CIPHERUNICORN-E の最大差分特性確率および最大線形特性確率について

評価者：NTT（神田　雅透）

2001 年 1 月 12 日

1　はじめに

1.1　CIPHERUNICORN-E の概要

CIPHERUNICORN-E は、1998 年に日本電気株式会社より提案された 64 ビットブロック暗号であり、1998 年暗号と情報セキュリティシンポジウム SCIS'98 [9] にて学会発表されている。

CIPHERUNICORN-E の基本構造は、データブロック長 64 ビット、鍵長 128 ビットの 16 段 Feistel 構造であり、さらに 2 段ごとに L 関数と呼ぶ鍵依存線形変換関数が挿入されている。暗号技術仕様書によれば、初等統計評価[1]により優れた特性を示すラウンド関数を構成することを主たる設計方針[2]として採用している。設計者らは、差分解読法や線形解読法に対する弱点がラウンド関数における攪拌の偏りに起因するとの考えのもと、以下の 5 項目を初等統計評価の対象とし、これらの評価項目において “ラウンド関数での攪拌の偏り（高い確率で成立する相関関係）が検出できない構造” を “強い暗号である” と主張している。また、CIPHERUNICORN-E で利用しているラウンド関数に攪拌の偏りが現れないことを自社の暗号評価支援システム [10] で確認したとしている。

[**入出力間関連**] 入力ビット（対象：1 ビットまたは 2 ビット）と出力ビット（対象：1 ビット）との間の相関関係

[**出力間関連**] 出力ビット間（対象：2 ビット）の相関関係

[**データアバランシュ効果**] 入力ビットの変化（対象：1 ビットまたは 2 ビット）と出力ビットの変化（対象：1 ビット）との間の相関関係

[**鍵アバランシュ効果**] 鍵ビットの変化（対象：1 ビットまたは 2 ビット）と出力ビットの変化（対象：1 ビット）との間の相関関係

[**ビットバランス**] 出力ビット（対象：1 ビット）の 0/1 頻度分布

なお、設計方針として、初等統計評価以外の項目、特に実装面での性能などを考慮しているようには思われない。

1.2　差分解読法及び線形解読法に対する安全性自己評価に関する記述

差分解読法及び線形解読法に対する自己評価は、自己評価書の第 3.1 節（線形解読）及び第 3.2 節（差分解読）に記述されている[3]。本レポートでは、自己評価書の記述内容について、その妥当性を検証する。なお、CIPHERUNICORN-E に関連する第三者評価は、評価者の知る限り、存在していない。

[1] FEAL の設計方針 [8] に採用された安全性評価手法と同様の指標である。
[2] L 関数の設計方針については特に記述が見当たらない。
[3] さらに関連するところでは第 3.5 節、第 3.6 節、第 3.7 節、第 3.10 節がある。

1.3 差分解読法や線形解読法に対する安全性指標

差分解読法や線形解読法に対する安全性を示す指標として以下の 4 つが知られている。いずれの指標を用いて評価したのかによって、差分解読法や線形解読法に対する安全性評価の厳密性が異なることに注意されたい。最近では、以下に示す、“provable security” もしくは “practical security” を備えた暗号が望ましいとされている。

最大平均差分確率／最大平均線形確率 差分解読法や線形解読法に対する真の安全性を示す指標 [3, 5]。これらの確率が十分に小さいことが保証されれば、差分解読法や線形解読法に対して理論的に安全であることが証明される。しかし、全数探索並みの計算量が必要であるため、暗号全体についてこれらの確率を算出することは極めて困難である。

最大差分特性確率／最大線形特性確率 攻撃者が、計算機などによって、差分解読法や線形解読法により暗号を実際に解読する場合の安全性を示す指標 [1, 4]。これらの確率は計算機実験などにより算出できることが多い。しかし、計算機能力の向上や探索アルゴリズムの改良等によって、これらの確率が変わることがあるので、評価時点での差分解読法や線形解読法に対する安全性の限界を示しているにすぎないと考えるべきである。したがって、これらの確率が十分に小さいことが差分解読法や線形解読法に対して安全であることの必要条件であって、十分条件ではない。

最大平均差分確率／最大平均線形確率の上界値 最大平均差分確率や最大平均線形確率の上界値を理論的に保証したことによって安全性を示す指標 [6]。これらの値が十分に小さいことが示されるのであれば、結果として最大平均差分確率や最大平均線形確率が十分に小さいことが保証される。この指標により差分解読法や線形解読法に対して安全であると示すことを “（差分解読法や線形解読法に対する）証明可能安全 (provable security)” という。

