Impossible Differential Cryptanalysis of Hierocrypt-3 Reduced to 3 Rounds

Jung Hee Cheon[1]**, MunJu Kim[2], and Kwangjo Kim[1]

[1] International Research center for Information Security (IRIS),
Information and Communications University (ICU), Korea
{jhcheon, kkj}@icu.ac.kr,
[2] Mathematics Department, Brown University, USA
mjkim@math.brown.edu

Abstract. In this paper, we describe an impossible differential attack on the block cipher Hierocrypt-3 reduced to three rounds which is based on two rounds impossible differential. Since one round in Hierocrypt-3 is equivalent to two rounds in other ciphers with Substitution-Permutation Network structure, our method can be considered to work for two additional rounds attached to the impossible differential. This is the first result on complexity of Hierocrypt against impossible differential attack.

Keywords: Block Cipher, Hierocrypt, Impossible Differential, Differential Cryptanalysis

1 Introduction

The block cipher Hierocrypt is one of the candidates for New European Schemes for Signatures, Integrity, and Encryption(NESSIE) Project [6] and also has submitted for evaluation of Cryptographic Techniques [4] by Information technology Promotion Agency(IPA) in Japan. Hierocrypt has two versions, one for 128-bit and the other for 64-bit. They are called Hierocrypt-3 and Hierocrypt-L1, respectively. Each of them has a nested Substitution-Permutation Network(SPN) structure as proposed in [7]. Nested SPN structure uses SPN structure in its component function repeatedly. That is, one large S-box consists of two substitution layers with smaller S-boxes and one permutation layer in the middle of them. Thus one round in nested SPN structure has two substitution layers, and so corresponds to two rounds in normal SPN structure.

Block ciphers with SPN structure has advantage that it is easy to design to resist against classical Differential Cryptanalysis and Linear Cryptanalysis. Most powerful attacks for those ciphers are usually square attacks and impossible differential attacks. The designers of Hierocrypt family have described square attacks on each version of Hierocrypt reduced to 2.5 rounds, which has five substitution layers, in the self-evaluation reports [9]. In [3], improved square attacks were reported on Hierocrypt-3 reduced to 3 rounds and Hierocrypt-L1 reduced to 3.5 rounds.

In this paper, we propose an impossible differential attack on Hierocrypt-3 reduced to 3 rounds using 2 rounds impossible differential. For the cases of Rijndael(AES) and Crypton with SPN structure, only 5 round impossible differential attacks are reported [2] and [8] using 4 round impossible differential. The proposed attack, however, is effective for Hierocrypt-3 with 6 substitution layers using impossible differentials with 4 substitution layers. This is the first result on complexity of Hierocrypt against impossible differential attack.

** Supported partially by Korea Information Security Agency

In Section 2, we introduce Hierocrypt-3 and analyze properties of its component functions. In Section 3, we describe an 2 round impossible differential of Hierocrypt-3. In Section 4 and 5, we describe differential attacks against Hierocrypt-3 reduced to 2.5 rounds and 3 rounds. We conclude in Section 6.

2 Description of Hierocrypt-3

2.1 Brief Description of Hierocrypt-3

Hierocrypt-3 consists of six rounds. The round function except for the last round is the composition of two transformations $\rho = MDS_H \circ XS$ as in Fig. 1. For the last round, it consists of XS transformation and the final key addition.

