# Meet-in-the-middle Attack with Splice-and-Cut Technique on the 19-round Variant of Block Cipher HIGHT

Yasutaka Igarashi[1], Ryutaro Sueyoshi[1], Toshinobu Kaneko[2], Takayasu Fuchida[1]

[1] Kagoshima University, 1-21-40 Korimoto, Kagoshima, 890-0065 Japan
igarashi@eee.kagoshima-u.ac.jp, fuchida@ibe.kagoshima-u.ac.jp
[2] Tokyo University of Science, 2641 Yamazaki, Noda, Chiba, 278-8510 Japan
kaneko@ee.noda.tus.ac.jp

**Abstract.** We show a meet-in-the-middle (MITM) attack with Splice-and-Cut technique (SCT) on the 19-round variant of the block cipher HIGHT. The original HIGHT having 32-round iteration was proposed by Hong et al. in 2006, which applies the 8-branch Type-2 generalized Feistel network (GFN) with 64-bit data block and 128-bit secret key. MITM attack was proposed by Diffie and Hellman in 1977 as a generic method to analyze symmetric-key cryptographic algorithms. SCT was proposed by Aoki and Sasaki to improve MITM attack in 2009. In this paper we show that 19-round HIGHT can be attacked with $2^8$ bytes of memory, $2^8+2$ pairs of chosen plain and cipher texts, and $2^{120.7}$ times of the encryption operation by using MITM attack with SCT.

**Keywords:** block cipher HIGHT, meet-in-the-middle attack, Splice-and-Cut technique

## 1 Introduction

We show a meet-in-the-middle (MITM) attack with Splice-and-Cut technique (SCT) on the 19-round variant of the block cipher HIGHT. The original HIGHT having 32-round iteration was proposed by Hong et al. in 2006, which applies the 8-branch Type-2 generalized Feistel network (GFN) with 64-bit data block and 128-bit secret key [1]. The designers said that HIGHT does not only consist of simple operations to be ultra-light but also has enough security as a good encryption algorithm.

Table 1 shows the complexity of attack on HIGHT. Sasaki et al. studied integral attack on 22-round HIGHT with data complexity $2^{62}$ and time complexity $2^{102.35}$ [2]. Chen et al. studied impossible differential attack on 27-round HIGHT with data complexity $2^{58}$ and time complexity $2^{126.6}$ [3]. Wen et al. studied zero-correlation attack on 27-round HIGHT with data complexity $2^{62.79}$ and time complexity $2^{120.78}$ [4]. Özen et al. studied related-key impossible differential attack on 31-round HIGHT with data complexity $2^{63}$ and time complexity $2^{127.28}$ [5]. Koo et al. studied related-key rectangle attack on full-round HIGHT with data complexity $2^{57.84}$ and time complexity $2^{125.833}$ [6]. Song et al. studied biclique attack on full-round HIGHT with



K.J. Kim (ed.), *Information Science and Applications,*
Lecture Notes in Electrical Engineering 339, DOI 10.1007/978-3-662-46578-3_50

data complexity $2^{48}$ and time complexity $2^{125.93}$ [7]. Previously security of HIGHT against MITM attack was not investigated.

MITM attack was proposed by Diffie and Hellman in 1977 as a generic method to analyze symmetric-key cryptographic algorithms [8]. Its basic idea is that if a target algorithm can be decomposed into two small consecutive segments and the computation of each segment only involves portions of a master key, then we can check the consistence of the intermediate data of each segment. Because separately analyzing two small segments does not require much effort, the overall time complexity to analyze the whole algorithm could decrease significantly compared to a brute force attack. Recently MITM attack has developed into multidimensional MITM attack [9], [10].

SCT was proposed by Aoki and Sasaki to improve MITM attack in 2009 [11]. In SCT an attacker chooses an arbitrary intermediate state of cipher by supposing a chosen plain text scenario. The data complexity of SCT would increase as compared with simple MITM attack, because the complexity is depend on key bits that we need to partially decrypt or encrypt an intermediate state to obtain a plain text or a cipher text. However the time complexity may decrease, because we have the freedom to choose the intermediate state.

