社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30（56）
2005／7／22

# GAを用いた差分攻撃・線形攻撃に強いDES S-boxの設計に関する検討

小山　淳†　村上　恭通††

†† 大阪電気通信大学通信工学科
〒572–8530 大阪府寝屋川市初町 18–8
E-mail: †m05112@webmail.osakac.ac.jp, ††yasuyuki@isc.osakac.ac.jp

**あらまし**　Feistel 型暗号は S-box の強度により全体の強度が決まることが知られている．DES は Feistel 型暗号であり，S-box の強度が十分でないため，差分攻撃・線形攻撃に弱い．従来，遺伝的アルゴリズム (Genetic Algorithm: GA) を用いて DES の S-box を設計することにより，差分攻撃に対して強度を改善する手法が報告されている．本稿では，GA におけるコーディング・交叉及び突然変異を更に改良し，評価関数を最大差分確率と最大線形確率の和とすることで，差分攻撃・線形攻撃の両攻撃に対して，従来より S-box の強度を改善することを試みる．
**キーワード**　DES, 遺伝的アルゴリズム，差分攻撃法，線形攻撃法

# Improving the security of S-boxes in DES using Genetic Algorithm

Atsushi KOYAMA† and Yasuyuki MURAKAMI††

†† Depertment of Telecommunications and Computer Networks Osaka Electro-Communication University,
18–8, Hatsu-Cho, Neyagawa, Osaka,572–8530, Japan
E-mail: †m05112@webmail.osakac.ac.jp, ††yasuyuki@isc.osakac.ac.jp

**Abstract**　As for the Feistel cipher, it is known that the security of DES depends on the strength of S-box. DES is broken with the differential attack and the linear attack. Genetic Algorithm (GA) to design secure S-boxes against the differential attack was proposed and reported. In this paper, we shall propose a new method of improving the security of S-box by using GA. We introduce a new medthod of the coding, the crossover, and the mutation. We also proposed a new fitness value by using sum of the maximum differential probability and the maximum linear probability. We confirm that the proposed GA is effective to design S-boxes which have a higer security than usual against both of the differential attack and the linear attack.
**Key words**　DES, GA, Differential Attack, Linear Attack

## 1. まえがき

DES [1] は秘密鍵長を 56bit とするアルゴリズム公開型の 64bit ブロック暗号であり，1970 年代に米国で制定されて以来，世界の標準暗号として長期に渡り使用されてきた実績を持つ．DES に対する攻撃法として，1990 年に Biham と Shamir により差分攻撃法 [2] が提案され，1993 年に松井により線形攻撃法 [3] が提案された．一般に Feistel 型暗号では，差分攻撃法・線形攻撃法に対する強度は，S-box の差分確率・線形確率により決定されるが，DES ではこれらの値が十分ではないため，安全ではない．

近年注目を集めている技術の一つに遺伝的アルゴリズム (GA: Genetic Algorithm) がある．GA は，生物進化の原理に着想を得たアルゴリズムであり，確率的探索，学習，最適化の一手法と考えることができる．事実，GA はスケジューリング問題，組み合わせ最適化問題，人工知能などの様々な分野で使用されている．GA は，基本的枠組みが規定されている程度の発展途上のアルゴリズムであるが，様々な問題を解決できる可能性を秘めている．

GA の利点の一つは，評価関数の設計の自由度の高さにある．設計者が任意に設定した評価関数により，比較的短時間で実用的な解を探索可能である．このため，暗号設計にも応用することが可能であると考えられる．しかしながら，GA は各問題に対する依存性が非常に高いため，詳細なアルゴリズムの規約がない．したがって，実用に際して普遍的な手法は存在しない．どのようにして解きたい問題に対して適した手法を提案できるかにより，得られる解の精度が左右される．

本研究では，GA により，強度の高い DES 暗号の S-box を設計する手法を提案する．従来，差分攻撃法に対して強度の高い S-box を GA により設計する手法が提案されている [1]．本

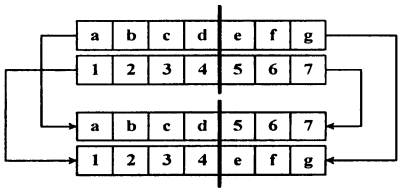


図 1 交叉の例
Fig. 1 Crossover.

