FEAL-NX 自己評価書

１．安全性に対する評価

１．１　差分解読法

計算機を用いた差分解読法に対する安全性証明手法[1]を拡張し、計算量を大幅に削減することに、青木と小林と盛合が成功し[2]、その結果，32 段以上の FEAL には差分解読法が適用不能であることが示された.

また、Biham らは Skipjack[3]に対する攻撃法として不能差分利用攻撃[4]を発表した. 通常，差分解読法は確率の高い差分特性を利用するが，不能差分利用攻撃は逆に確率が極めて低い，もしくは０の差分特性を攻撃に利用する．青木は，不能差分探索アルゴリズムを開発し，それを FEAL に適用した．その結果，高々９段の不能差分しか発見されなかった[5].

[1] Mitsuru Matsui, On correlation between the order of S-boxes and the strength of DES. In Alfredo De Santis, editor, Advances in Cryptology ---EUROCRYPT'94, volume 950 of Lecture Notes in Computer Science, pp.366--375. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[2] Kazumaro Aoki, Kunio Kobayashi, and Shiho Moriai. The best differential characteristic search of FEAL. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences Japan, Vol. E81-A, No. 1, pp. 98--104, 1998. (Japanese preliminary version was presented at ISEC96-31).

[3] U.S. Department of Defense. SKIPJACK and KEA Algorithms, 1998 (http://csrc.nist.gov/encryption/skipjack-kea.htm).

[4] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, Advances in Cryptology ---EUROCRYPT'99, volume 1592 of Lecture Notes in Computer Science, pp. 12--23. Springer-Verlag, Berlin, Heidelberg, New York, 1999 (A preliminary version was presented at CRYPTO'98 rump session).

[5] Kazumaro Aoki. On cryptanalysis with impossible differentials. In 1999 Symposium on Cryptography and Information Security, number T4-1.3 in SCIS'99, International Conference Center Kobe, Kobe, Japan, 1999. Technical Group on Information Security (IEICE). (in Japanese).

１．２　線形解読法

盛合と青木と太田は，線形解読法に対する安全性証明手法[6]を拡張し，26 段以上の FEAL では線形解読法が適用不能であることを示した[7]．この結果により FEAL は線形解読法による安全性の限界が知られている数少ない暗号となった．なお、共通鍵ブロック暗号で線形解読法に対する安全性限界が知られているものは DES，LOKI89，LOKI91 である．

[6] Mitsuru Matsui, On correlation between the order of S-boxes and the strength of DES. In Alfredo De Santis, editor, Advances in Cryptology ---EUROCRYPT'94, volume 950 of Lecture Notes in Computer Science, pp.366--375. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[7] Shiho Moriai, Kazumaro Aoki, and Kazuo Ohta. The best linear expression search of FEAL. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan), Vol. E79-A, No. 1, pp. 2--11, 1996 (The extended abstract was presented at CRYPTO'95).

１．３　FEAL 暗号解読の進展

FEAL 暗号に対する解読の進展が以下の表にまとめられる（文献[8]）．鍵長に依存しない差分解読法および線形解読法の場合、FEAL-NX（N≧32）が安全であることに関する傍証になる。

表１　FEAL 暗号解読の進展

発表年	選択平文攻撃	既知平文攻撃
1988	13.3 (4)	
1989		
1990	13.3 (8), 4.3 (4)	
1991	63 (31), 11.0 (8), 3 (4)	16.6 (4), 7.6 (4), 4.6 (4), 14.3 (6), 10.0 (6)
1992		2.3 (4), 6.6 (6), 14 (7), 15 (8), 28 (8)
1993	7 (8)	0 (4), 0 (5), 0 (6)
1994		25 (8), 24 (8), 62 (20)
1995	3.6 (8)	63.7 (25)

注：数値は解読に必要な選択平文数または既知平文数を 2^x とするときの、指数部 x．() 内は攻撃可能段数。

[8] 青木、太田、盛合、共通鍵暗号 FEAL の安全性評価、pp. 734-739, NTT R&D Vol. 48, No.

10，1999 年 10 月.

