Vol.37 No.6　　情 報 処 理　　June 1996

解　説

暗号安全性の最近の動向

6. 暗号の攻撃・解読法：差分攻撃法†

太田和夫††　青木和麻呂††

1. はじめに

差分攻撃法は，SECURICOM 89 で Shamir によって解読の実演の形で公表され，暗号研究者に大きな衝撃を与えた．難攻不落であると長らく信じられていた DES に対しても有効なこと，DES，FEAL など多くの秘密鍵暗号に広く適用可能であることなどにより，多くの人々の関心をひいた．

Shamir と当時彼の学生であった Biham は，FEAL 暗号の解読を通じて差分攻撃のアイデアに至ったと思われる．本稿では，差分攻撃法の位置付けを整理し，最新の研究状況を紹介するとともに，FEAL 暗号をケーススタディとして彼らが辿ったであろう思考経路を再訪することとしたい．

2. 差分攻撃法の位置付けと解読結果

差分攻撃法は，特定の条件☆を満たす 2 つの平文のペアに対応した暗号文のペアを解析することにより暗号化鍵を算出する．選択平文攻撃の一種である☆☆．

差分攻撃法を DES および FEAL に適用した場合の攻撃に必要な平文-暗号文の組数と演算時間の関係を**表-1** に示す．攻撃に必要となる平文-暗号文の組数は，差分確率(後述)の逆数として定まる．ここで，文献 1) と文献 3) は差分攻撃法を線形攻撃法[4]と組み合わせることで，攻撃に必要な組数を削減している．

3. 差分攻撃法の概要

秘密鍵暗号は☆は，暗号化と復号化に同一の秘密鍵を用いる．たとえば，DES や FEAL がある．多くの秘密鍵暗号は，F 関数を複数回繰り返して実現する．F 関数はそれほど安全でないが高速に実装可能であり，複数回繰り返すことで，暗号系の安全性を高めている(**図-1**)．F 関数の繰り返し回数を段数という．F 関数中には S 関数が非線形演算として組み込まれる(**図-2**)．

秘密鍵暗号では，すべての鍵候補を総当たりで調べれば，正しい鍵を発見できる．しかし，調べるべき場合数が膨大であり，この方法は非現実的である．差分攻撃法では，調べるべき鍵の場合数を現実的な範囲に抑えるように，ある条件をもった平文ペアをとり，影響をおよぼす鍵のビット数を小さくすることで，鍵の部分情報を順次決定していく．

差分攻撃法では，平文ペアの条件を 1. S 関数の差分特性の抽出，2. F 関数の差分特性の抽出，3. 暗号系の差分特性の抽出，の手順で事前処理として求めておき，選択平文に対する暗号文を入手後に 4. 秘密鍵の絞り込み，を行う．

3.1 FEAL 暗号[5]

FEAL は，IC カードなどの 8 ビットマイクロプロセッサ上のソフトウェア向きに設計された暗号アルゴリズムである．IC カードでは使用可能なメモリ量が制約されるため，DES でテーブルを参照することで実現していた非線形演算を，FEAL では，加算演算と回転演算を組み合わせた S 関数を用いて実現している(図-2)．S 関数は 2 つの 8 ビット入力を 8 ビット出力に変換する．

† On the Differential Cryptanalysis by Kazuo OHTA and Kazumaro AOKI (NTT Information and Communication Systems Laboratories).

†† NTT 情報通信研究所

☆ FEAL の場合の条件は，たとえば **3.6** の脚注を参照．DES については文献 2) を参照．

☆☆ 平文は解析対象に含まれないので，攻撃者は暗号文のみで暗号化鍵を算出できるが，平文が特定の条件をみたすことが必要である．

☆ 秘密鍵暗号は暗号鍵と復号鍵が共通なので，共通鍵暗号とよばれることもある．

表-1 差分攻撃法の DES と FEAL への適用結果 (ECB モード)

暗号方式	段数	平文-暗号文の組数	解読のための演算時間 注1)	文献
DES	8	50,000	2分 PC(2^{16})	2)
		2^9	10秒 WS 注2)	3)
	16	2^{47}	2^{37}	2)
FEAL	8	128	2分 PC	2)
		12	20分 WS	1)
	16	2^{29}	—(記述なし)	2)
	32	2^{66}	鍵の総当たりより大	2)