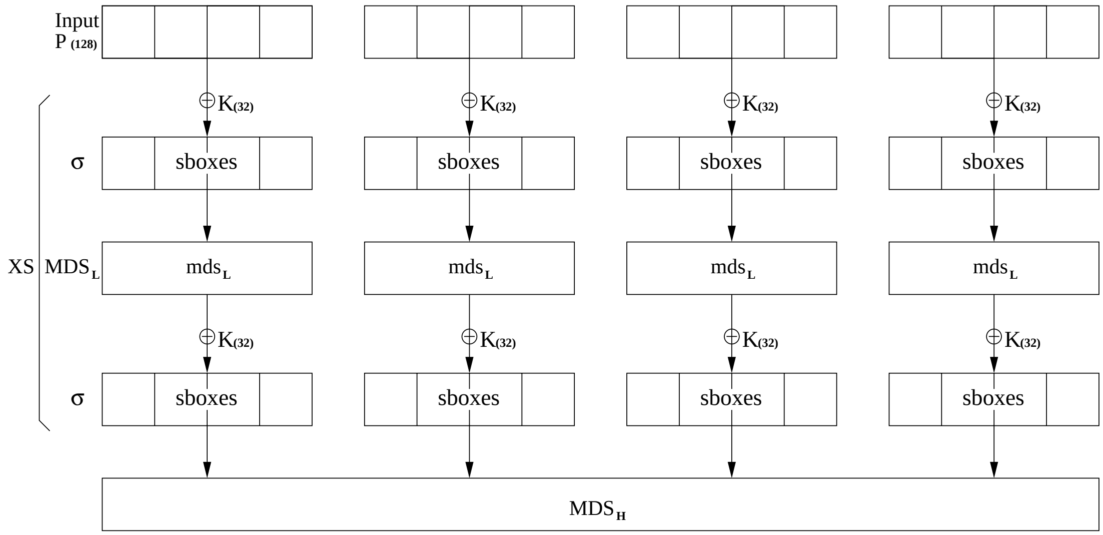

Fig. 1. 1 Round of Hierocrypt-3

Throughout this paper, we denote by $A_{(128)}$ a 128-bit data with name A, and by $a\|b$ a concatenation of two binary data a and b. In the following we describe the component functions.

- $X_{(128)}, K_{(256)}$: A 128-bit plaintext and 256-bit round key. $K_{(256)} = K_{(128)}\|K_{(128)}$.
- $\sigma = \underbrace{s\|s\|s\|\cdots\|s}_{16}$ where s is a 8×8 sbox.
- $MDS_L = \mathrm{mds}_L\|mds_L\|mds_L\|mds_L$ where mds_L is 4×4-byte linear permutation over $\mathbb{F}_{2^8}$ as in Table 1.
- $XS(X_{(128)}, K_{(256)}) = \sigma(MDS_L(\sigma(X_{(128)} + K_{(128)})) + K_{(128)}))$
- MDS_H and MDS_H^{-1} are 16×16 linear permutations over $\mathbb{Z}_2^8$ as in Table 2. The transformations are originated from 4×4 matrices over $\mathbb{Z}_2^4$.
- $\rho(X_{(128)}, K_{(256)}) = MDS_H(\mathrm{XS}(X_{(128)}, K_{(256)})$

Then the six round encryption is as follow:

$$P_{(128)} \equiv X^{(0)}_{(128)} \overset{\rho}{\longmapsto} X^{(1)}_{(128)} \overset{\rho}{\longmapsto} X^{(2)}_{(128)} \overset{\rho}{\longmapsto} \cdots \overset{\rho}{\longmapsto} X^{(5)}_{(128)} \overset{\mathrm{XS}}{\longmapsto} X^{(6)}_{(128)} \overset{\mathrm{AK}}{\longmapsto} C_{(128)}.$$

Table 1. The matrices of mds_L and mds_L^{-1}

$$\begin{pmatrix} C4 & 65 & C8 & 8B \\ 8B & C4 & 65 & C8 \\ C8 & 8B & C4 & 65 \\ 65 & C8 & 8B & C4 \end{pmatrix} \quad \begin{pmatrix} 82 & C4 & 34 & F6 \\ F6 & 82 & C4 & 34 \\ 34 & F6 & 82 & C4 \\ C4 & 34 & F6 & 82 \end{pmatrix}$$

