3-6 On Multi Rounds Elimination Method for Higher Order Differential Cryptanalysis

TANAKA Hidema, TONOMURA Yuji, and KANEKO Toshinobu

A multi rounds elimination method for higher order differential cryptanalysis is consisted of two rounds elimination attack and probabilistic higher order differential cryptanalysis. A probabilistic higher order differential cryptanalysis is a method using a value of higher order differential which holds with probability. The success of attack depends on the probability, however, the necessary number of chosen plaintext and computational cost become very small. ICEBERG is a block cipher with sixteen round SPN structure. In this paper, we analyze its higher order differential property, and estimate its strength against higher order differential attacks. As the result, we found that five round ICEBERG is attackable using eighth order differential with 2,304 chosen cipher texts and 2^{85} times round function calculations. And in the case using probabilistic seventh order differential, it is attackable with 1,152 chosen cipher texts and 283 times round function calculations and probability about 0.7.

Keywords
Chosen plaintext attack, Block cipher, Higher order differential cryptanalysis, Probabilistic higher order differential, SPN

1 Introduction

Higher order differential cryptanalysis is a general attack method for symmetric-key block ciphers. This attack method is based on the order of the non-linear functions used in the cryptographic algorithm, and is particularly effective when the order is relatively low. While much has been said on linear and differential cryptanalysis—typical general attacks for symmetric-key block ciphers—and methods of designing corresponding security functions are now well established, even with the deployment of these functions we are now seeing examples of attacks by higher order differential cryptanalysis.

ICEBERG (Involution Cipher Efficient for Block Encryption in Reconfigurable hardware) [4] is a 64-bit block cipher with a 128-bit key proposed by the UCL Crypto Group in 2004. The basic structure of the cipher is known as SPN, which consists of repeated non-linear layers and linear-substitution layers. This structure has been selected, for example, for use in AES [6] and Hierocrypt [7], and offers higher security with fewer rounds than the conventional generic Feistel structure. Thus, ICEBERG is particularly well adapted to implementation in smaller hardware structures.

This paper discusses the two-round elimination attack and probabilistic higher order differential cryptanalysis against block ciphers with the SPN structure, taking ICEBERG as an example. The two-round elimination attack method is discussed in Article **3-4**, in which it is described in detail as an attack method against block ciphers featuring the Feistel structure. Here, we will discuss a case involving the SPN structure. The basic algorithm is the same as that used with the Feistel structure. Probabilistic higher order differential cryptanalysis uses the higher order differen-

tials that satisfy the requisite probability conditions, and the attacks thus succeed based on this probabilistic approach. Section **2** outlines the higher order differentials. Section **3** discusses the structure and characteristics of ICEBERG. Section **4** discusses an analysis of the higher order differential properties of ICEBERG and shows the probabilistic higher order differentials. Section **5** shows the results of attacks applying the results of analysis. Section **6** provides a summary of the paper.

2 Higher order differential cryptanalysis

2.1 Higher order differential

Let us consider $F(X;K)$, which is a function of $GF(2)^n \times GF(2)^s \rightarrow GF(2)^n$.

$$\begin{aligned} &Y=F(X;K) \\ &X \in GF(2)^n,\ Y \in GF(2)^n,\ K \in GF(2)^s \end{aligned} \tag{1}$$

With $(a_0, a_1, ..., a_{N-1})$, a linearly independent set of vectors in $GF(2)^n$, we denote the subspace spanned by $(a_0, a_1, ..., a_{N-1})$ as $V[a_0, a_1, ..., a_{N-1}]$. Denoting the N-th differential of $F(X;K)$ with respect to X as $\Delta^{(N)}_{V_{[a_0,a_1,...,a_{N-1}]}}$, it can be calculated as follows:

$$\Delta^{(N)}_{V_{[a_0,a_1,...,a_{N-1}]}} F(X;K) = \sum_{A \in V_{[a_0,a_1,...,a_{N-1}]}} F(X+A;K) \tag{2}$$