注1) 時間の指定の数値は，1回の暗号化処理を1単位とした場合の演算量を表す．
注2) 鍵10ビットの導出時間．

3.2 差分の線形性

図-2 において，鍵成分(K)は入力(X)に対して排他的論理和(XOR，記号 $\oplus$ で表す)された後に S 関数で処理される．

鍵成分が一定なので，2つの入力 X, X^* に対して $(X \oplus K) \oplus (X^* \oplus K) = X \oplus X^*$ となることに注意しよう．もし，2つの入力 X, X^* に対して，

$$F(K, X) \oplus F(K, X^*) = F(0, X \oplus X^*) \quad (1)$$

の関係が成り立つならば，2つの入力の排他的論理和(差)とそれに対応した出力の排他的論理和(差)をとることで，鍵成分を用いて F 関数で処理しても，鍵に依らない関係を保存できることになる．以降，$X \oplus X^*$ を ΔX と記して入力差分とよび，F 関数の差分に注目してする場合には，鍵の影響を無視できるので，$F(K, X)$ を $F(X)$ と書く．

繰り返し型暗号は図-1 に示すように，XOR 演算と分岐演算を介して F 関数を複数回繰り返している．XOR 演算は

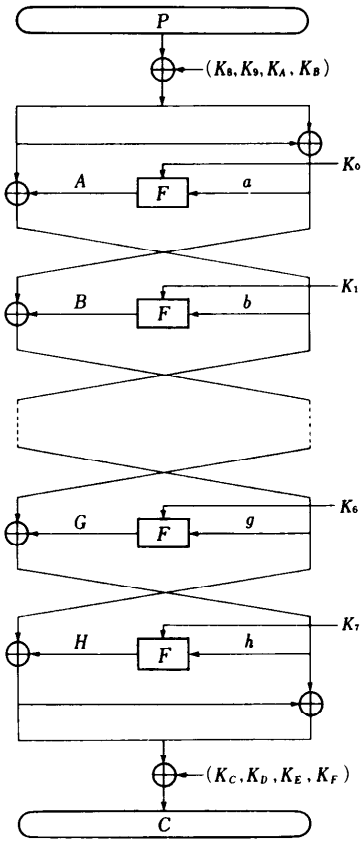
$$(X \oplus Y) \oplus (X^* \oplus Y^*) = (X \oplus X^*) \oplus (Y \oplus Y^*)$$

すなわち $\Delta(X \oplus Y) = \Delta X \oplus \Delta Y \quad (2)$

の関係を満たすことに注意しよう．差分に注目して2種類の線形性(式(1)，式(2))を繰り返し適用することで，複数の F 関数で用いられる鍵成分を無視できるようになる．

3.3 S 関数の性質

式(1)が常に成立するわけではないが，大きな確率で成立する特別な差分が存在する．ここでは，図-2 中の S_0 関数を例に説明する．



各鍵は16ビットであり，$K8 \sim K_B$, $K_C \sim K_F$ は64ビットの入力に対してビットごとに排他的論理和をとる．

図-1 繰り返し型暗号系 (FEAL-8 暗号の例)

S_0 関数で2ビットの左回転(ROL2)を無視すると，8ビットの2つの入力の加算演算を得る．256で剰余をとるので，最上位ビットの桁上がりは無視され，任意の8ビットデータ x_1, x_2 に対して

$$S_0(x_1, x_2) = S_0(x_1 \oplus 80, x_2 \oplus 80) \quad (3)$$

(ここで80は16進表現である)が常に成り立つ．

以降では，x_1, x_2 に対して

$$\Delta\delta = S_0(x_1, x_2) \oplus S_0(x_1 \oplus \Delta x_1, x_2 \oplus \Delta x_2) \quad (4)$$

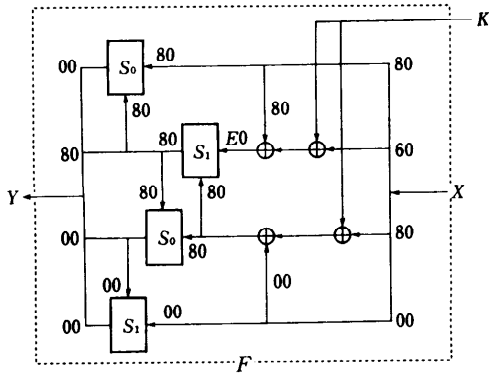
が確率 p で成り立つとき，

$$S_0(\Delta x_1, \Delta x_2) \rightarrow \Delta\delta \quad \text{with } p \quad (5)$$