最大差分特性確率／最大線形特性確率の上界値 最大差分特性確率／最大線形特性確率の上界値を理論的に保証したことによって安全性を示す指標 [2, 7]。これらの値と最大平均差分確率や最大平均線形確率との間に理論的な関係はないため、これらの値が十分に小さいからといって、直接的に最大平均差分確率や最大平均線形確率が十分に小さいことが保証されるわけではない。しかし、実際の暗号の多くは、これらの値と最大平均差分確率や最大平均線形確率の値が極端に大きく離れているとは考えにくい。したがって、この指標により差分解読法や線形解読法に対して安全であると示すことを “（差分解読法や線形解読法に対する）実用的証明可能安全 (practical security)” という。実用的証明可能安全であることを証明するためには、64 ビットブロック暗号の場合、最大差分特性確率及び最大線形特性確率の上界値が 2^{-64} 以下となることが必要であるとされている。

2 自己評価書の妥当性検証

2.1 提案者の評価モデル

CIPHERUNICORN-E のラウンド関数では、s-box を主体とする T 関数、32 ビット算術加算、シフトと 32 ビット算術加算からなる Y 関数、及び排他的論理和からなる K 関数の 4 つの構成要素からなる。また、内部構造では、これら 4 つの構成要素を用いるうえに、データ依存関数として構成されている。このため、32 ビット入出力のラウンド関数内に閉じたとしても、差分解読法や線形解読法に対する厳密な評価は困難である。そこで、提案者は、以下の仮定に基づいた変形ラウンド関数 mF 関数を利用して評価を行っている。

[**仮定 1**] 32 ビット算術加算は排他的論理和に置き換える

[**仮定 2**] Y 関数は、32 ビットデータの上位 1 バイトへ入力ビットを集めるだけの処理とみなす

また、差分解読法や線形解読法に対する安全性評価においては L 関数を除いて考えていると思われる。L 関数の解析は第 3.10 節で若干述べられている。

2.2 評価モデルの妥当性

ラウンド関数の構造が複雑である場合、解析が容易な演算に置き換えて差分解読法や線形解読法に対する安全性評価を行うことが多々ある。最も多いのは算術加算を排他的論理和に置き換えるやり方であり、これにより差分特性や線形表現を見つけやすくする効果がある。このような変換を行った変形ラウンド関数についての安全性評価は、近似的モデルの結果として、また安全性評価の初期段階の結果としてそれなりに有用であると考えられている。その意味で、**仮定 1 は妥当な置き換えである**。

しかし、**以下の 4 点について、評価者は評価モデルの妥当性を確認できない**。これらの点については、提案者を含めてさらなる検討が必要である。

[**仮定 2 の置き換え**] 仮定 2 の置き換えについては、その妥当性の根拠を自己評価書からは見出せない。評価者の知識では、なぜこのような置き換えを仮定したのか、また、その置き換えがどのような合理的な根拠をもとにしたものであるのかを理解出来ない。少なくとも、**仮定 1 ほど自明な置き換えであるとは考えられないので、提案者はその理由を説明すべき**であると考える。

[**T 関数での s-box の表記**] 仕様書上は 4 つの 8 ビット入力 8 ビット出力の s-box として構成されているが、**T 関数の構成からは 8 ビット入力 32 ビット出力の s-box と解釈すべき**である。しかし、既存解読法に対する安全性評価について、8 ビット入力 32 ビット出力の s-box ではなく、8 ビット入力 8 ビット出力の s-box（の組み合わせ）として評価を行っているように思われる記述が見られる。

[**T 関数連結時の評価**] 4 つの T 関数における特性確率の評価に際し、提案者はそれぞれの T 関数ごとの特性確率の積とみなしている。すなわち、

$$(T[0], T[1], T[2], T[3] \text{の特性確率}) = (T[0] \text{の特性確率}) \times (T[1] \text{の特性確率}) \times (T[2] \text{の特性確率}) \times (T[3] \text{の特性確率}) \quad (1)$$

としている。おそらく、s-box を用いた関数での特性確率の算出において、一般にそれぞれの s-box ごとの特性確率の積として表現されることから解釈したものと考えられる。