In the following, $\Delta^{(N)}_{V_{[a_0,a_1,...,a_{N-1}]}}$ is abbreviated as $\Delta^{(N)}$ when $V[a_0, a_1, ..., a_{N-1}]$ is obvious. If $\deg_X\{F(X;K)\}=d$ holds, the following property holds:

Property 1

$$\deg_X\{F(X;K)\} = d \rightarrow \Delta^{(d+1)}F(X;K) = 0 \tag{3}$$

2.2 Attack equation

Let us assume a block cipher consisting of R rounds. Let $E_i(\cdot)$ be the encryption function consisting of i rounds, and let $H_{(R-1)}(X)$ be the output corresponding to the plaintext X from round $(R-1)$.

$$H_{(R-1)}(X) = E_{(R-1)}(X;K_1,K_2,...,K_{(R-1)}) \tag{4}$$

Here, K_i is the sub-key for the i-th round.

If the order of $E_{(R-1)}(\cdot)$ with respect to X is $N-1$, the following equation holds:

$$\Delta^{(N)}H_{(R-1)}(X) = 0 \tag{5}$$

Denoting the decryption function that decodes only a single round from ciphertext $C(X)$ as $E'(\cdot)$, the following expression is derived:

$$H_{(R-1)}(X)=E'(C(X);K_R) \tag{6}$$

From Equations (5) and (6) and Property 1, the following equation holds:

$$\sum_{A \in V^{(N)}} E'(C(X+A);K_R) = 0 \tag{7}$$

The equation is valid when the value for K_R is correct. We refer to this equation hereinafter as the attack equation.

2.3 Number of required chosen plaintexts for attacks

This paper uses a brute force search to obtain K_R in the attack equation. Let l be the width of the attack equation. If the exhaustive search is conducted with a single set of attack equations, false keys satisfy the equations with a probability of 2^{-l}. Thus, we use an excess number of attack equations to eliminate false keys. Let $/K_R/$ be the width of the key to be obtained and M be the number of higher differential sets required. Then, M must be chosen to satisfy the following equation:

$$(2^{-l})^M \times 2^{/KR/} \leqq 1 \tag{8}$$

The number of required chosen plaintexts is then $M \times 2^N$, and the number of required round function calculations is $2^{/KR/} \times M \times 2^N$, if the N-th differentials are necessary for the attack.

3 ICEBERG

Figure 1 shows the structure of the ICEBERG round function. The symbol S indicates an eight-bit input/output S-box. Figure 2 shows the structure of the S-box. The symbols D and P4 indicate the four-bit diffusion layer and the four-bit inversion, respectively. The tables show the relevant operations. (See

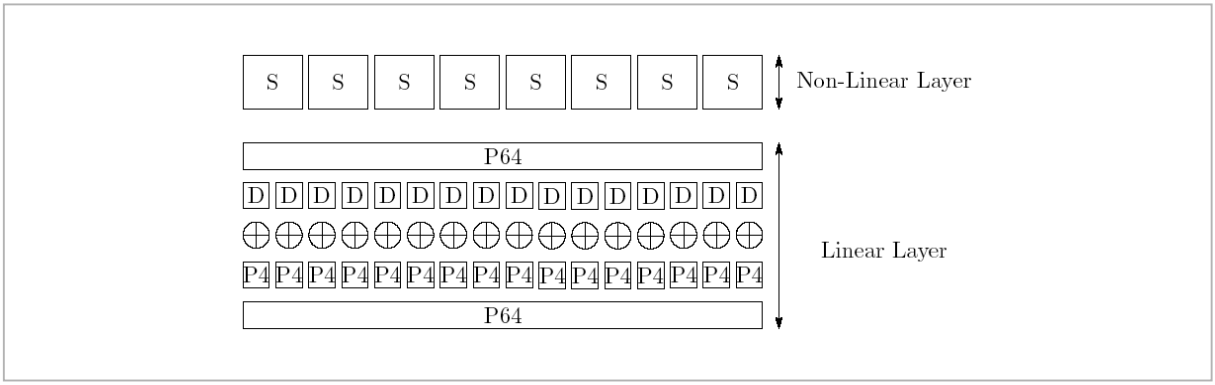

Fig.1 Round functions of ICEBERG (⊕ indicates EX-OR of the keys)

