社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

隣接S-boxの影響を一部考慮したDESの経路探索

青木和麻呂　首藤一幸 *

maro@isl.ntt.jp　shudoh@muraoka.info.waseda.ac.jp

NTT 情報通信研究所
〒 238–03 神奈川県 横須賀市 武 1–2356

*早稲田大学理工学部情報学科
〒 169 東京都 新宿区 大久保 3–4–1

あらまし　差分解読法や線形解読法に対する安全性を表す指標に最大差分特性確率、最大線形特性確率がある。松井が提案した探索アルゴリズムにより DES に対する最大差分特性確率や最大線形特性確率はすでに求められている。このアルゴリズムは DES の最小構造である S-box の差分特性確率や線形特性確率を求め、それから F関数の差分特性確率や線形特性確率を導き、最終的にアルゴリズム全体の差分特性確率や線形特性確率に拡張している。しかし実際には、計算量の問題から 1 つの F関数内の 8 つの S-box の差分特性確率や線形特性確率が独立に求められると仮定して差分特性確率や線形特性確率が求められていた。

今回の報告では DES の S-box の差分特性確率や線形特性確率が独立であるとの仮定を一部外して行なった最良経路探索法と探索結果を報告する。

和文キーワード　最大差分特性確率, 最大線形特性確率, 探索アルゴリズム, DES

*首藤は平成 8 年 3 月 NTT 情報通信研究所で本研究に参加

Characteristic Search for DES Considering Effect of Adjacent S-boxes

Kazumaro AOKI　Kazuyuki SHUDOH *

maro@isl.ntt.jp　shudoh@muraoka.info.waseda.ac.jp

NTT Laboratories
1–2356 Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan

*Department of Information and Computer Science, School of Science and Engineering, Waseda University
3–4–1 Ookubo, Shinjuku-ku, Tokyo-to, 169 Japan

Abstract　The maximum differential characteristic probability and maximum linear characteristic probability are security indicators for differential cryptanalysis and linear cryptanalysis. Matsui's search algorithm is used to find the maximum differential characteristic probability and maximum linear characteristic probability of DES. His algorithm first calculates the differential characteristic and linear characteristic probabilities of S-boxes which are the minimum structure of DES, and then introduces the differential characteristic and linear characteristic probabilities of an F function. Finally, the algorithm expands the differential characteristic and linear characteristic probabilities into an entire cipher algorithm. However, the differential characteristic and linear characteristic probabilities which Matsui's algorithm determines are calculated under the assumption that differential characteristic and linear characteristic probabilities of 8 S-boxes for an F function are independent due to the complexity of these probabilities. However, the differential characteristic and linear characteristic probabilities which Matsui's algorithm determines are calculated under the assumption that differential characteristic and linear characteristic probabilities of 8 S-boxes and that of an F function are independent due to the complexity of these probabilities.

This paper describes an investigation of the maximum differential characteristic and maximum linear characteristic probabilities using fewer assumptions for S-box independence than in differential characteristic and linear characteristic probabilities of the F function.

英文 key words　Maximum Differential Characteristic Probability, Maximum Linear Characteristic Probability, Search Algorithm, DES

*SHUDOH participated in this research at NTT Laboratories during March 1996.

1 はじめに

差分解読法 [BS91] および線形解読法 [M94] という共通鍵ブロック暗号に対する強力な解読法が発表されて以来、これらの解読法に対する安全性評価は重要な課題となった。

差分解読法、線形解読法のどちらも最初の発表では局所的な性質を解析し、それを暗号アルゴリズム全体に拡張し、解読に必要な選択平文量や、既知平文量を制する差分特性確率や線形特性確率を導出し、これらの値により安全性を評価していた。しかし、それぞれの解読法に対する安全性はいわゆる多重経路 (multiple paths) を考慮した評価によらなければ正確な評価ができないといわれている [LMM91, N95]。

そこで現在、多重経路を考慮した評価ができるような暗号系が設計されているが (例えば文献 [M96])、従来から存在する暗号系に対する評価も重要な課題として残っている。

すでに差分解読法や線形解読法に対する安全性評価手法として、最大差分特性確率や最大線形特性確率を導出するアルゴリズムが提案されている [M95]。しかし、実際の適用としては計算量の問題から、多重経路が考慮されていないばかりではなく、F関数内の局所構造である複数の S-box に対して成り立つ統計的性質が独立だと仮定されて最大差分特性確率や最大線形特性確率が導出されていた。実際この仮定が成り立たない実例も見つかっている [K93b, OMA95][1]。

本稿では DES 型暗号に対して、F関数内の複数の S-box の統計的性質が一部独立でないと仮定した最大差分特性確率や最大線形特性確率を導出するアルゴリズムを提案し、適用した結果を報告する。

アルゴリズムを適用した結果、線形解読法に対する安全性は、DES では従来知られていたものと同じであること、8 段以上の偶数段 s^2DES ではランダムに鍵を選んだときに確率 1/4 で安全性が従来知られていたものより若干低いこと、6,14 段の s^3DES ではランダムに鍵を選んだときに確率 1/2 で従来より低い、確率 1/2 で従来より高い安全性をもつことがわかった。

[1]文献 [OMA95] の Appendix で指摘されている DES の数値例は誤っている。正しい例として、$K_i[4,6] = K_i[5,7] = 0$ で、$(\Gamma O_i, \Gamma I_i) = (02100820, 00000193)$ のとき、Piling-up Lemma を使った場合は $p'_i(\Gamma O_i, \Gamma I_i) = 1.13 \times 2^{-6}$ で、式 (4) を使った定義通りの値は $p'_i(\Gamma O_i, \Gamma I_i) = 1.13 \times 2^{-4}$ というのがある。

