Hierocrypt-L1 の安全性詳細評価報告

要旨: 本報告では、Hierocrypt-L1 の安全性について弊社による評価の報告を行う。結果として Hierocrypt-L1 について、評価者が限られた時間内で安全性評価を行う限りでは、致命的な安全性の問題点は発見されなかった。
今回の評価を含めても、Hierocrypt-L1が安全性の評価が十分なされた暗号ブロック暗号ではなく、今後の安全性評価も必要であるが、現時点では、期待される安全性を備えると考えるための根拠を与える。

Abstract: In this report, we address our security evaluation of Hierocrypt-L1. As a result, we found no critical security flaw during the limited period available for security evaluation.
Hierocrypt-L1has not yet been evaluated enough even with our evaluation. Further evaluation results are necessary. We however show some evidences to consider Hierocrypt-L1to provide expected security at this moment.

1 はじめに

本報告は、弊社が IPA より委託された業務として行った詳細評価、及び Hierocrypt-L1 の安全性に関する収集した情報のまとめを行う。

Hierocrypt-L1 は 2000 年に大熊らによって開発されたブロック暗号アルゴリズムである。Hierocrypt-L1 の安全性に関する文献のうち、評価者が知るものは設計者らによる自己評価書のみである。このなかでは暗号の安全性について質の高い評価を行っている。この文献では従来の解読法のうち、特に Hierocrypt-L1 に対して有効であると考えられる攻撃法に対しての評価が中心である。また、Hierocrypt-L1 向けに考えられた攻撃法による安全性評価は行われていない。

本報告書では評価者が行った Hierocrypt-L1 の安全性に関する詳細評価について、詳細に報告を行う。報告は安全性評価の結果のみならず、評価者が検討した評価方針やその過程についてもなるべく実験結果などを多く掲載し、第三者が本報告の信憑性を検証できるようにした。

この結果、評価者による詳細評価では Hierocrypt-L1 の安全性について欠陥となる性質を見付けることはできなかった。

2 Hierocrypt-L1 評価方針

この章では、主に評価方針について述べる。その前に、評価者が最終的な評価方針に至るまでに考慮した Hierocrypt-L1 の特徴についてまず説明する。

Hierocrypt-L1 は鍵スケジュール部とデータ撹拌部分を持つブロック暗号である。データ撹拌部分は、典型的な SPN 構造によるものである。このうち S(ubstitution:非線形変換) の役割となる S ボックスは (評価者の知る限り) オリジナルの S ボックスを使っている。S ボックスのサイズは 8 ビット入力/出力であり、単射である。

これに対し、P(ermutation:線形変換) の役割となる変換は、二種類の線形変換を用いている。これらは MDS (maximum distance separation) となるものが用いられている。

これら Hierocrypt-L1 のデータ撹拌部分はバイト (8 ビット) 単位の処理でほぼ構成されているという特徴がある。

以上の特徴は、近年提案、評価されてきたブロック暗号 SQUARE, CRYPTON, Rijndael に似た構造となっており、特に新しい構造をしたアルゴリズム設計ではない。

特に AES の選定で注目されいくつかの評価結果が知られる Rijndael との相違点に注目すると次のようになる。

- 全体構造に関するもの
  1. 64 ビットブロック暗号であること
  2. 異なる鍵スケジュール部を使っていること
  3. ブロック全体の撹拌が (より複雑であるものの) S ボックス層二回に一度であること
- 構成部分
  1. 線形変換に用いる行列 (局所的な MDSL、全体的な MDSH)
  2. S ボックス
  3. 段数

本評価の大きな目標として、等価鍵や DES のビット反転特性など明らかな暗号の欠陥の特性がないことを重点的に確認することを第一の目標とした。そして第二の目標として、探索などの解析的な評価を伴う安全性の評価をできる限り行うこととした。

第一の目標は主に鍵スケジュール部の評価が中心となる。鍵スケジュール部に関するさまざまな特徴について最初に示す。

第二の目標については、データ撹拌部分の評価が主となる。評価者は第二の目標を達成するために構成要素中、最も重要と考えられる S ボックスへの集中的な評価に着手した。これは、差分解読法、線形解読法で用いた統計値のように、解析した性質がその他のデータ撹拌部分である MDSL, MDSH により保存されるものを中心に考える。さらにこの中でもさまざまな面から S ボックスの評価を行うよう努力した。

その結果、評価に許された限られた時間では、探索項目の検討や、探索プログラムの効率化などで不十分であり、暗号の安全性を保証するほど十分に網羅的な探索とは言えない。しかし、暗号を攻撃側から評価する立場という考え方から、なるべく多くの実験を行い、有効なものをひとつでも見付ける、という方針で評価を進めた。

以下の章では、これらについて別々に評価報告を行ってゆく。

3 有限体上の演算について

本稿では、頻繁に有限体 GF(2^k) 上の乗算を扱うが、本報告を通してその定義は次のとおりである。k ビットの値 (もしくは 10 進数で与えられているならばその整数の二進数表記) を上位から $b_1, \ldots, b_k$ とするとこの整数に体して次の多項式を対応づける、$f(x) = \sum_{i=1}^{k} b_i x^{k-i}$。これは $k-1$ 次以下の多項式で、係数は GF(2) の元である。これをある既約多項式 (拡大次数 k により定義される、本稿では表 1を用いる) による多項式の剰余環の要素として考えたときこの剰余環は体構造をなす。したがって、本稿で考える有限体 GF(2^k) 上の演算は表 1で定義される多項式環の演算に基づく。

表 1: 本報告で用いる GF(2^n) を定義する既約多項式

n	$P(x)$	n	$P(x)$
2	x^2+x+1	6	x^6+x+1
3	x^3+x+1	7	x^7+x+1
4	x^4+x+1	8	$x^8+x^6+x^5+x+1$
5	x^5+x^2+1	9	x^9+x^4+1

4 鍵スケジュール部

まず鍵スケジュール部の評価にあたり、一点確認をしておく。

暗号文側拡大鍵生成について

応募仕様書 [1](日本語 pp.10、右コラム、[拡大鍵生成 (暗号文側)] ($5 \leq t \leq 7$)) 中の $K^{(t)}_{3(32)}$ の定義式において、

$$K^{(t)}_{3(32)} = W^{(t-1)}_{2(32)} \oplus V^{(t)}_{(32)}$$

を

$$K^{(t)}_{3(32)} = W^{(t)}_{2(32)} \oplus V^{(t)}_{(32)}$$

であるとして扱う。

□

この記述は行列のサイズが異なるなど[1]の自明な誤りではなく、この変更を行わずとも暗号化、復号化を行うことはできる。評価者は仕様とおりの表記で暗号を実装しテストベクトルの整合/不整合を確認したわけではない。しかし、関連する文献 [4] や同一の設計者でありアルゴリズムとして酷似した Hierocrypt-3 の仕様 [2] などから、後者のような仕様であり、表記は誤りであるとして理解するのが設計者の意図にそぐうと考え、これらの状況判断より、評価者が勝手に訂正したものを評価した。 Hierocrypt-L1 の鍵スケジュール部は次の二つの部分からなる。

1. マスター鍵から各段の中間鍵の生成
2. 各段の中間鍵から拡大鍵への変換

評価者は、これらについて独立に評価を行った。その内容と結果について以下で述べてゆく。

4.1 中間鍵の生成部

ここで注目すべきは上記 1. である。中間鍵の生成はまず秘密鍵 128 ビットを 4 分割し、上位半分を典型的な Feistel 構造として更新し、Feistel 構造の鍵にあたる値を残りの下位半分より供給する。下位半分の更新は単なる線形変換として実現されている。また、中間鍵の更新は 4 段まで行い、それ以降はこれまで作った中間鍵を再利用する。

より具体的に中間鍵生成を見てゆく。$Z^{(-1)} = K$ とすると：

$$\begin{aligned}
Z^{(0)} &= \sigma_0(Z^{(-1)}, G^{(0)}) \\
Z^{(1)} &= \sigma(Z^{(0)}, G^{(1)}) \\
Z^{(2)} &= \sigma(Z^{(1)}, G^{(2)}) \\
Z^{(3)} &= \sigma(Z^{(2)}, G^{(3)}) \\
Z^{(4)} &= \sigma(Z^{(3)}, G^{(4)})
\end{aligned}$$

さらに、それ以降の中間鍵は：

$$\begin{aligned}
Z^{(5)} &= Z^{(8-5)} = Z^{(3)} \\
Z^{(6)} &= Z^{(8-6)} = Z^{(2)} \\
Z^{(7)} &= Z^{(8-7)} = Z^{(1)}
\end{aligned}$$

[1] 3.2.6 節最後の行の数式、$Z^{(t)}_{3(32)} || Z^{(t)}_{4(32)} = P^{(32)^{-1}}(W^{(t)}_{1(32)} || W^{(t)}_{2(32)})$ は変数のサイズから $P^{(16)^{-1}}$ の誤りであることは明らか。

である。

各中間鍵の更新関数 σ を見てゆくと、

$$\begin{aligned}(Z_1^{(t-1)}, Z_2^{(t-1)}, Z_3^{(t-1)}, Z_4^{(t-1)}) &:= Z^{(t-1)} \\ (Z_1^{(t)}, Z_2^{(t)}, Z_3^{(t)}, Z_4^{(t)}) &:= Z^{(t)} \\ (W_1^{(t-1)}, W_2^{(t-1)}) &:= P(Z_3^{(t-1)}, Z_4^{(t-1)})\end{aligned}$$

$$\begin{aligned}Z_3^{(t)} &= M_5(W_1^{(t-1)}) \oplus G^{(t)} \\ Z_4^{(t)} &= M_B(W_2^{(t-1)}) \\ Z_1^{(t)} &= Z_2^{(t-1)} \\ Z_2^{(t)} &= Z_1^{(t-1)} \oplus F_\sigma(Z_2^{(t-1)} \oplus Z_3^{(t)})\end{aligned}$$