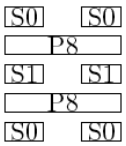

Fig.2 S-box

Table 1 D

0	1	2	3	4	5	6	7
0	e	d	3	b	5	6	8
8	9	a	b	c	d	e	f
7	9	a	4	c	2	1	f

Table 2 P4

0	1	2	3
1	0	3	2

Tables 1 and 2. The upper row shows the inputs and the lower row shows the corresponding outputs.) The symbol P64 indicates the 64-bit inversion, and Table 3 shows the relevant operations. ICEBERG has a convolution structure with 16 rounds of these round functions in specification. The symbols S0 and S1 in the structure of the S-box shown in Fig.2 each indicate an internal four-bit input/output S-box. Thus, the S-boxes have nested structures. Tables 4 and 5 show the operations for S0 and S1, respectively. The symbol P8 indicates the eight-bit inversion, and Table 6 shows the relevant operations.

The proponents of ICEBERG have stated that they designed the cipher mainly for implementation in small hardware structures. The non-linear functions involved are only the four-bit S0 and S1, which feature a maximum of three orders. As this value is extremely small relative to recent block ciphers, ICEBERG cannot ensure sufficient security against algebraic cryptanalysis, such as higher order differential cryptanalysis, if the diffusion through inversion is not sufficient. Accordingly, ICEBERG has been analyzed in detail against linear cryptanalysis and differential cryptanalysis, both general and powerful attack methods, and sufficient security has been demonstrated with the specified number of rounds.

This study discusses the security of ICEBERG in terms of higher order differentials.

4 Higher order differential properties of ICEBERG

4.1 Analysis with SQUARE attacks

The SQUARE attack is proposed in Reference[1]. It searches for an effective method of selecting higher order differentials for each sub-block of the plaintexts. As the S-boxes are eight-bit, the plaintexts are divided into eight-bit sub-blocks.

$$P=(p_0,p_1,...,p_7) \quad (9)$$

Figure 3 provides an illustration of four-round ICEBERG. Here, *Xr* is the output from round *r*. Analyzing the higher order differential with a selected value for *pi*, the following

Table 3 P64

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	23	25	38	42	53	59	22	9	26	32	1	47	51	61
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
24	37	18	41	55	58	8	2	16	3	10	27	33	46	48	62
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
11	28	60	49	36	17	4	43	50	19	5	39	56	45	29	13
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
30	35	40	14	57	6	54	20	44	52	21	7	34	15	31	63

Table 4 S0

0	1	2	3	4	5	6	7
d	7	3	2	9	a	c	1
8	9	a	b	c	d	e	f
f	4	5	e	6	0	b	8

Table 5 S1

0	1	2	3	4	5	6	7
4	a	f	c	0	d	9	b
8	9	a	b	c	d	e	f
e	6	1	7	3	5	8	2

Table 6 P8

0	1	2	3	4	5	6	7
0	1	4	5	2	3	6	7

expression is found to hold for the second round output, X_2:

$$\Delta^{(8)}X_2=0 \tag{10}$$

This equation is true for any value of p_i. Further, two or three sub-blocks are selected for the sixteenth and twenty-fourth higher order differentials to analyze their higher order differential properties. The result is zero for all higher order differentials for the second round output.

However, this result does not hold for outputs from the third and higher rounds. The results of these analyses show that the order of X_2 with respect to X is seven or less and that the order of X_3 with respect to X is 24 or more.

