付録D. Hierocrypt(-3,-L1)に対する代数的調査

1. はじめに

情報処理振興事業協会（IPA）詳細評価対象暗号 Hierocrypt(-3,-L1)に対して、耐代数的攻撃法という視点から調査した結果を報告する。本報告書の構成は以下の通りである。3 章で形式的代数次数調査、4 章で S-box に対する調査、5 章で XS 関数に対する調査、6 章でn層 Hierocrypt に対する調査を示し、7 章で高階差分／補間攻撃耐性を述べる。

2. Hierocrypt(-3,-L1)のアルゴリズム

Hierocrypt の概略構造を以下に説明する。詳細は、Hierocrypt(-3,-L1)の仕様書[IPA][IPA2]を参照頂きたい。

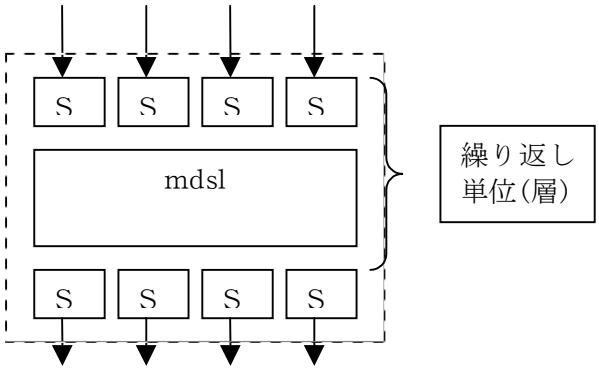

図1. XS 関数

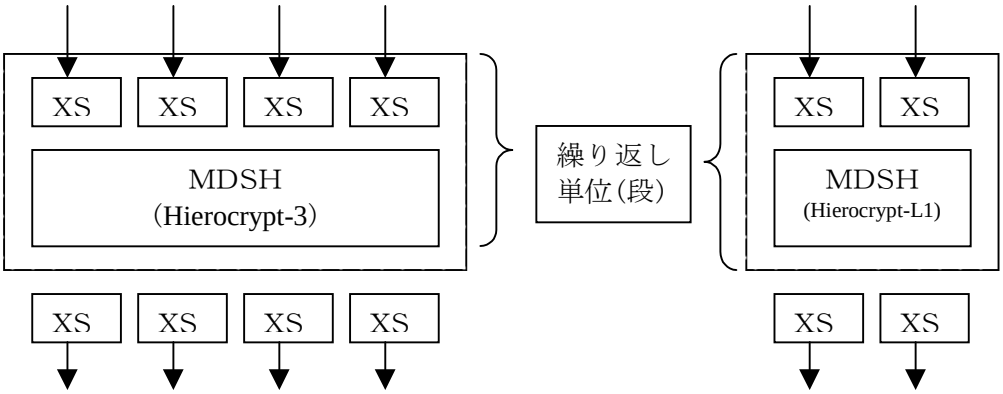

図2(a). Hierocrypt-3　　**図 2(b). Hierocrypt-L1**

Hierocrypt では 8 ビット入出力の S-box が非線形要素であり、それを4つ並列に並べ、行列 mdsl で攪拌し、S-box を通す処理を XS 関数と呼ぶ（図1）。XS 関数は 32 ビット入出力の全単射関数である。256b ビットブロック暗号 Hierocrypt-3 では、このXS関数を4つ並列に並べ、拡散行列MDSHで攪拌する。これが、基本の繰り返し単位（段）である。段数は 128 ビット鍵に対し、6 段、192 ビットで 7 段、256 ビットで 8 段である。その段数を繰り返し、最後に4つの XS 関数で処理を行う。拡大鍵は、各 S-box 入力及び最終段 S-box 出力に排他的論理和加算される。Hierocrypt-L1 は、XS が2並列構造の 128 ビットブロック暗号であり、MDSH 行列が異なる。、

