Impossible Differential Cryptanalysis of Zodiac

Deukjo Hong[1], Jaechul Sung[1], Shiho Moriai[2], Sangjin Lee[1], and Jongin Lim[1⋆]

[1] Center for Information Security Technologies(CIST),
Korea University, Anam Dong, Sungbuk Gu,
Seoul, Korea
{hongdj, sjames, sangjin, jilim}@cist.korea.ac.kr
[2] NTT Laboratories, 1-1 Hikarinooka, Yokosuka, 239-0847 Japan
shiho@isl.ntt.co.jp

Abstract. We discuss the impossible differential cryptanalysis of the block cipher Zodiac [7]. The main design principles of Zodiac are simplicity and efficiency. However the diffusion layer in its round function is too simple to offer enough security. An impossible differential cryptanalysis is a proper method to attack the weakness of Zodiac. Our attack using two 14-round impossible characteristics derives 128-bit master key of the full 16-round Zodiac with its complexity 2^{119} encryption times faster than the exhaustive search. The efficiency of the attack compared with exhaustive search increases as the key size increases.

1 Introduction

Differential cryptanalysis which was proposed by E. Biham and A. Shamir [3] is the most powerful attack for block ciphers. Later, it was regarded as a very useful method in attacking the known block ciphers – FEAL [10], LOKI [4], and so on. For these reasons, block ciphers have been designed to consider the differential cryptanalysis since the middle of 1990's. Differential cryptanalysis has also been advanced variously – Conditional Differential Cryptanalysis [1, 9], Truncated Differential Cryptanalysis [5], Impossible Differential Cryptanalysis [2], Higher Order Differential Cryptanalysis [5,6,8], Boomerang attack [11], and so on.

The conventional differential cryptanalysis finds a key using the differential characteristic with a high probability. The attacker chooses ciphertext pairs with a specific difference of plaintexts, discards wrong pairs by filtering, and then finds a key by applying the counting methods to the remaining pairs.

If a filtering method is efficient, the signal to noise ratio is greater than 1. However, the case that the signal to noise ratio is far less than 1 is also useful. Especially, the differential characteristic whose probability is zero is efficiently applied to attack block ciphers. This attack is called the impossible differential cryptanalysis.

⋆ This work is supported in part by the Ministry of Information & Communication of Korea ("Support Project of University Information Technology Research Center" supervised by IITA)

M. Matsui (Ed.): FSE 2001, LNCS 2355, pp. 300–311, 2002.

In general, it is possible that a cipher which has a cryptographically weak diffusion or permutation has a long impossible differential characteristic, . E. Biham et al. found a 24-round impossible differential characteristic to analyze 31-round Skipjack in [2].

The general impossible differential cryptanalysis is as follows:

1. Find impossible differential characteristics.
2. Obtain the ciphertext pairs for their plaintext pairs with the input difference of the impossible differential characteristic.
3. For each value in the key space of the final round, decrypt the ciphertext pairs with that value and determine whether they satisfy the impossible differential characteristic.
4. Discard the values with which the pairs satisfy it from the key space. Go to step 3 unless the number of elements in the key space is almost one.

In the above algorithm the remaining element in the key space is the correct key value with high probability.

The block cipher Zodiac is submitted to the ISO/IEC JTC1/SC27–Korea in September, 2000. It consists of Feistel structure with 16 rounds. Its design principles are as follows [7]:

- **Simplicity:** We tried not to include ad-hoc design elements based on any obscure reason. We do not believe that more complicated design could give the more secure structure.
- **Provability:** As possible as we can do, we tried to design the cipher to have a provably secure structure especially resistant to the well known typical attacks such as differential cryptanalysis, linear cryptanalysis and interpolation attack.
- **Accommodation and Performance:** Our cipher was designed to get high performance both on general 32-bit CPU and general 8-bit microprocessor (e.g. smart cards).

The byte-wise diffusion in its round function F is very simple and cryptographically weak. Therefore, our observation is concentrated on impossible differential cryptanalysis of Zodiac [1]. In our work we show that there exist 15-round impossible differential characteristics in Zodiac. It follows that there exist r-round impossible differential characteristics if $r \leq 15$. We also give an efficient method to find the last round key using two 14-round impossible differential characteristics.