In this article we decompose 19-round HIGHT into a 9.5-round forward segment and a 9.5-round backward segment, and show that HIGHT can be attacked with $2^8$ bytes of memory, $2^8+2$ pairs of chosen plain and cipher texts, and $2^{120.7}$ times of an encryption operation by MITM attack with SCT.

**Table 1.** Complexity of attack on HIGHT. Imp. diff. and zero-c. denote impossible differential and zero-correlation, respectively. Data complexity is represented by the number of pairs of plain and cipher text. Time complexity is represented by the number of encryption operations.

| Attack | MITM | Integral | Imp. diff. | Zero-c. | Related-key imp. diff. | Related-key rectangle | Biclique |
|---|---|---|---|---|---|---|---|
| Round | 19 | 22 | 27 | 27 | 31 | 32 | 32 |
| Data | $2^8+2$ | $2^{62}$ | $2^{58}$ | $2^{62.79}$ | $2^{63}$ | $2^{57.84}$ | $2^{48}$ |
| Time | $2^{120.7}$ | $2^{102.35}$ | $2^{126.6}$ | $2^{120.78}$ | $2^{127.28}$ | $2^{125.833}$ | $2^{125.93}$ |
| Reference | Sect. 3 | [2] | [3] | [4] | [5] | [6] | [7] |

## 2 Overview of data mixing part of 19-round HIGHT

We describe the brief overview of data mixing part of 19-round HIGHT to understand this manuscript. Refer to the original proposal [1] for more details.

Figure 1 shows the data mixing part of 19-round HIGHT, which consists of XOR ($\oplus$), arithmetic addition modulo 16 ($\boxplus$), linear functions $F_0$ and $F_1$. $F_0$ and $F_1$ are given by

$$F_0(x) = x^{\lll 1} \oplus x^{\lll 2} \oplus x^{\lll 7}, \qquad F_1(x) = x^{\lll 3} \oplus x^{\lll 4} \oplus x^{\lll 6} \tag{1}$$

