FEAL 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　FEAL の概要

FEAL は、1987 年に日本電信電話株式会社より提案された 64 ビットブロック暗号であり、1987 年に EUROCRYPT'87 [22] 及び信学会論文誌 [23] にて FEAL-NX の前身である FEAL-8 が発表された。その後、段数を可変とし、鍵長を伸ばした FEAL-NX に拡張されている。今回提案された FEAL-NX の基本構造は、データブロック長 64 ビット、鍵長 64/128 ビットの N 段 Feistel 構造であり、N は 32 以上を推奨している。

FEAL の設計方針では、8 ビットマイクロプロセッサ上のソフトウェア実装を重視しており、8 ビット算術加算とローテーションを組み合わせることで非線形変換を実現している。FEAL の設計当時には、差分解読法や線形解読法を始めとする理論的な暗号解析手法は知られておらず、安全性評価がランダム性評価（データ攪拌性）のみに依存していた。当時としてはやむを得ない面もあるが、設計者らはこの評価に基づき FEAL-8 を提案した。しかし、FEAL で用いられているラウンド関数の構造が極めて簡単であったことから、世界中の暗号研究者らの解読対象暗号に位置付けられた結果、多くの解析が行われ、FEAL-8 では安全性に問題が生じる可能性があることが示された。それらの解析結果のなかには、差分解読法や線形解読法の理論体系が構築されるきっかけとなったものなどが含まれているる。

そこで、設計者らは、FEAL 設計当時には想定されていなかった、差分解読法や線形解読法に対する安全性評価を行う必要に迫られ、その結果、推奨段数を 32 段以上としている。

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 1.1 節（差分解読法）及び第 1.2 節（線形解読法）に記述されている。しかし、自己評価書には具体的な評価結果が記載されていないので、自己評価書が指示している参考文献を主として安全性評価結果であると判断し、本レポートでは、その発表論文から、差分解読法及び線形解読法に対する安全性評価の妥当性を検証する。

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 [13, 19]。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 [7, 14]。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 [20]。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 [11, 21]。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 自己評価の妥当性

差分解読法や線形解読法に対する安全性の自己評価は、本来、提案者により自己評価書に記載されるべき内容であるはずだが、自己評価書には参考文献の提示のみをもって自己評価としている。この点は自己評価書という趣旨からして不十分な内容であるといわざるを得ないが、とりあえずここでは自己評価書が指示している参考文献の結果（文献 [1] 及び文献 [17]）を引用する。

2.1.1 差分解読法

文献 [1] では、FEAL での最大差分特性確率の探索アルゴリズムが記述されている。この探索アルゴリズムは、松井のアルゴリズム [15] と盛合らの改良アルゴリズム [17] をベースに、さらに探索計算量を削減するための改良を加えたものである。これにより、以下の結果が得られている。

- N 段 ($N \leq 3$) での最大差分特性確率は 1 である。
- 4 段での最大差分特性確率は 2^{-3} である。
- 5 段での最大差分特性確率は 2^{-4} である。
- 6 段での最大差分特性確率は 2^{-11} である。
- N 段 ($7 \leq N \leq 32$) での最大差分特性確率は 2^{-2N} で表される。

差分解読法において、解読に必要となる平文組数は、最大差分特性確率の逆数の定数倍で表されることが知られている。この “定数倍” は攻撃成功確率に影響する係数であるが、おおむね 2^3 もしくは 2^4 が使われるとき、攻撃成功確率がほぼ 80 ～ 100%になる。

FEAL-32 では、差分解読法における S/N 比から 1R 攻撃が想定されるので、31 段での最大差分特性確率 2^{-62} が利用されることになり、解読に必要となる平文組数は $2^3 \times 2^{62} = 2^{65}$ 以上となる。しかし、FEAL は 64 ビットブロック暗号であるため、全ての平文組数を集めたとしても 2^{64} にしかならない。ゆえに、FEAL-32 は差分解読法に対して安全であるということが出来る。なお、この結果は、現在知られている FEAL の差分解読法に対する安全性評価結果としては最良のものである。