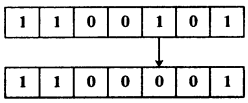


図 2 突然変異の例
Fig. 2 Mutation.

研究では，最大差分確率及び最大線形確率の和を適合度とするGA により，既に提案されている方式と違い，差分攻撃法及び線形攻撃法の両方に対して強度の高い S-box の設計を行うことが可能である．なお，コーディング・交叉及び突然変異の手法も，今までよりランダム性の高い方式を提案した．

## 2. 遺伝的アルゴリズム (GA: Genetic Algorithm)

本節では，遺伝的アルゴリズムについて述べる．

### 2.1 コーディング

解の持つ特徴を一定のルールに従って記述することにより，解を遺伝子として表現することをコーディングという．

### 2.2 初期集団

GA を行うには，まず初期集団を用意する．初期集団とは，コーディングした遺伝子の集合である．

### 2.3 選　　択

選択とは，遺伝子を評価することにより適合度を求め，次世代に残す遺伝子を決定する遺伝的操作をいう．ただし，適合度とは，評価することにより求まる値とする．

### 2.4 交　　叉

交叉とは，複数の遺伝子に対して，ある交叉位置において双方の遺伝子の一部ずつを交換することにより，子孫の遺伝子を作る遺伝的操作をいう．交叉の目的は，親から別々の良い形質を受け継ぐことにより，より良い遺伝子を作り出すことである．

代表的な交叉として一点交叉（図 1）がある．一点交叉は，任意に選んだ二つの親に対し，ランダムに選んだ一箇所において交叉点の遺伝子を入れ換えることにより，2 つの子を生成する．

### 2.5 突然変異

突然変異とは，遺伝子の一部を変化させる遺伝的操作をいう．突然変異の目的は，遺伝子が局所的な最適解に落ち着いてしまうことを防ぎ，より広い範囲で最適な解を探すことにある．

代表的な突然変異として一点突然変異（図 2）がある．一点突然変異は，ランダムに一つの値を変化させるものである．

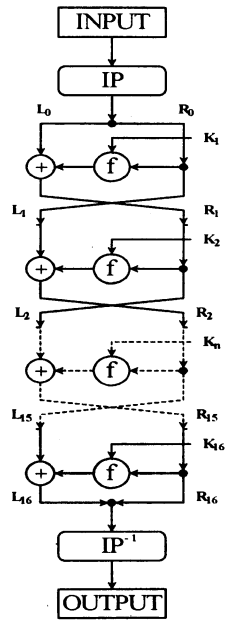


図 3 DES の基本構造
Fig. 3 Enciphering computation.

### 2.6 GA の概要

GA の流れの概略を以下に示す．

**step 1:** もとになる初期集団をいくつか用意する．

**step 2:** 遺伝子ごとに適合度を計算し，優秀な遺伝子を選択する．

**step 3:** 終了条件に合えば終了する．

**step 4:** 選んだ複数の遺伝子の交叉を確率 $P_c$ で行う．

**step 5:** 突然変異を確率 $P_m$ で行う．

**step 6:** **step 2** へ戻る．

GA の優れた点は，選択により適合度の小さい遺伝子は順次淘汰される仕組みになっていることである．これにより，良い方向に変化をした遺伝子が生き残っていくことが期待できる．進化の精度を向上させるためには，解読したい問題の性質に合わせて，コーディング・適合値の評価・選択及び交叉の手法を適切に設定することが重要である．

## 3. DES

本節では，DES について述べる．

### 3.1 DES の構造

DES の基本構造を図 3 に示す．

ただし，IP は初期置換であり，$K_n$ は鍵スケジューリング部で生成された鍵とし，$\oplus$ は bit 単位の排他的論理和を表し，$f$ は図 4 に示す暗号化関数である．$L_0, R_0$ はそれぞれ IP から出力された bit を前後半に 32bit ずつに分けたものであり，$IP^{-1}$ は最終置換である．