2 準備

本稿では、DES 型暗号の初期転置 IP、最終転置 IP^{-1}は評価対象とした差分特性確率および線形特性確率に全く影響を与えないので省略する。64 ビット鍵のパリティビットを除去する選択的転置 $PC{-}1$ も省略し、鍵は 56 ビットであるとして扱う。また、基本的に線形解読法に関してのみ記述するが、差分解読法と線形解読法の双対性 [M95] により本稿の結果はそのまま差分解読法にも適用可能である。

次に用いる記号、用語を定義する。括弧内の数字はその文字が表すビット数である。またビット位置は最下位ビットを 0 とおく。さらに S-box の番号 jは $1 \leqq j \leqq 8$ を代表値とするmod8 で考える。

P	平文 (64)
P_H	平文の上位半分 (32)
P_L	平文の下位半分 (32)
C	暗号文 (64)
C_H	暗号文の上位半分 (32)
C_L	暗号文の下位半分 (32)
K	鍵 (56)
I_i	第 i 段 F関数の入力値 (32)
O_i	第 i 段 F関数の出力値 (32)
K_i	第 i 段拡大鍵 (48)
I_i^j	第 i 段第 j番 S-box の入力値 (6)
O_i^j	第 i 段第 j番 S-box の出力値 (4)
K_i^j	I_i^jに排他的論理和する鍵 (6)
$F_i(I_i, K_i)$	第 i 段 F関数
$S_i^j(I_i^j)$	第 i 段第 j番 S-box
Γx	x に対するマスク値
Δx	x に対する差分値
$\oplus$	ビット毎の排他的論理和
$\bullet$	ビット毎の論理積
$\|\|$	ビット列の連結
$x[t]$	x の第 t ビット
$x[t:u]$	x の第 t ビットから第 u ビット
$x[t_1, \ldots, t_a]$	$x[t_1] \oplus \cdots \oplus x[t_a]$
$x[\Gamma x]$	$x \bullet \Gamma x$ の偶数パリティ

このとき、定義より明らかに以下の関係が成立する。

$$\begin{aligned} O_i &= F_i(I_i, K_i) \\ O_i^j &= S_i^j(I_i^j) \end{aligned}$$

上で定義した記号を用いると、第 i 段第 j番 S-box に対して、

$$I_i^j[\Gamma I_i^j] \oplus O_i^j[\Gamma O_i^j] = 0 \qquad (1)$$

第 i 段 F関数に対して、

$$I_i[\Gamma I_i] \oplus O_i[\Gamma O_i] \oplus K_i[\Gamma K_i] = 0 \qquad (2)$$

DES 型暗号全体に対して、

$$P[\Gamma P] \oplus C[\Gamma C] \oplus K[\Gamma K] = 0 \qquad (3)$$

という線形表現が定義できる。

またそれぞれの線形表現に対して、入力値 I または Pをランダムに与えた場合の成立確率を次のように定義する。

DES 型暗号全体	$p(\Gamma P, \Gamma C, \Gamma K)$
第 i 段 F関数	$p_i(\Gamma O_i, \Gamma I_i, \Gamma K_i)$
第 i 段第 j番 S-box	$p_i^j(\Gamma O_i^j, \Gamma I_i^j)$

マスク値が自明な場合は引数を省略する。

また任意の確率 qに対して偏差を $q' = q - 1/2$ と定義し、偏差を Piling-up したもの $[q'_1, q'_2, \ldots, q'_t]$ を以下の式で定義する。

$$[q'_1, q'_2, \ldots, q'_t] = \frac{1}{2}\prod_{i=1}^{t}(2q'_i) \qquad (4)$$

3 従来探索法の問題点

線形解読法に対する安全性を表す指標として最大線形特性確率がある。いくつかの DES 型暗号 (DES[U.S77], s^2DES[K93a], s^3DES[KPL93], s^5DES[KLPL95]) に対しては、文献 [M95] による探索アルゴリズムによりすでに求まっている [M95, TSM95, TSM94, STM94, LSK95][2]。

文献 [M95] の探索法は、局所的に求めた統計的性質を暗号アルゴリズム全体に拡張するという手法をとっている。すなわち単独の S-box について求めた性質を F関数に、F関数についての性質を暗号アルゴリズム全体に拡張する。具体的には、n 段 DES 型暗号において、第 i 段第 j番 S-box の

$$\Gamma I_i^j,\ \Gamma O_i^j,\ p_i^j\ (1 \leqq j \leqq 8)$$

から、第 i 段 F関数の

$$\Gamma I_i,\ \Gamma O_i,\ \Gamma K_i,\ p_i\ (1 \leqq i \leqq n)$$

を導き、これらから

$$\Gamma P,\ \Gamma C,\ \Gamma K,\ p$$

を導く。p_i^jから p_i、そして p を導くときに、Piling-up Lemma を用い、p_i,p は次のように計算される。

$$p'_i = [p'^1_i, p'^2_i, \ldots, p'^8_i]$$

$$p' = [p'_1, p'_2, \ldots, p'_n]$$

ここで近似が行なわれている。Piling-up Lemma は、Piling-up される確率変数が独立であることを要求する。しかし、隣接する S-box の統計的性質は独立ではない。F関数の入力はまず転置 Eで拡大されるため、第 j番、第 $(j+1)$番 S-box の入力 I_i^j、I_i^{j+1}は、F関数の入力 I_i中のある 2 ビットを共有しているからである (図 1)。

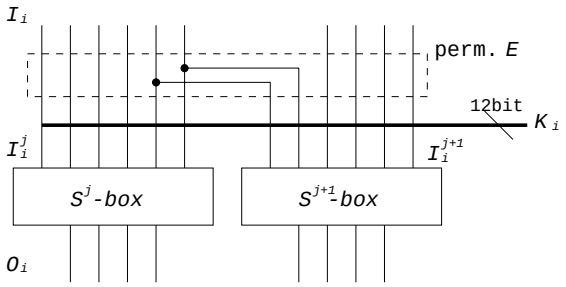


図 1: 入力の共有

それぞれの S-box の番号 jに対して、(1) 式が成立するか否かは独立ではないが、独立だという仮定をおいて Piling-up Lemma を用いている。このために、一般には、(2) 式の成立確率という定義通りの値と F関数の p_iの値が異なる。これは、文献 [OMA95] によって指摘されている。