この中間鍵更新関数を図示したものを図 1に示す。また、暗号全体の鍵スケジュールに展開したものを図 2に示す。ここで関数 F_σ は S ボックスと線形関数を組み合わせた単射かつ非線形な変

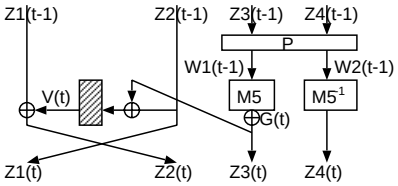

図 1: Intermediate keys' generation (partial)

換であり、M_5、M_B はバイト単位の排他的論理和から構成される単射な線形変換であり、P は 16 ビット単位の排他的論理和から構成される単射な線形変換である。よって、各 σ、σ_0 が単射であることは自明である。よって任意の t 段目の中間鍵を固定したとき Z^t について一意に秘密鍵 K、同時に他の段の中間鍵 Z も一意に決めることができる。

考察 4.1: すべての Z_3、Z_4 は鍵の下位半分 *(*と段毎の定数*)* のみに依存する *(*自明なので証明は省略*)*。

これらの導出はバイト単位の排他的論理和と定数加算 ($\mathrm{GF}(2^8)$) である。まず、中間鍵の下半分 Z_3 と Z_4、及び、拡大鍵導出に用いる中間値 W_1, W_2 を、鍵と定数の排他的論理和を使って書き表すと以下のようになる。ここで $K_{i:j}$ は、128 ビットの秘密鍵 K を四分割した 32 ビットワードのうち、上位 i 番目ワードの中のさらに上位から第 j 番目バイトを示す。すなわち

$$K_{1:1}||K_{1:2}||K_{1:3}||\ldots||K_{4:8} := K_{128}$$

$$\begin{aligned}Z(-1)_{3:1} &= K_{3:1} \\ Z(-1)_{3:2} &= K_{3:2}\end{aligned}$$

$$
\begin{aligned}
Z(-1)_{3:3} &= K_{3:3} \\
Z(-1)_{3:4} &= K_{3:4} \\
Z(-1)_{4:1} &= K_{4:1} \\
Z(-1)_{4:2} &= K_{4:2} \\
Z(-1)_{4:3} &= K_{4:3} \\
Z(-1)_{4:4} &= K_{4:4} \\
Z(0)_{3,1} &= K_{3:1} \oplus K_{3:3} \\
&\oplus G_{0:1} \\
Z(0)_{3,2} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:4} \\
&\oplus G_{0:2} \\
Z(0)_{3,3} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:3} \\
&\oplus G_{0:3} \\
Z(0)_{3,4} &= K_{3:2} \oplus K_{3:4} \\
&\oplus G_{0:4} \\
Z(0)_{4,1} &= K_{4:2} \oplus K_{4:4} \\
Z(0)_{4,2} &= K_{4:1} \oplus K_{4:3} \\
Z(0)_{4,3} &= K_{4:1} \oplus K_{4:2} \oplus K_{4:4} \\
Z(0)_{4,4} &= K_{4:1} \oplus K_{4:3} \oplus K_{4:4} \\
Z(1)_{3,1} &= K_{3:2} \oplus K_{4:1} \\
&\oplus G_{0:1} \oplus G_{0:3} \oplus G_{1:1} \\
Z(1)_{3,2} &= K_{3:3} \oplus K_{4:2} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:4} \oplus G_{1:2} \\
Z(1)_{3,3} &= K_{3:1} \oplus K_{3:4} \oplus K_{4:3} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \oplus G_{1:3} \\
Z(1)_{3,4} &= K_{3:1} \oplus K_{4:4} \\
&\oplus G_{0:2} \oplus G_{0:4} \oplus G_{1:4} \\
Z(1)_{4,1} &= K_{3:1} \\
&\oplus G_{0:2} \oplus G_{0:4} \\
Z(1)_{4,2} &= K_{3:2} \\
&\oplus G_{0:1} \oplus G_{0:3} \\
Z(1)_{4,3} &= K_{3:2} \oplus K_{3:3} \oplus K_{4:1} \\
&\oplus G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \\
Z(1)_{4,4} &= K_{3:1} \oplus K_{3:4} \oplus K_{4:4} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \\
W(1)(=W(7))_{1,1} &= K_{3:1} \oplus K_{3:2} \oplus K_{4:1} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:1} \\
W(1)(=W(7))_{1,2} &= K_{3:2} \oplus K_{3:3} \oplus K_{4:2}
\end{aligned}
$$

$$
\begin{aligned}
&\oplus\ G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:2} \\
W(1)(=W(7))_{1,3} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:3} \\
&\oplus\ G_{0:1} \oplus G_{0:4} \oplus G_{1:3} \\
W(1)(=W(7))_{1,4} &= K_{3:4} \\
&\oplus\ G_{0:1} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:4} \\
W(1)(=W(7))_{2,1} &= K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:3} \\
&\oplus\ G_{0:1} \oplus G_{0:2} \oplus G_{1:3} \\
W(1)(=W(7))_{2,2} &= K_{3:2} \oplus K_{3:4} \\
&\oplus\ G_{0:4} \oplus G_{1:4} \\
W(1)(=W(7))_{2,3} &= K_{3:1} \oplus K_{3:3} \\
&\oplus\ G_{0:1} \oplus G_{1:1} \\
W(1)(=W(7))_{2,4} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:2} \oplus K_{4:4} \\
&\oplus\ G_{0:1} \oplus G_{0:4} \oplus G_{1:2} \\
Z(2)_{3,1} &= K_{3:3} \oplus K_{3:4} \oplus K_{4:3} \\
&\oplus\ G_{0:2} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{1:3} \oplus G_{2:1} \\
{}_{3,2} &= K_{3:1} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:2} \\
&\oplus\ G_{0:3} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:2} \\
{}_{3,3} &= K_{3:2} \oplus K_{3:4} \oplus K_{4:2} \oplus K_{4:3} \\
&\oplus\ G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{2:3} \\
{}_{3,4} &= K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:2} \\
&\oplus\ G_{0:1} \oplus G_{0:2} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:4} \\
{}_{4,1} &= K_{3:1} \oplus K_{3:3} \oplus K_{4:2} \oplus K_{4:4} \\
&\oplus\ G_{0:1} \oplus G_{1:2} \oplus G_{1:4} \\
{}_{4,2} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:3} \\
&\oplus\ G_{0:2} \oplus G_{1:1} \oplus G_{1:3} \\
{}_{4,3} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:2} \oplus K_{4:3} \oplus K_{4:4} \\
&\oplus\ G_{0:2} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{1:4} \\
{}_{4,4} &= K_{3:3} \oplus K_{4:1} \oplus K_{4:2} \oplus K_{4:3} \oplus K_{4:4} \\
&\oplus\ G_{0:1} \oplus G_{0:2} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:3} \\
W(2)(=W(6))_{3,1} &= K_{3:1} \oplus K_{3:4} \oplus K_{4:2} \oplus K_{4:3} \oplus K_{4:4} \\
&\oplus\ G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:1} \\
{}_{3,2} &= K_{3:2} \oplus K_{3:3} \oplus K_{4:2} \oplus K_{4:3} \\
&\oplus\ G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:2} \\
{}_{3,3} &= K_{3:1} \oplus K_{4:1} \oplus K_{4:4} \\
&\oplus\ G_{0:2} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:4} \oplus G_{2:3} \\
{}_{3,4} &= K_{3:2} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:3} \oplus K_{4:4} \\
&\oplus\ G_{0:4} \oplus G_{1:1} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:4}
\end{aligned}
$$

$$
\begin{aligned}
{}_{4,1} &= K_{3:3} \oplus K_{4:1} \oplus K_{4:2} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{2:3} \\
{}_{4,2} &= K_{3:1} \oplus K_{4:4} \\
&\oplus G_{0:2} \oplus G_{0:4} \oplus G_{1:4} \oplus G_{2:4} \\
{}_{4,3} &= K_{3:2} \oplus K_{4:1} \\
&\oplus G_{0:1} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{2:1} \\
{}_{4,4} &= K_{3:2} \oplus K_{4:1} \oplus K_{4:4} \\
&\oplus G_{0:1} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{1:4} \oplus G_{2:2} \\
Z(3)_{3,1} &= K_{3:4} \oplus K_{4:1} \oplus K_{4:2} \oplus K_{4:3} \\
&\oplus G_{0:1} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{2:1} \oplus G_{2:3} \oplus G_{3:1} \\
{}_{3,2} &= K_{3:1} \oplus K_{3:3} \oplus K_{4:1} \oplus K_{4:3} \\
&\oplus G_{0:1} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{2:4} \oplus G_{3:2} \\
{}_{3,3} &= K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:1} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{2:3} \oplus G_{3:3} \\
{}_{3,4} &= K_{3:3} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:2} \oplus K_{4:4} \\
&\oplus G_{0:2} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{2:2} \oplus G_{2:4} \oplus G_{3:4} \\
{}_{4,1} &= K_{3:1} \oplus K_{3:2} \oplus K_{4:1} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{2:2} \oplus G_{2:4} \\
{}_{4,2} &= K_{3:2} \oplus K_{3:3} \oplus K_{4:2} \\
&\oplus G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:2} \oplus G_{2:1} \oplus G_{2:3} \\
{}_{4,3} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:3} \oplus K_{4:2} \\
&\oplus G_{0:3} \oplus G_{1:2} \oplus G_{2:2} \oplus G_{2:3} \oplus G_{2:4} \\
{}_{4,4} &= K_{3:3} \oplus K_{4:1} \oplus K_{4:2} \oplus K_{4:4} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{2:3} \\
W(3)(=W(5))_{3,1} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:4} \oplus K_{4:2} \oplus K_{4:3} \\
&\oplus G_{0:2} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{2:3} \oplus G_{2:4} \oplus G_{3:1} \\
{}_{3,2} &= K_{3:1} \oplus K_{3:2} \oplus K_{4:1} \oplus K_{4:2} \oplus K_{4:3} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:2} \oplus G_{2:3} \oplus G_{2:4} \oplus G_{3:2} \\
{}_{3,3} &= K_{3:1} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:2} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:4} \oplus G_{3:3} \\
{}_{3,4} &= K_{3:4} \\
&\oplus G_{0:1} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:3} \oplus G_{2:4} \oplus G_{3:4} \\
{}_{4,1} &= K_{3:2} \oplus K_{3:4} \oplus K_{4:2} \\
&\oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{3:3} \\
{}_{4,2} &= K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:2} \\
&\oplus G_{0:1} \oplus G_{0:2} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:4} \oplus G_{3:4} \\
{}_{4,3} &= K_{3:3} \oplus K_{3:4} \oplus K_{4:3}
\end{aligned}
$$