と表記して S_0 に関する差分特性，(Δx_1, Δx_2, $\Delta\delta$)を差分値，p を差分確率とよぶ．上記の例は，

$$S_0(80, 80) \rightarrow 00 \quad \text{with } p=1 \quad (6)$$

と表せる．これ以外の確率1の差分特性として



$S_i\ (x_1, x_2) = \mathrm{ROL}_2(x_1 + x_2 + i \bmod 256)$
注）図中の数字は差分値の 16 進表現

図-2 FEAL 暗号の F 関数

$$S_0(80, 00) \rightarrow 02 \quad \text{with } p=1 \qquad (7)$$

もある．2 ビット左回転により，80 は 02 となることに注意．

ところで，S 関数（たとえば図-2 中で始めに処理される S_1 関数）は加算後に 2 ビット左回転し，その出力は他の S 関数（たとえば図-2 中の S_0 関数）に引き継がれる．その S 関数で式(6)，式(7)を利用可能とするために，はじめの S 関数の出力差分（$\Delta\delta$）を $\Delta\delta$ =80 ととりたい．加算の出力差分（Δz）は Δz =20 ととればよい．2 ビット左回転により，20 は 80 となることに注意．

たとえば，

$$S_0(\mathrm{A0}, 80) \rightarrow 80 \quad \text{with } p=1/2 \qquad (8)$$

が成り立つ．その理由は，x_1 の 8 ビット目（最上位ビット）と 6 ビット目に差分があるが，x_1 の 6 ビット目が変化すると，常に z の 6 ビット目が変化する．7 ビット目への影響は，6 ビット目からの桁上がり差分の有無で決まり，確率 1/2 で桁上がり差分が生じる．一方，7 ビット目からの桁上がり差分がなければ，式(6)によって x_1, x_2 の 8 ビット目の影響は無視できる．6 ビット目からの桁上がり差分がなければ，7 ビット目からの桁上がり差分もない．よって，2 ビット左回転により 20 は 80 となるので，確率 1/2 で 80 となることが分かる．

同様にして，

$$S_0(60,80) \rightarrow 80 \quad \text{with } p=1/4 \qquad (9)$$

$$S_0(\mathrm{E0}, 80) \rightarrow 80 \quad \text{with } p=1/4 \qquad (10)$$

などが，S_0 関数の性質として求まる．

S_i 関数 の加算の定数項 i（図-2）は差分に影響を与えないため，S_0 関数と S_1 関数の差分確率が等しいことに注意しよう．

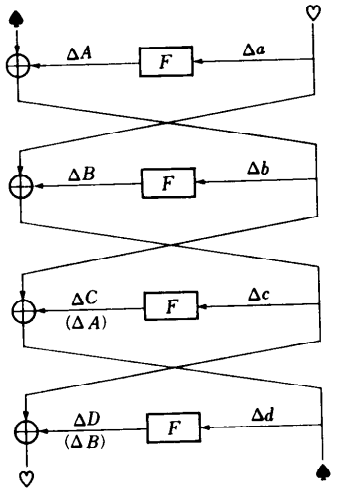


図-3 FEAL 暗号の 4 段繰り返し型差分特性

3.4 F 関数の性質

XOR 演算の性質（式（2））を利用して F 関数内部の差分の伝搬を解析する．たとえば，

$$F(80808080) \rightarrow 02000002 \quad \text{with } p=1 \qquad (11)$$

$$F(80608000) \rightarrow 00800000 \quad \text{with } p=1/4 \qquad (12)$$

を得る．図-2 に示すように，入力差分は 8 ビットずつ 4 つのブロックに分けられ，F 関数で処理される．図-2 は式（12）の場合の差分の伝搬の様子を示している．ここでは，式（6），式（7），式（10）が用いられる．

$$F(\Delta X) \rightarrow \Delta Y \quad \text{with } p \qquad (13)$$

を F に関する差分特性，（ΔX, ΔY）を差分値，p を差分確率とよぶ．

3.5 暗号系の性質

F 関数の性質を組み合わせて，暗号系の性質を求める方針を示す．

F 関数に関する連続した n 個の差分特性で，かつその出力差分を次の連続した n 個の差分特性の入力差分につなげることができるとき，繰り返し型の差分特性とよぶ．

繰り返し型の差分特性は任意の段数に適用可能なので，これを求めることは，F 関数の繰り返し回数と安全性のトレードオフを知る上で重要である．ここでは，特に 4 段繰り返し型差分特性の見つけ方を示す（**図-3**）．