2 Zodiac

Zodiac follows the conventional Feistel structure except for the initial and final 64-bit data whitening by two 64-bit keys. The initial and final permutation $\prod$ is shown in Figure 2.

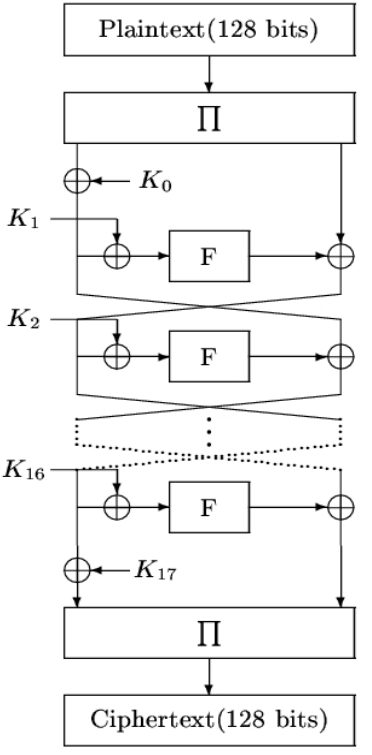

Fig. 1. The structure of Zodiac

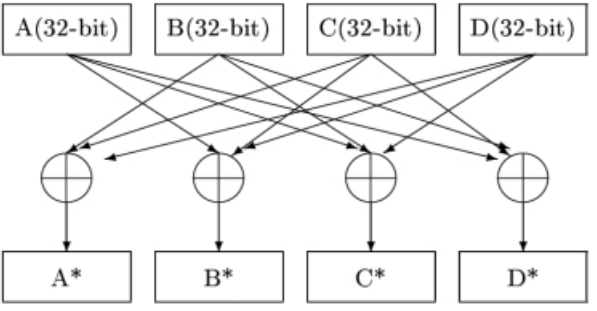

Fig. 2. Permutation $\prod$

[1] We also found two 15-round truncated differentials which can be useful for distinguishing the 15-round Zodiac from a random permutation, but impossible differential cryptanalysis succeeded in breaking the full Zodiac more efficiently.

Hereafter, we ignore the initial and final permutations and the whitening keys in the description of the attack because they don't affect on input or output difference values at all. Moreover, even in this case, the attack procedure and the required complexity is considered to be similar because whitening keys can be incorporated (XORed) into the internal round keys; i.e. K_0 can be XORed with the odd round keys, K_{17} can be XORed with the even round keys.

2.1 Round Function F

The round function F of Zodiac has very simple structure and all operations in F are XOR operation and 8-by-8 non-linear substitutions (S-boxes) i.e. table look-ups. The two S-boxes S1 and S2 are generated by the following functions $h(x)$ and $g(x)$, respectively:

$$h(x) = h_0(h_0(x)), \text{ where } h_0(x) = (45^x \bmod 257) \bmod 256$$
$$g(x) = (170 + x)^{-1} \text{ in GF}(2^8),$$

with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. The detailed structure is shown in Figure 3.

