Hierocrypt-L1 の最大線形 / 差分確率 および最大線形 / 差分特性確率について

盛合 志帆

日本電信電話株式会社

2001 年 1 月 12 日

概要　本報告書は CRYPTREC にて公募された共通鍵ブロック暗号 Hierocrypt-L1 の安全性の詳細評価報告であり、 (1) ブロック暗号の検証評価 — (a) 最大線形 / 差分確率もしくは最大線形 / 差分特性確率について報告するものである。

Hierocrypt-L1 では入れ子型 SPN 構造を採用しており、その拡散層 (diffusion layer) として最大距離分離符号 (Maximum Distance Separable Code) に用いられる行列を利用している。このような暗号の active S-box 数の下限は 容易に評価できることが知られており、自己評価書ではこの方法により最大差分／線形特性確率の上限を評価している。 Hierocrypt-L1 においてこの評価方法は妥当であり、提案者が示している数値も正しいと判断できる。よって、 Hierocrypt-L1 は 2 段以上で 2^{-90} の最大差分／線形特性確率を超えないことが保証できる。

最大差分／線形確率については、 Hong らの示した結果を利用して、 Hierocrypt-L1 の部分構造についての最大差分／線形確率を評価することができる。自己評価書では、これを利用して Hierocrypt-L1 の最大差分／線形確率を評価している。この評価には一部、厳密ではないところがあったため、再評価を行なった。再評価の結果、鍵スケジュールに問題がなく、その結果各段に与えられる鍵が一様でランダムに分布していると仮定した場合、 Hierocrypt-L1 は 2 段, 3 段で最大差分／線形確率はそれぞれ 2^{-48} を超えないことが保証でき、 4 段で 2^{-72} を超えないことが示された。

1　評価の方針 (はじめに)

本稿は CRYPTREC にて公募した共通鍵ブロック暗号 Hierocrypt-L1 の安全性の詳細評価報告であり、 (1) ブロック暗号の検証評価　(a) 最大線形 / 差分確率もしくは最大線形 / 差分特性確率について報告する。

Hierocrypt-L1 では入れ子型 SPN 構造を採用しており、その拡散層 (diffusion layer) として最大距離分離符号 (Maximum Distance Separable Code) に用いられる行列 (以下 MDS 行列と記述する) を利用している。このような暗号の active S-box 数の下限は容易に評価できることが知られており [3]、自己評価書 [1, 2.1.3 章] ではこれを利用して最大差分／線形特性確率の上限を評価している。 Hierocrypt-L1 においてこの評価方法は妥当であり、提案者が示している数値も正しいと判断できる。

また、 Hong[4] らにより、 SPN 構造をもつ暗号で、 MDS 行列を拡散層に利用したもので、差分解読法および線形解読法に対する証明可能安全性を持つものを構成できることが示された。これを利用して、自己評価書 (2.1.4 章) では最大差分／線形確率の上限の評価を試みている。 2 段の Hierocrypt-3 の評価は妥当と考えられるが、 3 段以上の評価は厳密ではない。よって Hong[4] らの結果を 3 段以上の SPN 構造に拡張する定理を導き、これを用いて最大差分／線形確率のより厳密な評価を行なう。

2 自己評価書の記述内容の解説 (妥当性検証)

本章では 2.1 章で最大差分／線形特性確率の評価について、 2.2 章で最大差分／線形確率の評価に関する記述内容を解説する。

Hierocrypt-L1 の差分解読法に対する安全性評価と線形解読法に対する安全性評価は同様の手法で行なえることが知られているので、以下では主に最大差分特性確率及び最大差分確率の評価について説明し、最大線形特性確率及び最大線形確率の評価についての詳細な説明は省略する。

2.1 最大差分／線形特性確率の評価

Hierocrypt-L1 の S-box は 8 ビット入出力の置換テーブル (permutation) である。具体的な演算は $\mathrm{GF}(2^8)$ 上の冪乗演算 x^{247} の入出力ビットにアフィン変換を加えたものであるから、 S-box の最大差分確率 dp^S, 最大線形確率 lp^S はともに 2^{-6} である。

$$dp^S = lp^S = 2^{-6} \tag{1}$$

拡大 S-box XS は 4 並列の S-box 層, MDS 行列を利用した拡散層 MDS_{L}, 4 並列の S-box 層からなる。よって拡大 S-box XS が active(入力差分値が非零) であれば、拡大 S-box XS に含まれる 8 個の S-box のうち、 5 個の S-box が active となる。