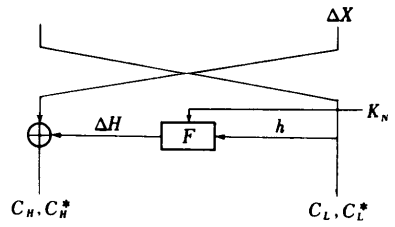


図-4 鍵の絞り込みにおける関係式

繰り返し型とするためには，図-3 に示すように，左上の入力差分と右下の出力差分，右上の入力差分と左下の出力差分はそれぞれ等しいことが要請される．XOR 演算の性質(式 (2))に注目すると，4 段繰り返し型差分特性では，$\Delta A = \Delta C = \Delta b \oplus \Delta d$, $\Delta B = \Delta D = \Delta a \oplus \Delta c$ が成り立つ必要がある．さらに，$F(\Delta a) \rightarrow \Delta A$, $F(\Delta c) \rightarrow \Delta A$, $F(\Delta b) \rightarrow \Delta B$, $F(\Delta d) \rightarrow \Delta B$ が要請される．

ここで，$\Delta A = \Delta B$, $\Delta a = \Delta d$ と仮定して☆，$F(\Delta a_1) \rightarrow \Delta A$, $F(\Delta a_2) \rightarrow \Delta A$ を満たす大きな確率をもった(ΔA, Δa_1, Δa_2)の組を探す．

[繰り返し型差分特性の探索]

Step 1:大きな確率 (p_1) をもつ差分特性 $F(\Delta a_1) \rightarrow \Delta A$ を選ぶ．

Step 2: $\Delta a_2 = \Delta A \oplus \Delta a_1$ とおいて $F(\Delta a_2) \rightarrow \Delta A$ を満たす確率 ($p2$) を求める．

図-3 において，ΔA= 00800000, Δa_1= 80??8000 とおく．これにより，F 関数の 2 つの S_0 関数で性質(式(6)) を適用でき，かつ下位の S_1 関数には差分が影響しないので，p_1 と p_2 を大きくとれると期待できる．

?? を 20 とおくと，上位の S_1 関数で性質(式(8))を適用でき，p_1=1/2 ととれる．しかし，Δa_2=80A08000 となり，

$$S_1(20, 80) \rightarrow 80 \quad \text{with } p=0 \qquad (14)$$

なので，p_2=0 となり，Δa_2= 80A08000 を差分値には採用できない．

次に，?? を 60 とおくと，Δa_2= 80E08000 となり，式(10)，式(9)によって，p_1=1/4, p_2=1/4 となる．

F 関数 1 つあたりの差分確率を 1/4 とできるので，F 関数を N 段近似するには確率 $p=2^{-2N}$ とな

☆ この仮定をおいて求めた差分特性が差分確率の最大値を与える保証はない．しかし，7 ～ 32 段については最大の差分確率を与えることが確認されている．

る差分特性がとれることが明らかとなった．

3.6 鍵候補の絞り込み

鍵候補の絞り込みの考え方は以下のとおり．

F 関数を N 段繰り返す暗号系を考える．複数 ($N-1$)段の F 関数を差分近似することとして，差分確率を p, 暗号文のペア数を m とする．このとき，$m \times p$ 個のペアは，それぞれの F 関数で差分特性で規定されたとおりの差分値を与えながら処理されると期待できる．(以降ではこのペアを正ペアとよぶ．)

最終の F 関数では，入力成分(**図-4** では h)の値が暗号文として与えられている☆ので，2 つの入力値 C_L, C_L* と出力差分値($\Delta H = C_H \oplus C_H^* \oplus \Delta X$)の間の関係式

$$\Delta H = F(K_N, C_L) \oplus F(K_N, C_L^*) \qquad (15)$$

が成立することを検査できる．以下では，F 関数の出力差分値を計算するのに必要な鍵の部分情報を部分鍵とよぶことにする．(差分特性で近似した($N-1$)段の F 関数で使用される鍵はすべて無視できることに注意しよう．)

部分鍵が正しければ，この関係式は pm 回成立すると期待できる．一方，正しくなければ，成立は偶然と考えられる．この 2 つの事象を区別するために，以下に示す数えあげ法を行う．

[数えあげ法]