$$
\begin{aligned}
&\oplus\ G_{0:2} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{1:3} \oplus G_{2:1} \oplus G_{3:1} \\
{}_{4,4} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:3} \oplus K_{4:3} \oplus K_{4:4} \\
&\oplus\ G_{0:3} \oplus G_{1:1} \oplus G_{1:3} \oplus G_{2:1} \oplus G_{2:4} \oplus G_{3:2} \\
Z(4)_{3,1} &= K_{3:2} \oplus K_{4:1} \oplus K_{4:3} \\
&\oplus\ G_{0:1} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:2} \oplus G_{2:3} \oplus G_{3:1} \oplus G_{3:3} \oplus G_{4:1} \\
{}_{3,2} &= K_{4:1} \\
&\oplus\ G_{1:1} \oplus G_{2:3} \oplus G_{2:4} \oplus G_{3:1} \oplus G_{3:2} \oplus G_{3:4} \oplus G_{4:2} \\
{}_{3,3} &= K_{3:1} \oplus K_{4:2} \\
&\oplus\ G_{0:2} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{2:4} \oplus G_{3:1} \oplus G_{3:2} \oplus G_{3:3} \oplus G_{4:3} \\
{}_{3,4} &= K_{3:1} \oplus K_{3:2} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:2} \oplus K_{4:3} \\
&\oplus\ G_{0:2} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{3:2} \oplus G_{3:4} \oplus G_{4:4} \\
{}_{4,1} &= K_{3:1} \oplus K_{3:4} \oplus K_{4:2} \oplus K_{4:3} \oplus K_{4:4} \\
&\oplus\ G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{3:2} \oplus G_{3:4} \\
{}_{4,2} &= K_{3:2} \oplus K_{3:3} \oplus K_{4:2} \oplus K_{4:3} \\
&\oplus\ G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:2} \oplus G_{3:1} \oplus G_{3:3} \\
{}_{4,3} &= K_{3:1} \oplus K_{3:2} \oplus K_{4:3} \oplus K_{4:4} \\
&\oplus\ G_{0:1} \oplus G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:3} \oplus G_{2:2} \oplus G_{3:2} \oplus G_{3:3} \oplus G_{3:4} \\
{}_{4,4} &= K_{3:1} \oplus K_{4:2} \oplus K_{4:4} \\
&\oplus\ G_{0:2} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{2:4} \oplus G_{3:1} \oplus G_{3:2} \oplus G_{3:3}
\end{aligned}
$$

4.2 拡大鍵の生成

アルゴリズムの設計者の指針では、中間値から拡大鍵の生成には平文側の規則と暗号文側の規則を変化することで、(1) 平文側と暗号文側で同じ拡大鍵が生成されることを避ける、(2) 単純な依存関係によって弱い鍵となることがないようにする、ことを目標としている。

Hierocrypt-L1 のほとんどのアルゴリズム設計では、その手法と方針が示されているが、この拡大鍵生成部分については、平文側と暗号文側を異なるものとしたこと以外は、ほとんど述べられていない。

評価者は拡大鍵生成についてさらに重点的に解析を行い、生成される拡大鍵の性質について評価を行った。

拡大鍵生成の単射性について

定理 4.2: 平文側の各段の拡大鍵生成 $(K^{(1)}, K^{(2)}, K^{(3)}, K^{(4)})$ は秘密鍵に対して単射である。

証明：秘密鍵から一意に中間鍵 Z が生成されることは仕様から自明、またこれら中間鍵 Z から一意に拡大鍵が生成されることも明らか。

逆にある段 t の拡大鍵 $K^{(t)}, 1 \leq t \leq 4$ を固定したとき、以下に示すように一意に *128* ビットの中間値 $Z^{(t)}$ を決定することができる、すなわち任意の $t, 1 \leq t \leq 4$ 段目の拡大鍵に対して一意

に秘密鍵が決定される。

$$\begin{aligned} V^{(t)} &= F_\sigma(K_2^{(t)} \oplus K_3^{(t)} \oplus K_4^{(t)}) \\ Z_1^{(t)} &= K_3^{(t)} \oplus K_4^{(t)} \oplus V^{(t)} \\ Z_2^{(t)} &= K_1^{(t)} \\ Z_3^{(t)} &= K_2^{(t)} \oplus V^{(t)} \\ Z_4^{(t)} &= K_3^{(t)} \oplus V^{(t)} \end{aligned}$$

□

観察 4.3: 暗号文側の各段の拡大鍵生成 $(K^{(5)}, K^{(6)}, K^{(7)})$ は秘密鍵に対して単射でないと考えられる。

根拠：これまでの評価より任意の秘密鍵と $Z^{(t-1)}, 5 \leq t \leq 8$ は単射である。以下では、$Z^{(t-1)}$ と拡大鍵 $K^{(t)}$ が単射でないと考えられる根拠を示す。

まず、拡大鍵 $K^{(t)}$ を $Z^{(t-1)}$ のみを使って表記すると以下のようになる。

$$\begin{aligned} K_1^{(t)} &= Z_3^{(t-1)} \oplus Z_2^{(t-1)} \oplus F_\sigma(Z_1^{(t-1)} \oplus Z_3^{(t-1)}) && (1) \\ K_2^{(t)} &= M_5(G^{(t-1)} \oplus Z_3^{(t-1)}) \oplus F_\sigma(Z_1^{(t-1)} \oplus Z_3^{(t-1)}) && (2) \\ K_3^{(t)} &= M_B(Z_4^{(t-1)}) \oplus F_\sigma(Z_1^{(t-1)} \oplus Z_3^{(t-1)}) && (3) \\ K_4^{(t)} &= Z_1^{(t-1)} \oplus M_B(Z_4^{(t-1)}) && (4) \end{aligned}$$

ここで媒介変数 x を用いて $Y^{(t-1)}$ を以下のように定義する。

$$\begin{aligned} Y_4^{(t-1)} &= M_B^{-1}(K_4^{(t)} \oplus x) \\ Y_3^{(t-1)} &= M_5^{-1}(x \oplus M_5(G^{(t-1)}) \oplus K_2^{(t)} \oplus K_3^{(t)} \oplus K_4^{(t)}) \\ Y_2^{(t-1)} &= x \oplus Y_3 \oplus K_1^{(t)} \oplus K_3^{(t)} \oplus K_4^{(t)}) \\ Y_1^{(t-1)} &= x \end{aligned}$$

$Y^{(t-1)}$ は固定した拡大鍵 $K^{(t)}$ と x に対して一意に決定されるが、x が異なると、異なる $Y^{(t-1)}$ が決定されることに注意する。$Z^{(t-1)} = Y^{(t-1)}$ が式 *(1)*〜*(4)* を同時に満たすためには

$$F_\sigma(Y_1^{(t-1)} \oplus Y_3^{(t-1)}) = Y_1^{(t-1)} \oplus K_3^{(t)} \oplus K_4^{(t)}$$

が成り立つような Y である必要がある。このような Y の個数は、関数 F_σ の性質に依存するが、*(1)*F_σ は非線形で複雑な関数であること、*(2)*x から Y の生成が F_σ に依存しない、線形な変換のみで行われること、の二点から、式 *(1)*〜*(4)* を満たす Z は *1* 個以上存在する場合があると強く予想される。

□

拡大鍵生成の段間の相関について

多くのブロック暗号では拡大鍵について、異なる段の間で相関のある場合は多い。DES では、ビットレベルで同じビットを 16 段のうち 13〜14 回繰り返し使っている。MISTY1 では、16 ビットデータを 5 回、または 4 回繰り返し用いている。

これらの使用では、拡大鍵の使用法が適切であったため、弱点として指摘されることはなかったが、その他の暗号では弱点となった例がある。SAFER+の 256 ビット鍵スケジュールでは、同じ拡大鍵データを繰り返し用いたことによる中間値一致攻撃が (minor flaw ではあるが) 指摘されている [5]。また、Magenta では明らかな拡大鍵の繰り返し使用で同じく中間値一致攻撃的な攻撃が指摘されている [6]。また、極端な例で毎段同じ鍵を用いることでスライド攻撃 [7] などを適用する条件を生む要素となる。

Hierocrypt-L1 では、中間鍵が段数の約半分だけしか生成されないため、評価者としては平文側、暗号文側で同じ中間値に対応する拡大鍵の生成に注目するべきである。具体的には、アルゴリズム設計者の記述から

$$Z^{(t)} = Z^{(8-t)}, 5 \leq t \leq 7$$

かつ $K^{(t)}, 1 \leq t \leq 4$ は主に $Z^{(t-1)}, Z^{(t)}$ で簡単に表記され、$K^{(t)}, 5 \leq t \leq 7$ は主に $Z^{(t-1)}, Z^{(t)}$ で簡単に表記されることから、

$$\begin{aligned} K^{(t)} &\longleftrightarrow K^{(8-t)} \\ K^{(t)} &\longleftrightarrow K^{(9-t)} \end{aligned}$$

