Vol.37 No.6　　情 報 処 理　　June 1996

解　説

暗号安全性の最近の動向

5. 暗号の攻撃・解読法：線形解読法†

松　井　　充††

1. はじめに

線形解読法は1993年筆者によって発表された解読法であり[1]，ブロック暗号の汎用的な解読法としてははじめて既知平文攻撃および暗号文単独攻撃を実現したものである．この方法を用いて筆者はDESの計算機による実験的な解読にはじめて成功した[2]．

線形解読法のアイデアの原形は，1991年から翌年にかけて発表されたFEAL暗号の既知平文攻撃法に見られる[3]．ここではFEAL暗号に含まれる加算演算の特性をとらえた解析が行われているが，線形解読法はこれを算術演算だけでなく一般の乱数表に対しても適用できるよう発展させたものと考えてよい．

現在では線形解読法は，差分解読法とともにブロック暗号の強度評価の最も重要な手段と考えられている．本稿では，線形解読法の原理をDESを具体例として述べてみたい．

2. DES暗号

DES暗号は1977年に米国で標準化されたブロック暗号アルゴリズムであり，その後ANSIにも採用されるなど，現在に至るまで世界的に利用されている[4]．DESは56ビットの鍵を用いて平文を64ビットごとに暗号化する．**図-1**にその構成図を示した．

入力された平文はまず初期転置でビットの順序が入れ替えられたのち，左右32ビットづつに分割される．続いてこの右32ビットは，F関数と呼ばれる32ビットの入出力を持つ変換関数で処理されたのち，左32ビットと排他的論理和され，さらに左右の32ビットが入れ替えられる．ここで，F関数処理と左右の入れ替え処理は1段と呼ばれる．

DESはこの処理を16回，つまり16段の操作を行った後，最終転置と呼ばれる初期転置の逆関数を用いてビットの順序を入れ換え，暗号文とする．なお，初期転置と最終転置は暗号の強度に影響を与えないため，通常省略して考える．

また暗号化鍵については，鍵スケジュール部と呼ばれる処理で，56ビットを768ビットに拡大し，これを1段につき48ビットずつ各F関数に供給する．本稿では第i段に入力される48ビットの拡大された鍵をKiと記述する．線形解読法や差分解読法では平文と暗号文のペアからこの拡大鍵を直接求めることができるので，本稿では鍵スケジュール部の詳細は省略する．

次に**図-2**にDESのF関数の構造を示した．F関数の入力32ビットは，まず48ビットに拡大され（従って16ビットは重複している）6ビットごとに，S-BOXと呼ばれる8つの置換表に入力される．各S-BOXは6ビットの入力を変換して4ビットを出力し，従って8つのS-BOXから出力された合計32ビットは，ビットの順序が入れ替えられたのちF関数の出力となる．

DES暗号で採用されたこの構造はInvolution型と呼ばれ，暗号操作と復号操作が拡大鍵の順序を入れ替えるだけで相互に実現できるという特徴をもっており，その後のブロック暗号アルゴリズムの手本となったものである．

ところでDESが発表された当時，その安全性に対する様々な論議が巻き起こった．その1つは設計基準が非公開となっている事実に起因するもの，すなわち設計者にだけに解読できる仕組みが組み込まれているのではないかとの疑惑である．またもう1つは，鍵の長さに関するものであり，DESの56ビットの鍵の長さは短かすぎて鍵の全

† Linear Cryptanalysis by Mitsuru MATSUI (Mitsubishi Electric Corporation Information Technology R&D Center).
†† 三菱電機情報技術総合研究所

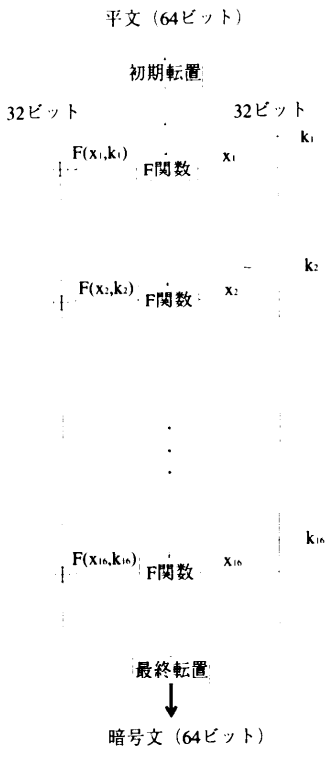

図-1 DESの構成図

数探索が可能であるという意見である．

このような疑問点がありながらも，現実的な弱点が見つからなかった上，実現性の点からもDESはよくできたアルゴリズムであったため，急速に広まり利用されようなった．

3. 線形解読法の原理

線形解読法の原理は，まず与えられた暗号化関数を部分的により簡単な関数に近似（線形近似）することから出発する．そして，もとの暗号化関数を解読するかわりに，この近似された関数を解読することにより，少ない計算量で未知の暗号化鍵を求めようというものである．