[2]我々の知る限りでは s^3DES, s^5DES の最大差分特性確率はまだ定まっていない。

しかし、p_iの真の値の算出は空間および時間計算量の双方の問題から困難である。そのため文献 [M95] の探索法では、計算量を抑えるために個々の S-box に成り立つ統計的性質は独立だという仮定をおいていた。

4 隣接 S-box の相関を一部考慮した経路探索

本章では、従来の探索法においては独立だと仮定されていた隣接する S-box の統計的性質を一部独立ではないと仮定しての、最良線形表現、およびその成立確率の探索アルゴリズムを述べる。このアルゴリズムは文献 [M95] のアルゴリズムの拡張となっている。

複数の S-box をまとめて近似する、というのが基本のアイディアである。8 個の S-box を同時に近似できれば、定義通りの真の特性確率が得られ、真の “最良” 表現が得られるが、計算量の問題からそれは困難である。よってここでは 2 個以上 8 個以下の S-box をまとめて近似する。このとき、一度に近似する S-box が 1 個である場合より探索の計算量が増す。どの程度増すかは、いくつまでの隣接 S-box をまとめて近似するかによる。今回の実験では、まとめて近似する S-box は 2 個までとした。

まず文献 [M95] の探索アルゴリズムを紹介し、次に提案探索アルゴリズムの詳細を述べる。

4.1 松井の探索アルゴリズム

文献 [M95] では、DES のように変換テーブルを用いるインボリューション構造の暗号方式において最良差分特性または最良線形表現、またその特性確率を導出する探索アルゴリズムが紹介されている。

既知の i 段 ($1 \leqq i \leqq n-1$) の最大特性確率 $BEST_i$から n 段の最大特性確率 $BEST_n$を導出する。探索中は、$BEST_n$の候補$\overline{BEST_n}$が更新されていき、実行終了時に $BEST_n = \overline{BEST_n}$ となる。$[p'_1, p'_2, \ldots, p'_t]$ の定義は (4) 式の通りである。

$\overline{BEST_n}$の初期値は、$BEST_n$の値よりも小さく取っておけばアルゴリズムは正しく動く。ただ、できるだけ大きく取っておけばそれだけ探索時間を短くできる。

Procedure Round-1:

For each candidate for ΓO_1, do the following:

- ▷ Let $p'_1 = \max_{\Gamma I} |p'_1(\Gamma O_1, \Gamma I)|$.
- ▷ If $[p'_1, BEST_{n-1}] < \overline{BEST_n}$, then try another candidate for ΓO_1.
- ▷ Call *Procedure Round-2*.

Let $BEST_n = \overline{BEST_n}$.

Exit the program.

Procedure Round-2:

For each candidate for ΓO_2 and ΓI_2, do the following:

- ▷ Let $p'_2 = |p'_2(\Gamma O_2, \Gamma I_2)|$.
- ▷ If $[p'_1, p'_2, BEST_{n-2}] < \overline{BEST_n}$, then try another candidate for ΓO_2 and ΓI_2.
- ▷ Call *Procedure Round-3*.

Return to the upper procedure.

Procedure Round-i ($3 \leqq i \leqq n-1$):

For each candidate for ΓI_i, do the following:

- ▷ Let $\Gamma O_i = \Gamma O_{i-2} \oplus \Gamma I_{i-1}$.
- ▷ Let $p'_i = |p'_i(\Gamma O_i, \Gamma I_i)|$.
- ▷ If $[p'_1, p'_2, \ldots, p'_i, BEST_{n-i}] < \overline{BEST_n}$, then try another candidate for ΓI_i.
- ▷ Call *Procedure Round-(i+1)*.

Return to the upper procedure.

Procedure Round-n:

Let $\Gamma O_n = \Gamma O_{n-2} \oplus \Gamma I_{n-1}$.

Let $p'_n = \max_{\Gamma I} |p'_n(\Gamma O_n, \Gamma I)|$.

If $[p'_1, p'_2, \ldots, p'_n] > \overline{BEST_n}$, then $\overline{BEST_n} = [p'_1, p'_2, \ldots, p'_n]$.

Return to the upper procedure.

4.2 Active S-box

今回の探索アルゴリズムで重要な役割を果たす active S-box と、その run—隣接した active S-box 群—について説明する。

active S-box とは、

$$\Gamma O_i^j \neq 0$$

である S^j-box を指す。

その集合 A^sは、第 i 段 F関数の出力マスク値 ΓO_iに対して

$$A^{\mathrm{s}(0\leqq \mathrm{s}<2^8)} = A(\Gamma O_i) = \{\mathrm{S}^j\text{-box}|\Gamma O_i^j \neq 0\}$$

と定義できる。ここで s は

$$s[8-j] = \begin{cases} 1 & \text{if } S^j \text{ is active.} \\ 0 & \text{if } S^j \text{ is not active.} \end{cases}$$

なる 8 ビットの値である。

隣接する active S-box の一群を、active S-box の run と呼ぶ。run に含まれる S-box の数を run の長さと呼ぶ。例えば、次の active S-box 群

$$A^{(11110110)_2} = \{S^1, S^2, S^3, S^4, S^6, S^7\} \quad (5)$$

に含まれる run は $\{S^1, S^2, S^3, S^4\}, \{S^6, S^7\}$ の 2 個、長さはそれぞれ 4, 2 で、run の集合 Rは以下の通りである。

$$R(A^{(11110110)_2}) = \{\{S^1, S^2, S^3, S^4\}, \{S^6, S^7\}\} \quad (6)$$

特に断らずに run と言った場合は、できる限り長い run を取ることとする。ここで S^8-box と S^1-box は隣接しているということに注意。隣接 S-box とは、本稿では F関数の入力値 I_i中のある共通するビットから影響を受ける複数の S-box を指すからである。

