Hierocryptのブール代数次数評価

吉名 晋一　　井上 博之　　金子 敏信

東京理科大学大学院
〒278-8510　千葉県野田市山崎 2641
kaneko@ee.noda.tus.ac.jp

あらまし　Hierocrypt の高階差分攻撃への耐性を調査するためにブール代数次数を評価した。まず、Boura らによって提案された多数の Sbox を並列に適用する関数の次数の上界を求める定理を S 層 2 層、3 層、4 層分に適用し、次数の上界として Hierocrypt-3 については S 層 2 層は 28 次、3 層は 116 次、4 層は 124 次、Hierocrypt-L1 については S 層 2 層は 28 次、3 層は 61 次、4 層は 62 次という結果を得た。次に、全単射性を使って次数を評価すると S 層 2 層の次数の上界は 28 次であり、S 層 4 層の次数の上界は Hierocrypt-3、-L1 がそれぞれ 124 次、62 次となった。また計算機で S 層 2 層の実際の次数を調べると 28 次であり、Boura らの定理や全単射性を使って求めた上界と一致した。これより、3 層、4 層については計算量が多すぎるため確かめられないが、本稿で求めた次数の上界がタイトなものであると予想できる。

Evaluation of Boolean algebraic degree of Hierocrypt

Shinichi Yoshina　　Hiroyuki Inoue　　Toshinobu Kaneko

Tokyo University of Science
2641 Yamazaki, Noda, Chiba, 278-8510 JAPAN
kaneko@ee.noda.tus.ac.jp

Abstract　We evaluated the Boolean algebraic degree of Hierocrypt in order to study its security against higher-order differential attack. We apply the theorem proposed by Boura et al. to the components of Hierocrypt. For Hierocrypt-3, we get the result that the function composed of two, three, and four rounds of s-box layer have degree at most 28, 116, and 124 respectively, and for Hierocrypt-L1, the result is 28, 61, and 62 respectively. As for two rounds of s-box layer, the degree is evaluated as 28 by the bijection property of s-box. As for four rounds of s-box layer in Hierocrypt-3 and -L1, the degree is evaluated as 124 and 62 respectively. The degree of two rounds of s-box layer is confirmed by a computer experiment of higher order differential, so the upper bounds on the degree deduced in this paper seem to be tight.

1　はじめに

Hierocrypt は 2000 年に東芝が提案した共通鍵ブロック暗号で、電子政府推奨暗号に認定されている。本稿では Hierocrypt の高階差分攻撃への耐性を調査するためにブール代数次数を評価した。まず Boura らによって提案された定理を適用し、次に全単射性を使ってそれぞれ独立に次数の上界を求めた。最後に計算量が比較的少なくて済む S 層 2 層分について実際の次数を求め、本稿で求めた次数の上界がタイトなものであることを示す。

2 Hierocrypt の構造

Hierocrypt にはブロック長が 128bit のものと 64bit のものがあり、前者を Hierocrypt-3、後者を Hierocrypt-L1 と呼ぶ。Hierocrypt は平文に段関数 ρ を $T-1$ 回、段関数とほぼ同じ構造の XS 関数を 1 回適用し暗号化する。T は 6、7、8 のいずれかである。

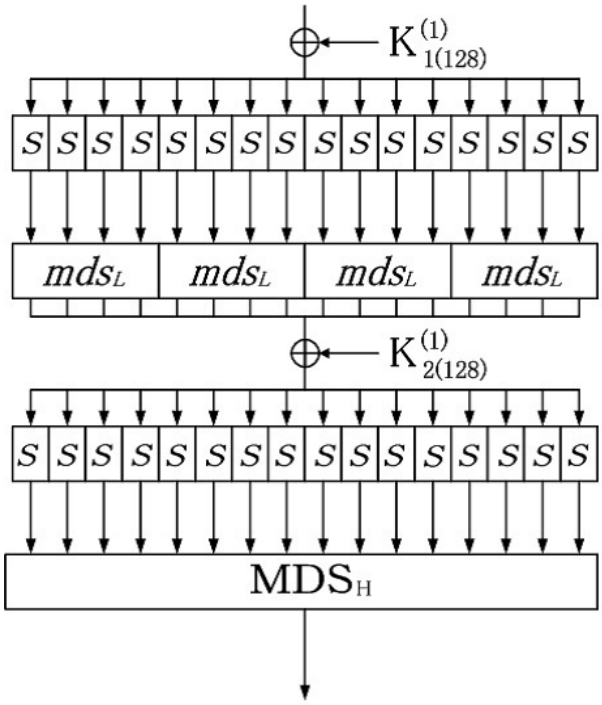

図 1: Hierocrypt-3 の段関数 ρ

上図は Hierocrypt-3 の段関数 ρ である。Hierocrypt-L1 の段関数 ρ は-3 のそれと同じ構成部品 ($\mathrm{MDS_H}$ 以外) を用いて入出力 bit 幅を半分にしたものである。