3. 形式的代数次数

Hierocrypt では、唯一用いられている非線形関数の S-box の代数次数が 7 次であることから、3 回 S-box 通過後、つまり 1.5 段通過後の形式的代数次数が $7^3 = 343 >> 128, (64)$ となる。出力側から入力側の関係するビッ

トのみの次数で評価するならば、1 層目（S-box 1 回通過）の最大次数は 7 次、2 層目の最大次数は 32 次、3 層目の最大次数は 128 次（-L1 は 64 次）となる。

4. S-box に対する諸調査

Hierocrypt（ -3, -L1）は 8 ビット S-box を使用している。設計方法は以下のような手順でテーブルを作成する。

$$s(x_{(8)}) = Add(Power(Perm(x_{(8)}))) \quad (D.1)$$

ここで、

$$y_{(8)} = Perm(x_{(8)}), \quad (D.2)$$

$$y_{i(1)} = x_{\pi[i](1)}, \quad (D.3)$$

I	1	2	3	4	5	6	7	8
π (i)	3	7	5	8	6	2	4	1

$$s : GF(2^8) \rightarrow GF(2^8)$$

$$s(x_{(8)}) = x_{(8)}^{247}, \quad (D.4)$$

$$Add(x_{(8)}) = x_{(8)} \oplus 0x07 \quad . (D.5)$$

ガロア体 $GF(2^8)$ の法多項式は $z^8+z^6+z^5+z+1$ その元は、多項式基底でベクトル表示に結びつけている。

4.1 ブール展開式

4.1.1 S-box のブール代数次数と項数

Hierocrypt の暗号化関数で、非線形な関数は S-box のみである。よって暗号の強度は S-box の強度に大きく依存する。耐高階差分攻撃を考慮する場合、S-box のブール代数次数と項数の最適化を計る必要がある。表 1 に Hierocrypt で用いられている S-box の各出力 bit の次数, 総項数及び最高次数項を示す。表では、S-box の入力を $x = (x_1, x_2, \cdots, x_8)$, 出力を $y = (y_1, y_2, \cdots, y_8)$ とし、最大次数項は、例えば x_1 の項が入っていない 7 次項を $x^7[1]$ と表記している。これから分かるように、この S-box の次数は 7 次と全単射 8bit 入出力関数の最大次数となっている。また、項数はどの出力 bit も最大項数(255 個)のおよそ半分になっており、極端な偏りはない。最大次数項も出力 8bit で見れば、すべての項が使われている.。

表1. Hierocrypt の S-box のブール代数次数と項数

出力 bit	最大次数	総項数	最大次数項
y_1	7	123	$x^7[1], x^7[2], x^7[3], x^7[4], x^7[5], x^7[6]$
y_2	7	118	$x^7[1], x^7[3], x^7[6], x^7[7], x^7[8]$
y_3	7	127	$x^7[5], x^7[6]$
y_4	7	117	$x^7[6], x^7[7]$
y_5	7	120	$x^7[3], x^7[5], x^7[7], x^7[8]$
y_6	7	116	$x^7[2], x^7[3], x^7[8]$
y_7	7	127	$x^7[2], x^7[3], x^7[4], x^7[5], x^7[7], x^7[8]$
y_8	7	131	$x^7[1], x^7[2], x^7[3], x^7[7]$

4.1.2 $GF(2^8)$ の定数倍。S-box のブール代数次数と項数

Hierocrypt の段関数では 1 層目の S-box 出力は線形変換 mds_L を通る。mds_L 変換の作用は、各要素による $GF(2^8)$ 上の定数倍により byte 内で線形拡散が起こり、その後 4byte の排他的論理和により byte 毎の線形拡散が起こる。ここで $GF(2^8)$ 上の定数倍に着目すると、S-box 出力のブール多項式によっては、定数倍後のブール多項式を見たとき、高次項がキャンセルされたり、総項数が極端に減少したりする可能性もある。そこで、$GF(2^8)$