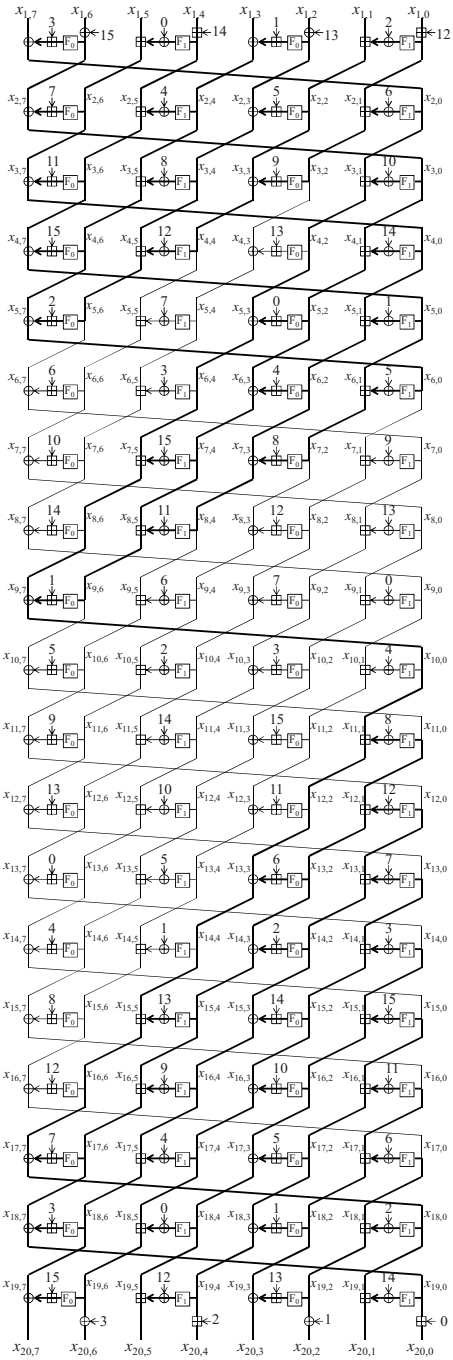

**Fig. 1.** Data mixing part of 19-round HIGHT.

where $x^{<<<i}$ denotes $i$-bit left rotation of 8-bit value $x$. $(x_{i,7}, x_{i,6}, x_{i,5}, x_{i,4}, x_{i,3}, x_{i,2}, x_{i,1}, x_{i,0}) = x_i$ denotes 64-bit input data to the $i$th round ($i$=1, 2, 3, …, 20) where $x_{i,j}$ is 8-bit data ($j$=0, 1, 2, …, 7). $x_0$ and $x_{20}$ represents a plain text and a cipher text, respectively. The numerical symbol $h$ (=0, 1, 2, …, 15) putted into XOR or arithmetic addition denotes 8-bit segment $MK_h$ of 128-bit secret key, to which the constant value [1] is added. For example, 8 pieces of $MK_h$ ($h$=0, 1, 2, 3, 12, 13, 14, 15) are used in the rounds 1 and 19.

## 3 Outline of MITM Attack with SCT and its application to the 19-round variant of HIGHT

MITM attack is based on the primary idea that we decompose a cipher algorithm into two consecutive parts [8]. Each part of them only involves partial information of a secret key. We encrypt/decrypt each part separately and check whether the intermediate data from each part correspond to each other. Because separately analyzing each part requires low computational complexity, the overall complexity to analyze the whole algorithm could decrease significantly. SCT allows an attacker to choose an arbitrary intermediate state of cipher by supposing a chosen plain text scenario as long as we can access to encryption and decryption oracles. SCT increases data complexity of MITM attack in return for decreasing the time complexity.

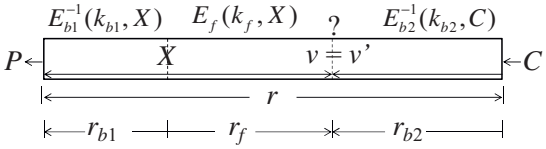


**Fig. 2.** General model of MITM attack with SCT.

Figure 2 shows the general model of MITM attack with SCT [10]. We suppose an encryption algorithm $E(k, P) = C$ can be decomposed into three consecutive parts $E_{b1}^{-1}(k_{b1}, X)$, $E_f(k_f, X)$, and $E_{b2}^{-1}(k_{b2}, C)$ where $P$ and $C$ are a plain text and a cipher text, respectively. $k_f$, $k_{b1}$, and $k_{b2}$ are subkeys used in $E_f$, $E_{b1}^{-1}$, and $E_{b2}^{-1}$, respectively. Subscript $f$ denotes forward process. Subscripts $b1$ and $b2$ denote back processes. We can choose an arbitrary value $X$ for the intermediate state. Then we partially decrypt $X$ to obtain a plain text i.e. $P = E_{b1}^{-1}(k_{b1}, X)$.

Supposing that $k_b = (k_{b1}, k_{b2})$, $k_f$ and $k_b$ are further given by $k_f = (k'_f, k_c)$ and $k_b = (k'_b, k_c)$, respectively where $k_c$ is a common key among $k_f$ and $k_b$. $k'_f$ is the independent key from $k'_b$. $k'_b$ is the independent key from $k'_f$. The number of bits of $k_f$ and $k_b$ are given by $|k_f| = |k'_f| + |k_c|$ and $|k_b| = |k'_b| + |k_c|$, respectively where $|x|$ denotes the number of bits of data $x$. $v = E_f(k_f, X)$ and $v' = E_{b2}^{-1}(k_{b2}, C)$ are intermediate data of an encryption process. $r$ is the total number of $F_i$ ($i$=0, 1) function in the whole algorithm. $r_f$, $r_{b1}$, and $r_{b2}$ represent the total numbers of $F_i$ function that must be calculated to derive $v$ and $v'$ through forward process $E_f$ and backward processes $E_{b1}^{-1}$ and $E_{b2}^{-1}$, respectively. We

can usually derive $r \neq r_f + r_{b1} + r_{b2}$, because some of $F_i$ functions in the whole algorithm are not calculated for the attack. The detailed steps of MITM attack with SCT are as follows [9], [10]:

1. Choose a fixed value for $X$.
2. For each guess of the common key $k_c$,
   (A) Encrypt $X$ and obtain all possible value of $v$ through $E_f(k_f, X)$ for all possible key $k'_f$. And then collect all $k'_f$ in a set $V$ indexed by $v$.
   (B) For each guess of the subkey $k'_b$,
      (a) Decrypt $X$ and obtain $P$ through $E_{b1}^{-1}(k_{b1}, X)$.
      (b) Obtain the corresponding cipher text $C$.
      (c) Decrypt $C$ and obtain $v'$ through $E_{b2}^{-1}(k_{b2}, C)$.
      (d) Check whether $v' \in V$. If so output the corresponding key triangle $(k_c, k'_f, k'_b)$ as a possible key.

The memory complexity of this attack is given by the size of $V$ in step 2(A), which is $2^{|k'_f|}$. The time complexity for the step 2(A) in terms of complete encryption is given by $2^{|k_f|} \times r_f/r$. In other words, the time complexity is the number of times of encryption or decryption operation of a target cipher. Similarly the time complexity of the step 2(B) is given by $2^{|k_b|} \times (r_{b1} + r_{b2})/r$. Therefore the time complexity $T$ for these steps is given by

$$T = 2^{|k_f|} \times r_f / r + 2^{|k_b|} \times (r_{b1} + r_{b2}) / r. \tag{2}$$

Because we check for a match as $v = v'$, the total number of possible keys is reduced to $2^{|k'_f|+|k'_b|+|k_c|-|v|}$ when we perform these steps, where $|v|$ is the number of bits of $v$.

We next apply this MITM attack with SCT to 19-round HIGHT. Bold data lines in Fig. 1 are necessary for MITM attack with SCT. We set the intermediate state $X$ as the 64-bit state given by

$$X = (x_{1,6}, x_{1,5}, x_{1,4}, x_{1,3}, x_{1,2}, x_{1,1}, x_{1,0}, x_{2,0}). \tag{3}$$

We set $v$ and $v'$ as the 8-bit state given by

$$v = v' = x_{10,0}. \tag{4}$$

From (3) and (4), the keys $k'_f$, $k'_b$, and $k_c$ are given by 8-bit segment, 8-bit segment, and 112-bit segment of 128-bit secret key as

$$k'_f = MK_8, \quad k'_b = MK_3, \tag{5}$$

$$\begin{aligned} k_c = (&MK_0, MK_1, MK_2, MK_4, MK_5, MK_6, MK_7, \\ &MK_9, MK_{10}, MK_{11}, MK_{12}, MK_{13}, MK_{14}, MK_{15}). \end{aligned} \tag{6}$$

The numbers of $F_i$ functions $r$, $r_f$, $r_{b1}$, and $r_{b2}$ are also derived from (3) and (4) with Fig. 1 as

$$r = 4 \times 19, \quad r_f = 23, \quad r_{b1} = 1, \quad r_{b2} = 24. \tag{7}$$

In other words, $r_f$, $r_{b1}$, and $r_{b2}$ are the numbers of $F_i$ functions on the bold line in forward process and backward processes, respectively. From (5)-(7), (2) can be rewritten as

$$T = 2^{8+112} \times 23/76 + 2^{8+112} \times (1+24)/76 \approx 2^{119.3}. \quad (8)$$