$n$ 段目の出力 $L_n, R_n$ は入力 $L_{n-1}, R_{n-1}$ を用いて次式により決定される．

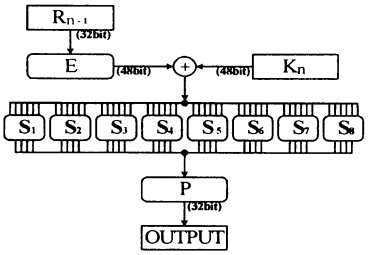


図 4 $f$ 関 数
Fig. 4 Calculation of $f$.

$$L_n = R_{n-1} \tag{1}$$

$$R_n = L_{n-1} \oplus f(K_n \oplus R_{n-1}) \tag{2}$$

### 3.2 $f$ 関 数

暗号化関数（$f$ 関数）の内部構造を図 4 に示す.

ただし，$E$ は 32bit のデータを 48bit に拡大する拡大型転置とし，$S_1 \sim S_8$ は S-box であり，$P$ は転置である.

### 3.3 S-box

S-box は DES の中に 8 個あり，図 4 のような 6bit 入力 4bit 出力の非線形テーブルの変換器である．この S-box を構成する非線形テーブルが DES 暗号の強度を決定する.

入力された 6bit のデータの両端の bit を合わせて 2bit のデータ (0 ~ 3) と考え，このデータにより，四つのテーブルの一つを決定する．残りの 4bit のデータ (0 ~ 15) を，先ほど決定したテーブルにより変換する.

データの処理は，48bit のデータを 6bit ずつ八つにわけ，出力された八つの 4bit のデータを合わせて，32bit のデータとして出力する.

## 4. DES に対する攻撃法

DES に対する有力な攻撃法である差分攻撃法・線形攻撃法と，これらに対する暗号の強度を示す最大差分確率・最大線形確率について簡単に述べる.

### 4.1 差分攻撃法 (Differential Attack)

差分攻撃法は，差分値（bit 単位の排他的論理和）が一定となる平文の組に対して，それぞれの暗号文の差分値の分布に統計的偏りを検出ことにより，解読する手法である.

平文の差分を入力差分，暗号文の差分を出力差分と呼ぶことにする．差分攻撃法は，入力差分が固定値 $\Delta x$ となる平文の対 $(x, x')$（ただし $x \oplus x' = \Delta x$）に対し，各々の暗号文 $(y, y')$ の差分 $y \oplus y'$ の値が $\Delta y$ となる確率が十分大きくなるような差分対 $(\Delta x, \Delta y)$ が求められた場合に解読することが可能となる．差分対 $(\Delta x, \Delta y)$ に対して，次式で計算される値を差分確率と呼ぶ.

$$C(\Delta x, \Delta y) = \sharp\{x \in \{0,1\}^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\} \tag{3}$$

$$\mathrm{DP}(\Delta x, \Delta y) = \frac{C(\Delta x, \Delta y)}{2^n} \tag{4}$$

ただし $\sharp\{S\}$ は集合 $S$ の位数を表す.

### 4.2 線形攻撃法 (Linear Attack)

線形攻撃法は，暗号化アルゴリズムを非線形関数と見なし，その偏りを調べることにより，解読する手法である.

一般に，暗号化アルゴリズムは，平文を入力値，暗号文を出力値とする一つの巨大な非線形関数と見なすことができる．暗号によっては，この非線形関数を適切に選ぶことにより，暗号化関数の統計的な偏りを攻撃者が得られる場合があり，解読することが可能となる．平文に関係する bit を取り出すマスク $\Gamma x$（入力マスクと呼ぶ）と，暗号文に関係する bit を取り出すマスク $\Gamma y$（出力マスクと呼ぶ）とし，線形対 $(\Gamma x, \Gamma y)$ に対して下式で計算される値を線形確率と呼ぶ.