以上の結果は、FEAL-N に対するものである。一方、差分解読法の考察上、鍵スケジューリング部の構成は考慮せず、各ラウンド関数に挿入される拡大鍵は一様かつランダムに生成されるとの仮定を置いており、また FEAL-N と FEAL-NX との差は鍵スケジューリング部のみである。したがって、差分解読法に対する FEAL-NX と FEAL-N との安全性は同じであると結論付けられる。ゆえに、**FEAL-32X 以上であれば差分解読法に対して安全**であるといえ、実用に耐えうると考えられる。

ただし、今回の評価は、差分解読法に対する安全性評価の下限ともいえる最大差分特性確率を利用した評価であり、かつ FEAL-32X では学術的に安全であるために必要とされる閾値ぎりぎりである。このことは、**現在主流の暗号設計指針に照らし合わせれば、セキュリティマージンがない**ことを意味している。

2.1.2 線形解読法

文献 [17] では、FEAL での最大線形特性確率の探索アルゴリズムが記述されている。この探索アルゴリズムは、松井のアルゴリズム [15] をベースに、さらに探索計算量を削減するための改良を加えたものである。なお、文献 [17] では最大線形特性確率の代わりに最大偏差で表現しているが、(最大線形特性確率) = (2 × 最大偏差)^2 で換算できることが知られているので、本レポートでは最大線形特性確率で表記する。

以下に主な結果を記載する[1]。

- N 段 $(10 \leq N \leq 32)$ での線形近似は、8 段繰り返し表現（線形特性確率 1.345×2^{-21}) により構成される。
- 7 段での最大線形特性確率は 1.32×2^{-14} である。
- 15 段での最大線形特性確率は 1.10×2^{-37} である。
- 25 段での最大線形特性確率は 1.21×2^{-62} である。
- 31 段での最大線形特性確率は 0.99×2^{-78} である。

線形解読法においても、解読に必要となる平文組数は、差分解読法と同様に、最大線形特性確率の逆数の定数倍で表されることが知られている。FEAL-26 では、線形解読法における S/N 比から 1R 攻撃が想定されるので、25 段での最大線形特性確率 1.21×2^{-62} が利用されることになり、解読に必要となる平文組数は $2^3 \times 1.21 \times 2^{62} \simeq 2^{65}$ 以上となる。ゆえに、FEAL-26 以上であれば線形解読法に対して安全であるということが出来る。なお、この結果は、現在知られている FEAL の線形解読法に対する安全性評価結果としては最良のものである。

以上の結果は、FEAL-N に対するものである。一方、差分解読法の場合と同様に、線形解読法の考察上、鍵スケジューリング部の構成は考慮せず、各ラウンド関数に挿入される拡大鍵は一様かつランダムに生成されるとの仮定を置いており、また FEAL-N と FEAL-NX との差は鍵スケジューリング部のみである。したがって、線形解読法に対する FEAL-NX と FEAL-N との安全性は同じであると結論付けられる。ゆえに、**FEAL-26X 以上であれば線形解読法に対して安全**であるといえる。なお、FEAL-32X の安全性を示すことになる 31 段の最大線形特性確率は、DES の 27 段の最大線形特性確率とほぼ同等である。

2.2 第三者評価

自己評価書の第 1.3 節に記述されているように、FEAL-8 が提案されてから 10 年以上が経過していること、さらには暗号の構成が簡単であったことなどから、第三者評価結果は数多く存在する。これらの結果の多くは、**独立した暗号研究者が様々な角度から追試実験を行っていると考えられるので、それらの結果に対する信憑性は高い**。

FEAL の解読には大きく二つの流れがある。一つは FEAL-8（以下）についてどれだけ解読が容易に行えるのかという観点から解読したもの、もう一つはどれだけ長い段数が攻撃可能であるのかという観点から解読したものである。表 1に今までの解読結果をまとめる。なお、差分解読法及び差分線形解読法は選択平文攻撃の一種であり、線形解読法は既知平文攻撃の一種である。

現在知られている解読可能段数で最も長いものは、Biham らが発見した差分解読法による 31 段攻撃 [6] であり、また、その結果の正当性が青木らにより再確認 [1] されたことから、提案者は、FEAL-32X 以上の場合に差分

