3-6　複数段消去型高階差分攻撃

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

田中秀磨　　殿村裕司　　金子敏信
TANAKA Hidema, TONOMURA Yuji, and KANEKO Toshinobu

要旨

複数段消去型高階差分攻撃は 2 段消去型攻撃と確率的高階差分攻撃で構成されている。確率的高階差分攻撃は、確率的に成立する高階差分値を利用する攻撃であり、攻撃の成功はその確率に依存する。確率的な攻撃になる反面、必要な平文数や計算量が削減できる。ICEBEREG は 16 段の SPN 構造を持つブロック暗号である。その高階差分特性について解析し、5段までの攻撃が可能であることを示す。8 階差分を用いた攻撃には 2,304 個の選択平文と 2^{85} 回のラウンド関数計算が必要である。一方で確率的に成立する 7 階差分値を用いた攻撃は、成功確率約 0.7 で 1,152 個の選択平文と 2^{83} 回のラウンド関数計算が必要である。

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 2^{83} times round function calculations and probability about 0.7.

［キーワード］
選択平文攻撃，ブロック暗号，高階差分攻撃，確率的高階差分，SPN
Chosen plaintext attack, Block cipher, Higher order differential cryptanalysis, Probabilistic higher order differential, SPN

1　はじめに

高階差分攻撃は共通鍵ブロック暗号の汎用な攻撃方法である。暗号アルゴリズムで使用されている非線形関数の次数に着目する攻撃方法であり、次数が低いとき効果的な攻撃方法となる。例えば、共通鍵ブロック暗号の汎用な攻撃方法として代表的なものである線形解読法と差分解読法については証明可能な安全性の議論が帰着し、そのような関数の設計方法が示されているが、そのような関数を用いている場合であっても高階差分攻撃で攻撃可能な例がある。

ICEBERG（Involution Cipher Efficient for Block Encryption in Reconfigurable Hardware）[4] は 2004 年に UCL Crypto Group によって提案された 128 ビット鍵の 64 ビットブロック暗号である。基本的な構造は SPN と呼ばれる非線形層と線形置換層の繰り返しである。この構造は例えば AES[6] や Hierocrypt[7] で採用され、これまでの一般的な構造であった Feistel 構造よりも、少ない段数で高い安全性に到達できる。そのため、ハードウェアなどにおいて小型実装の点で優れ

ている。

本論文では ICEBERG を攻撃例として、SPN 構造を持つブロック暗号に対する 2 段消去攻撃と確率的高階差分攻撃について示す。2 段消去攻撃は **3-4** で述べた攻撃方法であり、そこでは Feistel型ブロック暗号に対する攻撃法として詳解した。ここでは SPN 構造の場合について述べる。基本的なアルゴリズムは同じである。確率的高階差分攻撃は確率的に成立する高階差分値を利用する攻撃方法であり、攻撃は確率的に成功する。**2** で簡単に高階差分について示し、**3** で ICEBERG の構造と特徴について述べる。**4** で ICEBERG の高階差分特性の解析について述べ、確率的高階差分について示す。**5** でこの解析結果を応用した攻撃結果について示し、**6** でまとめる。

2 高階差分攻撃

2.1 高階差分

$F(X;K)$ を $GF(2)^n \times GF(2)^s \rightarrow GF(2)^n$ の関数とする。

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

$(a_0, a_1, \cdots, a_{N-1})$ を線形独立な $GF(2)^n$ のベクトルとし、これらによって張られる部分空間を $V[a_0, a_1, \cdots, a_{N-1}]$ とする。ここで、$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}}$ を $F(X;K)$ の X に関する N 階差分とすると、これは以下のように計算できる。

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

以下では $V[a_0, a_1, \cdots, a_{N-1}]$ が明らかなとき、$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}}$ を $\Delta^{(N)}$ と略記する。もし、$\deg_X\{F(X;K)\}=d$ であるならば、以下の性質が成立する。

性質 1

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

2.2 攻撃方程式

R 段で構成されているブロック暗号を仮定する。$E_i(\cdot)$ を i 段で構成される暗号化関数とし、$H_{(R-1)}(X)$ を $(R-1)$ 段目からの平文 X に対応する出力とする。