上の定数倍による線形拡散式と S-box 出力の定数倍後のブール展開式を調査した。Hierocrypt で使われている定数倍演算の行列表示を表2に、定数倍後のブール展開式の次数、項数を表,3 に示す。そこでは入力を $\tilde{x} = (x_1, x_2, \cdots, x_8)^T$, GF($2^8$)上の定数倍後の出力を $\tilde{y} = (y_1, y_2, \cdots, y_8)^T$ とする。結果からは、高次項が完全にキャンセルされたり、極端に項数が減少したりするような bit は見受けられなかった。

表 2: GF(2^8)上の定数倍による線形拡散式

定数	行列表示	定数	行列表示
C4	$\begin{pmatrix} 0&0&0&0&1&1&1&0 \\ 0&0&0&1&0&0&1&0 \\ 0&0&1&0&0&1&0&1 \\ 0&1&0&0&1&0&1&0 \\ 1&0&0&1&0&1&0&0 \\ 0&0&1&0&0&1&1&0 \\ 0&1&0&0&0&0&1&1 \\ 1&0&0&0&0&1&1&1 \end{pmatrix}$	8B	$\begin{pmatrix} 0&0&0&1&1&0&1&1 \\ 0&0&1&0&1&1&0&1 \\ 0&1&0&1&1&0&1&0 \\ 1&0&1&1&0&1&0&1 \\ 0&1&1&0&1&0&1&0 \\ 1&1&0&0&1&1&1&0 \\ 1&0&0&0&0&1&1&0 \\ 0&0&0&0&1&1&0&1 \end{pmatrix}$
65	$\begin{pmatrix} 1&1&0&1&1&1&0&1 \\ 0&1&1&0&0&1&1&0 \\ 1&1&0&0&0&1&0&1 \\ 1&0&0&1&1&0&1&0 \\ 0&0&1&1&0&1&0&0 \\ 1&0&1&1&0&1&0&1 \\ 1&0&1&1&0&1&1&1 \\ 0&1&1&0&1&1&1&0 \end{pmatrix}$	C8	$\begin{pmatrix} 1&1&1&0&1&1&1&0 \\ 0&0&1&1&0&0&1&0 \\ 0&1&1&0&0&1&0&0 \\ 1&1&0&0&1&0&0&1 \\ 1&0&0&1&0&0&1&0 \\ 1&1&0&0&1&0&1&0 \\ 0&1&1&1&1&0&1&1 \\ 1&1&1&1&0&1&1&1 \end{pmatrix}$