しかし、**CIPHERUNICORN-E に関していえば、この見積もり方法に理論的な誤りを含んでいることに注意**を要する。なぜならば、特性確率を s-box ごとの積として表現するためには、s-box で構成される関数がマルコフ性を満たしている[4]という仮定がある。関数がマルコフ性を満たすとは、簡単にいうと、関数を構成する各 s-box での振る舞いが互いに独立であるとみなしてよいことを意味する。このために、一般には、攻撃者にとって未知の値である拡大鍵を s-box の直前に挿入することによって、見かけ上、攻撃者が s-box 間の相関を正確に予測することを困難にし、実効的に各 s-box での振る舞いが互いに独立とみなせるように設計される。これに対し、CIPHERUNICORN-E では、T[0]、T[1]、T[2]、T[3] のそれぞれの T 関数の間に拡大鍵が挿入されていないため、それぞれの関数が独立関係にはない、すなわち T[0] への入力が決まった時点で、拡大鍵がわからなくても、一意に T[3] からの出力が決まるような構成をしている。つまり、T 関数の連結のところでは実効的にもマルコフ性を満たしていないことになり、一般には (1) 式が成立しないと考えるのが妥当である。このため、マルコフ性を満たしていないことを考慮した場合、どの程度評価結果が変わるのかについて更なる検討を行う必要がある。

[**L 関数の評価**] L 関数は、64 ビットの入力データ列を別の 64 ビットのデータ列に変換する鍵依存線形変換である。具体的には、この関数はビット演算によるものなので、第 i ビット入力データ $(X_{L_{(i)}}, X_{R_{(i)}})$ を以下のように出力データ $(Z_{L_{(i)}}, Z_{R_{(i)}})$ へ変換する。

$$\begin{aligned} Z_{L_{(i)}} &= X_{L_{(i)}} \cap (\overline{LK_{(i)}[0] \cap LK_{(i)}[1]}) \oplus X_{R_{(i)}} \cap LK_{(i)}[1] \\ Z_{R_{(i)}} &= X_{R_{(i)}} \cap (\overline{LK_{(i)}[0] \cap LK_{(i)}[1]}) \oplus X_{L_{(i)}} \cap LK_{(i)}[1] \end{aligned}$$

ここで、LK は L 関数への拡大鍵を表す。したがって、$(X_{L_{(i)}}, X_{R_{(i)}})$ に関して、L 関数は以下のように $(Z_{L_{(i)}}, Z_{R_{(i)}})$ を出力することになる。

[4] 理論的にはマルコフ性を満たしていなくても、実効的にマルコフ性を満たしていると解釈してよい場合を含む。

$LK_{(i)}[0]$	$LK_{(i)}[1]$	$Z_{L_{(i)}}$	$Z_{R_{(i)}}$	効果
どちらでもよい	0	$X_{L_{(i)}}$	$X_{R_{(i)}}$	効果なし
0	1	$X_{L_{(i)}} \oplus X_{R_{(i)}}$	$X_{L_{(i)}} \oplus X_{R_{(i)}}$	左右同じデータに変換
1	1	$X_{R_{(i)}}$	$X_{L_{(i)}}$	データの入れ替え (swap)

Feistel 暗号の場合、各段ごとに左右のデータ入れ替え (swap) が起こらないとラウンド関数の実効段数が減少することが知られている。L 関数の直後に左右のデータ入れ替えが行われるため、L 関数内でデータの入れ替えが起きると、結果として swap されないことになり、ラウンド関数の実効段数が減少することになる。そこで、提案者は、自己評価書の中で、拡大鍵 64 ビット全てが 1 となるような場合、完全に左右のデータが入れ替り、結果として F 関数の実効段数が少なくなるので、そのような拡大鍵を弱鍵であると呼んでいる（第 3.10 節）。さらに、そのような拡大鍵が連続して発生する確率はきわめて小さいとしている。

しかし、このように、L 関数がビット単位の演算である以上、一部分が（例えばバイト単位で）入れ替わっただけでも F 関数の実効段数が少なくなる場合も起こりうると思われる。つまり、自己評価書で記述されているような拡大鍵 64 ビット全てが 1 となるような場合だけが弱鍵になるのではなく、それ以外の場合の弱鍵も存在するのではないかと予測する。したがって、自己評価書の記載内容では、**1 種類の弱鍵についてのみ述べているだけであるので、自己評価として不十分あるように思われる。逆に、提案者がその内容で十分であるとするならば、その合理的理由を明記すべき**である。