When we perform the steps 1 and 2, the number of possible keys is reduced to $2^{8+8+112-8} = 2^{120}$. These $2^{120}$ pieces of possible key are furthermore reduced to $2^{120-64} = 2^{56}$ when we check these possible keys by exhaustive search with one independent pair of plain text and cipher text, because the block size of HIGHT is 64 bits. Similarly, these $2^{56}$ pieces of possible key are furthermore reduced to $2^{56-64} = 2^{-8}$ when we check these keys by exhaustive search with another independent pair of plain text and cipher text. In this way we can identify a true key because the true key definitely survives although the number of possible keys is less than 1. Therefore overall time complexity $T_a$ for this attack is given by $T$ and 2 times of exhaustive key search as

$$T_a = T + 2^{120} + 2^{56} \approx 2^{120.7}. \quad (9)$$

Memory complexity is given by $2^{|k'_f|} = 2^8$ bytes. Because $x_{1,7}$ has $2^8$ varieties depending on $MK_3$ and $MK_{15}$ on the step 2(B)-(a), a plain text $P$ has $2^8$ varieties. Therefore data complexity $D$ of this attack is given by

$$D = 2^8 + 2. \quad (10)$$

In other words, the data complexity is the number of pairs of pain text and cipher text required for the attack. The constant 2 on the right side of (10) is derived from 2 times of exhaustive key search. We believe that an experimental proof is not required because this theoretical result is not a hypothesis.

## 4 Conclusions

We have shown MITM attack with SCT on the 19-round variant of the block cipher HIGHT, which have not been studied so far. We decomposed 19-round HIGHT into a 9.5-round forward segment and a 9.5-round backward segment, and showed that HIGHT can be attacked with $2^8$ bytes of memory, $2^8+2$ pairs of chosen plain and cipher texts, and $2^{120.7}$ times of an encryption operation by MITM attack with SCT. Future work is the application of multidimensional MITM attack to HIGHT.

## References

1. Hong, D., Sung, J., Hong, S., et al.: HIGHT: A New Block Cipher Suitable for Low-Resource Device. CHES 2006, Lecture Notes in Computer Science, vol. 4249, pp 46-59, Springer (2006)
2. Sasaki, Y., Wang, L.: Meet-in-the-Middle Technique for Integral Attacks against Feistel ciphers. SAC 2012, Lecture Notes in Computer Science, vol. 7707, pp. 234-251, Springer (2013)

3. Chen, J., Wang, M., Preneel, B.: Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT, AFRICACRYPT 2012, Lecture Notes in Computer Science, vol. 7374, pp. 117-137, Springer (2012)
4. Wen, L., Wang, M., Bogdanov, A., Chen, H.: Multidimensional Zero-correlation Attacks on Lightweight Block Cipher HIGHT: Improved Cryptanalysis of an ISO Standard, Information Processing Letters, vol. 114, issue 6, pp. 322-330, ELSEVIER (2014)
5. Özen, O., Varıcı, K., Tezcan, C., Kocair, Ç.: Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT, Information Security and Privacy, Lecture Notes in Computer Science, vol. 5594, pp. 90-107, Springer (2009)
6. Koo, B., Hong, D., Kwon, D.: Related-Key Attack on the Full HIGHT, ICISC 2010, Lecture Notes in Computer Science, vol. 6829, pp. 49-67, Springer (2011)
7. Song, J., Lee, K., Lee, H.: Biclique Cryptanalysis on Lightweight Block Cipher: HIGHT and Piccolo, International Journal of Computer Mathematics, vol. 90, issue 12, pp. 2564-2580, Taylor & Francis (2013)
8. Diffie, M.E., Hellman, W.: Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Computer, vol. 10, issue 6, pp. 74-84, IEEE (1977)
9. Zhu, B., Gong, G.: Multidimensional Meet-in-the-Middle Attack and Its Applications to KATAN32/48/64. Cryptology ePrint Archive: Report 2011/619.
10. Boztaş, Ö., Karakoç, F., Çoban, M.: Multidimensional Meet-in-the-Middle Attacks on Reduced-Round TWINE-128. Lecture Notes in Computer Science, vol. 8162, pp. 55-67, Springer (2013)
11. Aoki, K., Sasaki, Y.: Meet-in-the-Middle Attack against Reduced SHA-0 and SHA-1. CRYPTO 2009, Lecture Notes in Computer Science, vol. 5677, pp 70-89, Springer (2009)