１．４　閉構造を利用した攻撃

閉構造を持つと解読が容易になると言われてきた．Kaliski らは，構造の有無を検出する MCT 法(meet-in-the-middle closure test)を開発し，DES に適用した[9]．森田と太田は MCT 法を改良した SCT 法(switching closure test) [10]を開発し FEAL に適用した[11]．その結果 FEAL-8 には高い確率で閉構造が存在しないことがわかった．この攻撃法は鍵長に依存するので、128 ビットの鍵長の FEAL-NX に対しては、2^{64} 程度の計算量の閉構造を利用した攻撃法がないことに示す傍証になる。

[9] Burton S. Kaliski Jr., Ronald L. Rivest, and Alan T. Sherman. Is the data encryption standard a group? (results of cycling experiments on des). Journal of Cryptology, Vol. 1, No. 1, pp. 3--36, 1988.

[10] Hikaru Morita and Kazuo Ohta. New proposal and comparison of closure tests ---more efficient than the Crypto'92 test for DES---. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan), Vol. E77-A, No. 1, pp. 15--19, 1994 (A preliminary version was presented at CRYPTO'91).

[11] Hikaru Morita, Kazuo Ohta, and Shoji Miyaguchi. Results of switching-closure-test on feal. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, Advances in Cryptology --- ASIACRYPT'91, volume 739 of Lecture Notes in Computer Science, pp. 247--252. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

１．５　統計的評価

データ撹拌性に関し独自の指標を定め、二項分布をベースに組立てた理論値、DES と FEAL を比較し、データ撹拌性が同様に満足していることを示した[12, 13]。

[12] Akihiro Shimizu and Shoji Miyaguchi: “Fast Data Encipherment Algorithm FEAL,” In David Chaum and Wyn L. Price, editors, Advances in Cryptology --- EUROCRYPT'87, volume 304 of Lecture Notes in Computer Science, pp. 267-278. Springer-Verlag, Berlin, Heidelberg, New York, 1988.

[13] 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, July 1987.

２．ソフトウェアでの実装評価

２．１　８ビットマイクロプロセッサ

IC カードでは、８ビットマイクロプロセッサが主流である。これに対する、性能評価値を以下に示す。

表２　FEAL-NX　速度性能

(a) 暗号化／復号化速度

回転数　N	暗号化／復号化速度　kb/s
32	18.2
64	9.4

注：Z80H（8bitCPU)、クロック 8MHz，アセンブラプログラム(278バイト)、実装アルゴリズムの最適化なし、使用ワークエリアは両方とも14バイト

(b) 鍵展開時間

回転数　N	鍵展開時間　ms
32	4.48
64	8.95

注：Z80H（8bitCPU)、クロック 8MHz，アセンブラプログラム（225バイト)、実装アルゴリズムの最適化なし、使用ワークエリアは両方とも35バイト(拡大鍵結果格納部を除く)

２．２　１６ビットマイクロプロセッサ

将来の IC カードや、小型通信機器では、１６ビットマイクロプロセッサが使われる。これの性能評価値を以下に示す[14]。なお、公表値は鍵長 64 ビットの FEAL-N であるが、データ撹拌の部分は同一であるため、鍵処理を行う部分を除いた暗号化速度は一致する。

表３　FEAL-NX　データ撹拌部の速度性能

回転数　N	暗号化／復号化速度　kb/s
32	220
64	120

注：i80286（16bitCPU)、クロック10MHz，アセンブラプログラム（450バイト）

[14] 宮口庄司，栗原定見，太田和夫，森田光: "FEAL暗号の拡張," NTT R&D, Vol. 39, No. 10, pp. 1439-1450, Oct. 1990. [英語版] Shoji Miyaguchi, Sadami Kurihara, Kazuo Ohta and Hikaru Morita: "Expansion of FEAL Cipher," NTT Review, Vol. 2, No. 6, pp. 117-123, Nov. 1990.