2.3 線形解読法に対する安全性評価

自己評価書の第 3.1 節に線形解読法に対する安全性評価が記載されている。それによれば、変形ラウンド関数での最大線形特性確率が $2^{-63.9}$、15 段での最大線形特性確率の上界値が $2^{-447.30}$ であり、線形解読法に対しては十分に安全であると述べている。

しかし、結論から言うと、**記載内容は完全に誤りであり、信用できないものであるといわざるを得ない**。以下に、その理由を示す。

[**理由 1**] 32 ビットラウンド関数でありながら、変形ラウンド関数 mF 関数での最大線形特性確率 LP_{mF} が $LP_{mF} = 2^{-63.90}$ となることはありえない。仮に、ラウンド関数での線形特性が一様分布になることを示したかったのだったとしても、$LP_{mF} = 2^{-32}$ とおくのが常識である。したがって、$LP_{mF} = 2^{-63.90}$ を利用して求めた最大線形特性確率 $LCP = 2^{-447.30}$ は全く信用できない。

[**理由 2**] ラウンド関数内での線形マスク値の経路を求めるときに、s-box を 8 ビット入力 8 ビット出力のままで経路探索をしているように見受けられる。その根拠として、S3 がそれ以外の s-box から独立した s-box であるかのような表記になっているためである。しかし、第 2.2節でも述べたように、本来 T 関数は 8 ビット入力 32 ビット出力であると考えるべきであり、S3 もそれ以外の s-box と組み合わせた（連結した）評価をすべきである。その理由として、自己評価書の表 3.1 でも示しているように、s-box 単体では最大線形確率が 2^{-6} になるように設計されていても、他の s-box と連結した評価では 2^{-3} 程度になっている。例えば、3 つの s-box (S0, S1, S2) を連結した場合、最大線形確率が $2^{-2.6}$ になることが記載されている。この類推からすれば、8 ビット入力 32 ビット出力とした場合の最大線形確率はさらに大きくなる可能性さえ否定できない。したがって、S3 を独立した s-box であるかのような特性確率の算出方法は誤りである。

本レポートでは、経路探索のための時間がなかったので、ラウンド関数での最大線形特性確率が実際どの程度になるのかまでは検討できなかった。しかし、**自己評価書の安全性評価が誤りとはいえ、CIPHERUNICORN-E の段数が 16 段であり、またおそらくはラウンド関数での最大線形特性確率が $2^{-9.2}$ よりも小さいであろうと思われるので、線形解読法に対して安全であろう**といえ、実用に耐えうると期待される。なぜなら、ラウンド関数での最大線形特性確率が $2^{-9.2}$ よりも小さければ、以下に示す定理により、15 段での最大線形特性確率の上界値は $2^{-64.4}$ となり、線形解読法に対して安全となるためである。

定理 1（文献 [2]）ラウンド関数での最大線形特性確率を p_F^* とする。このとき、R 段 Feistel 暗号での最大線形特性確率の上界値は $(p_F^*)^r$（$R = 2r, 2r+1$）で表される。

ただし、第 2.2節で示した問題点があることや、構造が複雑でありどこまで近似が正しく出来ているかはよくわからないこと等を考慮すると、現在主流の暗号設計指針に照らし合わせたときに、セキュリティマージンがどの程度になるのかを見積もることは現時点では困難である。

2.4 差分解読に対する安全性評価

自己評価書の第 3.2 節に差分解読法に対する安全性評価が記載されている。それによれば、変形ラウンド関数での最大差分特性確率が 2^{-12}、15 段での最大差分特性確率の上界値が 2^{-84} であり、差分解読法に対しては十分に安全であると述べている。第 2.2節で示した問題点があるものの、おおむね**自己評価書に記載されている内容は妥当**であると考えられる。

なお、自己評価書では変形ラウンド関数での最大差分特性確率 DP_{mF} を求めるときに、$DP_{mF} = (2^{-6})^2 = 2^{-12}$ としている。この 2^{-6} は 8 ビット入力 8 ビット出力 s-box での最大差分確率から引用したものと思われるが、実際には 8 ビット入力 32 ビット出力 s-box として考えるほうが妥当であるので、最大差分確率は 2^{-7} と置くほうがよいと考えられる。したがって、$DP_{mF} = 2^{-14}$ となるので、以下の定理により、15 段での最大差分特性確率は 2^{-98} 以下になる。