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

ただし K_i は i 段目の拡大鍵である。

もし $E_{(R-1)}(\cdot)$ の X に関する次数が $N-1$ であれば、以下が成立する。

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

$E'(\cdot)$ を暗号文 $C(X)$ から一段分だけ復号する復号関数とすれば、以下の式が導ける。

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

式 (5) (6) と性質 1 から、以下の式が成立する。

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

この方程式は K_R の値が正しい時は成立する。以下ではこれを攻撃方程式と呼ぶ。

2.3 攻撃に必要な選択平文数

本論文では攻撃方程式において K_R を求めるアルゴリズムに全数探索を用いた。l を攻撃方程式の幅とする。もし 1 組の攻撃方程式で全数探索を実行すると、偽の鍵であっても 2^{-l} の確率で攻撃方程式を成立させてしまうので、余計に攻撃方程式を解くことにより偽の鍵をふるいにかける。$|K_R|$ を求めるべき鍵の幅とし、M を必要な高階差分の組数とする。すると、M は以下の式を満足させる値を選ばなければならない。

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

すると、必要な選択平文組数は N 階差分を攻撃に要したとすれば $M\times 2^N$ 個であり、必要な計算量は $2^{|KR|}\times M\times 2^N$ 回のラウンド関数計算となる。

3.1 CEBERG

図 1 に ICEBERG のラウンド関数の構造を示す。記号 S は 8 [bit] 入出力の S-Box を表し、その構造を図 2 に示す。記号 D と P4 はそれぞれ 4 [bit] の拡散層と 4 [bit] の転置を表す。それぞれ表で演算が示されている (表 1 及び表 2。上段が入力でその下段が対応する出力を表す。)。記号 P64 は 64 [bit] の転置であり表 3 に示す。

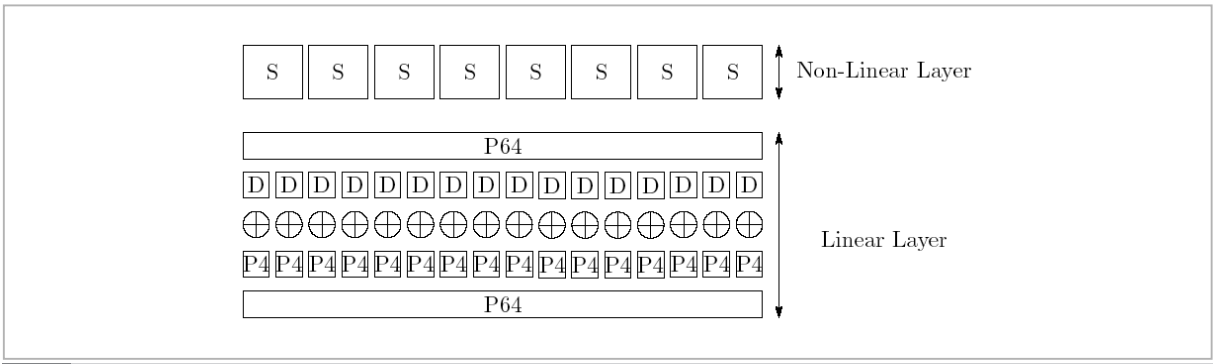

図1 ICEBER のラウンド関数（⊕は鍵の排他的論理和を表す）

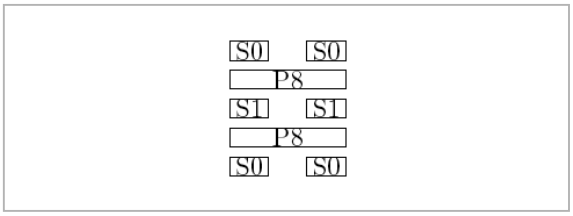

図2 S-box

表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

表2 P4

0	1	2	3
1	0	3	2

ICEBERG はこのようなラウンド関数を 16 段繰り返す構造が仕様となっている。図 2 は S-box の構造を示しているが、図中の記号 S0 と S1 は更に内部的な 4［bit］入出力の S-box であり、入れ子構造となっている。それぞれの演算を表 4 と表 5 に示す。記号 P8 は 8［bit］の転置であり、表 6 に示す。