表 3　Hierocrypt の定数倍 S-box のブール代数次数と項数

C4 倍			
出力 bit	最大次数	総項数	最大次数項
y_1	7	125	$x^7{}_{[6]}$
y_2	7	136	$x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[5]}, x^7{}_{[6]}, x^7{}_{[7]}$
y_3	7	119	$x^7{}_{[4]}, x^7{}_{[6]}, x^7{}_{[7]}$
y_4	7	123	$x^7{}_{[1]}, x^7{}_{[4]}, x^7{}_{[5]}, x^7{}_{[7]}, x^7{}_{[8]}$
y_5	7	138	$x^7{}_{[1]}, x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[6]}, x^7{}_{[7]}, x^7{}_{[8]}$
y_6	7	129	$x^7{}_{[1]}, x^7{}_{[5]}, x^7{}_{[6]}, x^7{}_{[7]}, x^7{}_{[8]}$
y_7	7	122	$x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[5]}, x^7{}_{[6]}, x^7{}_{[8]}$
y_8	7	108	$x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[8]}$
65 倍			
出力 bit	最大次数	総項数	最大次数項
y_1	7	137	$x^7{}_{[1]}, x^7{}_{[4]}, x^7{}_{[5]}, x^7{}_{[7]},$
y_2	7	140	$x^7{}_{[5]}, x^7{}_{[6]}, x^7{}_{[7]}$
y_3	7	122	$x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[6]}, x^7{}_{[7]}$
y_4	7	115	$x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[5]}, x^7{}_{[7]}, x^7{}_{[8]}$
y_5	7	123	$x^7{}_{[1]}, x^7{}_{[3]}, x^7{}_{[5]}, x^7{}_{[7]}$
y_6	7	119	$x^7{}_{[1]}, x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[7]}$
y_7	7	127	$x^7{}_{[1]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[8]}$
y_8	7	139	$x^7{}_{[1]}, x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[6]}, x^7{}_{[8]}$
8B 倍			
出力 bit	最大次数	総項数	最大次数項
y_1	7	123	$x^7{}_{[1]}, x^7{}_{[3]}, x^7{}_{[5]}$
y_2	7	131	$x^7{}_{[1]}, x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[6]}, x^7{}_{[7]}$
y_3	7	117	$x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[5]}, x^7{}_{[7]}$
y_4	7	133	$x^7{}_{[1]}, x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[5]}, x^7{}_{[7]}, x^7{}_{[8]}$
y_5	7	122	$x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[6]}, x^7{}_{[8]}$
y_6	7	136	$x^7{}_{[1]}, x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[8]}$
y_7	7	123	$x^7{}_{[1]}, x^7{}_{[3]}, x^7{}_{[6]}$
y_8	7	130	$x^7{}_{[1]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[6]}$
C8 倍			
出力 bit	最大次数	総項数	最大次数項
y_1	7	130	$x^7{}_{[1]}, x^7{}_{[3]}, x^7{}_{[5]}, x^7{}_{[8]}$
y_2	7	119	$x^7{}_{[4]}, x^7{}_{[5]}, x^7{}_{[6]}, x^7{}_{[7]}, x^7{}_{[8]}$
y_3	7	125	$x^7{}_{[5]}, x^7{}_{[7]}, x^7{}_{[8]}$
y_4	7	111	$x^7{}_{[1]}, x^7{}_{[8]}$
y_5	7	127	$x^7{}_{[1]}, x^7{}_{[4]}, x^7{}_{[7]}$
y_6	7	117	$x^7{}_{[1]}, x^7{}_{[2]}, x^7{}_{[5]}, x^7{}_{[7]}$
y_7	7	127	$x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[4]}, x^7{}_{[8]}$
y_8	7	126	$x^7{}_{[2]}, x^7{}_{[3]}, x^7{}_{[6]}, x^7{}_{[7]}$

4.2 S-box の補間多項式

Hierocrypt で用いられている S-box を GF(2^8)の多項式表現した場合の次数、項数を調査した。調査項目は以下の 2 つである。

① 8 次の原始多項式すべてに対し、S-box を GF(2^8)の多項式表現した場合の次数、項数を調査する。

② S-box の入力側で鍵が排他的論理和されることを想定し、鍵全通りに対し S-box を GF(2^8)の多項式表現した場合に係数が変化しない項を調査する。即ち、S-box を $S(X)$ として、関数 $S(X \oplus K)$ の多項式表現において、係数項に鍵が影響しない項を調査する。

結果を表4及び5に示す。表4より、Hierocrypt の S-box はどの原始多項式の下でも、253 以上の項数が出ており、補間攻撃に対し配慮した設計となっている事がわかる。また、表5に示された次数は、ブール展開式で考えたときの代数次数が7のものであり、表3の結果から予想されるものであり、Hierocrypt の S-box の新たな特徴を示す物では無い。

、

表4. 原始多項式と S-box の多項式項数

原始多項式	項数	原始多項式 (相反多項式)	項数
0x11d	255	0x171	254
0x169	253	0x12d	255
0x1e7	254	0x1cf	255
0x12b	254	0x1a9	255
0x165	254	0x14d	253