定理 2（文献 [2]）ラウンド関数での最大差分特性確率を p_F^* とする。このとき、R 段 Feistel 暗号での最大差分特性確率の上界値は $(p_F^*)^r$（$R = 2r, 2r+1$）で表される。

この結果から、自己評価書に記載された結果よりも若干安全性が高いのではないかと期待される。ゆえに、**差分解読法に対して安全**であるという提案者の主張は妥当である。

3 まとめ

本レポートでは、自己評価書の記述内容について、その妥当性を検証した。

CIPHERUNICORN-E では、差分解読法や線形解読法に対する安全性評価が（比較的容易に）できるような構造を設計時点で選択して暗号を構成するという現在主流とされる暗号設計指針とは異なり、初等統計評価により優れた特性を示すラウンド関数を構成することを主たる設計方針としている。そのため、最近の暗号としては珍しいほどラウンド関数の構成が複雑となり、差分解読法や線形解読法に対する安全性評価がどこまで正確に行われているのかよくわからないところがある。しかも、第 2.2節で述べたように近似評価モデルでの妥当性に関して、その正当性が確認できない点があるなど評価モデル自体の信頼性にも一抹の不安が残る。また、自己評価書の線形解読法に対する安全性評価（第 3.1 節）は完全に誤りである。

以上の点を考慮すると、**自己評価書の安全性評価に対する信頼性は、少なくとも学術的にはあまり高くない**といわざるを得ない。しかし、幸いにして、**CIPHERUNICORN-E の段数は 16 段であるので、差分解読法や線形解読法に対しておそらく安全であろう**と期待できる。なお、これらの結果からは、現在主流の暗号設計指針に照らし合わせた場合に、どれだけのセキュリティマージンがあるかを見積もることはかなり困難であるが、**学術的な意味においてセキュリティマージンが高いとは思われない**。

念のため付け加えるが、初等統計評価における入出力間関連及び出力間関連の特性は、線形解読法における線形マスク値のハミング重みを制限したときの特性と一致する。また、データアバランシュ効果の特性は、差分解読法における差分値のハミング重みを制限したときの特性と一致する。このことは、**初等統計評価が、差分解読法や線形解読法に対する特性の一部分だけを切り出した安全性評価のことと考えることが出来る**。したがって、差分解読法や線形解読法に対して安全であるならば、初等統計評価においても高い確率で成立する相関関係が検出できないことを意味する。しかし、その逆、すなわち、初等統計評価において高い確率で成立する相関関係が検出できないといって、そのことから差分解読法や線形解読法に対して安全であるとは直接的にはいえないことに注意を要する。

参考文献

[1] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," Springer-Verlag, 1993. (The extended abstruct appeared at CRYPTO'90 and Journal of Cryptology, Vol.4, No.1, 1991)

[2] L. R. Knudsen, "Practically secure Feistel ciphers," *Fast Software Encryption — Cambridge Security Workshop*, LNCS **809**, pp.211-222, 1994.

[3] X. Lai, J. L. Massy, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," *Advances in Cryptology — EUROCRYPT'91*, LNCS **547**, pp.17–38, 1991.

[4] M. Matsui, "Linear Cryptanalysis Method for DES cipher," *Advances in Cryptology — EUROCRYPT'93*, LNCS **765**, pp.386–397, 1994.

[5] K. Nyberg, "Linear Approximation of Block Ciphers," *Advances in Cryptology — EUROCRYPT'94*, LNCS **950**, pp.439–444, 1991.

[6] K. Nyberg and L. R. Knudsen, "Provable Security against a Differential Attack," *Journal of Cryptology*, Vol.8, No.1, pp.27–37, 1995.

[7] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. DcWin, "The Cipher SHARK," *Fast Software Encryption — Third International Workshop*, LNCS **1039**, pp.99–112, 1996.

[8] A. Shimizu and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL," *Advances in Cryptology — EUROCRYPT'87*, LNCS **304**, pp.267–280, 1988.

[9] 角尾幸保、久保博靖、宮内宏、中村勝洋、"統計的手法により安全性が評価された暗号," *1998* 年暗号と情報セキュリティシンポジウム *SCIS'98*, 4.2.B, 1998.

[10] 角尾幸保、太田良二、宮内宏、中村勝洋、"分散型暗号強度評価支援システム," *2000* 年暗号と情報セキュリティシンポジウム *SCIS2000*, A53, 2000.