ICEBERG の提案者は、特にハードウェアでの小型実装に主眼置き設計していると主張している。非線形関数は 4［bit］の S0 と S1 のみであり、最大でも 3 次にしか達しないため最近のブロック暗号と比較すると非常に小さいため、転置による拡散が十分でないと高階差分攻撃に代表される代数的解読法に対して十分な安全性が保てない。汎用で強力な攻撃方法である線形解読法と差分解読法に対しては十分な解析がなされ、仕様段数で十分な安全性が示されている。

本研究では、高階差分の観点から ICEBERG の安全性について考察する。

4　CEBERG の高階差分特性

4.1　SQUARE-Type 攻撃による解析

SQUARE-Type 攻撃は文献[1]で提案されたサブブロック単位で効果的な高階差分の選び方を探索する攻撃方法である。S-box が 8［bit］単位であるので、ここでは平文を 8［bit］のサブブロックに分割して考える。

$$P=(p_0,p_1,\ldots,p_7) \tag{9}$$

4 段構成の ICEBERG を図 3 に示す。ただし X_r は r 段目からの出力である。p_i を適当に選択し高階差分特性を解析したところ、2 段目出力 X_2 に対して以下が成立することが分かった。

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

これはどの p_i を選んでも必ず成立する。また、16 階差分や 24 階差分をそれぞれ適当の二つのサブブロックもしくは三つのサブブロックを選んで高階差分特性を解析したところ、2 段目出力に関してはすべて高階差分値が 0 となった。

しかしながら 3 段目出力以降では、これらは成立しないことを発見した。これらの解析結果から、X_2 の X に対する次数は 7 次以下であり、X_3 については 24 次以上であることが分かった。

表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

表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

表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

表6 P8

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

4.2 確率的高階差分攻撃による解析

ICEBERG の高階差分を解析するために、以下のような 8 個の線形独立なベクトルを使った別のアプローチを検討した。

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

ただし Δp_i は非ゼロのある定数である。これらを使った 8 階差分を 2 段目出力に対して計算した結果、8 階差分値が常に 0 となることを確認した。さらに、適当な $i(i<8)$ 個の A_i を選んで i 階差分を 2 段目出力に対して計算した結果、例えば 7 階差分の場合、確率約 0.7 で値が 0 となることを発見した。$P_r(i)=prob\{\Delta^{(i)}X_2=0\}$ とした場合の計算機実験の結果を表 7 に示す。

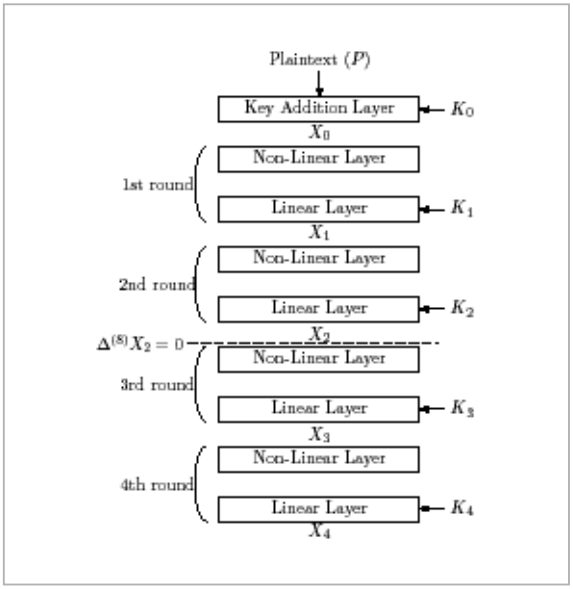

図3 2 段消去型攻撃

5 CEBERG に対する攻撃

5.1 1 段消去攻撃

X_2 に関する高階差分特性を利用した、1 段消去攻撃について示す。8[byte] 出力である $X_2=(x_{20}, x_{21}, \ldots, x_{27})$ は 3 段目の非線形層である S-box へ入力される。その出力を $Y_3=(y_{30}, y_{31}, \ldots, y_{37})$ とする。この Y_3 の値は 4 段構成 ICEBERG であれば暗号文側から K_3 の値を未知数として逆算できる。ここで変数を図 4 のように置くと、以下のように書ける。

$$\begin{aligned} &Y_3=A_2(A_1X_3+K_3)\\ &Y_3=A_2A_1X_3+A_2K_3=X_3'+K_3' \ (X_3'=A_2A_1X_3,\ K_3'=A_2K_3) \end{aligned} \tag{12}$$