表5. 鍵と S-box の多項式係数

係数項が変わらない次数	127,191,223,239,247,251,253,254

5. XS 関数に対する諸調査

XS 関数は Hierocrypt の段関数の一部であり、4byte の暗号化変換を行う関数である 4 並列の 8 ビット S-box を 2 組用意し、拡散層を挟んだ 2 段 SPN 構造となっている。

ここでの特徴は S-box の入力直前で必ず鍵加算を行っていることと、拡散層に MDS 行列を使用していることである。この MDS 行列を小 MDS と呼び、mds_Lと表記する。

Hierocrypt(-3, -L1)では、以下のような巡回型のmds_Lを採用している。

$$mds_L = \begin{pmatrix} C4 & 65 & C8 & 8B \\ 8B & C4 & 65 & C8 \\ C8 & 8B & C4 & 65 \\ 65 & C8 & 8B & C4 \end{pmatrix} \qquad \text{(D.6)}$$

ここで、S-box 入出力と行列要素は乗算の際、ガロア体 GF(2^8)の元と見なす。原始多項式は$z^8+z^6+z^5+z+1$ である。

5.1 ブール展開式

Hierocrypt で用いられている XS 関数に対して、ブール展開式表現時における1～8 次項までの項数を調査した。調査項目は項数の最大値,最小値,平均値である。その結果を表6に添付する。8 次までの範囲ではあるが、期待値に近い値が出ており、各次数項が偏り無く登場している事を伺わせる。

表6 XS 関数ブール多項式項数

次数	平均	最大値	最小値	期待値
1 次	15.750	19	10	16
2 次	243.625	257	230	248
3 次	2427.875	2514	2400	2480
4 次	17507.5	17593	17329	17980
5 次	98375.375	98639	98027	100688
6次	445443.25	446101	445007	453096

6. n層 Hierocrypt の調査

6.1 高階差分特性

Hierocrypt で用いられている XS 関数に対して bit-oriented で 1～8 階までの高階差分特性を全パターン調査した。調査項目は、出力差分値がランダムなユーザー鍵 1000 通りに対して常に 0 もしくは 1 となる入力差分組である。その結果、5.1 で述べる 8 階差分を用いた SQUARE 攻撃で使用される平文組（byte 毎の 8 階差分組）以外の平文について、調査項目の平文組は存在しなかった。

6.2 SQUARE 型攻撃に対する強度評価

SQUARE 攻撃は、Daemen らにより SQUARE 暗号に適用され、近年設計された CRYPTON や Rijndael など多くの SPN 型暗号で、この攻撃に対する強度評価がなされている。

SQUARE 攻撃では、暗号化部分関数の全単射性を利用している。Hierocrypt の場合、全単射性を持つ部分関数は、8 ビット入出力の S-box 及び 32 ビット入出力の XS 関数である。この二つに関し、SQUARE 攻撃の可能性を調査した。これは、1つの S-box 入力を変数とする 8 階差分及び1つのXS関数入力を変数とする 32 階差分による高階差分攻撃である。Hierocrypt-3 では、このような 8 階差分の選び方は 8 通り、32 階差分の選び方は 4 通りある。しかし、Hierocrypt 構造の対象性からどれを選んでも同じである。これは、Hierocrypt-L1 でも同様である。

1 層目の左 1byte の入力に 8 階差分組を用意し、それ以外の byte は固定する。この場合、1層目左 1byte の S-box 出力の集合は S-box が全単射関数であるため、8 次元ベクトル空間を張る。次にmds_L変換の出力 4byte はそれぞれ 8 次元ベクトル空間を張ることになる。よって 2 層目の S-box 通過後も 4byte それぞれ 8 次元ベクトル空間を張り、8 階差分は 0 である。MDS_H 変換は、線形変換であるため、3 層目入力においても、8 階差分は0である。1層消去型攻撃を考えれば、3 層 Hierocrypt が攻撃可能である。