[1] 文献 [17] には 32 段までの最大偏差が記載されている。

表 1: FEAL 解読の歴史

発表年	発表者	解読段数	解読方法	必要平文数	解読時間
1988	Den Boer [4]	4	選択平文	10,000	—
1990	Murphy [18]	4	選択平文	20	Sun 3/60 で 4 時間以内
	Gilbert, Chassé [8]	8	選択平文	10,000	Sun 4 で 2 時間以内
1991	Biham, Shamir [6]	4	差分解読	8	—
		8	差分解読	2,000	Compaq のパソコンで 2 分以内
		31	差分解読	2^{63}	—
		4	既知平文	10 万	—
	Tardy-Corfdir, Gilbert [24]	4	既知平文	200	Sun 4 で数分
		6	既知平文	20,000	Sun 4 で約 10 時間で 15bit 求まる
	金子 [10]	4	既知平文	24	パソコン (80386) で 14 秒
1992	松井, 山岸 [16]	4	既知平文	5	HP9425 で 6 分
		6	既知平文	100	HP9425 で 40 分
		7	既知平文	2^{14}	HP9425 で 170 時間
		8	既知平文	2^{15}	全数探索と同程度
		8	既知平文	2^{28}	50bit 鍵全数探索と同程度
	栗田, 金子 [12]	6	既知平文	約 1000	—
1993	Biham, Shamir [7]	8	差分解読	128	—
	角尾ら [25]	4	既知平文	1	2^9 回程度の暗号化
		5	既知平文	1	2^{17} 回程度の暗号化
		6	既知平文	1	2^{25} 回程度の暗号化
1994	Biham [5]	8	線形解読	2^{24}	—
		20	線形解読	2^{63}	—
	青木ら [3]	8	線形解読	2^{25}	SPARCstation10 で約 1 時間
1995	盛合ら [17]	25	線形解読	$2^{63.3}$	—
	Kaliski, Robshaw [9]	8	(拡張) 線形解読	2^{23}	—
	青木, 太田 [2]	8	差分線形解読	12	SPARCstation10 で平均約 9.4 時間

解読法及び線形解読法に対して安全であることが示されているとしている。これにより、**提案者が 32 段以上を推奨段数としているのは（セキュリティマージンの少なさを除けば）妥当**である。

なお、自己評価書の第 1.3 節の表 1 の何箇所かに、本レポートとの値の不一致と思われる点が散見されるが、単に換算誤差によるものと考えられる程度の差であることに注意されたい。

3 まとめ — 妥当性の判定

本レポートでは、自己評価書に記載の参考文献を中心に、差分解読法及び線形解読法に対する安全性評価の妥当性を検証した。

FEAL は差分解読法や線形解読法が発見される以前に設計された暗号であるため、設計時点においてこれらの解読法が考慮されていなくても、そのこと自体はやむを得ない。しかし、現時点において、差分解読法や線形解読法が強力な暗号解読手法であるとの認識がある以上、それらの解読法に対する安全性を評価することは重要である。その点、幸運なことに、FEAL は**差分解読法や線形解読法に対する第三者評価が充実しており、そのいずれもが独立に行われた結果であることを考え合わせると第三者評価結果の信憑性はきわめて高い**ものと考えられる。一方、提案者の評価結果は、それら第三者評価結果の全てを包括する結果であり、矛盾が生じていないことから、その評価結果もまた信頼するに足るものである。また、過去 10 数年にわたる多様な使用実績はその信頼性を裏打

ちするものでもある。

以上の結果より、提案者の主張どおり、**差分解読法及び線形解読法に対して 32 段以上の FEAL-NX ($N \geq 32$) であれば安全**であると期待できる。

なお、今回の評価が、差分解読法に対する安全性評価の下限ともいえる最大差分特性確率を利用した評価であり、かつ FEAL-32X が学術的に安全であるために必要とされる閾値ぎりぎりである。このことは、**現在主流の暗号設計指針に照らし合わせれば、セキュリティマージンがない**ことを意味している。また、自己評価書の中では、1995 年以降の新しい解読法に対する安全性評価の記述がほとんど見当たらないことから、実用上は問題にならないとしても、最近の解読法に対する安全性評価に関する学術的な意味での信頼性が、最近提案された暗号よりも低いことは否めない。

参考文献

[1] K. Aoki, K. Kobayashi, and S. Moriai, "The best differential characteristic search of FEAL," *IEICE Transactions Fundamentals of Electronics, Communications and Computer Science*, Vol.E81-A, No.1, pp.98–104, 1998.