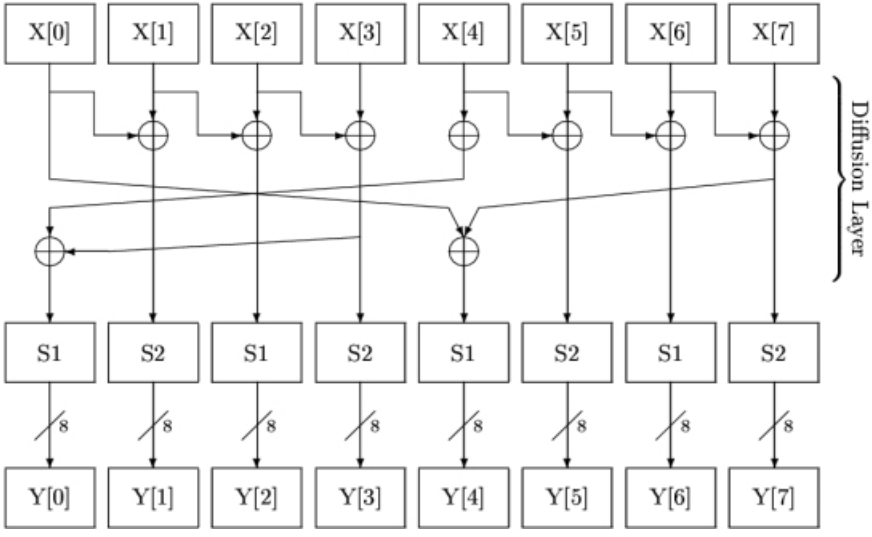

Fig. 3. Round function F

2.2 Key Schedule of Zodiac

Zodiac supports three types of key lengths, 128, 192, and 256 bits and needs sixteen 64-bit round keys and additionally two 64-bit keys for the input masking

and output masking of the processing data. The key scheduling algorithm of Zodiac is basically constructed from its round-function. For details, see [7]. We don't make use of the key schedule in our attack.

3 Notations

We use the following notations in this paper.

$I_L^i[j]$	the j-th byte in the left half of input difference of i-th round
$I_R^i[j]$	the j-th byte in the right half of input difference of i-th round
$O_L^i[j]$	the j-th byte in the left half of output difference of i-th round
$O_R^i[j]$	the j-th byte in the right half of output difference of i-th round
$S_I^i[j]$	the input difference of the j-th S-box (S1 or S2) of i-th round
$S_O^i[j]$	the output difference of the j-th S-box (S1 or S2) of i-th round
$K_i[j]$	the j-th byte in the round key of i-th round
$a, b, c, \ldots$	bytes with non-zero difference
$A, B, C, \ldots$	bytes with any (zero or non-zero) difference

4 Impossible Differential Characteristics of Zodiac

We found two 15-round impossible differential characteristics in Zodiac. Since the diffusion layer in the function F is performed by XORing two or three bytes, it is easy to compute zero-bytes in a difference and to find an impossible differential characteristic.

In Figure 4 if $(I_L^1, I_R^1) = (00000000, 00000aaa)$, then $I_L^8[3]$ must be zero, where $a, b, \ldots$ (small letters) denote nonzero one byte values and $A, B, \ldots$ (capital letters) denote any one byte values. Similarly, if $(O_L^{15}, O_R^{15}) = (00000a00, 00000000)$, then $O_R^8[3]$ must be nonzero. However, since $I_L^8 = O_R^8$, it is a contradiction. Therefore, this is a differential characteristic with zero probability, i.e. an impossible differential characteristic. In a similar way (and due to symmetry of the round function of Zodiac), we can see that the differential characteristic in Figure 5 is impossible.

Actually, these characteristics are impractical because there are too many zero bytes in the output differences of the 15th round. The more zero bytes are there, the fewer key-bits are derived and the more plaintext pairs are required for the attack. Nevertheless, the existence of 15-round impossible differential characteristics implies a cryptographically potential weakness of the block cipher Zodiac. It also follows that there exist r-round impossible differential characteristics if $r \leq 15$.

We also found two 15-round truncated differentials $(I_L^1, I_R^1) = (00000000, 00000a00)$, $(O_L^{15}, O_R^{15}) = (00000a00, 00000000)$ and $(I_L^1, I_R^1) = (00000000, 0a000000)$, $(O_L^{15}, O_R^{15}) = (0a000000, 00000000)$
with probability of about 2^{-120}. They may be useful for distinguishing the 15-round Zodiac from a random permutation, but failed to break the full Zodiac efficiently.