3 高階差分の性質

$\mathrm{F(X;K)}$ の X に関するブール代数次数を N 次とするとき、$\mathrm{F(X;K)}$ に高階差分を適用すると次のような性質があることが知られている。

1. $\mathrm{X,K}$ に依存せず $N+1$ 階差分値が常に 0
   $\Delta^{(N+1)}\mathrm{F(X;K)} = 0$
2. $\mathrm{X,K}$ に依存せず N 階差分値が常に定数
   $\Delta^{(N)}\mathrm{F(X;K)} = \mathrm{const}$

4 Boura らの定理を用いた次数の上界の算出

4.1 Boura の定理

文献 [4] において次のような定理が示されている。(以下、「Boura の定理」と呼ぶ。)

定理 F は図 2 のように $n$bit 入出力の関数で、$n_0$bit 入出力の全単射な m 個の Sbox の連結に相当するとする。そして、G を $n$bit 入力の任意の関数とすると、

$$\deg(G \circ F) \leq n - \frac{n - \deg(G)}{n_0 - 1}$$

が成り立つ。

(ここで $G \circ F(x) = G(F(x))$)

提案者らによるとこの定理は小さな Sbox が多数並列に適用されるような関数の次数の上界を求めるのに有効である。Hierocrypt はそのような構造をしているので効果が期待できる。

4.2 Hierocrypt-3 の次数の上界

4.2.1 S 層 2 層分

S 層 2 層分については入出力 32bit ごとにそれぞれ独立なので 32bit 分だけを考えればよい。

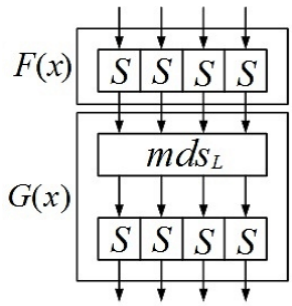

図 2: S 層 2 層分

上図のように Sbox の 4 連結を $F(x)$、mds_L と Sbox の 4 連結の合成関数を $G(x)$ とし、Boura の定理を適用する。

$$\begin{aligned} \deg(G \circ F) &\leq 32 - \frac{32-7}{8-1} \\ &= 28.\cdots \end{aligned}$$

S 層 2 層分の次数の上界として 28 を得る。

4.2.2 S 層 3 層分

図 3 のように最初の S 層 (Sbox の 16 連結) を $F(x)$、その下の $\mathrm{MDS_L}$ 関数と S 層と $\mathrm{MDS_H}$ 関数と S 層の合成関数を $G(x)$ とし、Boura の定理を適用すると

$$\begin{aligned}\deg(G\circ F) &\leq 128-\frac{128-49}{8-1}\\ &= 116.\cdots\end{aligned}$$

となり、S 層 3 層分の次数の上界として 116 を得る。

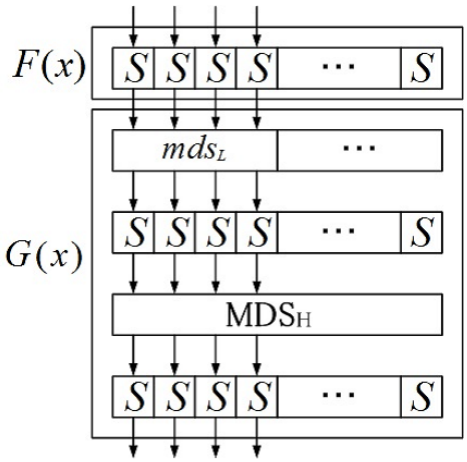

図 3: S 層 3 層分

4.2.3 S 層 4 層分

Hierocrypt は Sbox 4 つ毎に 1 つの mds_L を通るので、Sbox 4 つと mds_L と Sbox 4 つの合成関数を 32bit 入出力の大きな Sbox とみなすことができ、これを xs と定義する。図 4 のように xs を 4 つ連結した XS 関数を $F(x)$、その下の $\mathrm{MDS_H}$ と S 層と $\mathrm{MDS_L}$ と S 層の合成関数を $G(x)$ とし、Boura の定理を適用すると

$$\begin{aligned}\deg(G\circ F) &\leq 128-\frac{128-28}{32-1}\\ &= 124.\cdots\end{aligned}$$