Hierocrypt-L1 の “1 段” は 2 並列の拡大 S-box 層と MDS 行列を利用した拡散層 MDS_{H} からなる。従って、連続する 2 段に含まれる active S-box 数の最小値は $5{\times}3 = 15$ となる。よって、連続する 2 段の最大差分特性確率 DCP^{2R} は以下のように評価される。

$$DCP^{2R} \leq (dp^S)^{15} = (2^{-6})^{15} = 2^{-90} \tag{2}$$

同様に、最大線形特性確率についても、連続する 2 段の最大線形特性確率 LCP^{2R} は以下のように評価される。

$$LCP^{2R} \leq (lp^S)^{15} = (2^{-6})^{15} = 2^{-90} \tag{3}$$

よって、 Hierocrypt-L1 は 2 段以上で最大差分特性確率 2^{-90} および最大線形特性確率 2^{-90} をもつことが示される。

Hierocrypt-L1 の段数は 6 段であるので、最大差分特性確率および最大線形特性確率の観点からは十分なセキュリティマージンを有すると考えられる。

2.2 最大差分／線形確率の評価

Hierocrypt-L1 の最大差分／線形確率の評価については、 FSE2000 において Hong らの示した以下の定理 [4] が有用である。

定理 1 [4] n 並列の S-box 層, 拡散層 (P), n 並列の S-box 層を順につなげた SPS 構造について、拡散層のブランチ数 [2, 3] が $n+1$ であるとする。拡大鍵は独立で一様に分布している乱数であり、入力データに排他的論理和がとられているとする。この時、 S-box の最大差分確率を dp、最大差分確率を lp とすると、この SPS 構造の最大差分／線形確率はそれぞれ dp^n, lp^n を超えない。

Hierocrypt-L1 の拡大 S-box (XS) は定理 1の SPS 構造そのものであるから、定理 1より、拡大 S-box の最大差分／線形確率は以下のように評価できる。

$$dp^{XS} \leq (dp^S)^4 = (2^{-6})^4 = 2^{-24} \tag{4}$$

$$lp^{XS} \leq (lp^S)^4 = (2^{-6})^4 = 2^{-24} \tag{5}$$

次に 2 段の Hierocrypt-L1 を考える。 2 段目の MDS_{H} は線形変換であり、差分／線形確率に影響を与えないので、 2 段の Hierocrypt-L1 の最大差分／線形確率 DP^{2R}, LP^{2R} も定理 1を利用して以下のように評価できる。

$$DP^{2R} \leq (dp^{XS})^2 = (2^{-24})^2 = 2^{-48} \tag{6}$$

$$LP^{2R} \leq (lp^{XS})^2 = (2^{-24})^2 = 2^{-48} \tag{7}$$

よって、鍵スケジュールに問題がなく、その結果各段に与えられる鍵が一様でランダムに分布していると仮定した場合、 Hierocrypt-L1 は 2 段で最大差分／線形確率はそれぞれ 2^{-48} を超えないことが保証できる。

次に 3 段の Hierocrypt-L1 を考える。 1 段追加して 3 段とした時、最悪でも追加した段の拡大 S-box (XS) の 1 個は active であるので、その分の最大差分／線形確率は

式 (4), (5) より 2^{-24} であるから[1]、

$$DP^{3R} \leq DP^{2R} \times 2^{-24} = 2^{-72} \tag{8}$$

$$LP^{3R} \leq LP^{2R} \times 2^{-24} = 2^{-72} \tag{9}$$

と評価されている。しかしこの最大差分／線形確率の評価は、2 段目の拡大 S-box (XS) の全ての (可能性のある) 出力差分値についての総和をとって計算していないという点で、厳密な評価ではない。