Table 2. The matrix of MDS_H and MDS_H^{-1}

$$\begin{pmatrix} 5 & 5 & A & E \\ E & 5 & 5 & A \\ A & E & 5 & 5 \\ 5 & A & E & 5 \end{pmatrix} = \begin{pmatrix} 1\ 0\ 1\ 0 & 1\ 0\ 1\ 0 & 1\ 1\ 0\ 1 & 1\ 1\ 1\ 1 \\ 1\ 1\ 0\ 1 & 1\ 1\ 0\ 1 & 1\ 1\ 1\ 0 & 0\ 1\ 1\ 1 \\ 1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 & 1\ 1\ 1\ 1 & 0\ 0\ 1\ 1 \\ 0\ 1\ 0\ 1 & 0\ 1\ 0\ 1 & 1\ 0\ 1\ 0 & 1\ 1\ 1\ 0 \\[1ex] 1\ 1\ 1\ 1 & 1\ 0\ 1\ 0 & 1\ 0\ 1\ 0 & 1\ 1\ 0\ 1 \\ 0\ 1\ 1\ 1 & 1\ 1\ 0\ 1 & 1\ 1\ 0\ 1 & 1\ 1\ 1\ 0 \\ 0\ 0\ 1\ 1 & 1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 & 1\ 1\ 1\ 1 \\ 1\ 1\ 1\ 0 & 0\ 1\ 0\ 1 & 0\ 1\ 0\ 1 & 1\ 0\ 1\ 0 \\[1ex] 1\ 1\ 0\ 1 & 1\ 1\ 1\ 1 & 1\ 0\ 1\ 0 & 1\ 0\ 1\ 0 \\ 1\ 1\ 1\ 0 & 0\ 1\ 1\ 1 & 1\ 1\ 0\ 1 & 1\ 1\ 0\ 1 \\ 1\ 1\ 1\ 1 & 0\ 0\ 1\ 1 & 1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 \\ 1\ 0\ 1\ 0 & 1\ 1\ 1\ 0 & 0\ 1\ 0\ 1 & 0\ 1\ 0\ 1 \\[1ex] 1\ 0\ 1\ 0 & 1\ 1\ 0\ 1 & 1\ 1\ 1\ 1 & 1\ 0\ 1\ 0 \\ 1\ 1\ 0\ 1 & 1\ 1\ 1\ 0 & 0\ 1\ 1\ 1 & 1\ 1\ 0\ 1 \\ 1\ 1\ 1\ 0 & 1\ 1\ 1\ 1 & 0\ 0\ 1\ 1 & 1\ 1\ 1\ 0 \\ 0\ 1\ 0\ 1 & 1\ 0\ 1\ 0 & 1\ 1\ 1\ 0 & 0\ 1\ 0\ 1 \end{pmatrix}, \begin{pmatrix} B & E & E & 6 \\ 6 & B & E & E \\ E & 6 & B & E \\ E & E & 6 & B \end{pmatrix} = \begin{pmatrix} 0\ 1\ 0\ 1 & 1\ 1\ 1\ 1 & 1\ 1\ 1\ 1 & 0\ 1\ 1\ 0 \\ 1\ 0\ 1\ 0 & 0\ 1\ 1\ 1 & 0\ 1\ 1\ 1 & 1\ 0\ 1\ 1 \\ 1\ 1\ 0\ 1 & 0\ 0\ 1\ 1 & 0\ 0\ 1\ 1 & 0\ 1\ 0\ 1 \\ 1\ 0\ 1\ 1 & 1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 & 1\ 1\ 0\ 1 \\[1ex] 0\ 1\ 1\ 0 & 0\ 1\ 0\ 1 & 1\ 1\ 1\ 1 & 1\ 1\ 1\ 1 \\ 1\ 0\ 1\ 1 & 1\ 0\ 1\ 0 & 0\ 1\ 1\ 1 & 0\ 1\ 1\ 1 \\ 0\ 1\ 0\ 1 & 1\ 1\ 0\ 1 & 0\ 0\ 1\ 1 & 0\ 0\ 1\ 1 \\ 1\ 1\ 0\ 1 & 1\ 0\ 1\ 1 & 1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 \\[1ex] 1\ 1\ 1\ 1 & 0\ 1\ 1\ 0 & 0\ 1\ 0\ 1 & 1\ 1\ 1\ 1 \\ 0\ 1\ 1\ 1 & 1\ 0\ 1\ 1 & 1\ 0\ 1\ 0 & 0\ 1\ 1\ 1 \\ 0\ 0\ 1\ 1 & 0\ 1\ 0\ 1 & 1\ 1\ 0\ 1 & 0\ 0\ 1\ 1 \\ 1\ 1\ 1\ 0 & 1\ 1\ 0\ 1 & 1\ 0\ 1\ 1 & 1\ 1\ 1\ 0 \\[1ex] 1\ 1\ 1\ 1 & 1\ 1\ 1\ 1 & 0\ 1\ 1\ 0 & 0\ 1\ 0\ 1 \\ 0\ 1\ 1\ 1 & 0\ 1\ 1\ 1 & 1\ 0\ 1\ 1 & 1\ 0\ 1\ 0 \\ 0\ 0\ 1\ 1 & 0\ 0\ 1\ 1 & 0\ 1\ 0\ 1 & 1\ 1\ 0\ 1 \\ 1\ 1\ 1\ 0 & 1\ 1\ 1\ 0 & 1\ 1\ 0\ 1 & 1\ 0\ 1\ 1 \end{pmatrix}$$

where AK is the final key addition. The decryption can be done by performing the encryption in the reverse order.

2.2 Notation

For convenience of description of the attack, we use the following notation.

- $A[i][j]$: A 8-bit word in i-th row and j-th column of 4×4 matrix when using byte coordinate for 128-bit text as in Fig 2
- $\kappa 1, \sigma, L, \kappa 2, \tau, H$: The 128-bit transformation for the first key addition, the first substitution by S-box s, MDS_L, the second key addition, the second substitution by S-box s, and MDS_H, respectively (See Fig. 3).
- $A^i_{\kappa 1}$, A^i_{σ}, A^i_L, $A^i_{\kappa 2}$, A^i_{τ}, A^i_H: Input of $\kappa 1, \sigma, L, \kappa 2, \tau, H$ transformation in round i
- $B^i_{\kappa 1}$, B^i_{σ}, B^i_L, $B^i_{\kappa 2}$, B^i_{τ}, B^i_H: Output of $\kappa 1, \sigma, L, \kappa 2, \tau, H$ transformation in round i
- A': Differential value of a pair of A
- P, C: Plaintext, Ciphertext
- K^{i1}, K^{i2}: The 128-bit first or second round key in round i, resp.
- K^{i3}: The 128-bit final round key when the encryption consists of i rounds
- $+$: Bitwise addition(Exclusive-or)