同様に、1段目[1]の左 4byte の入力に 32 階差分組を用意すれば、3 段目 XS 関数の入力において 32 階差分が0であり、1段消去型攻撃で 3 段（＝6 層）Hierocrypt が攻撃可能である。

6.3 補間攻撃に対する強度評価

入力としてある 1byte の全通りを用いた場合、各層でにおいて、ある 1byte の出力を GF(2^8)の多項式表現した場合の次数、項数を調査した。これをランダムなユーザー鍵数通りに対して行い、その最大値を調査項目とする。この項数が 256 未満であれば補間攻撃が適用可能となる。その結果を表7に示す。2 層出力まで 256 項未満であり、1層消去型攻撃で 3 層まで攻撃可能である。

表7 各層出力の多項式表現

層数	項数	次数
1	255	254
2	255	254
3	256	255

[1] S 関数を基準に繰り返し回数を数える場合、層と数え、XS 関数が基準の場合段と呼ぶ。

7. 高階差分攻撃耐性の評価

前節の解析により、効果的な高階差分として、SQUARE 型高階差分の S-box 単位 8 階差分及び XS 関数単位 32 階差分がえられた。S-box を単位とする補間攻撃でも、8 階差分攻撃と同じ段数まで攻撃が可能である。以下、S-box 単位の 8 階差分及び XS 関数単位の 32 階差分に関し考察する。

＜S-box 単位の 8 階差分＞

1層消去型攻撃の場合、3 層攻撃が可能であり、攻撃方程式に関わる拡大鍵は、3 層目の1つの S-box に関わる 8 ビット分（最暗号文側の鍵）である。S-box のブール展開式には 3.1 節で述べたように、7 次まで殆ど全ての次数項が出ており、線形化手法で、攻撃方程式を高速に解くことはできず、8 ビット鍵の総当たりを行うことになる。攻撃に必要な計算量は、本文 3.2 節式(3.8)及び1層が、16 個（Hierocrypt-3）の S-box で構成される事より

$$T_{1H3} = \frac{2^{8+8+1}}{16} = 2^{13} \qquad \text{(D.7)}$$

の層関数計算量であり、必要平文数は、2^9 である。同様に、Hierocrypt-L1 では 1 層が 8 個の S-box であるから

$$T_{1HL1} = \frac{2^{8+8+1}}{8} = 2^{14} \qquad \text{(D.8)}$$

の層関数計算量であり、必要平文数は、2^9 である。

2 層消去型で、考えれば、4 層の暗号が攻撃できる。攻撃方程式では、mdsl 行列で結ばれた、4 層目の 4 つの S-box と 3 層目の 1 つの S-box に関わる 4*8+8=40 ビットの鍵を総当たりする事になる。同様に、3 層消去型で Hierocrypt-3 の場合、5 層目の全部の S-box、4 層目の 4 つの S-box と 3 層目の 1 つの S-box に関わる 16*8+4*8+8=168 ビット鍵の総当たりとなる。このように暗号文側に鍵総当たり層を延ばすのを TYPE1 拡張と呼ぶ。

