CIPHERUNICORN-A 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-A の概要

CIPHERUNICORN-A は、2000 年に日本電気株式会社より提案された 128 ビットブロック暗号であり、2000 年暗号と情報セキュリティシンポジウム SCIS2000 [10] にて学会発表されている。

CIPHERUNICORN-A の基本構造は、データブロック長 128 ビット、鍵長 128/192/256 ビットの 16 段 Feistel 構造である。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-A 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 [11] 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[2]。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-A 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 [9] に採用された安全性評価手法と同様の指標である。
[2] さらに関連するところでは第 3.5 節、第 3.6 節、第 3.7 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 [4, 6]。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, 5]。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 [7]。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 [3, 8]。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-A のラウンド関数は、64 ビット入出力の関数であり、s-box を主体とする T 関数、32 ビット算術乗算、32 ビット算術加算、ならびにローテーションと排他的論理和からなる A3 関数により構成された、かなり複雑な構造であるため、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が困難である。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 関数を利用して安全性評価を行っている。

[**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**] 32 ビット算術乗算は、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

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 3 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**] 本流処理部では T 関数が 10 個連結しており、また一時鍵生成処理部でも T 関数が 6 個連結している。これらの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。これは、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-A 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[3]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-A では、T 関数の間には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、すなわち最初の T_0 関数への入力が決まった時点で、本流処理部では最後の T_3 関数（ならびに K が特定できるなら最後の T_K 関数）からの出力が、また一時鍵生成部では最後の T_1 関数からの出力が、拡大鍵がわからなくても、一意に決まるような構成をしている。したがって、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るので、各々の T 関数での特性確率が積の形で全体の特性確率を表現することは一般には正しく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。

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 $2^{-22.47}$、15 段での最大線形特性確率の上界値が $2^{-157.29}$ 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、**記載内容の正当性を確認できない**といわざるを得ない。以下に、その理由を示す。

[**理由 1**] 自己評価書の図 3.2 に最大線形特性確率が最大となるケースが示されているが、なぜこのケースがありうるのか理解できない。評価者の理解では、図中の太線が非零線形マスク値を表しているように思われる。この理解が正しければ、A3 関数の出力側の線形マスク値は最上位バイトのみが非零であるのに対し、入力側の線形マスク値は下位 3 バイトが非零となっていることになる。しかし、A3 関数は $Y = X \oplus (X <<< 23) \oplus (X <<< 41)$ であるので、X の下位 3 バイトが非零であるならば、Y の最上位バイトのみが非零となることはありえないはずである。この矛盾点が解消されない限り、提案者の主張には同意できない。

[3] 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。

[**理由 2**] 提案者は、バイト単位での線形マスク値がゼロか非零かだけで区別する truncated linear mask によって線形マスク値の探索を行っているように思われる。さて、自己評価書の図 3.2 のケースから類推すると、truncated linear mask の探索において、非零 truncated linear mask 同士の排他的論理和の結果はゼロ truncated linear mask になると仮定しているように見える。これは、おそらく、非零 truncated linear mask 同士の排他的論理和の結果の扱いについて、ゼロ truncated linear mask になると仮定する場合が多いことに起因しているのではないかと推測する。しかし、非零 truncated linear mask 同士の排他的論理和の結果をゼロ truncated linear mask になると仮定するのは、一般に、これによって active s-box の個数を減らせるからである。したがって、以下の理由により、CIPHERUNICORN-A にこの仮定を適用することは適切ではない。

- 非零 truncated linear mask 同士の排他的論理和の結果がゼロ truncated linear mask になる確率はおおよそ 2^{-8} であり、ほとんどの場合非零 truncated linear mask となるはずである。
- CIPHERUNICORN-A の T 関数は、その構成上、8 ビット入力 32 ビット出力の s-box であると考えるべきである。このように出力側のビット数が入力側のビット数よりも多い s-box では、出力マスク値のハミング重みが大きくなるほど、つまり非零の truncated linear mask が増えるほど線形特性確率が大きくなる傾向にある。事実、このことは、自己評価書の表 3.1 の結果によって確認されている。
- T 関数には、4 つの truncated linear mask が同時に入力されることになるので、仮に一つがゼロ truncated linear mask としても、ほかの 3 つの truncated linear mask もゼロでない限り、active s-box の個数が減ることはない。

以上の理由により、T 関数に入力される 4 つの truncated linear mask が全てゼロにならないのであれば、むしろ 4 つとも非零の 4 つの truncated linear mask となるほうが最大線形特性確率を求める上で有効である。したがって、非零 truncated linear mask 同士の排他的論理和の結果は非零 truncated linear mask になると仮定するほうがむしろ妥当である。つまり、自己評価書の図 3.2 中の一時鍵生成部での最上位バイトも非零 truncated linear mask のままであると考えるべきである。この場合、提案者の評価式に従って変形ラウンド関数 mF 関数の最大線形特性確率 LP_{mF} を求めたとしても、$LP_{mF} = (2^{-2.71})^7 \times 2^{-2.39} = 2^{-21.36}$ となり、提案者の結果よりも大きな最大線形特性確率となる。