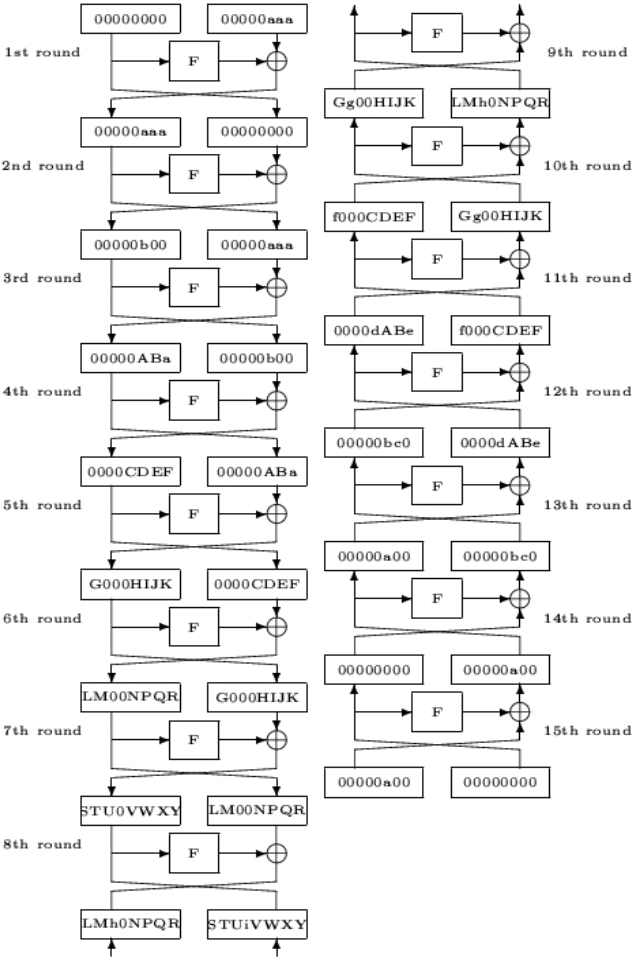

Fig. 4. 15-round impossible differential characteristic 15-I

5 Impossible Differential Cryptanalysis of Zodiac

Our attacks use two 14-round impossible characteristics shown in Figures 6 and 7 to derive the last round key. In our attack, we assume that the differential probability of the S-boxes is uniformly distributed and the round keys are random and uniformly distributed.

5.1 Attack on 15-Round Zodiac

First, we describe the attack on the 15-round Zodiac as a simple example. As we wrote in Section 2, we don't consider the whitening keys and let the round

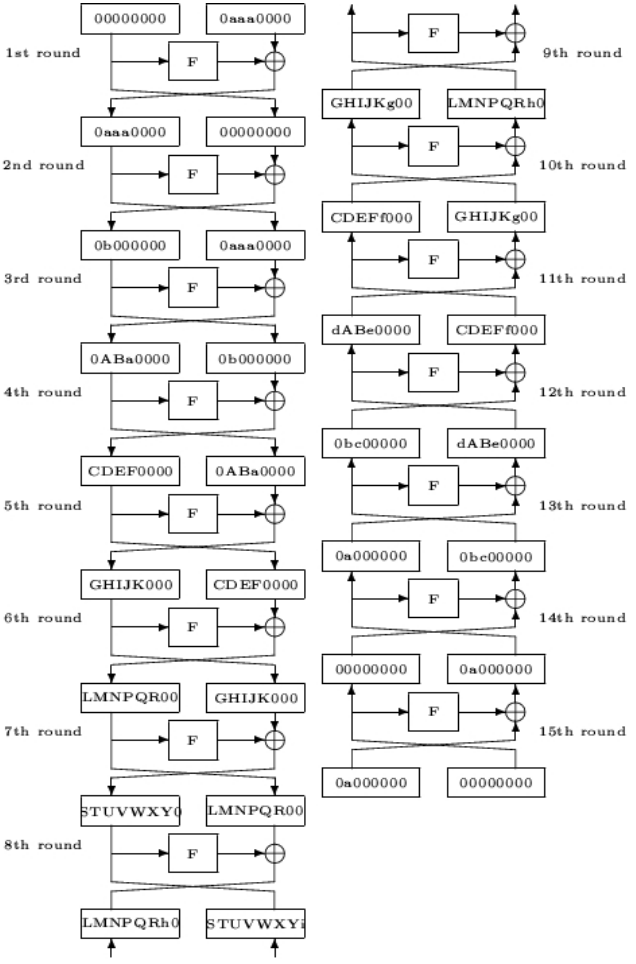

Fig. 5. 15-round impossible differential characteristic 15-II

keys $K_1, K_2, \ldots, K_{15}$. Our target is K_{15}. We define the key values K'_i to enter the S-boxes.