Step 1 ：大きな確率をもつ差分特性に対応した平文差分を選ぶ☆☆．

Step 2 ：平文差分をみたす平文ペアに対応した暗号文ペア($(C_H, C_L),(C_H^*, C_L^*)$)を，解読に必要な個数集めて記憶する．

Step 3 ：暗号文のペアを用いて，最終段の F 関数の期待される出力差文値 (ΔH) をペアごとに求める．

Step 4 ：期待される差文値を与える暗号文ペアの頻度を部分鍵の候補ごとに数えあげる．最大の頻度を示す部分鍵の候補値を，部分鍵として出力する．

数えあげ法が正解を出力するためには，差分確率にみあった個数の暗号文ペアが与えられており，収集した暗号文ペアの中に正ペアが上記の 2

☆ この状況を作るために，文献 2)では鍵成分(K_C, K_D, K_E,, K_F)の位置を他にずらす工夫をしている．

☆☆ 上で求めた 4 段繰り返し差分特性に対応した平文差分は 80608000 00000000 となる．

つの事象をを区別できる程度の個数存在する必要がある．

数えあげ法の成功を判定できる S/N 比について説明する．比が十分に大きい場合には，3～4個の正ペアが存在すれば十分なことが経験的に確認できている[2]．

S/N 比の定義とその意味は以下のとおり．

差分確率を p，部分鍵のビット数を k，暗号文のペア数を m，明かに正しくないペアをあらかじめ廃棄し（これを Filtering 技法とよぶ），βm 個のペアのみを解析対象とできれば，誤った鍵の候補値における平均出現頻度は $\frac{m\alpha\beta}{2^k}$ となる．ここで，α は，2つの入力値（h, h^*）と出力差分値（ΔH）が1つ与えられると，関係式（15）を満たす部分鍵の平均的な個数である．一方，真の部分鍵の出現頻度は mp なので，2つの比は $S/N=\frac{mp}{m\alpha\beta/2^k}=\frac{2^kP}{\alpha\beta}$ となる．S/N 比が十分大きければ，真の部分鍵が最大頻度を与えることになる．

4段繰り返し型差分特性を用いて，差分攻撃に対する FEAL-N の安全性を評価する．

$(N-2)$ 段分の F 関数を差分で近似し，2段分の情報を用いて Filtering ☆ を行う．$p=2^{-2}$ $^{(N-2)}$，$k=32$，$\alpha=1$，$\beta=2^{-19}$ となる．$S/N=\frac{2^{32}2^{19}}{2^{2(N-2)}}=2^{55-2N}$ なので，$N<28$ まで差分攻撃が動作することが分かる．たとえば，FEAL-16 では，$p=2^{-28}$ なので必要なペア数 $m=4\times p^{-1}=2^{30}$ となり，平文-暗号文は 2^{31} 組必要となる．さらに，差分のとり方を工夫して組数を 1/4 にできる[2]ので平文-暗号文は 2^{29} 組となる（表-1 参照）．

4. おわりに

差分攻撃法の概要を FEAL を中心に紹介した．DES に適用した場合については文献2）に詳細に述べられている．差分攻撃法の DES と FEAL への適用結果は表-1 のとおりである．

最後に私見を述べさせていただく．本来，暗号アルゴリズムは提供側において十分に安全性評価が行われるべきだが，多くの場合その評価がなされていない．安全な暗号に対する社会の要求が強いこと，暗号解読技術は常に進歩し，暗号強度の評価にはノウハウの蓄積が必要なことなどの理由から，ユーザが安心して自分のシステムに合った方式を選択するための情報を提供するような，暗号評価機関が必要と考える．

☆ β の値は Filtering 手法に依存して決まる．文献2）では $\beta=2^{-19}$ ととれる手法が示されている．

参考文献

1) Aoki, K. and Ohta, K.: Differential-Linear Cryptanalysis of FEAL-8, IEICE Trans. Fundamentals, Vol.E-79-A, No. 1 (1996).
2) Bihan, E. and Shamir, A. : Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag (1993).
3) Langford, S. and Hellman, M. : Differential-linear Cryptanalysis, CRYPTO '94
4) 松井：線形攻撃法，本特集．
5) Miyaguchi, S., Shiraishi, A. and Shimizu, A. : Fast Data Encipherment Algorithm FEAL-8, Review of ECL, Vol.36, No.4 (1988).

（平成8年1月23日受付）

太田 和夫（正会員）

昭和52年早稲田大学理工学部数学科卒業．昭和54年同大学院修士課程修了．同年電電公社（現 NTT）入社．情報セキュリティの研究に従事．現在，NTT 情報通信研究所主幹研究員．電気通信大学客員教授．理学博士．平成4年電子情報通信学会業績賞，小林記念特別賞受賞．電子情報通信学会，IACR 各会員．

青木和麻呂

平成5年早稲田大学理工学部数学科卒業．平成7年同大学院修士課程修了．同年 NTT 入社．情報セキュリティの研究に従事．現在 NTT 情報通信研究所社員．SCIS '95 および96論文賞受賞．電子情報通信学会会員．