A[0][0]	A[0][1]	A[0][2]	A[0][3]
A[1][0]	A[1][1]	A[1][2]	A[1][3]
A[2][0]	A[2][1]	A[2][2]	A[2][3]
A[3][0]	A[3][1]	A[3][2]	A[3][3]

Fig. 2. Byte Coordinate of 128 bits

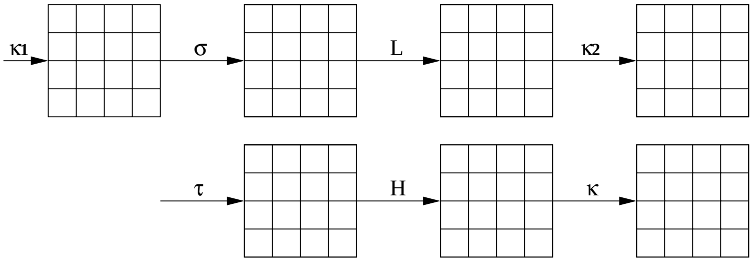

Fig. 3. Alternative Expression of One Round of Hierocrypt-3

2.3 Lower-level Diffusion MDS_L

MDS_L consists of four parallel 32×32 linear transformation mds_L. The lower-level diffusion mds_L has the branch number 5 as a transformation of 4 bytes. More precisely, we can compute the approximate probability $p(i,j)$ that the number of output bytes with nonzero difference is j when the number of input bytes with nonzero differences is i. In this case we have $4-j$ equations and i variables over $\mathbb{F}_{2^8}$. Since L is a 4×4 matrix of rank 4 over $\mathbb{F}_{2^8}$, if $i \leq 4-j$, it has no nonzero solution. If $i > 4-j$, it has $(2^8)^{i-(4-j)} - 1$ nonzero solutions. Thus we have $p(i,j) = 2^{8(j-4)} - 2^{-8i}$ when $0 \leq i,j \leq 4$ and $i+j > 4$. The inverse of mds_L has the same property. See Table 3.

Table 3. The approximate probability $p(i,j)$ of input pairs with i byte nonzero differences into output pairs with j byte nonzero differences by mds_L or its inverse

$i \setminus j$	0	1	2	3	4
1	0	0	0	0	1
2	0	0	0	2^{-8}	1
3	0	0	2^{-16}	2^{-8}	1
4	0	2^{-24}	2^{-16}	2^{-8}	1

2.4 Higher-level Diffusion MDS_H

Higher-level diffusion MDS_H is a transformation on 16 bytes, but it has good diffusion property over input columns. For example, even if only one column of the input difference is nonzero, every column of the output difference is nonzero. We can generalize this property. See the following definition.

Definition 1. *For any 128-bit transformation, we define the column branch number to be the minimal number of non-zero columns in input difference or output difference.*

Property 1. Both of 128-bit transformation H and H^{-1} has the column branch number 5.

Assume that two columns and i rows of the input difference of MDS_L are zero. Then we compute the probability $q(i)$ that the output difference assume zero in a column. Since we have $8-2i$ bytes with nonzero difference, we have $8-2i$ variables in bytes and 4 equations which corresponds to the $4 \times (8-2i)$ matrix made by getting rid of columns and rows from the MDS_H matrix which correspond to zero input difference. Note that this matrix has rank $4-i$ if we choose appropriate columns for zero outputs since every 4×16 sub-matrix of MDS_H has two identical 4×4 sub-matrices in it. Hence we have $q(i) = (2^8)^{4-i}/(2^8)^{8-2i} = 2^{8i-32}$ for $i = 0, 1, 2, 3, 4$. See Table 4.

Table 4. The probability $q(i)$ of input pairs with i row zero differences and 2 column nonzero differences into output pairs with a column zero difference by MDS_H

i	0	1	2	3	4
$q(i)$	2^{-32}	2^{-24}	2^{-16}	2^{-8}	1

3 A 2-Round Impossible Differential

In this subsection, we introduce 2-round impossible differential of Hierocrypt. Fig. 4 describes one pattern of an impossible differential.