$$
\begin{aligned}
K'_i[0] &= K_i[2] \oplus K_i[3] \oplus K_i[4] \\
K'_i[1] &= K_i[0] \oplus K_i[1] \\
K'_i[2] &= K_i[1] \oplus K_i[2] \\
K'_i[3] &= K_i[2] \oplus K_i[3] \\
K'_i[4] &= K_i[0] \oplus K_i[6] \oplus K_i[7] \\
K'_i[5] &= K_i[4] \oplus K_i[5] \\
K'_i[6] &= K_i[5] \oplus K_i[6] \\
K'_i[7] &= K_i[6] \oplus K_i[7]
\end{aligned}
$$

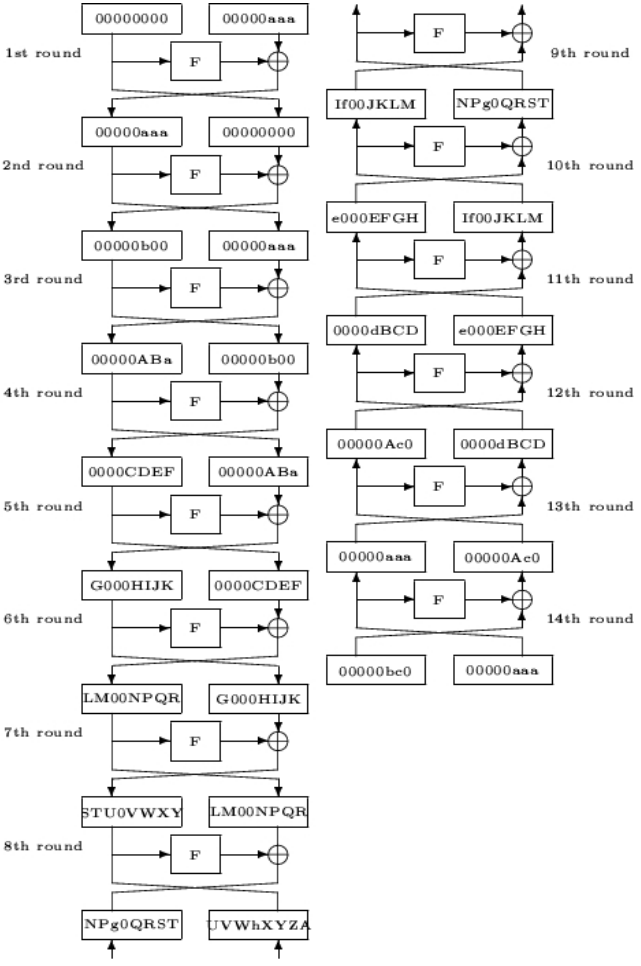

Fig. 6. 14-round impossible differential characteristic 14-I

We use the 14-round impossible differential shown in Figure 6. We choose a structure of 2^8 plaintext pairs with $(\Delta P_L, \Delta P_R) = (00000000, 00000aaa)$ and then, collect the pairs satisfying $\Delta C_L = 00000bc0, \Delta C_R[j] = 0 (0 \leq j \leq 3)$, and $\Delta C_R[4] \neq 0$ where the difference of the plaintexts $(\Delta P_L, \Delta P_R) = (I_L^1, I_R^1)$ and the difference of the ciphertexts $(\Delta C_L, \Delta C_R) = (O_R^{15}, O_L^{15})$. The probability that a plaintext pair satisfies these conditions is $(\frac{1}{2^8})^{10} \cdot (\frac{2^8-1}{2^8})^3 \simeq 2^{-80}$ (because there are 10 bytes with zero difference and 3 bytes with non-zero difference in $(\Delta C_L, \Delta C_R)$).

Since the input difference of F of the 15-th round is $00000bc0$, $S_I^{15}[4], S_I^{15}[5]$, and $S_I^{15}[7]$ are nonzero, and $S_I^{15}[6]$ takes any value. From the equation

$$S_O^{15}[4,5,6,7] \oplus \Delta C_R[4,5,6,7] = O_R^{14}[4,5,6,7],$$

an element in the key space of K_{15} is not a correct key value if $O_R^{14}[4] = 0$ and $O_R^{14}[5] = O_R^{14}[6] = O_R^{14}[7] \neq 0$ by computing with the ciphertexts and it. Thus, such elements should be eliminated from the key space. This method derives $4 \sim 7$th bytes of K'_{15}.