もちろん，本来の暗号化関数とは異なるものを解読の対象にしているのであるから，この解読の結果得られた暗号化鍵は一般には正しいものではない可能性もある．しかしその代償は情報量で補われる．すなわち解読者の得た情報量が多ければ解読の成功確率も上昇するのである．

これを次の例で見てみよう．暗号化関数をF，暗号化鍵をKとおくとき，任意の平文Pと暗号文Cに対して次の式が成立している（というよりもこれは本来，平文から暗号文をもとめる計算式であるから当然である）．

$$C_i = F(P, K)_i \quad (1)$$

この式は見方を変えると，任意に与えられた平文Pと暗号文Cに対して（暗号化関数Fと暗号化鍵Kは固定されているとの前提で），等式が確率1で成り立っていると見ることができる．線形解読法ではこれを特定の1ビットに注目して次のような関係式を考察するのである．

$$C[i] = F(P, K)[i] \quad (2)$$

ここで記号Aの第iビットをA[i]と表した．もちろん上式も確率1で成り立つ関係式である．しかしこれをFとは異なる別のF'におきかえたとすると次の式は当然ながら一般には必ずしも成立しなくなるであろう．

$$C[i] = F'(P, K)[i] \quad (3)$$

線形解読法の特徴は，これを確率的関係式と見なす点である．たとえば，F'がまったくでたらめに選ばれた関数なら上式が成り立つ確率は1／2になるであろう．このことは言いかえれば，左辺と右辺は相関性がないことを意味している．しかし，もしこの式が1／2ではない確率で成り立ったとすれば，左辺と右辺とは相関性があるので，PとCからKに関する何らかの情報を得ることができることがある．たとえばF'(P, K)＝P⊕Kであったとすれば上式を整理すると次の式を得ることができる．

$$K[i] = P[i] \oplus C[i] \quad (4)$$

ここで，この左辺は鍵を表しているため解読者にとっては未知の値であるが，右辺は既知の値である．したがって，たとえばこの式が確率1で成立するならば，平文と暗号文の組が1つあれば鍵の1ビット情報K[i]が必ず正しく求められる．

また上式の成立確率が1／2より大きいならば，多数の平文と暗号文の組が得られるという条件のもとでは多数決法によって，つまりP[i]⊕C[i]＝0なる平文と暗号文の組が，P[i]⊕C[i]＝1なる平文と暗号文の組よりも多ければK[i]＝0，そうでなければK[i]＝1と推定できるのである．

なお，成立確率が1／2より小さかったならば逆の推定をすればよい．

先に述べたように，この推定は一般には間違っ

ている可能性もある．その確からしさはつぎの2つの要因が支配する．

要因1．(3)式の成立確率

要因2．平文と対応する暗号文のペアの個数

明らかに要因1の確率が1／2から遠ければ遠いほど，必要な平文数は減少する．線形解読法の理論によれば，(3)式の成立確率をpとする時，鍵K（の部分情報）の解読に必要な平文と暗号文のペアの個数は$1/(p-0.5)^2$に比例することが知られている（ここで比例定数はF'の形に依存する）．

したがって線形解読法の効率を高めるためには，(3)式の成立確率と1／2との差の絶対値がなるべく大きくなるようなF'をとる必要がある．線形解読法では，このF'のとり方を，関数Fの線形近似の観点からとらえるところが大きな特徴である．

次節ではDESを具体例として暗号アルゴリズムの線形近似の実際を見ることにする．

4. DESの線形近似

暗号化関数の線形近似はまず局所的な部分からはじめ，それを大局的に延長するというプロセスをとる．まず**図-3**のようなnビット入力，mビット出力の関数Sを考えよう．このときまずランダムに入力されたXに対して次の確率を考察する．

$$\mathrm{Prob}\{X[i]=S(X)[j]\} \qquad (5)$$

この確率が1／2ならば，これらのビットの間に線形相関はないと言ってよいが，1／2でなければ前節でのべた方法によってSの出力からS[i]が有意に推測可能である．

線形解読法ではこの概念を次のように拡張する．すなわち，与えられた関数に対して次の確率を考えるのである．

$$\mathrm{Prob}\{X[i1,i2,\ldots]=S(X)[j1,j2,\ldots]\} \qquad (6)$$

ここで記号X[i1,i2,...]は，Xの第i1ビット，第i2ビット，... の排他的論理和値を表したものである．言い換えれば，入力のいくつかの（固定された）ビット排他的論理和値と，出力のいくつかの（固定された）ビットの排他的論理和値が一致する確率ということである．