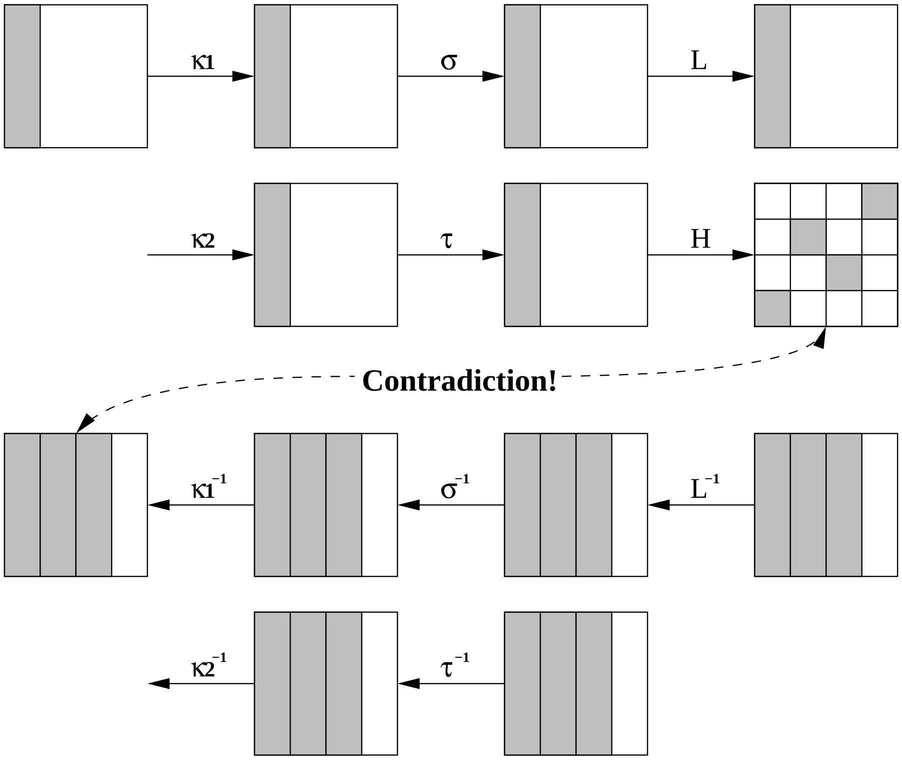

Fig. 4. A Two Round Impossible Differential of Hierocrypt-3

The impossible differential comes from the following observation.

1. $\kappa 1$, σ, L, $\kappa 2$, and τ transform a column with zero difference into a column with zero difference.
2. If only one column of the input difference is nonzero, every column of the output difference of H is nonzero since H has column branch number 5.
3. τ^{-1}, σ^{-1}, $\kappa 2^{-1}$, and $\kappa 1^{-1}$ transform a column with zero difference into a column with zero difference.

Property 2 (An Impossible Differential). Given input pairs whose difference is zero in three columns, the difference of output pairs can not be zero in any column after byte substitution τ in round 2.

4 Hierocrypt-3 Reduced to 2.5 Rounds

In this subsection, we describe a cryptanalysis of Hierocrypt-3 reduced to 2.5 rounds. The attack is based on the 2-round impossible differential with additional a half round at the end as in Fig. 5. The half round ends with 128-bit key addition, but the same attack holds even if the half round has additional σ transformation. The attack is as follows:

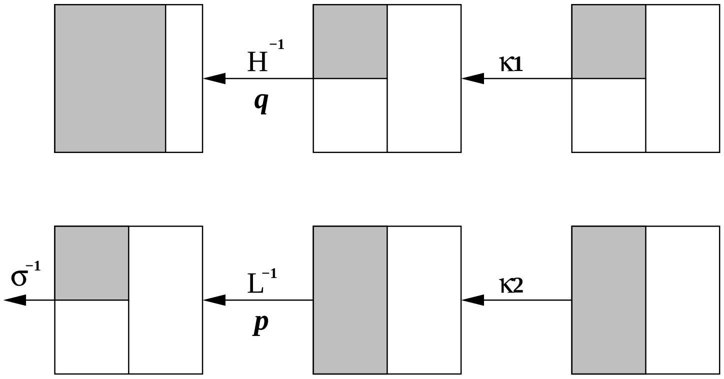

Fig. 5. 2.5 Round Impossible Attack of Hierocrypt-3

1. A structure is defined as a set of plaintexts which have certain fixed values in the columns 1, 2, and 3. One structure consists of 2^{32} plaintexts and proposes $2^{32} \times 2^{32} \times \frac{1}{2} = 2^{63}$ pairs of plaintexts.
2. Take 2^{54} structures(2^{86} plaintexts, 2^{117} plaintext pairs) over total 2^{96} structures. Choose pairs whose ciphertext pairs have zero difference at the columns 2 and 3. The expected number of such pairs is $2^{117} \times 2^{-64} = 2^{53}$ when we assume the 2.5 round encryption is random.
3. Among the ciphertext pairs (C, C^*) chosen in Step 2, choose pairs whose difference $L^{-1}(C + C^*)$ is zero at the rows 2 and 3. Since the probability p is $p(4,2)^2 = 2^{-32}$ as in Table 3, the expected number of the remaining pairs is $2^{53} \times 2^{-32} = 2^{21}$.
4. For such pairs (C, C^*), assume 32-bit value of K_{eq}^{32} with zero at the columns 2 and 3 and the rows 2 and 3 and calculate