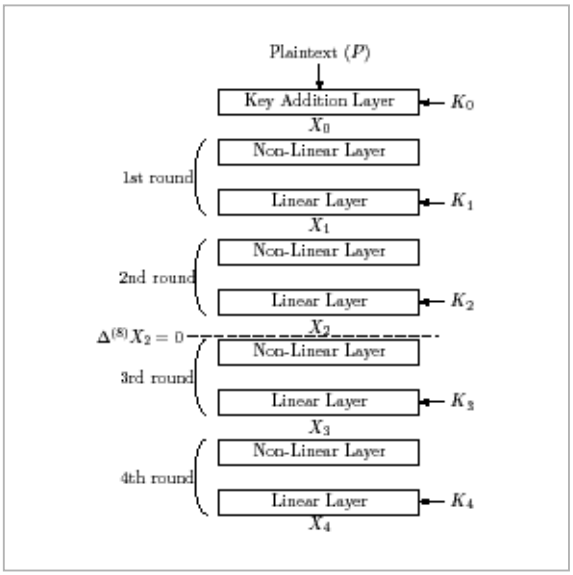

Fig.3 Two-round elimination attack

4.2 Analysis with probabilistic higher order differential cryptanalysis

To analyze the higher order differential property of ICEBERG, another approach is taken, using the following eight linearly independent vectors:

$$\begin{aligned} A_1&=(\Delta p_0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0)\\ A_2&=(0 \;\; \Delta p_1 \; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0)\\ &\cdots\\ A_7&=(0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; \Delta p_7) \end{aligned} \tag{11}$$

Here, Δpi are constants, at least one of which is not zero. The eighth differentials are calculated for the second round output using these vectors. The result confirms that the eighth differentials are always zero. Further, selecting appropriate values for A_i, where ($i<8$), the i-th differentials are calculated for the second round output. For the seventh differentials, for example, the values are zero with a probability of approximately 0.7. Table

Table 7 *Probability of the value of higher order differential equals to zero*

i	$P_r(i) = Prob\{\Delta^{(i)}_{V^{(i)}} X_2 = 0\}$
8	1
7	0.7
6	0.4
5	0.25
4	0.07
3	0.02
2	0.002
1	$0(\simeq 2^{-44.7})$

7 shows the results of simulation studies for $P_r(i)=prob\{\Delta^{(i)}X_2 = 0\}$.

5 Attacks against ICEBERG

5.1 Single round elimination attack

This section discusses the single round elimination attack, which uses higher order properties with respect to X_2. The eight-byte output $X_2 = (x_{20}, x_{21}, ..., x_{27})$ is input into the third round non-linear layer S-box. The output is denoted $Y_3 = (y_{30}, y_{31}, \ldots, y_{37})$. The value for Y_3 can be inversely calculated for four-round ICEBERG from the ciphertexts with the value of K_3 as an unknown. Denoting the variables as shown in Fig.4, the following expressions are derived:

$$Y_3=A_2(A_1X_3+K_3)$$
$$Y_3=A_2A_1X_3+A_2K_3=X_3'+K_3' \ (X_3'=A_2A_1X_3,\ K_3'=A_2K_3) \quad (12)$$

As the relationship $x_{2i} = S(y_{3i})$ holds, the following is true for each i:

$$\Delta^{(8)}S(x_{3i}'+k_{3i}')=0 \quad (13)$$

Let us consider solving this equation with a brute force search with respect to k_{3i}'. This equation has an eight-bit width, so that $M=1$. Thus, the number of required plaintexts is $M\times 2^N = 1\times 2^8=256$ and the number of required round function calculations is $2^{|KR|}\times M\times 2^N = 2^8\times 1\times 2^8=2^{16}$.

If the probabilistic seventh-order differentials shown in Section **4.2** are used for the attack, the number of required plaintexts is $M\times 2^N=1\times 2^7=128$ and the number of required round function calculations is $2^{|KR|}\times M\times 2^N = 2^8\times 1\times 2^7=2^{15}$ to succeed in attacks with a probability of 0.7.