[2] K. Aoki and K. Ohta, "Differential-linear cryptanalysis of FEAL-8," *IEICE Transactions Fundamentals of Electronics, Communications and Computer Science*, Vol.E79-A, No.1, pp.20–27, 1996.

[3] K. Aoki, K. Ohta, S. Moriai, and M. Matsui, "Linear cryptanalysis of FEAL," *IEICE Transactions Fundamentals of Electronics, Communications and Computer Science*, Vol.E81-A, No.1, pp.88–97, 1998.

[4] B. Den Boer, " Cryptanalysis of F.E.A.L.," *Advanced in Cryptology — EUROCRYPT'88*, LNCS **330**, pp.293–299, 1988.

[5] E. Biham, "On Matsui's linear cryptanalysis," *Advances in Cryptology — EUROCRYPT'94*, LNCS **950**, pp.341–355, 1995.

[6] E. Biham and A. Shamir, "Differential cryptanalysis of Feal and N-hash," *Advances in Cryptology — EUROCRYPT'91*, LNCS **547**, pp.1–16, 1991.

[7] 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)

[8] H. Gilbert and G. Chassé, "A statistical attack of the FEAL-8 cryptsystem," *Advances in Cryptology — Crypto'90*, LNCS **537**, pp.22–33, 1991.

[9] B. S. Kaliski Jr. and M. J. B. Robshaw, "Linear cryptanalysis usng multiple approximations and FEAL," *Fast Software Encryption — Second International Workshop*, LNCS **1008**, pp.249–264, 1995.

[10] T. Kaneko, " A known-plaintext attack of FEAL-4 based on the system of linear equations on difference," *IEICE Transactions Fundamentals of Electronics, Communications and Computer Science*, Vol.E76-A, No.5, pp.781–786, 1993.

[11] L. R. Knudsen, "Practically secure Feistel ciphers," *Fast Software Encryption — Cambridge Security Workshop*, LNCS **809**, pp.211-221, 1994.

[12] 栗田大、金子敏信、"差分方程式を用いた FEAL-6 の既知平文攻撃," 信学会秋季大会 *A-190*, 1992.

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

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

[15] M. Matsui, "On correlation between the order of S-boxes and the strength of DES," *Advances in Cryptology — EUROCRYPT'94*, LNCS **950**, pp.366–375, 1995.

[16] M. Matsui and A. Yamagishi, "A new method for known plaintext attack of FEAL cipher," *IEICE Transactions Fundamentals of Electronics, Communications and Computer Science*, Vol.E77-A, No.1, pp.2–7, 1994.

[17] S. Moriai, K. Aoki, and K. Ohta, "The best linear expression search of FEAL," *IEICE Transactions Fundamentals of Electronics, Communications and Computer Science*, Vol.E79-A, No.1, pp.2–11, 1996.

[18] S. Muphy, "The cryptanalysis of FEAL-4 with 20 chosen plaintexts," *Journal of Cryptology*, Vol.2, No.3, pp.145–154, 1990.

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

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

[21] 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.

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

[23] 清水明宏、宮口庄司、"高速データ暗号アルゴリズム FEAL," 電子情報通信学会論文誌, Vol.J70-D, No.7, pp.1413–1423, 1987.

[24] A. Tardy-Corfdir and H. Gilbert, " A known plaintext attack of FEAL-4 and FEAL-6," *Advances in Cryptology — Crypto'91*, LNCS **576**, pp.172–182, 1992.

[25] 角尾幸保、岡本栄司、土井洋、"既知平文による FEAL-4 の解析的攻撃と FEAL-4 の改良," *1993* 年暗号と情報セキュリティシンポジウム *SCIS'93*, 3A, 1993.