となり、S 層 4 層分の次数の上界として 124 を得る。

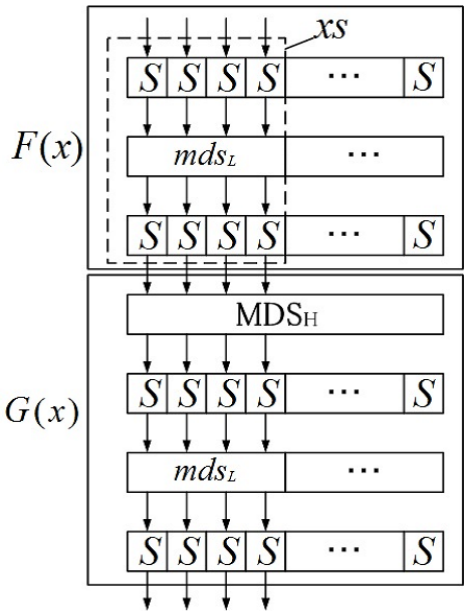

図 4: S 層 4 層分

4.3 Hierocrypt-L1 の次数の上界

4.3.1 S 層 2 層分

4.2.1 と同様にして次数の上界は 28 である。

4.3.2 S 層 3 層分

4.2.2 と同様にして

$$\begin{aligned}\deg(G\circ F) &\leq 64-\frac{64-49}{8-1}\\ &= 61.\cdots\end{aligned}$$

より、次数の上界は 61 である。

4.3.3 S 層 4 層分

4.2.3 と同様にして

$$\begin{aligned}\deg(G\circ F) &\leq 64-\frac{64-28}{32-1}\\ &= 62.\cdots\end{aligned}$$

より、次数の上界は 62 である。

5 全単射性を使った次数推定

Hierocrypt の部分的な全単射性に注目することで次数を推定する。

5.1 Hierocrypt-3 の次数の上界

5.1.1 S 層 2 層分

4.2.1 と同様に入出力 32bit 分のみを考えればよい。

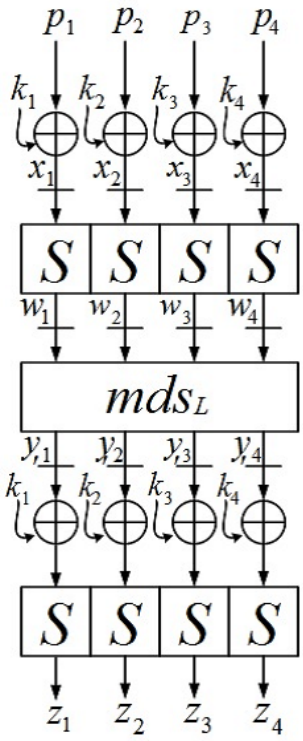

図 5: S 層 2 層分

図 5 のように各 1byte データを p_i、k_i、x_i、w_i、y_i、$\acute{k}_i$、$z_i(1 \leq i \leq 4)$ とおく。p_1 を変数とし、p_2、p_3、p_4 と鍵 k_i と $\acute{k}_i(1 \leq i \leq 4)$ を固定値とすると、p_1 と x_1 は一対一であり、x_1 と w_1 も一対一であるので p_1 と w_1 も一対一である。また、p_2、p_3、p_4 が固定値なので w_2、w_3、w_4 も固定値である。次に

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} C4 & 65 & C8 & 8B \\ 8B & C4 & 65 & C8 \\ C8 & 8B & C4 & 65 \\ 65 & C8 & 8B & C4 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix}$$

より

$$\begin{aligned} y_1 &= C4w_1 + 65w_2 + C8w_3 + 8Bw_4 \\ &= C4w_1 + const \end{aligned}$$