の相関に着目した。この評価にあたり、拡大鍵を生成する際に用いられる変数 $V^{(t)}$ についての以下の補題を示しておく。

補題 1: $V^{(t)} = V^{(9-t)}, 5 \leq t \leq 7$

自明なので、証明は与えない。

この補題を用いることで以下の定理を示すことができる。

定理 4.4: $K_1^{(t)} = K_1^{(9-t)} \oplus K_2^{(9-t)}, 5 \leq t \leq 7$

証明：平文側の拡大鍵導出の式から $(5 \leq t \leq 7)$

$$\begin{aligned} K_1^{(9-t)} \oplus K_2^{(9-t)} &= Z_1^{(9-t-1)} \oplus Z_3^{(9-t)} \\ &= Z_1^{(8-(9-t-1))} \oplus Z_3^{(8-(9-t))} \\ &= Z_1^{(t)} \oplus Z_3^{(t-1)} \end{aligned}$$

さらに暗号文側の拡大鍵導出の式から

$$K_1^{(t)} = Z_1^{(t)} \oplus Z_3^{(t-1)}$$

□

次に平文側のみの線形相関として以下のものが導かれる。

定理 4.5: $K_1^{(t)} \oplus K_2^{(t)} \oplus K_4^{(t-1)} = Z_3^{(t)} \oplus Z_4^{(t-1)}, 2 \leq t \leq 4$

証明：平文側の拡大鍵導出の式から $(2 \le t \le 4)$

$$\begin{aligned} K_1^{(t)} &= Z_1^{(t-1)} \oplus V^{(t)} \\ &= Z_2^{(t)} \\ K_2^{(t)} &= Z_3^{(t)} \oplus V^{(t)} \\ &= Z_3^{(t)} \oplus Z_2^{(t)} \oplus Z_1^{(t-1)} \\ K_4^{(t)} &= Z_2^{(t-1)} \oplus Z_4^{(t)} \\ &= Z_1^{(t)} \oplus Z_4^{(t)} \end{aligned}$$

これらより

$$\begin{aligned} K_4^{(t-1)} &= Z_1^{(t-1)} \oplus Z_4^{(t-1)} \\ K_1^{(t)} \oplus K_2^{(t)} \oplus K_4^{(t-1)} &= Z_2^{(t)} \oplus Z_3^{(t)} \oplus Z_2^{(t)} \oplus Z_1^{(t-1)} \oplus Z_1^{(t-1)} \oplus Z_4^{(t-1)} \\ &= Z_3^{(t)} \oplus Z_4^{(t-1)} \end{aligned}$$

□

ここで、Z_3、Z_4 は鍵と定数による線形変換であったことを思い出す。これらの鍵と定数を使った表記は以下のようになる。

$$\begin{aligned} (Z_3^{(2)} \oplus Z_4^{(1)})_1 &= K_{3:1} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:3} \\ &\oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:3} \oplus G_{2:1} \\ (Z_3^{(2)} \oplus Z_4^{(1)})_2 &= K_{3:1} \oplus K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:2} \\ &\oplus G_{0:1} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:2} \\ (Z_3^{(2)} \oplus Z_4^{(1)})_3 &= K_{3:3} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:2} \oplus K_{4:3} \\ &\oplus G_{0:2} \oplus G_{0:3} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{2:3} \\ (Z_3^{(2)} \oplus Z_4^{(1)})_4 &= K_{3:1} \oplus K_{3:2} \oplus K_{3:3} \oplus K_{4:2} \oplus K_{4:4} \\ &\oplus G_{0:3} \oplus G_{1:2} \oplus G_{1:4} \oplus G_{2:4} \\ (Z_3^{(3)} \oplus Z_4^{(2)})_1 &= K_{3:1} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:1} \oplus K_{4:3} \oplus K_{4:4} \\ &\oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:3} \oplus G_{3:1} \\ (Z_3^{(3)} \oplus Z_4^{(2)})_2 &= K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \\ &\oplus G_{0:1} \oplus G_{0:2} \oplus G_{1:1} \oplus G_{1:4} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{2:4} \oplus G_{3:2} \\ (Z_3^{(3)} \oplus Z_4^{(2)})_3 &= K_{3:1} \oplus K_{3:3} \oplus K_{4:2} \oplus K_{4:3} \oplus K_{4:4} \\ &\oplus G_{0:1} \oplus G_{1:2} \oplus G_{1:3} \oplus G_{2:1} \oplus G_{2:2} \oplus G_{2:3} \oplus G_{3:3} \\ (Z_3^{(3)} \oplus Z_4^{(2)})_4 &= K_{3:4} \oplus K_{4:3} \\ &\oplus G_{0:1} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:3} \oplus G_{2:2} \oplus G_{2:4} \oplus G_{3:4} \\ (Z_3^{(4)} \oplus Z_4^{(3)})_1 &= K_{3:1} \oplus K_{4:3} \\ &\oplus G_{0:2} \oplus G_{0:4} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:3} \oplus G_{2:4} \oplus G_{3:1} \oplus G_{3:3} \oplus G_{4:1} \\ (Z_3^{(4)} \oplus Z_4^{(3)})_2 &= K_{3:2} \oplus K_{3:3} \oplus K_{4:1} \oplus K_{4:2} \\ &\oplus G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:2} \oplus G_{2:1} \oplus G_{2:4} \oplus G_{3:1} \oplus G_{3:2} \oplus G_{3:4} \oplus G_{4:2} \\ (Z_3^{(4)} \oplus Z_4^{(3)})_3 &= K_{3:2} \oplus K_{3:3} \end{aligned}$$

$$
\begin{aligned}
&\oplus \quad G_{0:2} \oplus G_{0:3} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{2:2} \oplus G_{2:3} \oplus G_{3:1} \oplus G_{3:2} \oplus G_{3:3} \oplus G_{4:3} \\
(Z_3^{(4)} \oplus Z_4^{(3)})_4 \;&= \quad K_{3:1} \oplus K_{3:2} \oplus K_{3:3} \oplus K_{3:4} \oplus K_{4:3} \oplus K_{4:4} \\
&\oplus \quad G_{0:1} \oplus G_{0:4} \oplus G_{1:1} \oplus G_{1:3} \oplus G_{1:4} \oplus G_{2:3} \oplus G_{3:2} \oplus G_{3:4} \oplus G_{4:4}
\end{aligned}
$$

これらは、上記で示した拡大鍵の排他的論理和が、秘密鍵と定数の排他論理和で表現できることを示している。

異なる秘密鍵間の拡大鍵の相関について

上記で示したように、平文側の拡大鍵生成について、t 段目の拡大鍵と秘密鍵は単射であったことから、異なる秘密鍵は異なる拡大鍵を生成する。これにより、鍵スケジュール部に起因する等価鍵は起こらないと強く考えられる。

また、データ撹拌部分の構造が SPN 構造であり、複数の反転した拡大鍵間の (反転の) キャンセルアウトによる F 関数入力の固定は起こり得ず、LOKI89 のような (データ撹拌部分と鍵スケジュール部の相互作用による) 等価鍵 [8] も存在しにくい。

DES の反転特性 [9] のような、平文の反転と拡大鍵の反転のキャンセルアウトによる自明な特性については、以下のように考察することで、Hierocrypt-L1 には起こりにくいと考える。

DES の反転特性は、非線形な関数である F 関数へのすべての入力を (異なる平文、鍵入力に対して) 固定することで得られる。Hierocrypt-L1 では、平文は第 1 段目の拡大鍵との排他的論理和が行われる。よって、異なる平文 P_A, P_B と第一段拡大鍵 $K_A^{(1)}, K_B^{(1)}$ の差分のキャンセルアウト (すなわち $P_A \oplus K_A^{(1)} = P_B \oplus K_B^{(1)}$) により、最初の S ボックスへの入力が固定されることはある。しかし、そのあとの拡大鍵 $(K_A^{(t)}, K_B^{(t)})$ は異なりながらも、データ撹拌部分の (鍵加算前の) 中間値が同じであることから、鍵加算により中間値に差分が生じ S ボックスで差分が拡散されてしまう。よって、秘密鍵と平文側の拡大鍵が単射であることと、データ撹拌部分が SPN 構造であることから、DES のような反転特性は生じないと強く予想される。

ただし、中間鍵には DES 構造全体で起こる反転特性のような、F 関数の入力を固定するものは存在することを注意しておく。

定理 4.6: 以下に示す差分関係にある二つの中間鍵 $Z_A^{(1)}, Z_B^{(1)}$ は、これから生成されるすべての中間鍵 $Z_A^{(t)}, Z_B^{(t)}, 2 \le t \le 4$ についても自明な差分が生まれる *(*表記：ただし、x はあるバイト差分値 *(*任意*)*、*0* はバイトの *0* 差分を示す*)* 。

Case 1:*(*一段繰り返し*)*

$$
\begin{aligned}
\Delta Z^{(0)} &= 000x, 000x, 000x, x0x0 \\
\Delta Z^{(1)} &= 000x, 000x, 000x, x0x0 \\
\Delta Z^{(2)} &= 000x, 000x, 000x, x0x0 \\
\Delta Z^{(3)} &= 000x, 000x, 000x, x0x0 \\
\Delta Z^{(4)} &= 000x, 000x, 000x, x0x0
\end{aligned}
$$