$$C(\Gamma x, \Gamma y) = \sharp\{x \in \{0,1\}^n \mid x \cdot \Gamma x = f(x) \cdot \Gamma y\} \tag{5}$$

$$\mathrm{LP}(\Gamma x, \Gamma y) = \left(2 \cdot \frac{C(\Gamma x, \Gamma y)}{2^n} - 1\right)^2 \tag{6}$$

### 4.3 最大差分確率と最大線形確率

差分攻撃法を適用する場合において，まず，攻撃対象となる共通鍵ブロック暗号に対して，あらゆる入力差分と出力差分の組の中でできるだけ大きな差分確率を持つものを求める必要がある．このような差分確率の最大値を最大差分確率（以下 MDP ）と呼ぶ.

同様に，線形攻撃法を適用する場合において，まず，攻撃対象となる共通鍵ブロック暗号に対して，あらゆる入力マスクと出力マスクの組の中でできるだけ大きな線形確率を持つものを求める必要がある．このような線形確率の最大値を最大線形確率（以下 MLP）と呼ぶ.

MDP 及び MLP は，次式で定義される.

$$\mathrm{MDP} = \max\{\mathrm{DP}(\Delta x, \Delta y) \mid \Delta x \neq 0, \Delta y\} \tag{7}$$

$$\mathrm{MLP} = \max\{\mathrm{LP}(\Gamma x, \Gamma y) \mid \Gamma x, \Gamma y \neq 0\} \tag{8}$$

## 5. GA による S-box の設計

DES の S-box を，GA により進化させることにより，差分攻撃・線形攻撃に強い S-box の設計を試みる.

### 5.1 提案設計法の概論

以下に，提案設計法のアルゴリズムを示す.

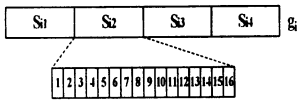


図 5　コーディング
Fig. 5　Coding.

GA による S-box の設計

初期遺伝子 $g_1, g_2, \ldots, g_N$ 生成
**for** $l = 1$ **to** $T$ {　//世代ループ
　$f_i = a \cdot \mathrm{MDP}(g_i) + b \cdot \mathrm{MLP}(g_i)$　$(a + b = 1)$
　　for $i = 1, 2, \ldots, N$; //適合度評価
　$(g_1, g_2, \ldots, g_N) \leftarrow \mathtt{select}(g_1, g_2, \ldots, g_N)$; //選択
　(最高評価遺伝子を別に保存)
　乱数 $0 \leqq r \leqq 1$ 発生
　**if** ( $r < P_c$ ){　//交叉実行確率判定
　　$i, j$ を選ぶ
　　$(g_i, g_j) \leftarrow \mathtt{crossover}(g_i, g_j)$; // $g_i$ と $g_j$ を交叉
　　　for $i, j = 1, 2, \ldots, N$;
　}
　乱数 $0 \leqq r \leqq 1$ 発生
　**if** ( $r < P_m$ ){　//突然変異実行確率判定
　　$i$ を選ぶ
　　$g_i \leftarrow \mathtt{mutation}(g_i)$; // $g_k$ を突然変異
　　　for $i = 1, 2, \ldots, N$;
　}
}
$f_i$ の小さい遺伝子を出力 for $i = 1, 2, \ldots, N$;

ただし，$g_i$および $f_i (i = 1, 2, \ldots, N)$ はそれぞれ遺伝子および遺伝子の適合度とし，$N$ 及び $T$ はそれぞれ遺伝子数と世代数であり，$P_c$ 及び $P_m$ は交叉確率，突然変異確率とする．

### 5.2　コーディング・遺伝子生成

S-box を 256bit のデータ列の遺伝子としてコーディングする．S-box は，$4 \times 16$ の行列 $S = (s_{ij})$ により，一意に表現することができる．各行には 0 ～ 15 の値が一つずつ格納されている．すなわち，

$$s_{ij} \in \{0, 1, \ldots, 15\} \quad s_{im} \neq s_{in} (m \neq n)$$

である．この行列の全成分を 4-bit で表現し，次式のように連接することにより，256-bit の遺伝子 $g$ を一意にコーディングすることができる．

$$g = [s_{11}|\cdots|s_{1,16}|s_{21}|\cdots|s_{2,16}|s_{31}|\cdots|s_{3,16}|s_{41}|\cdots|s_{4,16}]$$