さらに 4 段の Hierocrypt-L1 については 2 段の Hierocrypt-L1 を 2 つつなげたものとみなし、以下のように評価しているにすぎない。

$$DP^{4R} \leq (DP^{2R})^2 = 2^{-96} \tag{10}$$

$$LP^{4R} \leq (LP^{2R})^2 = 2^{-96} \tag{11}$$

よって、3 段以上の Hierocrypt-L1 の最大差分／線形確率については次章で再評価を行なう。

3　再評価

Hong らにより示された定理 1[4] を 3 段以上の SPN 構造に拡張する定理を導き、これを用いて最大差分／線形確率のより厳密な評価を行なう。

定理 2 n 並列の S-box 層, 拡散層 (P) を順につなげた SPN 構造について、拡散層のブランチ数 [2, 3] が $n+1$ とする。拡大鍵は独立で一様に分布している乱数であり、入力データに排他的論理和がとられているとする。この時、 S-box の最大差分確率を dp とし、 k を正の整数 k とすると、このような $2k$ 段, $2k+1$ 段 SPN 構造の最大差分確率 DP^{2k}, DP^{2k+1} はともに $dp^{k(n-1)+1}$ を超えない。同様に S-box の最大線形確率を lp とすると、 $2k$ 段, $2k$+1 段 SPN 構造の最大線形確率 LP^{2k}, LP^{2k+1} はともに $lp^{k(n-1)+1}$ を超えない。

定理 2より、 Hierocrypt-L1 は 3 段で最大差分／線形確率は 2^{-48} に達し、 4 段での最大差分／線形確率は 2^{-72} に達することが保証できる。

4　再評価結果

自己評価書に記述されている最大差分／線形特性確率は妥当であると判断できるが、最大差分／線形確率については再評価の必要性があると考え、再評価を行なった。その結果、自己評価書においては、 Hierocrypt-L1 は 3 段で最大差分／線形確率 2^{-72}、4 段で 2^{-96} と評価されていたが、再評価により、 3 段で最大差分／線形確率 2^{-48}、 4 段で 2^{-72} であることが分かった。

[1] 自己評価書では 2^{-12} となっているが、ここに関しては単純な間違いとみなす。

表 1: Hierocrypt-L1 の最大差分／線形確率の再評価結果

段数	最大差分／線形確率	自己評価書の値
2	2^{-48}	2^{-48}
3	2^{-48}	2^{-72*}
4	2^{-72}	2^{-96}

* 2^{-60} と書かれているが、単なる書き間違いとみなす。

5 まとめ

CRYPTREC にて公募された共通鍵ブロック暗号 Hierocrypt-L1 の安全性の詳細評価報告として、(1) ブロック暗号の検証評価 — (a) 最大線形 / 差分確率もしくは最大線形 / 差分特性確率について報告した。

最大差分／線形特性確率の上限については自己評価書において提案者が示している評価方法および数値も妥当であると考える。よって、 Hierocrypt-L1 は 2 段以上で 2^{-90} の最大差分／線形特性確率を超えないことが示される。

最大差分／線形確率については、自己評価書の評価方法およびその結果には一部、厳密ではないところがあったため、再評価を行なった。再評価の結果、鍵スケジュールに問題がなく、その結果各段に与えられる鍵が一様でランダムに分布していると仮定した場合、 Hierocrypt-L1 は 2 段, 3 段で最大差分／線形確率はそれぞれ 2^{-48} を超えないことが保証でき、 4 段で 2^{-72} を超えないことが示された。

なお、 Hierocrypt-L1 が十分に小さい最大線形 / 差分確率および最大線形 / 差分特性確率をもつことが示されたが、これは差分解読法および線形解読法一般に対する安全性を保証するものではない [5, 6] ことに注意が必要である。

参考文献

[1] 「自己評価書:Hierocrypt-L1」株式会社 東芝, 平成 12 年 7 月 27 日.

[2] Joan Daemen, “Cipher and hash function design strategies based on linear and differential cryptanalysis,” Doctoral Dissertation, March 1995, K.U.Leuven.

[3] Joan Daemen, Lars Knudsen and Vincent Rijmen “The Block Cipher SQUARE,” Fast Software Encryption, FSE’97, Lecture Notes in Computer Science 1267, pp.54–68, Springer-Verlag, 1997.

[4] Seokhie Hong, Sanjin Lee, Jongin Lim, Jaechul Sung, Donghyeon Cheon, “Provable Security against Differential and Linear Cryptanalysis for the SPN Struc-

ture" in preproceedings of Fast Software Encryption Workshop 2000, 10–12 April, 2000.

[5] David Wagner, "The boomerang attack," Fast Software Encryption Workshop 99, FSE'99, Lecture Notes in Computer Science 1636, pp.156–170, Springer-Verlag, 1999.

[6] Eli Biham, Alex Biryukov, Adi Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials," Advances in Cryptology — EUROCRYPT'99, Lecture Notes in Computer Science 1592, Springer-Verlag, 1992, pp.12–23.