Case 2:*(*二段繰り返し*)*

$$
\begin{aligned}
\Delta Z^{(0)} &= 0000, 000x, 0000, x0xx \\
\Delta Z^{(1)} &= 000x, 0000, 000x, 000x
\end{aligned}
$$

$$
\begin{aligned}
\Delta Z^{(2)} &= 0000, 000x, 0000, x0xx \\
\Delta Z^{(3)} &= 000x, 0000, 000x, 000x \\
\Delta Z^{(4)} &= 0000, 000x, 0000, x0xx
\end{aligned}
$$

Case 3:*(*二段繰り返し、*Case 2* の逆*)*

$$
\begin{aligned}
\Delta Z^{(0)} &= 000x, 0000, 000x, 000x \\
\Delta Z^{(1)} &= 0000, 000x, 0000, x0xx \\
\Delta Z^{(2)} &= 000x, 0000, 000x, 000x \\
\Delta Z^{(3)} &= 0000, 000x, 0000, x0xx \\
\Delta Z^{(4)} &= 000x, 0000, 000x, 000x
\end{aligned}
$$

5 データ撹拌部の解析

この章では、Hierocrypt-L1 のデータ撹拌部分について安全性の詳細評価の結果をまとめる。Hierocrypt-L1 は SPN 構造に基づいたデータ撹拌部分の設計であり、バイトオリエンティッドな構造である。

このような構造をもつブロック暗号には、SQUARE[10]、Rijndael[11]、CRYPTON [12] がある。これらのブロック暗号に対する有効な安全性評価としては、同様にバイト単位の特性に着目した SQUARE 攻撃 [10]、truncated-differential[13] などが一般的かつ効果的であると考えられる。

これに対して Hierocrypt-L1 の設計者はアルゴリズムの提案時に、評価書中の安全性評価の項で、これら解読法に対する詳細な安全性評価結果を示している。これらの信憑性は高いものと評価者は考え、一般的に有効と考えられる Square 攻撃や truncated-differential については今回の詳細評価では言及しない。しかし、Hierocrypt-L1 に適用可能なバイトオリエンティッドな特徴は安全性評価の観点から重要視する必要がある。

データ撹拌部分を構成する四つの部分関数をまとめると：

1. 鍵加算 (排他的論理和)
2. S ボックス (8 ビット単位の非線形変換)
3. MDSL(GF(2^8) 上の乗算と加算)
4. MDSH(バイト単位の排他的論理和)

ここで S ボックス以外のすべての演算は有限体 GF(2^8) 上の演算として簡単に表現される。しかし、設計者はこれを懸念し、S ボックスの設計では S ボックスと MDSL との組み合わせが最も複雑となる (より具体的には重み付き項数による評価の最大となる) S ボックス、ならびに MDSL を設計している。つまり単純な代数補間についても設計者により評価済みである。

評価者は、まず S ボックスについて詳細な評価を行い発見した性質について (暗号全体の安全性の議論への影響はほぼ関係なく) 列挙する。

5.1 Hierocrypt-L1 の S ボックス評価

評価を行った S ボックスを表 2に示す。

S ボックスの設計について

設計者は S ボックスの導出について Hierocrypt-L1 の仕様書にて記述している。ここでは S ボックスは

$$s(x) = Add(Power(Perm(x)))$$

のように、ビット並び替え $Perm()$、有限体 GF(2^8) 上のべき乗演算 $Power()$、それに排他的論理和 $Add()$ の合成関数として表現されている。このうち排他論理和 Add は定数 0x11 を加算することになっているが、$x = 0$ のときの S ボックスの出力は 7 であり矛盾している。

また、実際に $s(Perm^{-1}(x))$ を多項式により近似してみたとき、その結果は $x^{247} + 7$(これらはすべて GF(2^8) 上の要素、および演算) であった。

S ボックスの代数的性質

上記の S ボックスを $x^8 + x^6 + x^5 + x + 1$ の既約多項式で決定される有限体 GF(2^8) 上の関数として表すと以下のようになる。ここで係数は 10 進数表記であるが、GF(2^8) の元への対応は表記の項で示した通りである。

$$\begin{aligned}
F(x) &= 7\times x^0+198\times x^1+233\times x^2+39\times x^3+186\times x^4+205\times x^5+92\times x^6+197\times x^7\\
&+ 239\times x^8+90\times x^9+175\times x^{10}+107\times x^{11}+142\times x^{12}+91\times x^{14}+179\times x^{15}\\
&+ 255\times x^{16}+66\times x^{17}+172\times x^{18}+12\times x^{19}+196\times x^{20}+114\times x^{21}+219\times x^{22}+42\times x^{23}\\
&+ 181\times x^{24}+162\times x^{25}+71\times x^{26}+227\times x^{27}+86\times x^{28}+213\times x^{29}+15\times x^{30}+141\times x^{31}\\
&+ 68\times x^{32}+37\times x^{33}+220\times x^{34}+144\times x^{35}+96\times x^{36}+130\times x^{37}+107\times x^{38}+47\times x^{39}\\
&+ 192\times x^{40}+107\times x^{41}+89\times x^{42}+161\times x^{43}+157\times x^{44}+186\times x^{45}+135\times x^{46}+159\times x^{47}\\
&+ 141\times x^{48}+93\times x^{49}+245\times x^{50}+96\times x^{51}+103\times x^{52}+113\times x^{53}+145\times x^{54}+189\times x^{55}\\
&+ 92\times x^{56}+76\times x^{57}+141\times x^{58}+244\times x^{59}+205\times x^{60}+22\times x^{61}+79\times x^{62}+253\times x^{63}\\
&+ 202\times x^{64}+205\times x^{65}+140\times x^{66}+195\times x^{67}+74\times x^{68}+226\times x^{69}+220\times x^{70}+171\times x^{71}\\
&+ 182\times x^{72}+116\times x^{73}+182\times x^{74}+57\times x^{75}+177\times x^{76}+105\times x^{77}+240\times x^{78}+45\times x^{79}\\
&+ 106\times x^{80}+94\times x^{81}+241\times x^{82}+124\times x^{83}+215\times x^{84}+168\times x^{85}+193\times x^{86}+16\times x^{87}\\
&+ 137\times x^{88}+39\times x^{89}+50\times x^{90}+116\times x^{91}+78\times x^{92}+55\times x^{93}+201\times x^{94}+5\times x^{95}\\
&+ 119\times x^{96}+70\times x^{97}+91\times x^{98}+10\times x^{99}+165\times x^{100}+117\times x^{101}+194\times x^{102}+155\times x^{103}\\
&+ 191\times x^{104}+230\times x^{105}+252\times x^{106}+151\times x^{107}+181\times x^{108}+203\times x^{109}+21\times x^{110}+29\times x^{111}\\
&+ 178\times x^{112}+104\times x^{113}+86\times x^{114}+101\times x^{115}+71\times x^{116}+108\times x^{117}+168\times x^{118}+96\times x^{119}\\
&+ 211\times x^{120}+160\times x^{121}+2\times x^{122}+117\times x^{123}+255\times x^{124}+135\times x^{125}+60\times x^{126}+151\times x^{127}\\
&+ 46\times x^{128}+130\times x^{129}+58\times x^{130}+54\times x^{131}+105\times x^{132}+157\times x^{133}+156\times x^{134}+28\times x^{135}\\
&+ 24\times x^{136}+242\times x^{137}+67\times x^{138}+79\times x^{139}+149\times x^{140}+214\times x^{141}+126\times x^{142}+109\times x^{143}\\
&+ 81\times x^{144}+129\times x^{145}+202\times x^{146}+67\times x^{147}+69\times x^{148}+207\times x^{149}+117\times x^{150}+236\times x^{151}\\
&+ 172\times x^{152}+144\times x^{153}+73\times x^{154}+160\times x^{155}+26\times x^{156}+214\times x^{157}+62\times x^{158}+51\times x^{159}\\
&+ 40\times x^{160}+54\times x^{161}+132\times x^{162}+173\times x^{163}+191\times x^{164}+240\times x^{165}+13\times x^{166}+252\times x^{167}\\
&+ 177\times x^{168}+58\times x^{169}+23\times x^{170}+104\times x^{171}+122\times x^{172}+85\times x^{173}+36\times x^{174}+187\times x^{175}\\
&+ 119\times x^{176}+76\times x^{177}+17\times x^{178}+227\times x^{179}+92\times x^{180}+180\times x^{181}+216\times x^{182}+230\times x^{183}\\
&+ 139\times x^{184}+8\times x^{185}+171\times x^{186}+37\times x^{187}+120\times x^{188}+231\times x^{189}+55\times x^{190}+244\times x^{191}
\end{aligned}$$

$$
\begin{aligned}
&+ \quad 195\times x^{192}+214\times x^{193}+169\times x^{194}+62\times x^{195}+183\times x^{196}+113\times x^{197}+121\times x^{198}+63\times x^{199}\\
&+ \quad 92\times x^{200}+106\times x^{201}+204\times x^{202}+29\times x^{203}+78\times x^{204}+180\times x^{205}+233\times x^{206}+115\times x^{207}\\
&+ \quad 214\times x^{208}+214\times x^{209}+211\times x^{210}+24\times x^{211}+49\times x^{212}+62\times x^{213}+153\times x^{214}+218\times x^{215}\\
&+ \quad 214\times x^{216}+76\times x^{217}+67\times x^{218}+212\times x^{219}+52\times x^{220}+152\times x^{221}+159\times x^{222}+185\times x^{223}\\
&+ \quad 198\times x^{224}+90\times x^{225}+105\times x^{226}+19\times x^{227}+147\times x^{228}+142\times x^{229}+58\times x^{230}+141\times x^{231}\\
&+ \quad 48\times x^{232}+103\times x^{233}+238\times x^{234}+114\times x^{235}+29\times x^{236}+92\times x^{237}+146\times x^{238}+63\times x^{239}\\
&+ \quad 135\times x^{240}+97\times x^{241}+16\times x^{242}+94\times x^{243}+127\times x^{244}+181\times x^{245}+52\times x^{246}+78\times x^{247}\\
&+ \quad 30\times x^{248}+116\times x^{249}+124\times x^{250}+88\times x^{251}+137\times x^{252}+173\times x^{253}+188\times x^{254}
\end{aligned}
$$

