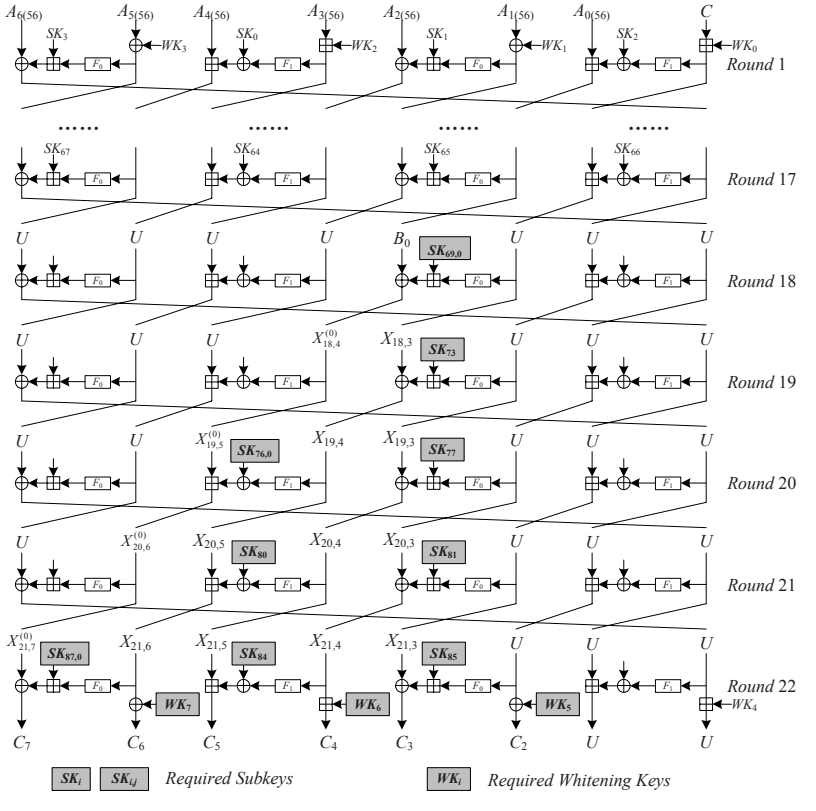

Fig. 3. 22-Round Attack Based on 17-Round Distinguisher(I)

Step1. Chose a set of 2^{56} plaintexts which has the following format:

$$S = (A_{6(56)}, A_{5(56)}, A_{4(56)}, A_{3(56)}, A_{2(56)}, A_{1(56)}, A_{0(56)}, C).$$

Ask for the corresponding ciphertexts C_7, C_6, C_5, C_4, C_3 and C_2 after the 22-round encryptions.

Step2. Guess the subkeys and the whitening keys as follows:

$$SK_{69,0}, SK_{73}, SK_{76,0}, SK_{77}, SK_{80}, SK_{81}, SK_{84}, SK_{85}, SK_{87,0},$$
$$WK_5, WK_6, WK_7.$$

Since the value $X_{17,3}$ which is a Balance$_0$ state can be calculated by the guessed keys and the ciphertexts obtained in Step1. Then the correct keys can be checked by the following equation.

$$\bigoplus_{P \in S} X_{17,3}^{(0)} = \bigoplus_{P \in S} F(C_i, SK_{j,0}, SK_k, WK_l) = 0, \tag{1}$$

where P is the plaintext, i=7,6,5,4,3,2, $j = 69, 76, 87$, $k = 73, 77, 80, 81, 84, 85$ and $l = 5, 6, 7$.

If the equation is satisfied, accept the guessed keys as the candidates for the correct keys. Otherwise, discard the keys.

Step3. For the key candidates kept in Step2, chose another set which has the format shown in Step1 and check whether Eq.1 is satisfied. If it is satisfied, keep the keys. Otherwise, discard the ones. Repeat this step, until all the correct keys are obtained exclusively.