$$H^{-1}\{\sigma^{-1} \cdot (L^{-1}(C) + K_{eq}^{32}) + \sigma^{-1} \cdot (L^{-1}(C^*) + K_{eq}^{32})\},$$

   where $K_{eq}^{32} = L^{-1}(K^{32})$. Choose pairs whose differences are zero at a column after H^{-1} transformation. The probability is $q(2) = 2^{-16}$ as in Table 4.
5. Since such a difference is impossible, every key that proposes such a difference is a wrong key. After analyzing 2^{21} ciphertext pairs, there remain only about $2^{32}(1 - 2^{-16})^{2^{21}} \approx 2^{32}e^{-2^5} \approx 2^{-14}$ wrong values of K_{eq}^{32}.
6. If we repeat Step 3 through Step 5 after changing the rows 2 and 3 into the rows 0 and 1, we can get the exact value of K_{eq}^{32} in the columns 0 and 1. We can compute the round key K^{32} in the columns 0 and 1 from $K^{32} = L(K_{eq}^{32})$.
7. If we repeat Step 2 through Step 6 after changing the columns 2 and 3 with the columns 0 and 1, we can get the whole value of the round key K^{32}.

Step 3 requires about 2^{53} L^{-1} transformations. Step 4 requires at most 2^{54} $(= 2 \times 2^{21} \times 2^{32})$ $H^{-1} \circ \sigma^{-1} \circ L^{-1}$ transformations. Since we don't need to test anymore the key which is discarded once, however, the expected complexity would be about 2^{48} $H^{-1} \circ \sigma^{-1} \circ L^{-1}$ transformations since

$$2^{32}\{1 + (1 - 2^{-16}) + (1 - 2^{-16})^2 + \cdots + (1 - 2^{-16})^{2^{21}}\} \approx 2^{48}.$$

Consequently, since we repeat this procedure four times, this attack requires about 2^{42} *encryptions and* 2^{86} *chosen plaintexts.*

If we change the number of zero rows in B'_σ in Step 3, the complexity and the required plaintext pairs change as in Table 5. In Table 5, we use the notation below:

- i: The number of zero rows in B'_σ.
- p: The probability of input pairs with 4 byte nonzero differences into output pairs with i byte nonzero differences by the inverse of mds_L as in Table 3.
- q: The probability of input pairs with i rows and 2 columns nonzero differences into output pairs with one column zero differences by MDS_H as in Table 4.
- 2^k: The number of equivalent round keys K_{eq}^{32} with zero at the columns 2 and 3 and the fixed i rows.
- N : The number of ciphertext pairs required for this attack. To guarantee the number of remaining wrong keys is less than 1, we should have

  $$2^k(1 - q)^{Np} \approx 2^k e^{-Npq} < 1$$

  which implies $N > kp^{-1}q^{-1}\ln 2$.
- Plaintext: The number of original plaintexts required for this attack. $N \times 2^{64} \times 2^{31}$.
- Time: The complexity of this attack. In Step 2, L^{-1} transformation should be done $CP_1 = 2^k \times N$ times. In Step 3, $H^{-1} \circ \sigma^{-1} \circ \kappa_1^{-1}$ transformation should be done

  $$CP_2 = 2 \times 2^k(1 + (1 - q) + (1 - q)^2 + \cdots + (1 - q)^{Np}) \approx 2^k q^{-1}$$

  times. Since we have to repeat this procedure 4 times(8 times for $i = 3$), the total complexity is about $4(CP_1/9 + CP_2/3)(8(CP_1/9 + CP_2/3)$ for $i = 3)$ encryption of Hierocrypt-3 reduced to 2.5 round.