２．３　３２ビットマイクロプロセッサ

現在 PC および WS の主流は、３２ビットマイクロプロセッサが使われる。これの性能評価値を以下に示す。

表４　FEAL-NX　速度性能

(a) 暗号化／復号化速度

回転数　N	暗号化／復号化速度　Mb/s
32	124
64	64

注：Pentium ＩＩＩ（32bitMPU)、クロック 1 GHz, アセンブラプログラム（N=32 は 2434 バイト、N=64 は 4609 バイト。使用ワークエリアは両方とも 2044 バイト。実装アルゴリズムの最適化あり。）

(b) 鍵展開時間

回転数　N	鍵展開時間　μs
32	1.375
64	3.232

注：Pentium ＩＩＩ（32bitMPU)、クロック 1 GHz,アセンブラプログラム（N=32,N=64 とも 388 バイト。使用ワークエリアは両方とも 116 バイト(拡大鍵結果格納部を除く)。実装アルゴリズムの最適化なし。）

３．ハードウェアでの実装評価

FEAL のハードウェア実装はこれまで２例ある。１例目は、1.5μm CMOS ゲートアレイで、FEAL-8 を実装した結果[15]から、FEAL-NX の実装結果を予想する。但し、鍵展開部分とデータ撹拌部分（暗号化処理）は独立の実装だったため、暗号化／復号化速度の精度は高い。暗号化処理部分のゲート量はほぼ同一とし、以下が導かれる。

表５　FEAL-NX　速度性能（換算値）

回転数　N	暗号化／復号化速度　Mb/s
32	24
64	12

注：1.5μm CMOS ゲートアレイ、クロック 12MHz、乱数部のゲート量：3.9 KGate

２例目は、0.8μm CMOS ゲートアレイで、FEAL-32 を実装した結果[16]から、FEAL-NX の実装結果を予想する。但し、上述の FEAL-8 実装と同様に、暗号化／復号化速度の精度

は高い。設計ツール類は異なる実装であったが、クロック同期的に作られていた為、FEAL-NX(N=32)に関しては、ほぼ同じ性能を出していることが分かる。

表６　FEAL-NX　速度性能

回転数　N	暗号化／復号化速度　Mb/s
32	23
64	11.5（換算値）

注：0.8μm CMOS ゲートアレイ、クロック 12.5MHz

[15] 森田光, 宮口庄司: "FEAL-LSIとその応用," NTT R&D, Vol. 40, No. 10, pp. 1371-1380, Oct. 1991. [英語版] Hikaru Morita and Shoji Miyaguchi: "FEAL-LSI and its Application," NTT Review, Vol. 3, No. 6, pp. 57-63, Nov. 1991.
[16] 青山政夫, 森田光, 阿部正幸: "PKC/FEAL LSIとその情報セキュリティへの応用," NTT R&D, Vol. 44, No. 10, pp. 923-930, Oct. 1995. [英語版] Masao Aoyama, Hikaru Morita and Tatsuhiro Naganawa: "Cipher and Authentication LSI for Communication Terminals," ITU, 7th World Telecommunication Forum, Vol. 1, 2.2B, pp. 251-255, Oct. 1995.

４．　第三者評価実績

オーストラリアで DES タイプのブロック暗号に対する解析・比較パッケージが開発され、FEAL は DES と Madryga 暗号とともにその統計的評価が発表されている[17]。χ^2 テスト、シリアルテスト、ランテストからなる統計的評価に加え、シーケンス・コンプレキシティー、バイナリー・デリバティブ（派生）なる指標に関して評価された。また、アバランチェ効果に関しても、平文と暗号文との相関、鍵と暗号文との相関の２種に関して評価された。報告されている結果によれば、FEAL-N と DES は、すべての指標に対して、平文と暗号文の独立性など好ましい統計的性質が示されている。

なお、公表結果は、鍵長 64 ビットの FEAL-N であるが、データ撹拌の部分は同一であるため、鍵を固定で評価された指標に関しては同じ統計的性質を保有する。又、FEAL-NX における鍵 128 ビットの鍵展開処理は、FEAL-N における鍵 64 ビットの鍵展開処理を上位互換的に拡張しているので、鍵の変化に対する指標も同様の統計的性質を示す傍証となりうる。

[17] Helen Gustafson, Ed Dawson, Bill Caelli, Comparison of Block Ciphers In Jennifer Seberry and Josef Pieprzyk , editors, Advances in Cryptology --- AUSCRYPT'90, volume 453 of Lecture Notes in Computer Science, pp. 208--220. Springer-Verlag, Berlin,

Heidelberg, New York, 1990.