Using the similar method, we can get another 22-round saturation attack based on 17-round distinguisher(II). And the following keys require to be guessed in the attack.

$$SK_{71,0}, SK_{75}, SK_{78,0}, SK_{79}, SK_{82}, SK_{83}, SK_{85,0}, SK_{86}, SK_{87},$$
$$WK_4, WK_5, WK_7.$$

4.2 Complexity Analysis

From the key schedule, it is clear that all the guessed keys in the attack are generated by the master key bytes $MK_i (0 \leq i \leq 15)$, respectively. And the generations are shown in Table 1 and Table 2.

In the tables, we can find that some guessed keys are generated by the same master key byte. Thus we need not guess all of them. In addition, the guessed keys in the attack based on distinguisher(II) which have been obtained in the attack based on distinguisher(I) are not required anymore.

Consequently, the guessed keys in the attack based on distinguisher(I) are listed as follows:

$$MK_0, MK_1, MK_2, MK_3, MK_4, MK_7, MK_{8,0}, MK_9, MK_{13}.$$

Table 1. Generation of Guessed Keys in the Attack Based on Distinguisher(I)

$SK_{69,0}$	SK_{73}	$SK_{76,0}$	SK_{77}	SK_{80}	SK_{81}	SK_{84}	SK_{85}	$SK_{87,0}$	WK_5	WK_6	WK_7
$MK_{1,0}$	MK_{13}	$MK_{8,0}$	MK_9	MK_3	MK_4	MK_7	MK_0	$MK_{2,0}$	MK_1	MK_2	MK_3

Table 2. Generation of Guessed Keys in the Attack Based on Distinguisher(II)

$SK_{71,0}$	SK_{75}	$SK_{78,0}$	SK_{79}	SK_{82}	SK_{83}	$SK_{85,0}$	SK_{86}	SK_{87}	WK_4	WK_5	WK_7
$MK_{3,0}$	MK_{15}	$MK_{10,0}$	MK_{11}	MK_5	MK_6	$MK_{0,0}$	MK_1	SK_2	MK_0	MK_1	MK_3

And we merely need guess the following keys in the attack based on distinguisher(II):

$$MK_5, MK_6, MK_{10,0}, MK_{11}, MK_{15}.$$

In the attack, the probability that a key candidate in the key space survives the discarding step is expected to be 2^{-1}. And we need to guess 65-bit and 33-bit key values in the attack based on distinguisher(I) and (II), respectively. Then if we suppose that N sets are required, it is satisfied that

$$2^{65} \cdot 2^{-N} < 1, \text{ and } 2^{33} \cdot 2^{-N} < 1.$$

Besides, the sets used in the attack based on distinguisher(I) can also be used in the attack based on distinguisher(II). Therefore, 66 sets of 2^{56} plaintexts are required to obtain the correct key values exclusively. That is to say, we need $66 \times 2^{56} \approx 2^{62.04}$ plaintexts in the attack. Additionally, we need $(2^{56} \times 2^{65} + 2^{56} \times 2^{64} + \cdots + 2^{56}) + (2^{56} \times 2^{33} + 2^{56} \times 2^{32} + \cdots + 2^{56}) \approx 2^{122}$ F-function computations to get the correct keys. Consequently, the time complexity is $2^{122} \times \frac{9}{22 \times 4} \approx 2^{118.71}$ 22-round encryptions.

5 Conclusion

In this paper, a new saturation attack on HIGHT is discussed. We first point out and correct an error in the 12-round saturation distinguishers shown by the HIGHT proposers. And then two new 17-round saturation distinguishers are described. Finally, we present a 22-round saturation attack on HIGHT including full whitening keys with $2^{62.04}$ chosen plaintexts and $2^{118.71}$ 22-round encryptions. The attack presented in this paper shows that the reduced versions of HIGHT are less secure than they should be.

Acknowledgments. The authors would like to thank the anonymous reviewers for many helpful comments and suggestions. The work in this paper is supported by the Natural Science Foundation of China (No:60803156) and the open research fund of State Key Laboratory of Information Security(No: 01-07).