4.3 隣接する複数 S-box の同時近似

今回の探索法において、active S-box 群を run 集合へ分割するということは、まとめて近似する S-box の決定という意味を持つ。本節では隣接する S-box をまとめて近似する方法を説明する。

DES 型暗号において、単独の S-box への入力は 6 ビットである。隣接した n 個の S-box への入力は、6 ビット $\times\, n$ ではなく転置 Eで拡大される前の I_i中の

$$\begin{cases} 6n - 2(n-1) = 4n+2 & \text{if } 1 \leqq n \leqq 7 \\ 32 & \text{if } n = 8 \end{cases}$$

ビットが意味を持つ。

以下では、第 i 段について、隣接した n 個の S-box、$S^j, S^{j+1}, \ldots, S^{j+n-1}$への転置 Eへの入力値を、$I_i^{j,j+1,\ldots,j+n-1}$と表す。同様に、以下の記号を定義する。

$$\Gamma I_i^{j,j+1,\ldots,j+n-1},$$
$$O_i^{j,j+1,\ldots,j+n-1}, \Gamma O_i^{j,j+1,\ldots,j+n-1},$$
$$p_i^{j,j+1,\ldots,j+n-1}$$

$O_i^{j,\ldots,j+n-1}$、$\Gamma O_i^{j,\cdots,j+n-1}$は、単に $O_i^j, O_i^{j+1}, \ldots, O_i^{j+n-1}$、$\Gamma O_i^j, \Gamma O_i^{j+1}, \ldots, O_i^{j+n-1}$を連結しただけのものである。

$I_i^{j,j+1,\ldots,j+n-1}$が転置 Eで拡大され、第 i 段拡大鍵 K_iとの排他的論理和がとられて $I_i^j, I_i^{j+1}, \ldots, I_i^{j+n-1}$が求まり、S-box に入力される。

文献 [M95] の探索アルゴリズムでは、転置 E による拡大後の I_i^j を S-box の入力だと考えていたが、転置 Eで拡大される前の I_iを隣接 S-box 群への入力だと考えて近似を行なうことで、S-box の統計的性質が独立であるという仮定は必要なくなる。

隣接していない active S-box 群については、I_i の段階で近似せずとも統計的性質が独立であるので個々の S-box 群の線形特性確率に Piling-up Lemma を適用しても問題はない。I_iの段階でまとめて近似するのは active S-box が隣接している場合のみで充分である。

4.4 同時近似する S-box の組の決定

active S-box 群を run 集合に分割することで、まとめて近似する隣接 S-box 群が決まる。しかし、ここで単にできるだけ長い run に分割しただけでは最大 8 個の S-box をまとめて近似することになってしまう。例えば、(6) 式に従うと最大 4 個の S-box をまとめて近似することになる。

計算量を現実的な範囲に収めるためには、まとめて近似する S-box 数を制限する必要ある。そこで、run の集合 Rの各要素を、それぞれさ

らに部分 run に分割する。例えば、同時に近似する S-box 数を 2 までと決定した場合、(6) 式の run 集合中の第 1 要素 $\{S^1, S^2, S^3, S^4\}$ は、

1. $\{S^1\}, \{S^2, S^3\}, \{S^4\}$
2. $\{S^1, S^2\}, \{S^3, S^4\}$

のどちらか分割する。

第 2 要素 $\{S^6, S^7\}$ はこれ以上分割しない。$\{S^6\}, \{S^7\}$ と分割して独立に近似した後 Piling-up Lemma で結び付けるには、S^6, S^7が独立であると仮定する必要がある。まとめて近似すればその仮定は必要ないので、近似はできる限りまとめて行なうこととした。

以上により、active S-box の集合 (5) 式から、まとめて近似する S-box の組は次のように 2 通り求まる。

$$\{\{S^1\}, \{S^2, S^3\}, \{S^4\}, \{S^6, S^7\}\}$$
$$\{\{S^1, S^2\}, \{S^3, S^4\}, \{S^6, S^7\}\}$$

4.5 鍵に依存した線形特性確率

$n(2 \leqq n \leqq 7)$ 個の隣接 active S-box をまとめて特性確率を求めるためには、鍵に関する情報を $2(n-1)$ ビット仮定する必要がある[3]。その理由を述べる。以下では簡単のために、まとめて考える隣接 S-box を S^j, S^{j+2}の 2 個とする。

定義通りに特性確率を求めるならば、入力値 $I_i^{j,j+1}$ 2^{10}通りに対して、次の線形表現が成立するかどうかを調べることになる。

$$I_i^{j,j+1}[\Gamma I_i^{j,j+1}] \oplus O_i^{j,j+1}[\Gamma O_i^{j,j+1}] = 0$$

$O_i^{j,j+1}$は以下のように求められる。

$$\begin{aligned} & O_i^{j,j+1} \\ = \;& O_i^j || O_i^{j+1} \\ = \;& S_i^j(I_i^j) || S_i^{j+1}(I_i^{j+1}) \\ = \;& S_i^j(I_i^{j,j+1}[4:9] \oplus K_i^j) \\ & || \; S_i^{j+1}(I_i^{j,j+1}[0:5] \oplus K_i^{j+1}) \end{aligned}$$

S_i^j, S_i^{j+1}への直接の入力値を連結して 12 ビットと考えた

$$I_i^j || I_j^{j+1} \;\; = \;\; (I_i^{j,j+1}[4:9] \oplus K_i^j) \;||\; (I_i^{j,j+1}[0:5] \oplus K_i^{j+1})$$