この構造は、補間攻撃を避けるのに十分、複雑な構造となっている。

しかし、その他の構造 (鍵加算、MDSH、MDSL) が GF(2^8) で簡単に表記できるようなものであるため、以降、S ボックスについて GF(2^k) 上の性質について詳細に評価した結果を示す。

GF(2^k) 上の近似の概要

ここでは、S ボックスの GF(2^k),$k < 8$ 上の近似について考える。S ボックスの入出力サイズが 8 ビットであって，GF(2^k) への近似を考える場合，入出力の値 $x \in$(GF2)^8 を $y \in$GF(2^k) へ変換する写像 ϕ をまず探索する．暗号の解析の場合には S ボックスの入力に用いる写像と出力に用いる写像が異なったものについても探索可能であるが，本稿では入出力に対する写像は同じものを考えた．

探索した ϕ は，n ビットの偶数パリティ値の組み合わせを考える．すなわち

$$
\begin{aligned}
\phi : x &\rightarrow y = (y_{k-1}y_{k-2}\ldots y_0)\\
y_i &= parity(x, mask_i)
\end{aligned}
$$

となる ϕ であり，$mask_i$ は一次独立であるものを考える．

ある写像 ϕ については，d 次のすべての GF(2^k) 上の関数

(ただし，d 次の係数は非ゼロ) について確率評価を行う．GF(2^k) 上の関数 f に対する確率評価の定義は以下の通り．

$$
bias_{(\phi,f)} = \#\{x | f(\phi(x)) = \phi(S(x))\} - 2^8/2^k \tag{5}
$$

GF(2^2) 上の近似

上記で考えたような 8 ビット値から GF(2^2) への写像の取り方は、0 でない異なるマスク値 $mask0, mask1$ の組み合わせであるので 255×254 とおり存在する。これらについてすべてのマスクの組み合わせを探索し、GF(2^2) 上の d 次関数による近似の確率を評価した。この結果を次に示す。

一次式による近似

一次式の近似で、最も確率の高かったもの (近似確率 88/256=24/256+1/4、よって $bias$ = 24/256)9 例を以下に示す。ここで第三者が容易に検証できるように、$\phi(x)$ と $\phi(S(x))$ の分布 $dist$

も一緒に示す。これは 4×4 の二次元配列として考え、$dist[a][b]$ は $\phi(x) = a$ かつ $\phi(s(x)) = b$ となる入力 x の個数を示している。

$$
\begin{aligned}
mask &= (7, 233), f(x) = x + 3 \\
dist &= \{10, 16, 10, 28, 12, 18, 24, 10, 24, 18, 12, 10, 18, 12, 18, 16)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (7, 233), f(x) = 2x + 3 \\
dist &= \{10, 16, 10, 28, 12, 18, 24, 10, 24, 18, 12, 10, 18, 12, 18, 16)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (7, 238), f(x) = x + 1 \\
dist &= \{10, 28, 10, 16, 18, 16, 18, 12, 24, 10, 12, 18, 12, 10, 24, 18)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (7, 238), f(x) = 3x + 1 \\
dist &= \{10, 28, 10, 16, 18, 16, 18, 12, 24, 10, 12, 18, 12, 10, 24, 18)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (121, 129), f(x) = x + 3 \\
dist &= \{12, 12, 12, 28, 14, 18, 20, 12, 16, 18, 16, 14, 22, 16, 16, 10)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (121, 248), f(x) = x + 1 \\
dist &= \{12, 28, 12, 12, 22, 10, 16, 16, 16, 14, 16, 18, 14, 12, 20, 18)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (129, 248), f(x) = x + 1 \\
dist &= \{12, 28, 12, 12, 22, 10, 16, 16, 14, 12, 18, 20, 16, 14, 18, 16)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (233, 238), f(x) = x + 1 \\
dist &= \{10, 28, 16, 10, 18, 16, 12, 18, 12, 10, 18, 24, 24, 10, 18, 12)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (233, 238), f(x) = 2x + 1 \\
dist &= \{10, 28, 16, 10, 18, 16, 12, 18, 12, 10, 18, 24, 24, 10, 18, 12)
\end{aligned}
$$

二次式による近似

二次式の近似で、最も確率の高かったもの (近似確率 88/256=24/256+1/4)6例を以下に示す。

$$
\begin{aligned}
mask &= (7, 233), f(x) = x^2 + 3 \\
dist &= (10, 16, 10, 28, 12, 18, 24, 10, 24, 18, 12, 10, 18, 12, 18, 16)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (7, 238), f(x) = 2x^2 + 1 \\
dist &= (10, 28, 10, 16, 18, 16, 18, 12, 24, 10, 12, 18, 12, 10, 24, 18)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (86, 147), f(x) = x^2 \\
dist &= (24, 12, 14, 14, 12, 24, 14, 14, 14, 14, 16, 20, 14, 14, 20, 16)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (86, 197), f(x) = 2x^2 \\
dist &= (24, 14, 14, 12, 14, 16, 20, 14, 14, 20, 16, 14, 12, 14, 14, 24)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (147, 197), f(x) = 3x^2 \\
dist &= (24, 14, 12, 14, 14, 16, 14, 20, 12, 14, 24, 14, 14, 20, 14, 16)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (233, 238), f(x) = 3x^2 + 1 \\
dist &= (10, 28, 16, 10, 18, 16, 12, 18, 12, 10, 18, 24, 24, 10, 18, 12)
\end{aligned}
$$

三次式による近似

三次式の近似で、最も確率の高かったもの (近似確率 $94/256{=}30/256{+}1/4$)6例を以下に示す。

$$
\begin{aligned}
mask &= (7, 233,), f(x) = x^3 + 2x^2 + 2x + 3 \\
dist &= (10, 16, 10, 28, 12, 18, 24, 10, 24, 18, 12, 10, 18, 12, 18, 16)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (7, 233,), f(x) = 3x^3 + 3x^2 + 1x + 3 \\
dist &= (10, 16, 10, 28, 12, 18, 24, 10, 24, 18, 12, 10, 18, 12, 18, 16)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (7, 238,), f(x) = x^3 + 3x^2 + x + 1 \\
dist &= (10, 28, 10, 16, 18, 16, 18, 12, 24, 10, 12, 18, 12, 10, 24, 18)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (7, 238,), f(x) = 3x^3 + x^2 + 3x + 1 \\
dist &= (10, 28, 10, 16, 18, 16, 18, 12, 24, 10, 12, 18, 12, 10, 24, 18)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (233, 238,), f(x) = x^3 + 2x^2 + x + 1 \\
dist &= (10, 28, 16, 10, 18, 16, 12, 18, 12, 10, 18, 24, 24, 10, 18, 12)
\end{aligned}
$$

$$
\begin{aligned}
mask &= (233, 238,), f(x) = 2x^3 + x^2 + 2x + 1 \\
dist &= (10, 28, 16, 10, 18, 16, 12, 18, 12, 10, 18, 24, 24, 10, 18, 12)
\end{aligned}
$$

$\mathbf{GF}(2^3)$ 上の近似

8 ビット値から $\mathrm{GF}(2^3)$ への写像の取り方は、0 でない異なるマスク値 $mask0, mask1, mask2$ の組み合わせであるので $255 \times 254 \times 253$ とおり存在する。このうち三つのマスク値が一次独立であるもののみを探索したので実際に探索したマスク値の組み合わせは $255 \times 254 \times 253$ よりわずかに少ない。マスクの組み合わせについて探索し、$\mathrm{GF}(2^3)$ 上の d 次関数による近似の確率を評価した。この結果を次に示す。

一次式による近似

一次式の近似で、最も確率の高かったもの (近似確率 57/256=25/256+1/8)7例を以下に示す。

$$
\begin{aligned}
mask &= (40, 99, 215), f(x) = 2x + 7 \\
mask &= (61, 83, 185), f(x) = 3x + 4 \\
mask &= (61, 185, 234), f(x) = 5x + 6 \\
mask &= (83, 110, 234), f(x) = 7x + 4 \\
mask &= (99, 180, 255), f(x) = 2x + 1 \\
mask &= (110, 132, 185), f(x) = 7x + 6 \\
mask &= (132, 215, 234), f(x) = 3x + 7
\end{aligned}
$$

二次式による近似

二次式の近似で、最も確率の高かったもの (近似確率 58/256=26/256+1/8)2例を以下に示す。

$$
\begin{aligned}
mask &= (1, 7, 222), f(x) = 4x^2 + 3 \\
mask &= (7, 217, 223), f(x) = x^2 + 7
\end{aligned}
$$

三次式による近似

三次式の近似で、最も確率の高かったもの (近似確率 66/256=34/256+1/8)5例を以下に示す。

$$
\begin{aligned}
mask &= (7, 27, 238), f(x) = 7x^3 + 5x^2 + x + 3 \\
mask &= (7, 238, 245), f(x) = 3x^3 + 7x^2 + x + 5 \\
mask &= (27, 28, 245), f(x) = 6x^3 + 4x^2 + x + 5 \\
mask &= (28, 233, 238), f(x) = x^3 + x^2 + x + 2 \\
mask &= (233, 242, 245), f(x) = 5x^3 + 3x^2 + x + 5
\end{aligned}
$$