平文側の拡大鍵を総当たりして、ある層の 1 つの S-box 入力で 8 階差分入力を構成する事も可能である。例えば、2 層目左端の S-box にのみ、8 階差分入力を入れたいのであれば、左端の XS 関数入力の全ての平文 2^{32} 組を用意し、この中から、仮定する拡大鍵に応じ、2^8 の平文を選べば良い。同じ S-box で別の 8 階差分組を選ぶ場合も、この 2^{32} 組の平文から選び出すことが出きる。このように平文側に鍵総当たり層を延ばす手法を TYPE2 拡張という。基本の 1 層消去型攻撃に TYPE2 拡張を1層分適用するならば、必要平文数は 2^{32} 組、仮定する拡大鍵ビット数が、32+8=40 ビットとなるので計算量は Hierocrypt-3 であれば、$2^{32}\frac{2^{17}}{16} = 2^{45}$ の層関数計算である。これは平文側で 1 層、暗号文側で 1 層消去を行う攻撃であるので、1+1 層消去攻撃と呼ぶ。同様に、平文側で 1 層、暗号文側で 2 層消去ならば 1+2 層消去型と呼ぶ。さらに消去層を増やす場合、暗号文側、平文側何れでも、推定すべき拡大鍵ビット数は層当たり、Hierocrypt-3 で 128 ビットづつ、Hierocrypt-L1 で 64 ビットづつ増加する。この 8 階差分特性を利用した攻撃法で、必要な平文数が全平文種類数未満かつ計算量が秘密鍵総当たり回数以下のものを示せば、表 8 である。TYPE2 拡張時に平文側の鍵推定を省略する事で、計算量を削減する事が出きるが[FKLSSWW][OSMM]、これは 8 階差分を使う攻撃では無く、後述の XS 関数に対する 32 階差分を使う攻撃と考える方が理解しやすい。

＜XS 関数単位の 32 階差分＞

XS 関数は、32 ビット入出力の全単射関数であり、32 階差分は 0 となる。XS 関数単位に繰り返し階数を数えたものを段数と呼ぶことにすれば、1 段＝2 層である。1 段消去型攻撃を考えれば、3 段(＝6 層)攻撃が 32 階差分で可能であり、攻撃方程式に関わる拡大鍵は、3 段目の1つの XS 関数に関わる 64 ビットである。32 ビットの攻撃方程式を、1 つのものとして、総当たりで拡大鍵を求めるならば、1 段が 4 個（Hierocrypt-3）の XS 関数で構成される事より、計算量は、

$$T_{1H3} = \frac{2^{32+64+1}}{4} = 2^{95} \qquad \text{(D.9)}$$

の段関数計算量であり、必要平文数は、2^{34} である。同様に、Hierocrypt-L1 では 1 段が 2 個の XS 関数であるから

$$T_{1HL1} = \frac{2^{32+64+1}}{2} = 2^{96} \qquad \text{(D.10)}$$

の段関数計算量であり、必要平文数は、2^{34} である。

層を単位に数えるならば、これは 2 層消去型である。32 階差分が 32 ビット変数について 0 であることは、それを構成する各 4 バイトについても 0 であることを意味し、32 ビットの攻撃方程式を 8 ビット幅の方程式 4 つと考え、順次解いていくならば、1 段（＝2 層）消去の場合、関係する鍵は 1 層目 4 個、2 層目 1 個の計 5 個の S-box に係わるものであり、40 ビットとなる。この鍵を総当たりで求めるならば、計算量は、それぞれ

$$T_{1H3} = \frac{5*2^{32+40+1}}{32} \cong 2^{71} \quad \text{(Hierocrypt-3)} \qquad \text{(D.11)}$$

$$T_{1HL1} = \frac{5*2^{32+40+1}}{16} \cong 2^{72} \quad \text{(Hierocrypt-L1)} \qquad \text{(D.12)}$$

であり、必要平文数は、8 ビット幅の方程式で 40 ビット推定するので、$2^{32+3}=2^{35}$ となる。なお、段関数の計算量に換算する為、1 段当たり Hierocrypt-3 では 32 個、Hierocrypt-L1 では 16 個の S-box を使っていることを使用した。2 層目の残りの S-box に係わる鍵を求める際は、1 層目の 4 個の S-box 鍵は決定済みであるので、各々8 ビットの鍵推定を総当たりで行えば良く、その計算量は上式に比べ無視できる。さらに、最初の 40 ビット拡大鍵推定において、生き残り候補が 1 つになるように 2^{35} の平文を用いているが、生き残り候補が複数個あっても、次の S-box の鍵を求める際に、偽鍵のふるい落としが可能である。この考えを用いれば、必要平文数は、さらに削減できる。また、32 階差分値を暗号文から計算する際に、部分和に関するテーブルを用いて S-box テーブルを引く回数を削減する（部分総和法）ならば、計算量は、$1/2^{20}$ に削減できる[OSMM]。