は、$(000000000000)_2$から $(111111111111)_2$の任意の値を取るわけではない。

S-box を単独で近似して Piling-up Lemma で結び付けている限り、S-box への入力値 I_i^jが取り得る値の集合 $\{I_i^j\}$ は常に $\{(000000)_2, \ldots, (111111)_2\}$ で、鍵に依存することはない。ところが、まとめて近似する場合の $\{I_i^j || I_i^{j+1}\}$ は鍵に依存して決まる。$I_i^j[2:5], I_i^{j+1}[0:3]$ は I_i^j, I_i^{j+1}中の他のビットとは独立しているものの、$I_i^j[0:1], I_i^{j+1}[4:5]$ の 4 ビットが取り得る組合せが鍵のあるビットに依存するからである。

DES 型暗号の F関数には転置 Eによる拡大があり、下式のように I_i^j, I_i^{j+1}それぞれのあるビットが $I_i^{j,j+1}$中の共通のビットの影響を受けるようになっている (図 1)。

$$\begin{aligned} I_i^j[0] &= I_i^{j,j+1}[4] \oplus K_i^j[0] \\ I_i^{j+1}[4] &= I_i^{j,j+1}[4] \oplus K_i^{j+1}[4] \\ I_i^j[1] &= I_i^{j,j+1}[5] \oplus K_i^j[1] \\ I_i^{j+1}[5] &= I_i^{j,j+1}[5] \oplus K_i^{j+1}[5] \end{aligned}$$

これより

$$\begin{aligned} I_i^j[0] \oplus I_i^{j+1}[4] &= K_i^j[0] \oplus K_i^{j+1}[4] \\ I_i^j[1] \oplus I_i^{j+1}[5] &= K_i^j[1] \oplus K_i^{j+1}[5] \quad (7) \end{aligned}$$

となる。これは、鍵の情報 2 ビットにより、$I_i^j[0], I_i^j[1], I_i^{j+1}[4], I_i^{j+1}[5]$ の 4 ビット、ひいては $I_i^j || I_i^{j+1}$の取り得る値が制約を受けることを示している。

隣接する 2 個の S-box を独立とみなして Piling-up Lemma で結びつけた場合、線形表現の成立確率は $I_i^j || I_i^{j+1} 2^{12}$通りに対して求められていた。独立だと仮定しないで同時に近似するということは、(7) 式の 2 ビットによって 2^{12}を 4 等分し、4 つの領域それぞれについて確率を求めることになる。線形表現成立の場合の数が、分割された領域に均等に分かれるならば、求まる確率は領域分割なしと変わらない。均等でなければ、Piling-up Lemma で結びつけるよりも大きな $|p_i'|$、特性確率が導出されることになる。従って安全性の評価結果が異なってくる可能性がある。

以上のように隣接 S-box をまとめて近似すると、(7) 式の値に依存して特性確率が複数求まる

[3] $n = 8$ のときは、鍵に関する情報を 16 ビット仮定する必要がある。

場合がある。特性確率が鍵に依存するわけである。今回の探索では (7) 式の値として解読者にとってもっとも都合のよいものを選択した。その結果得られる線形表現、特性確率は (7) 式の値がある条件を満たした場合のものとなる。鍵がその条件を満たさない場合、その線形表現は本稿で示す値以下の特性確率を持つことになる。

本節では隣接 S-box 2 つの同時近似について述べたが、3 つ以上の S-box の同時近似も同様に考えることができる。

4.6 提案探索アルゴリズム

文献 [M95] の探索アルゴリズムを基に、提案アルゴリズムを構成する。

今回の探索アルゴリズムと文献 [M95] のアルゴリズム (Matsui's Algorithm) の相違を n 段探索について述べる。主に active S-box に関するもので、以下の通りである。

- *Procedure Round-1,2*:

  Matsui's Algorithm: S-box を順に辿り、特性確率を Piling-up していく。

  Our Algorithm: active S-box 群 A^s の候補それぞれ ($0 \leqq s < 2^8$) に対して、同時近似する S-box の組 (run) を決定、run を順に辿って特性確率を Piling-up していく。

- *Procedure Round-i* ($3 \leqq i \leqq n-1$):

  F関数の出力値に対するマスク値が決まる。
  $\Gamma O_i = \Gamma O_{i-2} \oplus \Gamma I_{i-1}$

  Matsui's Algorithm: S-box を順に辿り、特性確率を Piling-up していく。

  Our Algorithm: $A(\Gamma O_i)$ を求め、同時近似する S-box の組 (run) を決定し、run を順に辿って特性確率を Piling-up していく。

5 実験結果

第 4章で述べたアルゴリズムを実装、探索を行なった結果を報告する。

5.1 DES についての探索

1 段から 20 段の DES について探索を行なった。得られた最良線形表現、最大線形特性確率は、既知の値 [M94] と全く同じであった。

5.2 s^2DES についての探索

1 段から 20 段の s^2DES について探索を行なった結果、8 段以上の偶数段 s^2DES について、鍵の値によっては従来知られていたよりも安全性が低いことがわかった。

図 2に、8 段以上の偶数段 s^2DES の最良線形表現を示す。最終段では S^7, S^8がまとめて近似されていて、特性確率が鍵の値に依存している。図の線形表現は、鍵がある条件を満たしている場合の最良表現である。