四次式以上による近似

ここの近似は探索が終了しておらず、上記の確率を上回る確率近似が見付かっていない。参考までに見付かった近似のいくつかを示す。

$$
\begin{aligned}
65/256 : mask &= (7, 117, 238), f(x) = 7x^4 + 2x^3 + 6x^2 + 6x + 1 \\
62/256 : mask &= (1, 54, 239), f(x) = 7x^5 + 6x^4 + 6x^3 + 2x^2 + 3x + 5 \\
62/256 : mask &= (1, 55, 238), f(x) = 3x^5 + 2x^4 + 4x^3 + 5x^2 + 4x + 3 \\
62/256 : mask &= (1, 60, 185), f(x) = x^5 + 4x^3 + x^2 + 7x + 7 \\
62/256 : mask &= (1, 61, 185), f(x) = 6x^5 + 2x^4 + x^3 + 4x + 5
\end{aligned}
$$

MDSL、MDSH への評価

Hierocrypt-L1 では二種類の線形関数、MDSL と MDSH、を用いている。MDSL では主にビット毎の撹拌と隣接する 4 つの S ボックスとの撹拌を行っている。これとは対照的に MDSH ではバイト単位による撹拌で、データブロック全体的な撹拌を目的とする。

このため、上記で評価を行ったSボックスの代数近似を暗号全体への評価に拡張するときには、各マスク値を線形撹拌層に応じて伝播させて、各段のマスク値 (すなわち ϕ) を決定する必要がある。

MDSH はバイト毎の排他論理和であるため、上記のSボックスの代数近似は出力多項式の和として表現することができる。したがって、(鍵加算)-(Sボックス)-(MDSH)-(鍵加算)-(Sボックス) の部分は効率的に近似が可能であるが、MDSL については (MDS のため) 複雑なビット単位の演算が含まれ、上記の近似ではうまく表現できない。ゆえに、暗号全体での近似もうまく表現できないと考えられる。

5.2 Hierocrypt-L1 の S ボックスの部分補間

これまで Hierocrypt-L1 のデータ撹拌部分はSボックスを除いた、鍵加算、MDSH、HDSL のどれもが $x^8 + x^6 + x^5 + x + 1$ により定義される有限体上の演算上で簡単に表記することができる。

Sボックスの完全な補間については上でも示したように次数、項数ともに十分大きな値となっている。しかし、部分的な補間 (すなわち入力空間 256 ではなくそのうちの一部) を行った補間をすることで次数や項数が減ることは自明である。ただし、この場合、暗号全体の代数近似の確率がより小さくなるため必要な既知平文数が増加すると考えられる。したがって、効率的な攻撃を考える場合、近似の確率と近似の項数および次数のトレードオフを考えてSボックスを近似する必要があるが、このトレードオフは以下の (自明な) 定理以上の評価についてはあまり知られていない。

定理 5.1: *Sボックスの 256 個の入力のうち n 個の入力に対して補間を行った場合、$n-1$ 次以下の多項式により近似が可能でその場合の項数は n 項以下である。*

以下では、部分的なSボックスの補間を行った実験結果についてまとめる。

部分補間の探索

評価者による部分空間に対する補間の探索では、以下の手順を繰り返して、いくつかの t について探索を行った。

1. t 個の入力からなる部分空間を選択
2. 補間式適用
3. 入力全体に対して、いくつの入力を補間たことになっているか計測

この結果を表 3に示す。係数は GF(2^8) 上の元であるが、10 進数表記をしている。点も 10 進数表記である。$t = 2, 3, 4$ の場合については探索を終了したが、5 以上については現時点で見付かったもののうちもっとも補間した点の多いものを示している。

その他 S ボックスの解析

暗号の安全性には全く言及できない性質であるが、Sボックスの解析結果として以下のものを列挙しておく。

S ボックスの固定点:$S(67_{16}) = 67_{16}$
S ボックスを OFB 的に用いたときの周期: 周期 30738=$109 \times 47 \times 2 \times 3$
個々の要素の周期 (要素は 16 進数表記):
周期が 109(素数) のもの
00 → 07 → 4e → ec → 8d → 58 → 94 → 6b → b6 → 26 → 3d → 3e → f9 → cb → 14 → 9d
→ f0 → ea → db → 40 → 21 → 9b → 33 → c9 → 8a → 4a → 57 → b1 → d4 → 93 → f8 → 8f
→ 0a → ce → 35 → ed → dc → cd → cf → 45 → 0d → e9 → 4c → bd → a6 → e3 → 76 → b7
→ 2b → f7 → 1d → 5f → 0f → 80 → 06 → 84 → 1b → a4 → 0e → 5d → c0 → ad → 5c → fb
→ 4f → 1e → 19 → 7a → 7d → b0 → 49 → 01 → fc → 16 → f5 → 0c → 02 → 55 → 09 → 75
→ 23 → d3 → 74 → 12 → 78 → d0 → 50 → 37 → 27 → 6f → df → a3 → 63 → 56 → f1 → 15
→ 2e → ac → 38 → 69 → 03 → 70 → d6 → da → e4 → 36 → de → 97 → b8 → 00
周期が 141($= 3 \times 47$**) のもの**
04 → 98 → 22 → 9c → e7 → 3a → 72 → cc → 6e → 9e → 71 → 83 → c5 → c7 → f2 → dd
→ ba → 90 → 2c → 8c → ef → 2a → 4d → 85 → 79 → 39 → 30 → 3c → 95 → e6 → 28 → b9
→ 86 → 4b → e5 → 32 → 41 → 8b → c4 → eb → d9 → 53 → 9a → b3 → f3 → c2 → a1 → 89
→ 88 → bf → 05 → 8e → 3f → d8 → a9 → 64 → 96 → 20 → 0b → 18 → c6 → e2 → 25 → 77
→ 65 → 13 → 42 → 44 → 11 → 60 → 61 → 7f → 1f → 87 → 66 → c1 → 68 → 99 → 43 → d7
→ ae → f4 → a5 → 6d → fa → b4 → bb → ff → a0 → 52 → b5 → 54 → 7c → d5 → e1 → 31
→ 5a → 82 → 34 → 29 → 2d → a7 → be → 7b → 3b → a8 → 59 → 81 → c8 → 46 → 48 → 6a
→ 5e → 51 → 9f → 7e → af → 5b → 08 → bc → fe → aa → ee → 62 → 1a → 2f → 17 → e8
→ 24 → c3 → 10 → 1c → b2 → e0 → 91 → 73 → a2 → 47 → fd → ab → f6 → 04
周期が 1 のもの
67 → 67
周期が 2 のもの
6c → ca → 6c
周期が 3 のもの
92 → d1 → d2 → 92

6 まとめ

Hierocrypt-L1 は、新しい構造の鍵スケジュールと、SPN 構造に基づくデータ撹拌部分からなるブロック暗号アルゴリズムである。

評価者は、Hierocrypt-L1 に対していくつかの限られた方向からの安全性評価を行い、いくつかの考察を述べた。

自明な欠点の発見を目的とした注意深い鍵スケジュール部の解析では、拡大鍵間の簡単な依存関係のいくつかを示したが、これらは暗号全体の安全性にはまったく影響がないと考えられる。

データ撹拌部分では、特にバイトオリエンティッドな構造に着目して限られた種類の S ボックスの解析を示したが、いずれも Hierocrypt-L1 の安全性を言及するに及ばない性質である。しかし、バイト単位の処理がすべてであり、これについては特に代数的な性質に注意を払う必要がある。

今回の詳細評価は Hierocrypt-L1 の安全性の保証には足りない内容であり、今後、特にバイト単位の処理に着目した安全性評価を期待したい。

参考文献

[1] 暗号技術仕様書: Hierocrypt-L1, available at http://www.toshiba.co.jp/rdc/security/hierocrypt/.

[2] 暗号技術仕様書: Hierocrypt-3, available at http://www.toshiba.co.jp/rdc/security/hierocrypt/.

[3] Specification on a Block Cipher: Hierocrypt-L1, available at http://www.toshiba.co.jp/rdc/security/hierocrypt/.

[4] 大熊建司, 村谷博文, 佐野文彦, 本山雅彦, 川村信一, 「ブロック暗号 Hierocrypt-3 および Hierocrypt-L1 に対する強度/性能評価」, 信学技報 ISEC2000-71, 電子情報通信学会, 2000.

[5] J. Kelsey, B. Schneier, "Key Schedule Weakness in SAFER+," *Second AES Candidate Conference*, 1999, available at http://www.counterpane.com/safer.html

[6] E. Biham, A. Biryukov, N. Ferguson, L. Knudsen, B. Schneier, A. Shamir, "Cryptanalysis of Magenta," *Second AES Candidate Conference*, 1999, available at http://www.counterpane.com/magenta-cryptanalysis.html

[7] A. Biryukov, D. Wagner, "Slide Attacks," *Fast Software Encryption, 6th International Workshop, FSE'99, Proceedings, Lecture Notes in Computer Science Vol. 1636, Springer-Verlag*, 1999.

[8] L. Knudsen, "Cryptanalysis of LOKI," *Advances in Cryptology, –ASIACRYPT'91, Lecture Notes in Computer Science Vol. 739, Springer-Verlag*, 1991.

[9] C. H. Meyer, S. M. Matyas, *Cryptography: A New Dimension in Coputer Data Security*, New York: John Wiley & Sons, 1982.

[10] J. Daemen, L. Knudsen, V. Rijmen, "The Block Cipher SQUARE," *Fast Software Encryption, 4th International Workshop, FSE'97, Proceedings, Lecture Notes in Computer Science Vol. 1267, Springer-Verlag*, 1997.

[11] J. Daemen, V. Rijmen, "AES Proposal: Rijndael," available at http://www.esat.kuleuven.ac.be/~rijmen/rijndael/index.html

[12] C. H. Lim, "A Revised Version of CRYPTON -CRYPTON V1.0," *Fast Software Encryption, 6th International Workshop, FSE'99, Proceedings, Lecture Notes in Computer Science Vol. 1636, Springer-Verlag*, 1999.