なので w_1 と y_1 も一対一であり、同様にして y_2、y_3、y_4 も w_1 と一対一である。さらに、p_1 と w_1 が一対一であるのと同様に y_i と $z_i(1 \leq i \leq 4)$ も一対一である。以上より p_1 と各 $z_i(1 \leq i \leq 4)$ は一対一である。よって各 $z_i(1 \leq i \leq 4)$ は p_1 に関して高々 7 次である。p_1 以外のどれかの入力 byte を変数としてそれ以外の入力 3byte を固定値とした場合も同様なので、各 $z_i(1 \leq i \leq 4)$ は各 $p_j(1 \leq j \leq 4)$ に関して高々 7 次である。よって、各 $z_i(1 \leq i \leq 4)$ は $p(= p_1 \| p_2 \| p_3 \| p_4)$ に関し高々$7 \cdot 4 = 28$ 次である。以上より、S 層 2 層分の次数の上界は 28 である。

5.1.2 S 層 4 層分

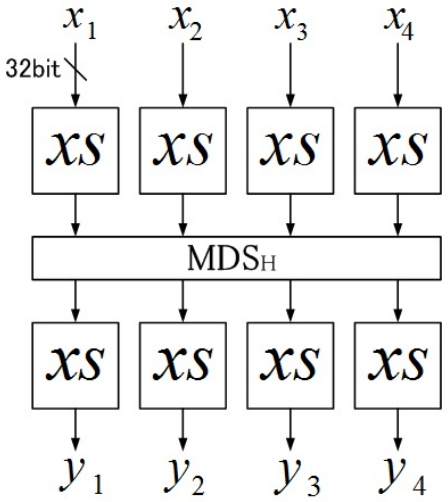

図 6: S 層 4 層分

図 6 のように入出力を 32bit ずつに分け、入力を x_i、出力を $y_i(1 \leq i \leq 4)$ とする。5.1.1 と同様に考えると各 $x_i(1 \leq i \leq 4)$ と各 $y_j(1 \leq j \leq 4)$ は一対一であり、各 $y_j(1 \leq j \leq 4)$ は各 $x_i(1 \leq i \leq 4)$ に関して高々31 次なので、各 $y_j(1 \leq j \leq 4)$ は $x(= x_1 \| x_2 \| x_3 \| x_4)$ に関して高々$31 \cdot 4 = 124$ 次である。よって、S 層 4 層分の次数の上界は 124 である。

5.2 Hierocrypt-L1 の次数の上界

5.2.1 S 層 2 層分

5.1.1 と同様にして次数の上界は 28 である。

5.2.2 S 層 4 層分

5.1.2 と同様に考える。入出力を 32bit ずつに分け、入力を x_1、x_2、出力を y_1、y_2 とすると各 $x_i(i = 1, 2)$ と各 $y_j(j = 1, 2)$ は一対一であり、各 $y_j(j = 1, 2)$ は各 $x_i(i = 1, 2)$ に関して高々31 次なので各 $y_j(j = 1, 2)$ は $x(= x_1 \| x_2)$ に関して高々$31 \cdot 2 = 62$ 次である。よって、S 層 4 層分の次数の上界は 62 である。

本章では Hierocrypt-3 と-L1 の両方について全単射性を使って S 層 2 層分と 4 層分の次数の上界を求めたが、それらはすべて前章で Boura の定理を用いて求めた上界と一致した。

6 計算機実験による実際の次数の調査

前章、前々章で求めた Hierocrypt の次数の上界がタイトなものであるかどうかを知りたい。そこで、比較的計算量の少ない S 層 2 層分について計算機を使って高階差分を計算し、実際の次数を求めた。

6.1 入力 1byte に関する次数の調査

5.1.1 で各出力 $z_i(1 \leq i \leq 4)$ は各入力 $p_j(1 \leq j \leq 4)$ に関して高々 7 次であることを求めた。8 階差分を計算し、このことが正しいことを確認する。

入力 4byte(p_1〜p_4) のうち 1byte を変数とし、残りの 3byte を固定値とした 8 階差分を計算して出力 4byte の 8 階差分値を求める。これを固定値全通り (2^{24} 通り) と、変数とする入力 byte 全通り (p_1〜p_4 の 4 通り) について行ったところ、変数と固定値のすべての取り方について 8 階差分値は 4byte すべて 0 となった。これより、各出力 $z_i(1 \leq i \leq 4)$ は各入力 $p_j(1 \leq j \leq 4)$ に関して高々 7 次であることが確認できた。

6.2 入力全 bit に関する次数の調査

前章、前々章で求めた S 層 2 層分の次数の上界は 28 であった。その上界がタイトなものかどうかを調べるため、S 層 2 層分の実際の次数を高階差分を用いて求める。