この確率が1／2から遠いほどSは部分的に線形関数に近いということができる．したがってDESにおける線形解読法の最初の目標は，S-BOXにおいてそのようなビット位置i1,i2,... とj1,j2,... の組を求めることである．たとえば，5番目のS-BOX S5では，次が成り立っていることが容易に調べられる．これはDESにおけるすべてのS-BOXとあらゆるビット位置の組合せの

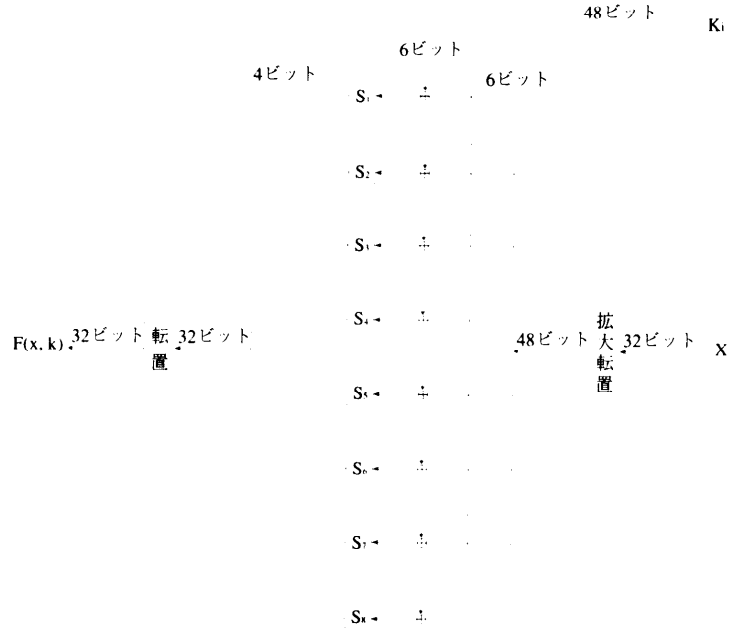

図-2 DESのF関数

中でもっとも線形に近い（(6)式の成立確率が1／2から遠い）ものである．

$$\mathrm{Prob}\{X[4]=S(X)[0,1,2,3]\}^3 = 12/64 \qquad (7)$$

さてDESのF関数の構造から，S-BOXの線形近似式は一意的にF関数の線形近似式に拡張することができる．たとえば上に示したS5の最良な線形近似は，同じ確率で成立する次のようなF関数の最良近似と等価になる．

$$\mathrm{Prob}\{Xi[15]\oplus F(Xi,Ki)[7,18,24,29]= Ki[22]\} = 12/64 \qquad (8)$$

さらにこのF関数の線形近似をアルゴリズム全体に拡張する．ここで注意しなければならない点は各段におけるF関数の良い線形近似が，必ずしもアルゴリズム全体の良い線形近似に結び付くとは限らない点である．これは，各段のF関数の線形近似が，全体として矛盾なく連結されなければならないからである．DES型暗号の場合，具体的には，第i段のF関数の近似式の入力に現われたビット位置は，第i-1段または第i+1段のいずれか一方（のみ）のF関数の近似式の出力に現われなければならない．

このような束縛条件のもとで各段のF関数を確率Piで近似すると，アルゴリズム全体の近似確率は次の公式で与えられる．

$$\frac{1}{2} + 2^{n-1}\prod_i (Pi - \frac{1}{2}) \qquad (9)$$

したがって暗号アルゴリズム全体の最良の線形近似確率を求める問題とは，上に示した束縛条件のもとで，(9)の確率と1／2との差の絶対値の最大値を求める問題に帰着される．一般に与えられたアルゴリズムについてこれを求めることは容易ではないが，DESについては完全に決定されている[5]．DESアルゴリズム全体が近似されると(4)式と同様，1ビットの未知数を含む次のタイプの式が得られ，それは多数決法によって決定することができる．

$$K[m1,m2,....] = P[i1,i2,...] \oplus C[j1,j2,....] \qquad (10)$$

さて実際のDESの解読では一度に多くの鍵を求めることのできるよう，アルゴリズム全体を近似するのではなく，意図的に最初の段と最後の段を残し，第2段から第15段までを近似するのである．すなわち次の形の式を得る．