Table 5. The complexity of IDC reduced to 2.5 rounds when taking i zero rows in B'_σ

i	p	q	2^k	N	Plaintext	Time
0	1	2^{-32}	2^{64}	2^{38}	2^{71}	2^{101}
1	2^{-16}	2^{-24}	2^{48}	$2^{45.6}$	$2^{78.6}$	$2^{92.6}$
2	2^{-32}	2^{-16}	2^{32}	2^{53}	2^{86}	2^{84}
3	2^{-48}	2^{-8}	2^{16}	2^{60}	2^{93}	2^{76}

5 Hierocrypt-3 Reduced to 3 Rounds

In this subsection, we describe cryptanalysis of Hierocrypt-3 reduced to 3 rounds. The attack is based on the 2-round impossible differential with additional one round at the end as in Fig. 6. Note that the last round of Hierocrypt has the additional 128-bit key(say, K^{33}) addition instead of H transformation. An attack is as follows:

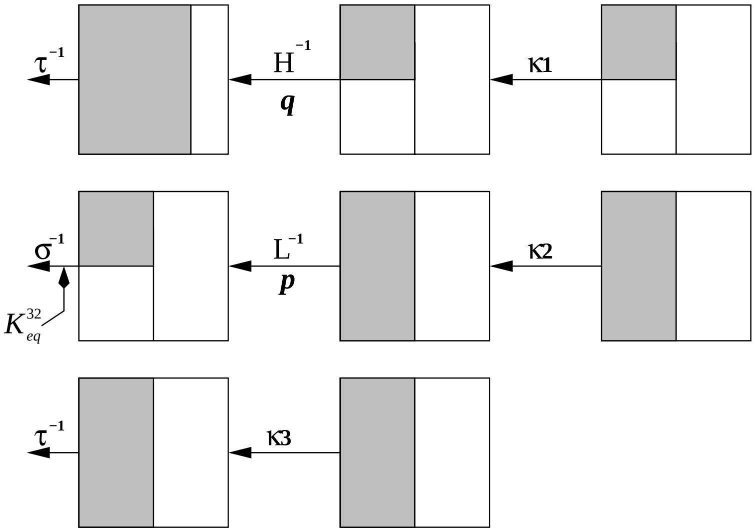

Fig. 6. Three Round Impossible Attack of Hierocrypt-3

1. A structure is defined as a set of plaintexts which have certain fixed values in columns 1, 2, and 3. One structure consists of 2^{32} plaintexts and proposes $2^{32} \times 2^{32} \times \frac{1}{2} = 2^{63}$ pairs of plaintexts.
2. Take $2^{55.5}$ structures($2^{87.5}$ plaintexts, $2^{118.5}$ plaintext pairs). Choose pairs whose ciphertext pairs have zero difference at the columns 2 and 3. The expected number of such pairs is $2^{118.5} \times 2^{-64} = 2^{54.5}$.
3. Assume a 64-bit value of the columns 0 and 1 of the last round key K^{33}.
4. For each ciphertext pair (C, C^*), compute $B_L^3 = \tau^{-1}(C + K^{33})$ and $B_L^{3*} = \tau^{-1}(C^* + K^{33})$ and choose pairs whose difference $L^{-1}(B_L^3 + B_L^{3*})$ is zero at the rows 2 and 3. Since the probability p is $p(4,2)^2 = 2^{-32}$ as in Table 3, the expected number of the remaining pairs is $2^{54.5} \times 2^{-32} = 2^{22.5}$.
5. For such pairs (B_L^3, B_L^{3*}), assume 32-bit value of K_{eq}^{32} with zero at the columns 2 and 3 and the rows 2 and 3, and calculate

$$H^{-1}\{\sigma^{-1}(L^{-1}(B_L^3) + K_{eq}^{32}) + \sigma^{-1}(L^{-1}(B_L^{3*}) + K_{eq}^{32})\}.$$

   Choose pairs whose differences are zero at a column after H^{-1} transformation. The probability is $q(2) = 2^{-16}$ as in Table 4.
6. Since such a difference is impossible, every key that proposes such a difference is a wrong key. Observe that we have 2^{96} possibility for a pair (K_{eq}^{32}, K^{33}) and for each key pair we perform impossible differential attack with probability of 2^{-48}. After analyzing $2^{54.5}$ ciphertext pairs passing Step 2, there remain only about $2^{96}(1-2^{-48})^{2^{54.5}} \approx 2^{96}e^{-2^{6.5}} \approx 2^{-2.5}$ wrong values of (K_{eq}^{32}, K^{33}). Hence if there remains a value of (K_{eq}^{32}, K^{33}), we may assume that the key pairs are the right key pair. If we repeat Step 2 through Step 5 after changing the columns 2 and 3 into the columns 0 and 1, we can get the whole value of K^{33}.

Step 4 requires about $2^{119.5}(= 2 \times 2^{64} \times 2^{54.5})$ τ^{-1} transformations and $2^{118.5}$ L^{-1} transformations. Step 5 requires at most $2^{119.5}$ $(= 2^{96} \times 2^{22.5} \times 2)$ $H^{-1} \circ \sigma^{-1} \circ \kappa 1^{-1} \circ L^{-1}$ transformations.