同様に、1.5 段（=3 層）消去型攻撃を 8 ビット幅方程式として順次解くならば、最初の方程式に関係する鍵は Hierocrypt-3 の場合 1+4+16=21 バイト=168 ビット、Hierocrypt-L1 の場合 1+4+8=13 バイト＝104 ビットとなり、計算量は、それぞれ

$$T_{1H3} = \frac{13*2^{32+168+1}}{32} \cong 2^{200} \quad \text{(Hierocrypt-3)} \qquad \text{(D.13)}$$

$$T_{1HL1} = \frac{13*2^{32+104+1}}{16} \cong 2^{137} \quad \text{(Hierocrypt-L1)} \qquad \text{(D.14)}$$

の段関数計算量である。部分総和法を使えば、同様に計算量を $1/2^{20}$ 程度に削減する事ができる[OSMM]。

以上のような考察で、必要平文数が平文総数未満で、計算量が秘密鍵の総当たり以下となる可能性を持つものを表にまとめれば、表9である。

表8 Hierocrypt への SQUARE 型攻撃（8階差分）

Hierocrypt-L1				
攻撃のタイプ	適用層数	拡大鍵ビット数	必要選択平文数	計算量（層関数＝1）
1 層消去型	3 層	8	2^{9}	2^{14}
2 層消去型	4 層	40	2^{11}	2^{46}
3 層消去型	5 層	104	2^{13}	2^{110}
1+1 層消去型	4 層	40	2^{32}	2^{46}
1+2 層消去型	5 層	104	2^{32}	2^{110}
Hierocrypt-3				
攻撃のタイプ	適用層数	拡大鍵ビット数	必要選択平文数	計算量（層関数＝1）
1 層消去型	3 層	8	2^{9}	2^{13}
2 層消去型	4 層	40	2^{11}	2^{45}
3 層消去型	5 層	168	2^{14}	2^{173}
1+1 層消去型	4 層	40	2^{32}	2^{45}
1+2 層消去型	5 層	168	2^{32}	2^{173}

表8 Hierocrypt への SQUARE 型攻撃（32階差分）

Hierocrypt-L1				
攻撃のタイプ	適用段数	拡大鍵ビット数	必要選択平文数	計算量（段関数＝1）
1 段消去型	3 段=6 層	64	2^{34}	2^{96}
2 層消去型	6 層	40	2^{35}	2^{72}
1.5 段消去型	7 層	104	2^{36}	2^{137}
Hierocrypt-3				
攻撃のタイプ	適用層数	拡大鍵ビット数	必要選択平文数	計算量（段関数＝1）
1 段消去型	3 段＝6 層	64	2^{34}	2^{95}
2 層消去型	6 層	40	2^{35}	2^{71}
1.5 段消去型	7 層	168	2^{37}	2^{200}

[IPA] 東芝、"暗号技術応募書／暗号技術仕様書:Hierocrypt-L1／自己評価書 Hierocrypt-L1", IPA 提出資料

[IPA2] 東芝、"暗号技術応募書／暗号技術仕様書:Hierocrypt-3／自己評価書 Hierocrypt-3", IPA 提出資料

[FKLSSWW] N.Ferguson,J.Kelsey,S.Lucks,B.Schnier,M.Stay,D.Wagner, and D.Whiting,"Improved Cryptanalysis of Rijndael",2000,http://www.counterpane.com/rijndael/html

[OSMM] 大熊健司、佐野文彦、村谷博文、本山雅彦、川村信一"ブロック暗号 Hierocrypt-3 および Hierocrypt-L1 の安全性について",SCIS2001,11A-4,(2001)