図 2から最終段を除いたものは 7 段以上の奇数段 s^2DES の最良線形表現となっている。この場合は鍵に関する条件はない。

得られた条件付き最良線形表現とその特性確率を、文献 [M95] のアルゴリズムで得られる値と比較する。

文献 [M95] のアルゴリズムで得られる最良線形表現と特性確率は、

$$P_L[5,10,11] \oplus C_H[5,10,11] = \bigoplus_{i=1}^{8} K_{2i}[4,5,6,7]$$

$$BEST_{16} = 1.19 \times 2^{-26} \qquad (8)$$

今回の探索法で得られた最良線形表現と特性確率は

$$\begin{aligned} & P_L[5,10,11] \oplus C_H[5,10,11] \oplus C_L[0,5,6,8] \\ = \quad & K_{16}[1,8,9,11] \oplus \bigoplus_{i=1}^{7} K_{2i}[4,5,6,7] \end{aligned}$$

$$BEST_{16} = 1.51 \times 2^{-26} \qquad (9)$$

ただし、上の線形表現が (9) 式の特性確率を持つのは、鍵が次の条件を満たす場合のみである[4]。

$$K_{16}[4,6] = 0 \text{ かつ } K_{16}[5,7] = 1$$

[4] この場合、鍵準備アルゴリズムを考慮してもこのような条件を満たす鍵は存在する。

この条件が満たされないと特性確率は以下のように小さくなる。

$$|p'| = \begin{cases} 1.59 \times 2^{-28} & \text{if } K_{16}[5,7]{=}0 \\ 1.75 \times 2^{-27} & \text{if } K_{16}[4,6]{=}K_{16}[5,7]{=}1 \end{cases}$$

同様に、8 段以上の偶数 (n) 段について図 3、表 1の最大線形特性確率が得られるのは、鍵が次の条件を満たす場合のみである。

$$K_n[4,6] = 0 \text{ かつ } K_n[5,7] = 1$$

つまり表1の最大線形特性確率は、鍵が持つ情報 56 ビットのうち 2 ビットに仮定をおいての値、ということになる。

表 1: s^2DES についての最大線形特性確率

n rounds	最大線形特性確率$-1/2$
2	$+1.13 \times 2^{-2}$
3	$+1.27 \times 2^{-3}$
4	-1.91×2^{-6}
5	$+1.20 \times 2^{-7}$
6	$+1.12 \times 2^{-10}$
7	$+1.65 \times 2^{-11}$
$\star$ 8	$+1.96 \times 2^{-14}$
9	$+1.54 \times 2^{-14}$
$\star$ 10	$+1.83 \times 2^{-17}$
11	$+1.45 \times 2^{-17}$
$\star$ 12	$+1.72 \times 2^{-20}$
13	$+1.36 \times 2^{-20}$
$\star$ 14	$+1.61 \times 2^{-23}$
15	$+1.27 \times 2^{-23}$
$\star$ 16	$+1.51 \times 2^{-26}$
17	$+1.19 \times 2^{-26}$
$\star$ 18	$+1.42 \times 2^{-29}$
19	$+1.12 \times 2^{-29}$
$\star$ 20	$+1.33 \times 2^{-32}$

$\star$:鍵の情報 56 ビットのうち
2 ビットを仮定した場合の値

5.3 s^3DES についての探索

1 段から 20 段の s^3DES について探索を行なった。6 段,14 段 s^3DES は、鍵の値によっては従来知られていたよりも安全性が低いことがわかった。

6,14 段 s^3DES について文献 [M95] のアルゴリズムで得られるものとは異なった最大線形特性確率を得たが、その特性確率に対応する最良線形表現は、文献 [M95] のアルゴリズムで得られるものと同じであった。つまり、S^4, S^5が独立だと仮定した場合としない場合で、異なる特性確率が算出されたことになる。

14 段 s^3DES についての結果について比較する。

文献 [M95] のアルゴリズムで得られる最大特性確率は

$$BEST_{14} = 1.48 \times 2^{-21} \qquad (10)$$

今回の探索で得た最大特性確率は

$$BEST_{14} = 1.58 \times 2^{-21} \quad \text{if } K_1[16,18] = 0$$
$$BEST_{14} = 1.38 \times 2^{-21} \quad \text{if } K_1[16,18] = 1$$