Let $\mathcal{K}$ be the key space of $K'_{15}[i](4 \leq i \leq 7)$. The probability that an element in $\mathcal{K}$ survives the test with such a pair is $1 - (\frac{1}{2^8} \cdot \frac{2^8-1}{2^8} \cdot \frac{1}{2^8} \cdot \frac{1}{2^8}) \simeq 1 - 2^{-24}$. Therefore, the number of the pairs required for narrowing down to one correct key is N such that $2^{32} \cdot (1 - 2^{-24})^N \simeq 1$. N is about $2^{28.5}$. Hence, the number of required chosen plaintext pairs is $2^{80} \cdot 2^{28.5} = 2^{108.5}$.

Since we can collect ${}_{2^8}C_2 = 2^{15}$ pairs from such one structure, we need $2^{93.5}$ structures. It follows that the attack requires $2^{93.5} \cdot 2^8 = 2^{101.5}$ chosen plaintexts.

This method is summarized as follows.
Goal: Finding $K'_{15}[4] \sim K'_{15}[7]$.

1. Collect sufficiently many ($2^{101.5}$) plaintext pairs from the structures whose ciphertext differences satisfy $\Delta C_L = 00000bc0, \Delta C_R[j] = 0(0 \leq j \leq 3)$, and $\Delta C_R[4] \neq 0$.
2. Choose a pair in the collection.
3. For each $k \in \mathcal{K}$,
   a) Compute $O_R^{14}[4], \ldots, O_R^{14}[7]$.
   b) Remove k from $\mathcal{K}$ if $O_R^{14}[4] = 0, O_R^{14}[5] = O_R^{14}[6] = O_R^{14}[7] \neq 0$.
   c) If $|\mathcal{K}| \leq \epsilon$, stop. Otherwise, go to 2. (ϵ is a sufficiently small integer.)

Using the characteristic in Figure 7, $K'_{15}[0] \sim K'_{15}[3]$ are also derived with $2^{101.5}$ chosen plaintext pairs. It is easy to compute K_{15} from K'_{15}.

5.2 Attack on 16-Round Zodiac

The impossible differential cryptanalysis for the 16-round Zodiac is a 2R-attack using two characteristics in Figures 6 and 7.

Similar to Section 5.1, we use the structures of 2^8 plaintexts satisfying $(\Delta P_L, \Delta P_R) = (00000000, 00000aaa)$ (with the characteristic in Figure 6) and collect the pairs whose ciphertext differences satisfy $\Delta C_L[j] = 0(0 \leq j \leq 3), \Delta C_L[4] \neq 0, \Delta C_R[0] \neq 0$, and $\Delta C_R[i] = 0(1 \leq i \leq 3)$ where the difference of the plaintexts $(\Delta P_L, \Delta P_R) = (I_L^1, I_R^1)$ and the difference of the ciphertexts $(\Delta C_L, \Delta C_R) = (O_R^{16}, O_L^{16})$. Therefore, the probability that any plaintext pair satisfies these conditions is $(\frac{1}{2^8})^7 \cdot (\frac{2^8-1}{2^8})^2 \simeq 2^{-56}$. Let $\mathcal{K}_1$ be the key space of $K'_{16}[0]$ and $K'_{16}[i](4 \leq i \leq 7)$ and let $\mathcal{K}_2$ be the key space of $K'_{15}[j](4 \leq j \leq 7)$. This attack is summarized as follows.
Goal: Finding $K'_{16}[0], K'_{16}[i](4 \leq i \leq 7)$, and $K'_{15}[j](4 \leq j \leq 7)$

1. Collect sufficiently many (discussed later) plaintext pairs from the structures whose ciphertext differences satisfy $\Delta C_R[0] \neq 0, \Delta C_R[i] = 0(1 \leq i \leq 3), \Delta C_L[j] = 0(0 \leq j \leq 3)$, and $\Delta C_L[4] \neq 0$.
2. Choose a pair in the collection.
3. For each $k_1 \in \mathcal{K}_1$,