以上のことより、**自己評価書に記載の内容は、誤りであるとまでは断定しないものの、信ずるに足る評価結果であるとも思えない**。したがって、評価者は、**提案者の評価結果のみをもって、CIPHERUNICORN-A が線形解読法に対して十分に安全であるとの主張には同意できない**。

一方、現在主流となっている暗号設計指針では、以下の定理によって最大線形特性確率の上界値を評価することがある。

定理 1（文献 [3]） 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。

これを CIPHERUNICORN-A の仕様を当てはめると、15 段での最大線形特性確率の上界値が 2^{-128} となるためには、ラウンド関数での最大線形特性確率が $2^{-18.29}$ 以下であることが必要になる。

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、信憑性が高いとは思えない提案者の自己評価でさえ変形ラウンド関数での最大線形特性確率が $2^{-22.47}$ としていることから、より正確な評価を行った結果、ラウンド関数での最大線形特性確率が $2^{-18.29}$ よりも大きくなる可能性は否定できない。

以上の点ならびに第 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、現状の評価結果レベルでは、CIPHERUNICORN-A が**実用上の使用に関して線形解読法に対して安全であると期待されるが、学術的な安全性評価の観点からは線形解読法に対して安全であるとはいえない**といわざるを得ない。したがって、全体を通じて、**提案者による線形解読法に対する安全性自己評価結果には同意できない**。

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、15 段での最大差分特性確率の上界値を 2^{-120} であると提案者は主張している。

しかし、結論から言うと、**記載内容の正当性を確認できない**といわざるを得ない。なぜなら、探索手法についてはおおむね妥当であると考えるが、その探索結果から差分解読法に対する安全性評価結果の導き方に問題がある。つまり、**提案者は、CIPHERUNICORN-A のラウンド関数が全単射関数ではないことを考慮していない**からである。

暗号全体の最大差分特性確率の上界値を求める定理は以下のように知られている。

定理 2（文献 [3]）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。

定理 3（文献 [2]）全単射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、$(p_F^*)^{2r}$（$R = 3r, 3r+1$ のとき）もしくは $(p_F^*)^{2r+1}$（$R = 3r+2$ のとき）で表される。

ここで重要なのは、CIPHERUNICORN-A のラウンド関数が全単射関数ではないのであるから、定理 2 を使って評価しなければならない。さもなければ、出力差分値がゼロとなる場合の最大差分特性確率 $(p^*)'_f$ を求め、その確率を定理 2 に適用して求めた最大差分特性確率の上界値が、自己評価書に記載の最大差分特性確率の上界値よりも小さいことを示さなければならない。ところが、**提案者は、定理 3 での評価結果しか示していないので、差分解読法に対する安全性評価としては不十分である**。

評価者の見解としては、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[4]と、自己評価書の図 3.3 の場合のラウンド関数の最大差分特性確率は 2^{-14} であり、**15 段での最大差分特性確率の上界値は、定理 2 より、2^{-98} となる**。さもなければ、定理 3 より 15 段での最大差分特性確率の上界値が 2^{-140} となることから、出力差分値がゼロとなる場合の最大差分特性確率 $(p^*)'_f$ を求め、その確率を定理 2 に適用して求めた最大差分特性確率の上界値も 2^{-128} 以下となることを示すべきである。

以上の点ならびに第 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、現状の自己評価書からは、CIPHERUNICORN-A は**実用上の使用に関して差分解読法に対して安全であると期待されるが、学術的な安全性評価の観点からは差分解読法に対して安全であるとはいえない**といわざるを得ない。特に、**提案者による差分解読法に対する安全性自己評価結果が不十分であることから、提案者が主張する安全性（最大差分特性確率の上界値が 2^{120}）さえ担保されるかどうか、現時点では判断できない**という点は、安全性の自己評価書としての信憑性を著しく低下させるものである。したがって、全体を通じて、**提案者による差分解読法に対する安全性自己評価結果には同意できない**。

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-A 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、**自己評価書における差分解読法及び線形解読法に対する安全性評価結果は、定理や仮定の誤用があると考えられ、少なくとも学術的には信憑性があるとは認められない**といわざるを得ない。つまり、全体を通じて、**提案者による差分解読法及び線形解読法に対する安全性自己評価結果には同意できない**。

[4]提案者は、8 ビット入力 8 ビット出力 s-box での最大差分確率 2^{-6} を引用したものと思われる。

評価者の現時点の見解として、CIPHERUNICORN-A は、**実用上の使用に関して、差分解読法や線形解読法に対して安全であると期待されるが、学術的な安全性評価の観点からは差分解読法及び線形解読法に対して安全であるとはいえない**と判断する。

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およ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] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Ohta, "A Strategy for Constructing Fast Round Functions with Practical Security," *Selected Areas in Cryptography — 5th Annual International Workshop, SAC'98*, LNCS **1556**, pp.264–279, 1999.

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

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

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

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

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

[8] 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.

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

[10] 角尾幸保、久保博靖、宮内宏、中村勝洋、"128 ビットブロック暗号 CIPHERUNICORN-A," *2000* 年暗号と情報セキュリティシンポジウム *SCIS2000*, A18, 2000.

[11] 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.