まず 28 階差分を計算し、出力 32bit に 27 次以下の bit が存在するかどうかを調べる。各入力 byte $p_i(1 \leq i \leq 4)$ において 8bit 中 $k_i(1 \leq k_i \leq 8)$bit 目の値を $c_i(= 0 \text{ or } 1)$ で固定し、残りの 7bit を変数とした 28 階差分を計算し、出力 4byte の 28 階差分値を求める。

その結果を表 1 に示す。

表 1: S 層 2 層分の 28 階差分値

固定 bit 位置				固定値				28 階差分値			
k_1	k_2	k_3	k_4	c_1	c_2	c_3	c_4	z_1	z_2	z_3	z_4
1	2	3	4	1	1	0	0	10111011	11101001	00111100	11111101
1	1	2	2	1	1	0	0	01110001	10101110	10110101	11111101
3	4	2	2	0	0	0	1	01111110	10100011	00010010	11010010
7	8	6	4	1	0	1	0	01111100	11110010	11101011	11100101

表の見方を簡単に説明すると、例えば一番上の行は p_1 の 1bit 目を 1、p_2 の 2bit 目を 1、p_3 の 3bit 目を 0、p_4 の 4bit 目を 0 で固定し、残りの 28bit を変数としたときの z_1 の 28 階差分値は 1bit 目から順に 10111011 だという意味である。表を見ると出力 32bit すべてにおいて少なくとも一度は 28 階差分値が 1 となっているので、出力 32bit すべてが 28 次以上であることがわかる。

次に 29 階差分を計算し、次数が実際に 28 次以下かどうかをを確かめる。入力 32bit のうち 29bit を変数、残りの 3bit を固定値として 29 階差分を計算し、出力 32bit の 29 階差分値を求める。これを変数とする 29bit の選び方 ($_{32}C_{29}$ 通り) と、固定する 3bit の値の選び方 (2^3 通り) の全通りについて行う。その結果、どの 29bit を変数とし、残りの 3bit をどのような値にしても出力 32bit の 29 階差分値はすべて 0 となった。これより出力 32bit すべてが 28 次以下であることがわかる。

以上より S 層 2 層分の全出力 bit の実際の次数は 28 である。S 層 2 層分について実際の次数が前章と前々章で求めた次数の上界と一致したため、S 層 3 層分、4 層分についても前章と前々章で求めた次数の上界はタイトなものであると予想できる。

7 まとめ

Hierocrypt のブール代数次数を 2 つの方法で評価した。

まず Boura らが提案した定理を適用し、Hierocrypt-3 の S 層 2 層分、3 層分、4 層分の次数の上界をそれぞれ 28、116、124、Hierocrypt-L1 の S 層 2 層分、3 層分、4 層分の次数の上界をそれぞれ 28、61、62 と求めた。

次に全単射性を使って Hierocrypt の次数を推定し、Hierocrypt-3 の S 層 2 層分、4 層分の次数の上界をそれぞれ 28、124、Hierocrypt-L1 の S 層 2 層分、4 層分の次数の上界をそれぞれ 28、62 と求めた。

Hierocrypt は S 層を最低でも 12 回適用するので、これらの上界がタイトであれば Hierocrypt は高階差分攻撃に対して安全性を有すると予想できる。

最後に計算機を使って S 層 2 層分の実際の次数を求めたところ、2 つの方法で求めた次数の上界と一致した。これより本稿で求めた Hierocrypt の次数の上界はタイトなものであると予想できる。よって Hierocrypt は高階差分攻撃に対して安全性を有すると予想できる。

参考文献

[1] 株式会社 東芝. 暗号技術仕様書:Hierocrypt-3.
http://www.toshiba.co.jp/rdc/security/hierocrypt/files/hc3_02jspec.pdf

[2] 株式会社 東芝. 暗号技術仕様書:Hierocrypt-L1.
http://www.toshiba.co.jp/rdc/security/hierocrypt/files/hcl1_02jspec.pdf

[3] L. Knudsen. Truncated and Higher Order Differentials. In FSE2nd International Workshop, LNCS.1008.

[4] Christina Boura, Anne Canteaut, and Christophe De Cannière. Higher-order Differential properties of Keccak and Luffa. In: A. Joux(Ed.):FSE 2011, LNCS 6733, pp.252-269, 2011.