[13] L. Knudsen, T. Berson, "Truncated Differentials of SAFER," *Fast Software Encryption, third International Workshop, Proceedings, Lecture Notes in Computer Science Vol. 1039, Springer-Verlag*, 1999.

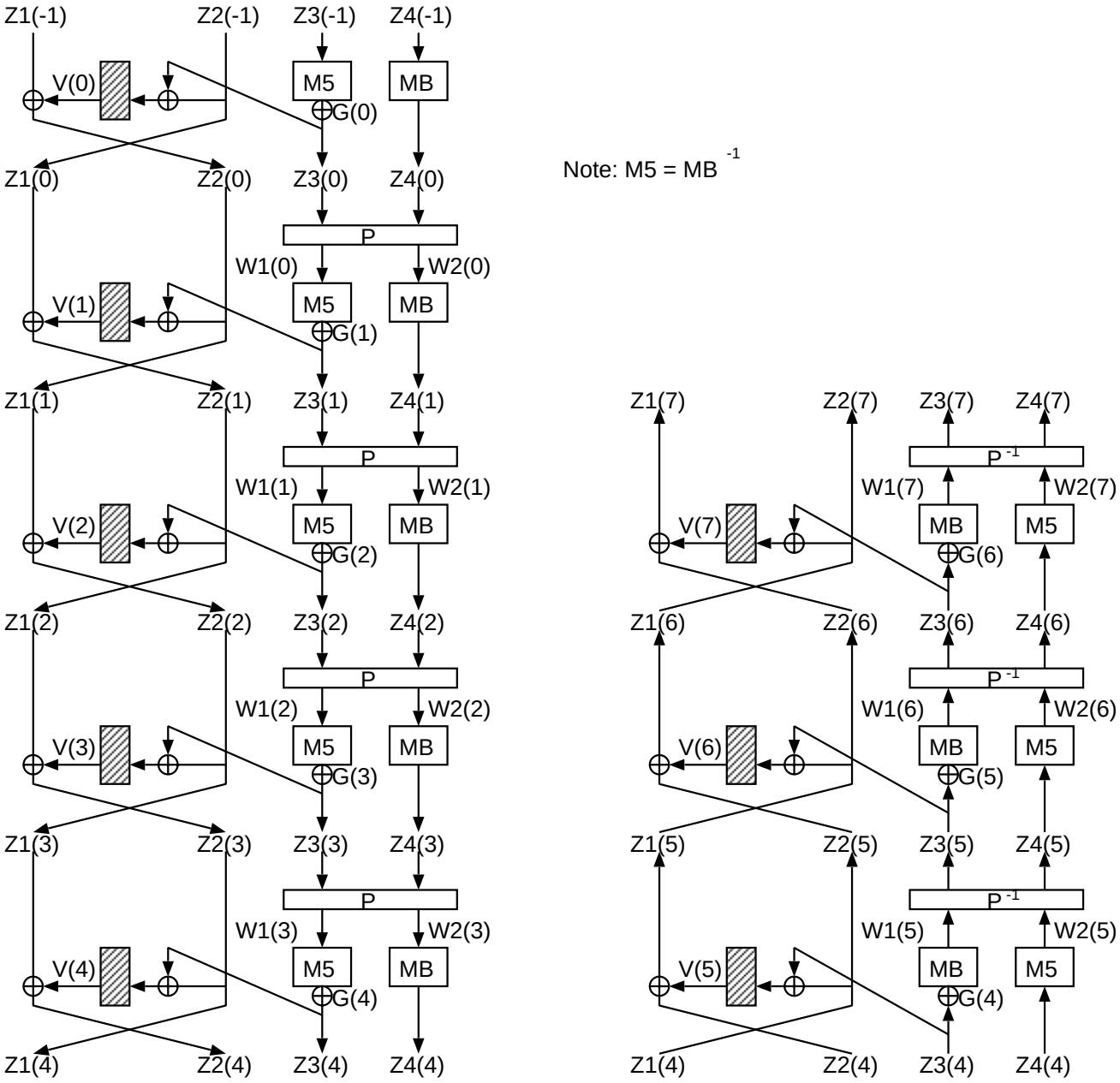

図 2: Intermediate keys' generation (whole structure)

表 2: Evaluated S box (Hierocrypt-L1)

0x07,	0xFC,	0x55,	0x70,	0x98,	0x8E,	0x84,	0x4E
0xBC,	0x75,	0xCE,	0x18,	0x02,	0xE9,	0x5D,	0x80
0x1C,	0x60,	0x78,	0x42,	0x9D,	0x2E,	0xF5,	0xE8
0xC6,	0x7A,	0x2F,	0xA4,	0xB2,	0x5F,	0x19,	0x87
0x0B,	0x9B,	0x9C,	0xD3,	0xC3,	0x77,	0x3D,	0x6F
0xB9,	0x2D,	0x4D,	0xF7,	0x8C,	0xA7,	0xAC,	0x17
0x3C,	0x5A,	0x41,	0xC9,	0x29,	0xED,	0xDE,	0x27
0x69,	0x30,	0x72,	0xA8,	0x95,	0x3E,	0xF9,	0xD8
0x21,	0x8B,	0x44,	0xD7,	0x11,	0x0D,	0x48,	0xFD
0x6A,	0x01,	0x57,	0xE5,	0xBD,	0x85,	0xEC,	0x1E
0x37,	0x9F,	0xB5,	0x9A,	0x7C,	0x09,	0xF1,	0xB1
0x94,	0x81,	0x82,	0x08,	0xFB,	0xC0,	0x51,	0x0F
0x61,	0x7F,	0x1A,	0x56,	0x96,	0x13,	0xC1,	0x67
0x99,	0x03,	0x5E,	0xB6,	0xCA,	0xFA,	0x9E,	0xDF
0xD6,	0x83,	0xCC,	0xA2,	0x12,	0x23,	0xB7,	0x65
0xD0,	0x39,	0x7D,	0x3B,	0xD5,	0xB0,	0xAF,	0x1F
0x06,	0xC8,	0x34,	0xC5,	0x1B,	0x79,	0x4B,	0x66
0xBF,	0x88,	0x4A,	0xC4,	0xEF,	0x58,	0x3F,	0x0A
0x2C,	0x73,	0xD1,	0xF8,	0x6B,	0xE6,	0x20,	0xB8
0x22,	0x43,	0xB3,	0x33,	0xE7,	0xF0,	0x71,	0x7E
0x52,	0x89,	0x47,	0x63,	0x0E,	0x6D,	0xE3,	0xBE
0x59,	0x64,	0xEE,	0xF6,	0x38,	0x5C,	0xF4,	0x5B
0x49,	0xD4,	0xE0,	0xF3,	0xBB,	0x54,	0x26,	0x2B
0x00,	0x86,	0x90,	0xFF,	0xFE,	0xA6,	0x7B,	0x05
0xAD,	0x68,	0xA1,	0x10,	0xEB,	0xC7,	0xE2,	0xF2
0x46,	0x8A,	0x6C,	0x14,	0x6E,	0xCF,	0x35,	0x45
0x50,	0xD2,	0x92,	0x74,	0x93,	0xE1,	0xDA,	0xAE
0xA9,	0x53,	0xE4,	0x40,	0xCD,	0xBA,	0x97,	0xA3
0x91,	0x31,	0x25,	0x76,	0x36,	0x32,	0x28,	0x3A
0x24,	0x4C,	0xDB,	0xD9,	0x8D,	0xDC,	0x62,	0x2A
0xEA,	0x15,	0xDD,	0xC2,	0xA5,	0x0C,	0x04,	0x1D
0x8F,	0xCB,	0xB4,	0x4F,	0x16,	0xAB,	0xAA,	0xA0

表 3: Partial interpolations of the S box

terms	deg	points	equation	points
2	1	8	$237+59\times x$	(56, 92, 93, 106, 158, 172, 227, 241)
3	2	9	$142+147\times x+81\times x^2$	(4, 38, 107, 136, 165, 176, 209, 241, 255)
3	2	9	$103+219\times x+191\times x^2$	(11, 14, 42, 62, 70, 100, 233, 243, 245)
3	2	9	$101+216\times x+239\times x^2$	(13, 40, 53, 55, 174, 232, 235, 249, 255)
3	2	9	$98+196\times x+34\times x^2$	(15, 122, 143, 170, 175, 210, 211, 219, 226)
3	2	9	$206+36\times x+205\times x^2$	(21, 44, 98, 117, 175, 196, 228, 238, 247)
3	2	9	$3+114\times x+139\times x^2$	(23, 63, 73, 122, 124, 131, 139, 150, 214)
3	2	9	$77+119\times x+33\times x^2$	(24, 75, 99, 107, 111, 134, 150, 201, 231)
3	2	9	$192+112\times x+124\times x^2$	(26, 60, 68, 113, 123, 133, 154, 199, 206)
3	2	9	$187+94\times x+61\times x^2$	(32, 46, 111, 153, 188, 200, 209, 217, 245)
3	2	9	$89+72\times x+16\times x^2$	(36, 53, 69, 78, 103, 120, 170, 242, 250)
3	2	9	$10+143\times x+109\times x^2$	(40, 63, 92, 94, 96, 150, 175, 186, 192)
3	2	9	$212+236\times x+211\times x^2$	(41, 71, 78, 121, 141, 143, 158, 171, 248)
3	2	9	$46+183\times x+148\times x^2$	(65, 73, 77, 79, 112, 143, 153, 194, 225)
4	3	13	$65+190\times x+101\times x^2+171\times x^3$	(21, 33, 35, 61, 77, 82, 90, 104, 171, 173, 190, 213, 246)