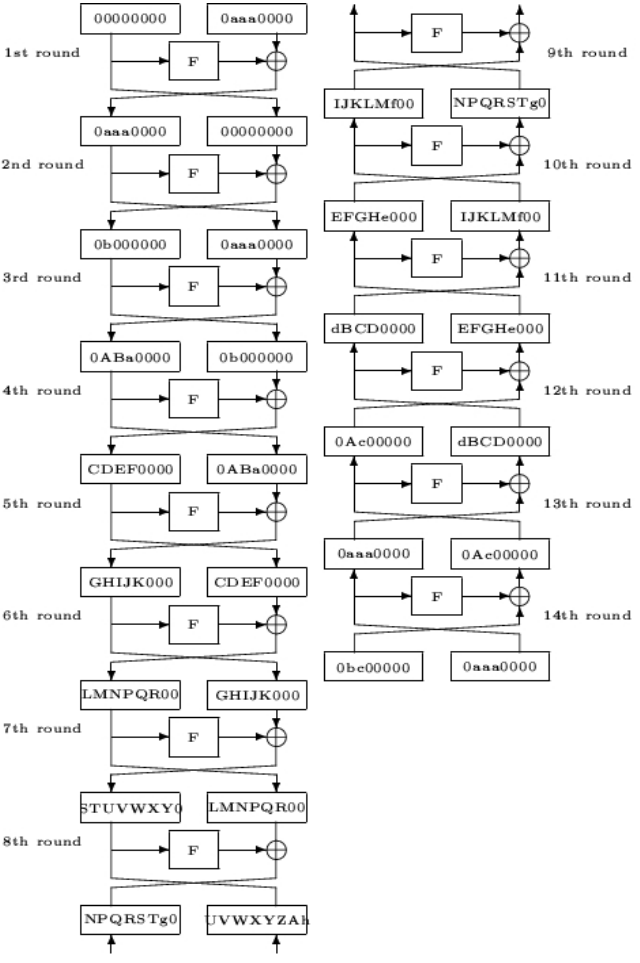

Fig. 7. 14-round impossible differential characteristic 14-II

a) Compute $O_R^{15}[0], O_R^{15}[l] (4 \leq l \leq 7)$.

b) Unless $O_R^{15}[0] = O_R^{15}[4] = O_R^{15}[7] = 0$, $O_R^{15}[5] \neq 0$, and $O_R^{15}[6] \neq 0$, choose another $k_1 \in \mathcal{K}_1$ and go to 3.(a).

c) For each $k_2 \in \mathcal{K}_2$,

   i. Compute $O_R^{14}[s] (4 \leq s \leq 7)$.

   ii. Remove k_1 and k_2 from $\mathcal{K}_1$ and $\mathcal{K}_2$, respectively, if $O_R^{14}[4] = 0$ and $O_R^{14}[5] = O_R^{14}[6] = O_R^{14}[7] \neq 0$.

4. If $|\mathcal{K}_1| \leq \epsilon$ and $|\mathcal{K}_2| \leq \epsilon'$, stop. Otherwise, go to 2. (ϵ and ϵ' are small integer.)

We obtain 72 bits of K'_{15} and K'_{16}. The probability that any $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$ survives the test with such a pair is

$$1-\left\{\left(\frac{1}{2^8}\right)^2 \cdot \left(\frac{2^8-1}{2^8}\right)^2 \cdot \frac{1}{2^8-1}\right\} \cdot \left\{\left(\frac{1}{2^8}\right)^3 \cdot \frac{2^8-1}{2^8}\right\} \simeq 1-\left(\frac{1}{2^8}\right)^6 = 1-2^{-48}.$$

Thus, the number of the pairs collected for the attack is N such that $2^{72} \cdot (1 - 2^{-48})^N \simeq 1$. N is about $2^{53.6}$. Therefore, the required number of chosen plaintext pairs is $2^{56} \cdot 2^{53.6} = 2^{109.6}$.

Since we can collect 2^{15} pairs from one structure, we need $2^{94.6}$ structures. It follows that the attack requires $2^{94.6} \cdot 2^8 = 2^{102.6}$ chosen plaintexts.