この様子を図 5 に示す．

そして，$g$ を遺伝子数 $N$ 個生成する．

### 5.3　評価関数と適合度

評価関数 $E(\cdot)$ および $i$ 番目の遺伝子の適合度 $f_i$ を以下に与える．

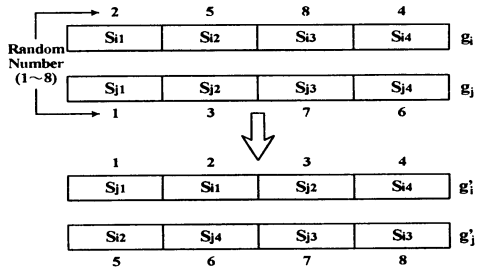


図 6　ランダム交叉
Fig. 6　Random crossover.

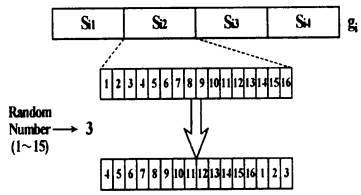


図 7　シフト突然変異
Fig. 7　Shift mutation.

$$E(g) = a \cdot \mathrm{MDP}(g) + b \cdot \mathrm{MLP}(g) \tag{9}$$

$$f_i = E(g_i) \quad (\text{for } i = 1, 2, \ldots, N) \tag{10}$$

ただし，$a, b$ はそれぞれ，MDP および MLP に対する重みとし，$a + b = 1$ とする．なお，MDP および MLP の計算にはライブラリ(注1) を使用させていただいた．

### 5.4　交　　叉

二つの遺伝子 $g_i$および $g_j$ を，それぞれコーディングにより，$S_{i1} \sim S_{i4}$ および $S_{j1} \sim S_{j4}$ 分割する．図 6 に示すように，それぞれに，1 ～ 8 の番号を割り振り，割り振られた数をキーとして，並べ替えることにより，順番を入れ替える．このように，新たな二つの遺伝子 $g_i', g_j'$ を生成する手法を交叉手法とする．本稿ではこの手法をランダム交叉と呼ぶ．

### 5.5　突 然 変 異

同様に，遺伝子 $g_i$ を，コーディングし，図 7 に示すように，$S_{i1} \sim S_{i4}$ に分割する．次に，0 ～ 15 のデータが 16 個格納された集合である．1 ～ 15 までの数をランダムに生成し，4 個の $S_i$ の中の一つを乱数により選び，生成した数だけ左に巡回シフトさせ，新たな遺伝子 $g_i'$ とする手法を突然変異手法とする．本稿ではこの手法をシフト突然変異と呼び，図 7 に示す．

### 5.6　GA のパラメータ

以下に示すパラメータを用いて GA を行った．遺伝子数 $N = 200$，世代数 $T = 2000$，交叉確率 $P_c = 0.3 \sim 0.6$，突然変異確率 $P_m = 0.1$，重み $a = 0.1, 0.2, \ldots, 0.9$ とする．最後に世代毎に評価した $f_i (i = 1, 2, \ldots, N)$ が小さい遺伝子を出力する．

(注1)：東京理科大学理工学部電気工学科の金子研究室が開発した，共通鍵ブロック暗号のための強度評価ライブラリ [5]

表 1　S-box の MDP', MLP' の比較
Table 1　MDP', MLP' of S-box.

| S-box | DES MDP' | DES MLP' | GA MDP' | GA MLP' |
|---|---|---|---|---|
| $S_1$ | 1024 | 1296 | 896 | 576 |
| $S_2$ | 1024 | 1024 | 896 | 576 |
| $S_3$ | 1024 | 900 | 896 | 576 |
| $S_4$ | 1024 | 1024 | 896 | 576 |
| $S_5$ | 1024 | 1600 | 896 | 576 |
| $S_6$ | 1024 | 784 | 896 | 576 |
| $S_7$ | 1024 | 1296 | 768 | 784 |
| $S_8$ | 1408 | 1600 | 768 | 784 |