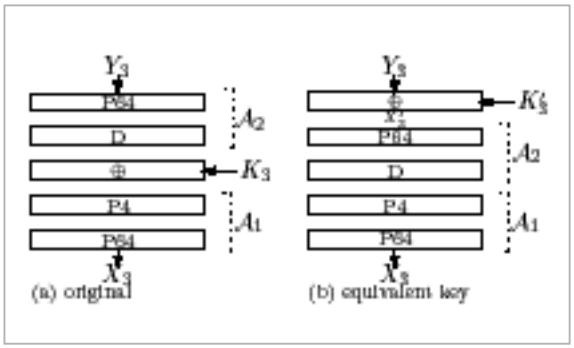

Fig.4 *Linear layer and key addition*

5.2 Two-round elimination attacks

The attack method discussed in Section **5.1** can be expanded into the two-round elimination attack. This section decodes X_4 while estimating the total bits of the keys for K_4 with a brute force search, and derives the attack equation indicated in Section **5.1**.

$$X_3=E'(X_4;K_4) \quad (14)$$

The attacker must then estimate the 64 bits of K_4 and the eight bits of k_{3i}, which make 72 bits in total. From Equation (8), the false keys can be eliminated with $M=9$. Thus, the number of required plaintexts is $M\times 2^N=9\times 2^8=2304$ and the number of required round function calculations is $2^{|KR|}\times M\times 2^N=2^{72}\times 9\times 2^8<2^{85}$.

If probabilistic higher order differentials are used, success is based on the corresponding probability, but the cipher can be attacked with fewer plaintexts and a lower computational cost. For example, if the seventh order differentials are used, the success rate for the attack is approximately 0.7, but the number of required plaintexts is $M\times 2^N=9\times 2^7=1152$ and the number of required round function calculations is $2^{|KR|}\times M\times 2^N=2^{72}\times 9\times 2^7<2^{83}$.

6 Conclusions

This paper describes the multi-round elimination method for higher order differential cryptanalysis against block ciphers with the SPN structure, taking ICEBERG as a specific example. ICEBERG is a newly proposed cipher algorithm and the investigation of its

security remains incomplete. The results of the attacks studied in this paper show that five or more rounds of attacks are not possible even with a combination of two-round elimination attacks and probabilistic higher order differential values. Thus, the 16 rounds specified for ICEBERG are considered to provide sufficient strength against higher order differential cryptanalysis.

References

1 Daemen, Govaerts, Rijmen, "The Block Cipher SQUARE", 4th Fast Software Encryption. LNCS1267, pp.149-165, Springer-Verlag, 1997.

2 Jakobsen, Knudsen, "The interpolation attacck on block cipher", FSE96, LNCS1008, pp.28-40, Springer-Verlag, 1997.

3 Lai, "Higher order derivatives and differential cryptanalysis", Communications and Cryptology, pp.227-233, Kluwer Academic Publishers, 1994.

4 Standacrt, Piret, Rouvroy, Quisquator, Legat, "ICEBERG : an Involution Cipher Efficient for Block Encryption in Reconfigurable Hardware", FSE2004 pre-proceedings.

5 Tanaka, kaneko "An attack of 6-round MISTY1 without FL function", Technical Report of IEICE, ISEC2002-41, 2002.

6 NIST homepage http://csrc.nist.gov/CryptoToolKit/aes

7 Toshiba homepage http://www.toshiba.co.jp/rdc/security/hierocrypt/CRYPTREC/2000/

***TANAKA Hidema**, Ph.D.*
Researcher, Security Fundamentals Group, Information and Network System Department
Cryptology, Information security

***KANEKO Toshinobu**, Ph.D.*
Professor, Tokyo university of science
Cryptology, Information security

TONOMURA Yuji
Professor, Tokyo university of science
Cryptology, Information security