$x_{2i}=S(y_{3i})$ が成立するので、各 i に対して以

表7　高階差分値が0と等しくなる確率

i	$P_r(i) = Prob\{\Delta^{(i)}_{V^{(i)}} X_3 = 0\}$
8	1
7	0.7
6	0.4
5	0.25
4	0.07
3	0.02
2	0.002
1	$0(\simeq 2^{-44.7})$

下が成立する。

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

この方程式を k_{3i}' に対して全数探索で解くことを考える。今、この方程式は8[bit]幅なので $M=1$ である。したがって、必要な選択平文は $M \times 2^N = 1 \times 2^8 = 256$ 個であり、必要な計算量は $2^{|KR|} \times M \times 2^N = 2^8 \times 1 \times 2^8 = 2^{16}$ 回のラウンド関数計算となる。

また、**4.2** で示した確率的に成立する7階差分を用いて攻撃すれば、選択平文は $M \times 2^N = 1 \times 2^7 = 128$ 個であり、必要な計算量は $2^{|KR|} \times M \times 2^N = 2^8 \times 1 \times 2^7 = 2^{15}$ 回のラウンド関数計算で成功確率0.7で攻撃を実行できる。

5.2　2段消去攻撃

5.1 で示した攻撃方法は、2段消去型攻撃に発展できる。K_4 の鍵の全ビットを全数探索により見積もりながら X_4 を復号し、**5.1** で示した攻撃方程式を導出する。

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

すると、攻撃者は K_4 の64[bit]と k_{3i} の8[bit]、合計72[bit]を推定しなければならない。式(8)から、$M=9$ であれば偽鍵を排除できるので、必要な選択平文は $M \times 2^N = 9 \times 2^8 = 2304$ 個であり、

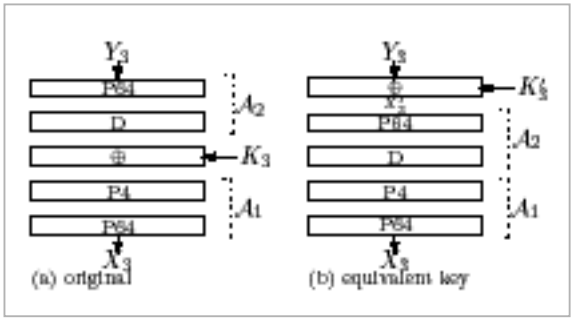

図4　線形層と鍵加算

必要な計算量は $2^{|KR|} \times M \times 2^N = 2^{72} \times 9 \times 2^8 < 2^{85}$ 回のラウンド関数計算となる。

確率的に成立する高階差分値を利用すれば、確率的な成功となるが、攻撃をより少ない選択平文数と計算量で実行できる。例えば7階差分を用いた場合は攻撃成功確率は約0.7であるが、必要な選択平文は $M \times 2^N = 9 \times 2^7 = 1152$ 個であり、必要な計算量は $2^{|KR|} \times M \times 2^N = 2^{72} \times 9 \times 2^7 < 2^{83}$ 回のラウンド関数計算となる。

6　まとめ

本論文では、SPN構造を持つブロック暗号に対して複数段消去型の高階差分攻撃をICEBERGを具体的な例として示した。ICEBERGは新しく提案された暗号アルゴリズムであり、安全性評価が十分になされていない。本論文が示した攻撃結果により、2段消去型攻撃と確率的な高階差分値を利用しても5段以上の攻撃は不可能であった。それゆえ、ICEBERGの仕様段数である16段は十分に高階差分攻撃に対して強度を有すると考えられる。

参考文献

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/

田中秀磨（たなかひでま）
情報通信部門セキュリティ基盤グループ研究員　博士（工学）
暗号理論、情報セキュリティ

金子敏信（かねこ としのぶ）
東京理科大学教授　博士（工学）
暗号理論、情報セキュリティ

殿村裕司（とのむらゆうじ）
東京理科大学教授
暗号理論、情報セキュリティ