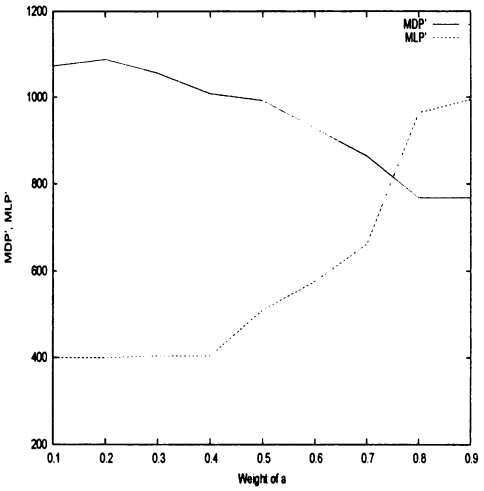


図 8　重みの変化による MDP', MLP'($P_c : 0.5, P_m : 0.1$)
Fig. 8　Fitness value by weight($P_c : 0.5, P_m : 0.1$).

## 6. 結　　果

表 1 に DES および GA により設計した S-box の MDP' 及び MLP' を示す．ただし，MDP', MLP' は，次式で定義される整数である．

$$\mathrm{MDP'} = \mathrm{MDP} \cdot 2^{2n} \tag{11}$$

$$\mathrm{MLP'} = \mathrm{MLP} \cdot 2^{2n} \tag{12}$$

ただし，GA により設計した S-box のうち，MDP' 及び MLP' の両方が小さいものを 8 個選び，その MDP' 及び MLP' を示した．DES の S-box の MDP 及び MLP に比べ，GA により設計した S-box は，MDP 及び MLP の両確率が小さいことが確認できた．

重みを変えた場合の MDP' 及び MLP' の平均値を図 8 に示す．

図 8 より，重み $a = 0.7$ 付近が MDP 及び MLP がともに小さいことがわかる．

GA により設計した S-box の一部を表 2 に示す．

表 2　GA により設計した S-box
Table 2　S-box generate by GA

| S-box | MDP' | MLP' |
|---|---|---|
| 9 12 4 3 8 15 10 2 7 13 5 11 0 1 14 6 | | |
| 6 13 11 8 0 15 14 12 2 9 10 1 7 5 3 4 | | |
| 13 4 6 1 9 8 14 3 7 10 2 15 11 0 5 12 | | |
| 12 15 1 10 4 9 7 2 6 5 11 13 8 14 3 0 | 768 | 784 |
| 5 2 7 15 9 10 4 3 11 6 1 13 8 14 12 0 | | |
| 2 14 4 9 7 6 1 11 8 5 3 0 10 13 12 15 | | |
| 0 1 12 11 7 14 8 13 2 9 15 4 6 3 5 10 | | |
| 13 2 14 15 3 4 10 12 7 11 1 0 8 5 9 6 | 768 | 784 |
| 10 14 9 4 5 6 1 15 12 11 0 2 7 13 3 8 | | |
| 7 13 15 14 4 10 0 6 9 11 3 8 5 1 12 2 | | |
| 7 12 11 3 13 10 8 6 2 15 14 4 1 9 0 5 | | |
| 4 15 11 5 0 13 14 10 9 12 7 3 8 6 2 1 | 768 | 784 |
| 12 2 11 0 1 9 6 10 8 13 4 3 14 7 15 5 | | |
| 8 12 6 10 9 1 14 5 2 15 4 11 7 0 13 3 | | |
| 8 0 15 1 14 12 13 9 11 4 6 5 2 7 10 3 | | |
| 10 6 4 1 2 14 15 0 8 13 5 11 3 7 12 9 | 768 | 784 |
| 11 2 8 9 7 1 10 5 12 13 3 15 0 14 6 4 | | |
| 12 11 0 3 15 8 13 14 9 5 2 10 6 4 1 7 | | |
| 10 13 12 15 2 1 14 8 5 0 3 9 4 7 6 11 | | |
| 6 10 1 13 0 2 14 8 5 7 11 4 12 15 3 9 | 768 | 784 |
| 5 8 15 9 3 12 14 0 4 1 11 13 10 7 6 2 | | |
| 5 3 11 2 12 15 9 6 14 8 13 10 1 7 4 0 | | |
| 15 8 12 5 11 14 13 0 4 6 7 3 9 2 1 10 | | |
| 0 5 8 4 13 6 1 12 2 10 3 9 11 15 14 7 | 896 | 576 |
| 6 4 12 13 5 15 0 10 1 14 2 7 11 9 8 3 | | |
| 15 2 3 5 11 8 0 7 9 10 4 6 12 14 13 1 | | |
| 13 10 11 15 2 1 7 12 14 0 5 6 4 9 3 8 | | |
| 7 13 3 15 12 1 9 8 0 4 10 2 5 14 6 11 | 896 | 576 |
| 14 11 6 13 2 0 4 10 12 5 7 8 15 3 9 1 | | |
| 1 7 15 5 2 9 11 14 10 8 4 0 6 3 12 13 | | |
| 4 15 5 2 1 13 7 3 6 11 14 10 12 0 9 8 | | |
| 10 7 2 6 15 12 14 3 1 8 9 0 13 5 4 11 | 896 | 576 |