Using the characteristic in Figure 7, we obtain $K'_{16}[i](0 \leq i \leq 4)$ and $K'_{15}[j](0 \leq j \leq 3)$ with the same complexity, and then do K_{15} and K_{16} from K'_{15} and K'_{16}. The time complexity of this attack is computed as follows.

- $2^{103.6} (= 2 \times 2^{102.6})$ encryptions of chosen plaintexts
- Finding K'_{15} and K'_{16} : $2 \cdot \{2^{72} + 2^{72} \cdot (1-2^{-48}) + \cdots + 2^{72} \cdot (1-2^{-48})^{2^{53.6}-1}\} \simeq 2^{121} - 2^{49}$ two-round encryptions. $\Rightarrow 2^{118} - 2^{46}$ encryptions.

We can find every round key similarly to the above method. The total time complexity is about 2^{119} at most, since complexity decreases as the number of rounds reduces.

6 Conclusion

The design principles of Zodiac are the simplicity, provability, accommodation and performance. By the simplicity Zodiac attains the accommodation and good performance. However, Zodiac has crucial weakness in security from the theoretical point of view because of its poor design of the diffusion layer.

In this paper we did find the 15-round and 14-round impossible differentials of Zodiac. Using two 14-round impossible differential we attacked the 15-round Zodiac with $2^{102.5}$ chosen plaintext pairs and the full-round Zodiac with $2^{103.6}$ chosen plaintext pairs. The complexity of our full round attack is at most 2^{119} encryption, which means that this attack is more effective than the exhaustive key search attack. Furthermore, when the key length is 192-bit or 256-bit, its security decreases more seriously.

We think the diffusion layer should be changed. This result shows the importance of the design for the diffusion layer as well as the substitution layer.

References

1. I. Ben-Aroya and E. Biham, *Differential Cryptanalysis of Lucifer*, Journal of Cryptology, vol.9, no.1, pp.21–34, 1996.
2. E. Biham, A. Biryukov, and A. Shamir, *Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials*, Advances in Cryptology — EUROCRYPT'99, LNCS 1592, Springer-Verlag, 1999, pp.12–23.

3. E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Advances in Cryptology — CRYPTO'90, LNCS 537, Springer-Verlag, 1991, pp.2–21.
4. L. Brown, J. Pieprzyk, and J. Seberry, *LOKI - A cryptographic primitive for authentication and secrecy applications*, Advances in Cryptology — AUSCRYPT'90, LNCS 453, pp.229–236, Springer-Verlag, 1990.
5. L. R. Knudsen, *Truncated and Higher Order Differential*, Fast Software Encryption Workshop 94, LNCS 1008, pp.229–236, Springer-Verlag, 1995.
6. L. R. Knudsen and T. Jakobsen, *The Interpolation Attack on Block Ciphers*, Fast Software Encryption Workshop 97, LNCS 1267, pp. 28–40, Springer-Verlag, 1997.
7. ChangHyi Lee, KyungHwa Jun, MinSuk Jung, SangBae Park, and JongDeok Kim, *Zodiac Version 1.0(revised) Architecture and Specification*, Standardization Workshop on Information Security Technology 2000, Korean Contribution on MP18033, ISO/IEC JTC1/SC27 N2563, 2000, Available at the KISA's web page, http://www.kisa.or.kr/seed/index.html.
8. S. Moriai, T. Shimoyama, and T. Kaneko, *Higher Order Differential Attack of a CAST cipher*, Fast Software Encryption Workshop 98, LNCS 1372, pp.17–31, Springer-Verlag, 1998.
9. B. Van Rompay, L. R. Knudsen, and V. Rijmen, *Differential cryptanalysis of the ICE encryption algorithm*, Fast Software Encryption Workshop 98, LNCS 1372, pp.270–283, Springer-Verlag, 1998.
10. A. Shimizu and S. Miyaguchi, *Fast Data Encipherment Algorithm FEAL*, Advances in Cryptology — EUROCRYPT'87, LNCS 304, pp.267–278, Springer-Verlag, 1988.
11. D. Wagner, *The boomerang attack*, Fast Software Encryption Workshop 99, LNCS 1636, pp.156–170, Springer-Verlag, 1999.