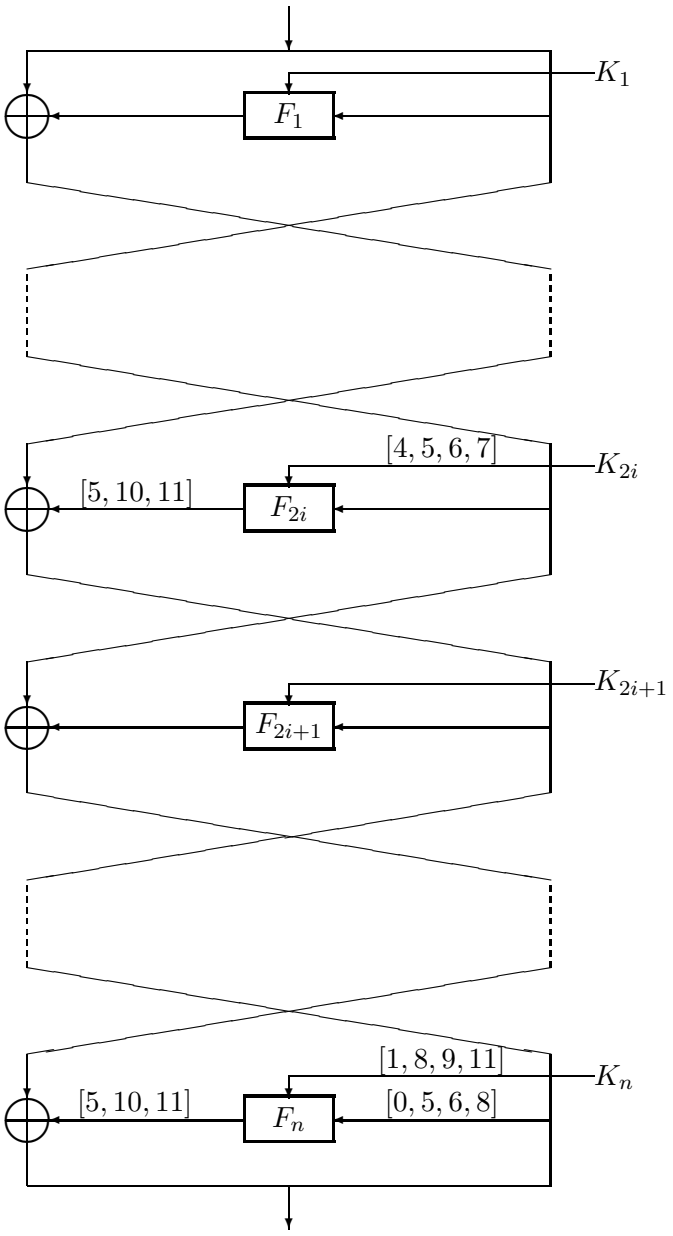
最大線形特性確率が鍵の情報 1 ビットに依存している。

6 まとめ

我々は文献 [M95] の経路探索アルゴリズムを拡張し、F関数内の S-box に成り立つ統計的性質が独立であるとの仮定を一部はずした経路探索を可能とした。

また、その拡張アルゴリズムを DES, s^2DES, s^3DES に適用し、線形解読法に対する安全性を評価した。その結果、DES については同じ、s^2DES と s^3DES については安全性が従来知られているより若干低いことがわかった。

今回は時間の制約上 s^5DES の評価、および差分解読法に対する安全性評価ができなかった。今後の予定として、まずこの残された問題を解決し、また、さらに仮定が少ない経路探索アルゴリズムを樹立する。探索アルゴリズム中で F関数の特性確率が必要になったときにその値を少ない計算量で導出できれば、F関数の特性確率算出に関しては仮定が必要なくなる。このためには多少の事前計算と、転置 Eと S-box の関係の細かい解析をすればよいだろう。