## 7. 考　　察

MDP 及び MDP という二つの基本的適合度の線形結合を評価関数とした．しかしながら，暗号の場合，適合度が小さくても，MDP 及び MLP の一方が小さくならない場合には必ずしも，安全とはいえない．もう一方が下がらなければ，安全とはいえない．

したがって，実験結果より，重みを変化させると，MDP 及び MLP 収束速度が異なることがわかった．均等に両確率を下げるためには，更なる評価法，遺伝処理手法の検討が必要であると考えられる．

例えば，次式のような非線形の評価関数を用いたほうがより良い結果が得られる．

$$E'(g) = \mathrm{MDP}(g) + \mathrm{MLP}(g) + |\mathrm{MDP}(g) - \mathrm{MLP}(g)|$$

$$E''(g) = \max(\mathrm{MDP}(g), \mathrm{MLP}(g))$$

## 8. む　す　び

本稿では，DES において差分攻撃法及び線形攻撃法に対して強固な暗号を設計するために，GA を用いて S-box を設計する方法を提案した．

GA により設計した S-box は，DES の S-box に比べ，MDP 及び MLP ともに小さいことを確認することができた．すなわち，高強度の S-box を設計することができたといえる．

したがって，GA は，暗号の設計にも利用可能であることがわかった．

また，評価関数に重み付けを行うことにより，MDP 及び MLP を，均等に低下させることができること重み付けが存在することを確認することができた．同時に低下させることができることを確認することができた．したがって，差分攻撃法・線形攻撃法の両攻撃法に強い S-box の生成に GA は有効であることを確認することができた．

更なる評価関数や遺伝的手法の検討を行うことが，今後の課題である．

### 文　　献


[1] Data Encryption Standard ( DES ). National Bureau of Standards FIPS Publication 46, 1977.

[2] E.Biham and A.Shamir, "Differential Cryptanalysis of DES-Likes Cryptosystems," Advances in Cryptology-CRYPTO '90 Proceedings, Springer Verlag, 1991, pp.2-21

[3] M.Matsui, "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology -EUROCRAFT '93 Proceeding, Springer Verlag, 1994, pp.386-397.

[4] 松井良道，山口晃由，橘山智訓，大熊繁: "GA を用いた DES 暗号の S ボックス設計に関する検討", The 2001 Symposium on Cryptography and Information Security, Oiso, Japan, January 23-26, 2001 The Institute of Electronics, Information and Communication Engineers

[5] 東京理科大学理工学部電気工学科 金子研究室: "共通鍵ブロック暗号のための強度評価ライブラリ Ver1.0", 2004 年 2 月 2 日, http://www.rs.noda.tus.ac.jp/ kanekolb/