References

1. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
2. Biham, E., Dunkelman, O., Keller, N.: Related-key boomerang and rectangling attacks. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525. Springer, Heidelberg (2005)
3. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991)
4. Biryukov, A., Shamir, A.: Structural cryptanalysis of SASAS. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 394–405. Springer, Heidelberg (2001)
5. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
6. Daemen, J., Knudsen, L.R., Rijmen, V.: The Block Cipher SQUARE. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997)
7. Duo, L., Li, C., Feng, K.: New observation on Camellia. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 51–64. Springer, Heidelberg (2006)
8. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.: Improved Cryptanalisis of Rijndael. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 213–230. Springer, Heidelberg (2001)
9. He, Y., Qing, S.: Square Attack on Reduced Camellia Cipher. In: Qing, S., Okamoto, T., Zhou, J. (eds.) ICICS 2001. LNCS, vol. 2229, pp. 238–245. Springer, Heidelberg (2001)
10. Hong, D., Sung, J., Hong, S., Kim, J., Lee, S., Koo, B.-S., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S.: HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer, Heidelberg (2006)
11. Knudsen, L.R.: Trucated and higher order differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995)
12. Knudsen, L.R., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
13. Lim, C., Korkishko, T.: mCrypton — A Lightweight Block Cipher for Security of Low-cost RFID Tags and Sensors. In: Song, J.-S., Kwon, T., Yung, M. (eds.) WISA 2005. LNCS, vol. 3786, pp. 243–258. Springer, Heidelberg (2006)
14. Liu, F., Ji, W., Hu, L., Ding, J., Lv, S., Pyshkin, A., Weinmann, R.-P.: Analysis of the SMS4 block cipher. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 158–170. Springer, Heidelberg (2007)
15. Lu, J.: Cryptanalysis of Reduced Versions of the HIGHT BLOCK Cipher from CHES 2006. In: Nam, K.-H., Rhee, G. (eds.) ICISC 2007. LNCS, vol. 4817, pp. 11–26. Springer, Heidelberg (2007)
16. Lucks, S.: The Saturation Attack—A Bait for Twofish. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 1–15. Springer, Heidelberg (2002)
17. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)

18. National Institute of Standards and Technology: FIPS 197: Advanced Encryption Standard (2001), http://csrc.nist.gov
19. Özen, O., Vaici, K., Tezcan, C., Kocair, C.: Lightweight Block Cipher Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT. In: Boyd, C., González Nieto, J. (eds.) ACISP 2009. LNCS, vol. 5594, pp. 90–107. Springer, Heidelberg (2009)
20. Robshaw, M.J.B.: Searching for compact algorithms: CGEN. In: Nguyên, P.Q. (ed.) VIETCRYPT 2006. LNCS, vol. 4341, pp. 37–49. Springer, Heidelberg (2006)
21. Sony Corporation: The 128-bit Blockcipher CLEFIA: Security and Performance Evaluation. Revision 1.0 (2007)
22. Standaert, F.-X., Piret, G., Gershenfeld, N., Quisquater, J.-J.: SEA: A Scalable Encryption Algorithm for Small Embedded Applications. In: Domingo-Ferrer, J., Posegga, J., Schreckling, D. (eds.) CARDIS 2006. LNCS, vol. 3928, pp. 222–236. Springer, Heidelberg (2006); IFIP International Federation for Information Processing (2006)
23. Wang, W., Wang, X.: Saturation cryptanalysis of CLEFIA(in Chinese). Journal on Communications 29(10), 88–92 (2008)
24. Wangner, D.: The boomerang attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)
25. Wheeler, D., Needham, R.: TEA, a Tiny Encryption Algorithm. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 363–366. Springer, Heidelberg (1995)
26. Wu, W., Zhang, W., Feng, D.: Integral Cryptanalysis of Reduced FOX Block Cipher. In: Won, D.H., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 229–241. Springer, Heidelberg (2006)
27. Yeom, Y., Park, S., Kim, I.: On the security of Camellia against the Square attack. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 89–99. Springer, Heidelberg (2002)
28. Z'aba, M.R., Raddum, H., Henricksen, M., Dawson, E.: Bit-Pattern Based Integral Attack. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 363–381. Springer, Heidelberg (2008)