最終段以外は 2 段の繰り返し線形表現で構成されている。

図 2: 8 段以上 20 段以下の偶数段 s^2DES についての最良線形表現

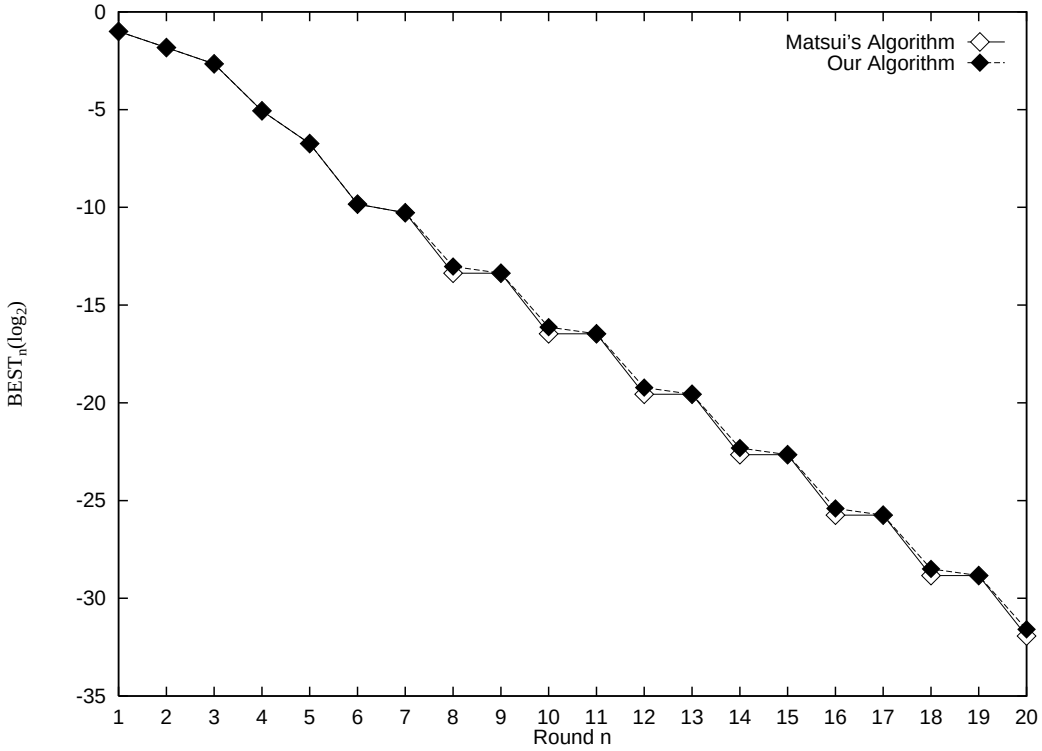


図 3: s^2DES についての $BEST_n$

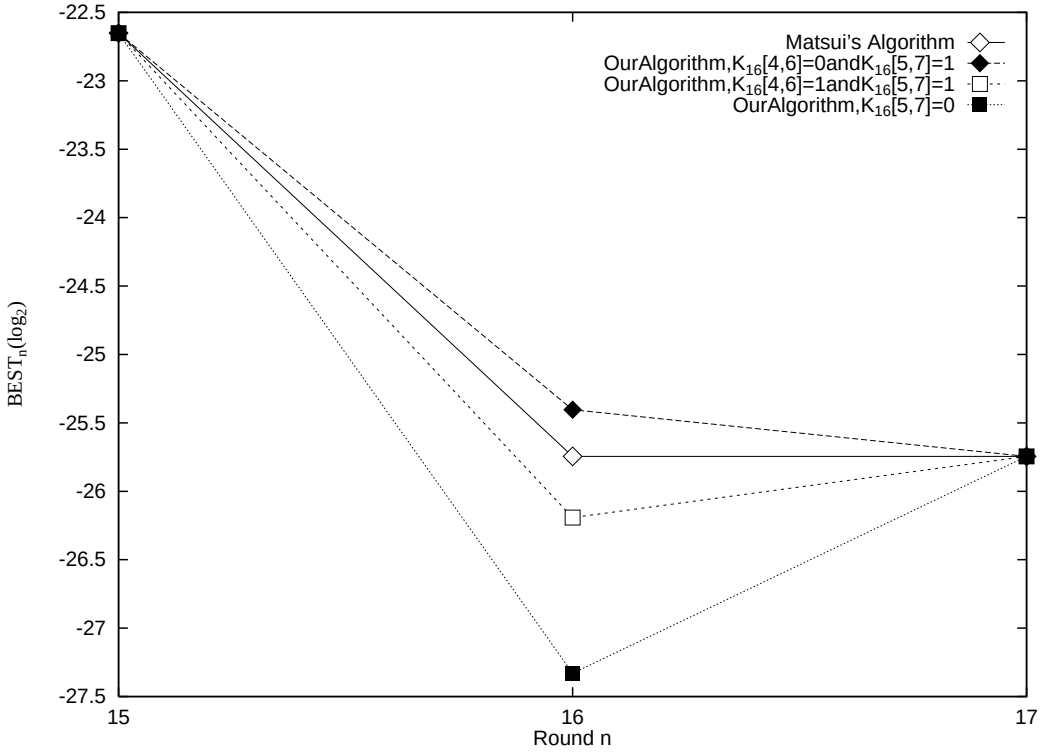


図 4: 16 段 s^2DES についての最良表現における 鍵と特性確率の関係

参考文献

[BS91] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1, pp. 3–72, 1991. (The extended abstract appeared at CRYPTO'90).

[K93a] K. Kim. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. In H. Imai, R. L. Rivest, and T. Matsumoto, editors, *Advances in Cryptology — ASIACRYPT'91*, volume 739 of *Lecture Notes in Computer Science*, pp. 59–72. Springer-Verlag, Berlin Heidelberg New York, 1993.

[K93b] L. R. Knudsen. Iterative Characteristic of DES and s^2-DES. In E. F. Brickell, editor, *Advances in Cryptology — CRYPTO'92*, volume 740 of *Lecture Notes in Computer Science*, pp. 497–511. Springer-Verlag, Berlin Heidelberg New York, 1993.

[KLPL95] K. Kim, S. Lee, S. Park, and D. Lee. How to Strengthen DES against Two Robust Attacks. In *1995 Japan-Korea Joint Workshop on Information Security and Cryptology*, pp. 173–182, Inuyama, Aichi, JAPAN, 1995. ISEC Group of IEICE (Japan) and KIISC (Korea).

[KPL93] K. Kim, S. Park, and S. Lee. Reconstruction of s^2DES S-boxes and their Immunity to Differential Cryptanalysis. In *1993 Japan-Korea Joint Workshop on Information Security and Cryptology*, pp. 386–397, Seoul, KOREA, 1993. KIISC (Korea) and ISEC Group of IEICE (Japan). (Technical report appeared at ISEC93-63).

[LMM91] X. Lai, J. L. Massey, and S. Murphy. Markov Ciphers and Differential Cryptanalysis. In D. W. Davies, editor, *Advances in Cryptology — EUROCRYPT'91*, volume 547 of *Lecture Notes in Computer Science*, pp. 17–38. Springer-Verlag, Berlin Heidelberg New York, 1991.

[LSK95] S. Lee, S. H. Sung, and K. Kim. An Efficient Method to Find the Linear Expressions for Linear Cryptanalysis. In *1995 Japan-Korea Joint Workshop on Information Security and Cryptology*, pp. 183–190, Inuyama, Aichi, JAPAN, 1995. ISEC Group of IEICE (Japan) and KIISC (Korea).

[M94] M. Matsui. Linear Cryptanalysis Method for DES Cipher. In T. Helleseth, editor, *Advances in Cryptology — EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pp. 386–397. Springer-Verlag, Berlin Heidelberg New York, 1994.

[M95] M. Matsui. On Correlation Between the Order of S-boxes and the Strength of DES. In A. D. 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.

[M96] M. Matsui. New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis. In D. Gollmann, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 1996, Proceedings*, volume 1039 of *Lecture Notes in Computer Science*, pp. 205–218. Springer-Verlag, Berlin Heidelberg New York, 1996.

[N95] K. Nyberg. Linear Approximation of Block Ciphers. In A. D. Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pp. 439–444. Springer-Verlag, Berlin Heidelberg New York, 1995.

[OMA95] K. Ohta, S. Moriai, and K. Aoki. Improving the Search Algorithm for the Best Linear Expression. In D. Coppersmith, editor, *Advances in Cryptology —*

CRYPTO'95, volume 963 of *Lecture Notes in Computer Science*, pp. 157–170. Springer-Verlag, Berlin Heidelberg New York, 1995.

[STM94] T. Sorimachi, T. Tokita, and M. Matsui. On a Cipher Evaluation Method Based on Differential Cryptanalysis (II). In *The 1994 Symposium on Cryptography and Information Security*, number 4C in SCIS94, Lake Biwa, Japan, 1994. Technical Group on Information Security (IEICE). (in Japanese).

[TSM94] T. Tokita, T. Sorimachi, and M. Matsui. An Efficient Search Algorithm for The Best Expression on Linear Cryptanalysis. Technical Report ISEC93-97, The Institute of Electronics, Information and Communication Engineers, 1994. (in Japanese).

[TSM95] T. Tokita, T. Sorimachi, and M. Matsui. Linear Cryptanalysis of LOKI and s^2-DES. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology — ASIACRYPT'94*, volume 917 of *Lecture Notes in Computer Science*, pp. 293–303. Springer-Verlag, Berlin Heidelberg New York, 1995.

[U.S77] U.S. Department of Commerce, National Bureau of Standards. *Data Encryption Standard (Federal Information Processing Standards Publication 46)*, 1977.