Since we don't need to test anymore the key which is discarded once, however, the expected complexity would be about 2^{113} $H^{-1} \circ \sigma^{-1} \circ \kappa 1^{-1} \circ L^{-1}$ transformations since

$$2^{64} \times 2 \times 2^{32}\{1 + (1 - 2^{-16}) + (1 - 2^{-16})^2 + \cdots + (1 - 2^{-16})^{2^{22.5}}\} \approx 2^{113}.$$

Consequently, since we repeat this procedure two times, this attack requires about $2^{117.5}$ *encryptions of Hierocrypt-3 reduced to 3 round and* $2^{87.5}$ *chosen plaintexts.*

We can do the same attack by taking differential $B^{3'}_{\sigma}$ in which 0,1 or 3 rows are 0. The complexity and the required plaintext pairs change as in Table 6. In Table 6, we use the same notation as used in Table 5. But some quantity has the different value.

- N: The number of ciphertext pairs required for this attack. To guarantee the probability that a wrong key remains in each K^{33} is less than 2^{-64}, we should have

  $$2^k(1-q)^{Np} \approx 2^k e^{-Npq} < 2^{-64}$$

  which implies $N > (k + 64)p^{-1}q^{-1}\ln 2$.
- Plaintext: The number of original plaintexts required for this attack. $N \times 2^{64} \times 2^{31}$.
- Time: The complexity of this attack. In Step 4, $L^{-1} \circ \tau \circ \kappa 2$ transformation should be done $CP_1 = 2^{64} \times N$ times. In Step 5, $H^{-1} \circ \sigma^{-1} \circ \kappa 1^{-1} \circ L^{-1}$ transformation should be done

  $$CP_2 = 2^{64} \times 2 \times 2^k(1 + (1-q) + (1-q)^2 + \cdots + (1-q)^{Np}) \approx 2^{65+k}q^{-1}$$

  times. Since we have to repeat this procedure 2 times, the total complexity is about $2(CP_1/4 + CP_2/3)$ encryption of Hierocrypt-3 reduced to 3 round.

Table 6. The complexity of IDC reduced to 3 rounds when taking i zero rows in B'_{σ}

i	p	q	2^k	N	Plaintext	Time
0	1	2^{-32}	2^{64}	2^{39}	2^{72}	$2^{160.5}$
1	2^{-16}	2^{-24}	2^{48}	$2^{46.5}$	$2^{79.5}$	$2^{136.5}$
2	2^{-32}	2^{-16}	2^{32}	$2^{54.5}$	$2^{87.5}$	$2^{117.5}$
3	2^{-48}	2^{-8}	2^{16}	2^{62}	2^{95}	2^{125}

6 Conclusion

In this paper, we proposed two round impossible differentials of Hierocrypt-3 and describe an impossible differential attack on Hierocrypt-3 reduced to 2.5 rounds and 3 rounds. The attack requires 2^{86} chosen plaintexts and 2^{42} encryptions in the case of Hierocrypt-3 reduced to 2.5 rounds, and $2^{87.5}$ chosen ciphertexts and $2^{117.5}$ encryptions in the case of Hierocrypt-3 reduced to 3 rounds. However, since both have 6 rounds in the original versions of Hierocrypt it is still infeasible to attack them with impossible differential.

References

1. E. Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” J. of Cryptology, Vol. 3, pp.27-41, 1990.
2. E. Biham and N. Keller, “Cryptanalysis of Reduced Variants of Rijndael,” Preprint, http://csrc.nist.gov/encryption/aes/round2/conf3/aes3papers.html, 2000.
3. P. Barreto, V. Rijmen, J. Nakahara Jr., B. Preneel, J. Vanderwalle, and H. Kim, “Improved Square Attacks Against Reduced-Round Hierocrypt,” Proc. of FSE2001, pp.173-182, 2001.
4. Evaluation of Cryptographic Techniques, http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html
5. M. Matsui, “Linear Cryptanalysis Method for DES cipher,” Proc. of Eurocrypt’93, pp.386-397, Springer-Verlag, 1993.
6. New European Schemes for Signatures, Integrity, and Encryption, http://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions.html
7. K. Ohkuma, H. Muratani, F. Sano and S. Kawamura, “The block cipher Hierocrypt,” Proc. of SAC2000, Springer-Verlag, 2000.
8. H. Seki and T. Kaneko, “Cryptanalysis of Five Rounds of CRYPTON Using Impossible Differentials,” Proc. of Asiscrypt’99, pp.43-51,1999.
9. Toshiba Corporation, “Block Cipher Family Hierocrypt,” http://www.toshiba.co.jp/rdc/security/hierocrypt/index.htm