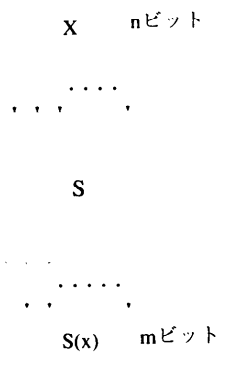

図-3 関数S

$$K[m1,m2,....] = P[i1,i2,...] \oplus C[j1,j2,....] \oplus F(P,K_1)[k_1,k_2,...] \oplus F(C,K16)[l_1,l_2,...] \qquad (11)$$

この式には未知数としてK1とK16（および左辺の1ビット情報）が残っている．そこで先に述べた多数決原理を拡張した最尤法によってこれらの値を決定してやるのである．具体的には，各K1とK16の候補に対して(11)式の成立確率を実際に計算し，その値が1／2から最も遠かったものを正しい鍵とする．

筆者によるDESの計算機による解読実験も(11)式を解くことによって実行されたのである．この実験では2^{43}ブロック（2^{46}バイト）の平文および対応する暗号文を用いて，暗号化に使われた56ビットの鍵を推定した．計算にはワークステーション12台を用い，50日後に正しい鍵に到達した．

5. 最近の話題

最良線形近似探索問題は，それ自身興味ある問題として各種の暗号アルゴリズムについて調べられている[6,7]が，未解決な暗号アルゴリズムも数多く，重要な研究テーマとなっている．

ところで最良線形近似探索アルゴリズムは，まったく同様に最良差分値探索にも用いることができることが知られているが[5]，この他差分解読法と線形解読法の類似点も数多く指摘される[8]点はきわめて興味深い．

さらに暗号設計の点では，差分解読法や線形解読法に対して証明可能安全性(Provable Security)をもった構造が考案される[9,10]など，新たな視点からも研究が進められている．

6. おわりに

本稿ではDESを例にとり，線形解読法の原理を解説した．実用的な秘密鍵暗号設計の目標は，固定長の鍵を一度共有すれば，いくら多くの平文や暗号文に関する情報を通信路に流しても安全性が保たれることである．

これは言い換えれば，秘密の情報量に比べて露呈する情報量が圧倒的に多いと仮定した上での安全性であり，したがって無条件の安全性（無限の計算能力を仮定しても解読できない）を持つことは不可能である．

我々にとって必要な安全性とは，現実の世界で解読ができないことであり，したがって安全性の意味づけも時代や状況によって変わり得るものである．暗号解読の意義も，この点から正しく理解されることが望まれる．

参 考 文 献

1) Matsui, M. : Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology -Eurocrypt '93, Lecture Notes in Computer Science 765, Springer-Verlag, pp.386-pp.397 (1993).

2) Matsui, M. : The First Experimental Cryp-tanalysis of the Full 16-round DES, Advances in Cryptology -Crypto '94, Lecture Notes in Comp-uter Science 839 Springer-Verlag, pp.1-11 (1994).

3) Matsui, M. and Yamagishi, A. : A New Cryptanalytic Method for FEAL Cipher, IEICE Trans. Fundamentals, Vol.E77-A, No.1, pp.2-7 (1994).

4) National Bureau of Standards, Data Encryp-tion Standard, Federal Information Processing Standard, Publication 46-2 (1977).

5) Matsui, M. : On Correlation Between the Order of S-boxes and the Strength of DES, Advances in Cryptology - Eurocrypt '94, Lecture Notes in Computer Science 950 Springer-Verlag, pp.366-375 (1994).

6) Kaliski, B.S. and Robshaw, M.J.B. : Linear Cryptanalysis using Multiple Approximations, Advances in Cryptology - Crypto '94, Lecture Notes in Computer Science 839 Springer-Verlag, pp.26-39 (1994).

7) Ohta, K., Moriai, S. and Aoki, K. : Improving the Search Algorithm for the Best Linear Expression, Advances in Cryptology -Crypto'95, Lecture Notes in Computer Science 963 Springer-Verlag, pp.157-170 (1995).

8) Chabaud, F. and Vaudenay, S. : Links between Differential and Linear Cryptanalysis, Advances in Cryptology - Eurocrypt '94, Lecture Notes in Computer Science 950 Springer-Verlag, pp.356-365 (1994).

9) Nyberg, K. and Knudsen, L. : Provable Sec-urity against Differential Cryptanalysis, Journal of Cryptology, Vol.8, No.1 (1995).

10) Matsui, M. : New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, the third International Workshop of Fast Software Encryption, Lecture Notes in Computer Science 1039, Springer-Verlag, pp.205-218 (1996).

（平成8年1月25日受付）

松井 充

昭和60年京都大学理学部卒業．昭和62年同大学院理学研究科修士課程数学専攻修了．同年三菱電機(株)入社．以来，符号理論・暗号理論の研究，開発に従事．平成7年電子情報通信学会論文賞受賞．電子情報通信学会，IACR各会員．