Linear Cryptanalysis of LOKI and s^2DES

Toshio Tokita Tohru Sorimachi Mitsuru Matsui

Computer & Information Systems Laboratory
Mitsubishi Electric Corporation
5-1-1, Ofuna, Kamakura, Kanagawa, 247, Japan
tokita@mmt.isl.melco.co.jp sori@mmt.isl.melco.co.jp matsui@mmt.isl.melco.co.jp

Abstract. This paper discusses linear cryptanalysis of LOKI89, LOKI91 and s^2DES. Our computer program based on Matsui's search algorithm has completely determined their best linear approximate equations, which tell us applicability of linear cryptanalysis to each cryptosystem. As a result, LOKI89 and LOKI91 are resistant to linear cryptanalysis from the viewpoint of the best linear approximate probability, whereas s^2DES is breakable by a known-plaintext attack faster than an exhaustive key search. Moreover, our search program, which is also applicable to differential cryptanalysis, has derived their best differential characteristics as well. These values give a complete proof that characteristics found by Knudsen are actually best.

1 Introduction

LOKI is a DES-like cryptosystem that was proposed by Brown *et al.* [5] in 1990. It has four 12-bit input/8-bit output S-boxes, all of which are the same. The first version of LOKI was redesigned due to a weakness of its key schedule part found by Knudsen *etc.* [6][8][9]. Knudsen also showed that neither of the first version, called LOKI89, nor the second version, called LOKI91, has any differential characteristics whose probability is high enough for successful differential cryptanalysis [9][10].

s^2DES was proposed by Kim [7] in 1991, which has the same structure as DES except its S-box tables. Knudsen [11] found that s^2DES has several iterative characteristics which lead to successful differential cryptanalysis. However, the best differential characteristics of LOKI89, LOKI91 and s^2DES are unknown, while those of DES have been recently calculated [3]. Moreover, as far as we know, there has been no discussion about applicability of linear cryptanalysis to these cryptosystems.

This paper for the first time discusses linear cryptanalysis of LOKI89, LOKI91 and s^2DES. We begin by studying statistical properties of their S-boxes, and then using Matsui's search algorithm [3], completely determine their best linear approximate equations. We also take into consideration, for comparison, DES variants whose S-boxes are reordered so that they are stronger in regard to differential or linear cryptanalysis [3]. As a result, we show that LOKI89 and LOKI91 are resistant to linear cryptanalysis from the viewpoint of the best linear approximate probability and even stronger than the modified DES whose

S-boxes are rearranged in the strongest order against linear cryptanalysis. On the other hand, s^2DES is just slightly stronger than the original DES, and hence breakable by a known-plaintext attack faster than an exhaustive key search.

We have implemented a computer program for breaking LOKI91 reduced to six round to estimate the number of known-plaintexts required for successful linear cryptanalysis of LOKI with arbitrary number of rounds. Our experimental results suggest that the strength of n-round LOKI89/91 corresponds to $2n$-round DES in regard to linear cryptanalysis.

Our search program has also derived the best differential characteristics of these cryptosystems, which give us a complete proof that characteristics found by Knudsen *etc.* [1][6][9][10][11] are actually best. We also show that LOKI89 and LOKI91 are even stronger than the modified DES such that the order of its S-boxes is the strongest choice in regard to differential cryptanalysis.

2 Preliminaries

2.1 Notations

Figure 1 shows the data randomization part and F-function of DES-like cryptosystems, which are the scope of this paper. We omit the initial and final permutations. Throughout this paper, the notations described here are used unless otherwise mentioned.

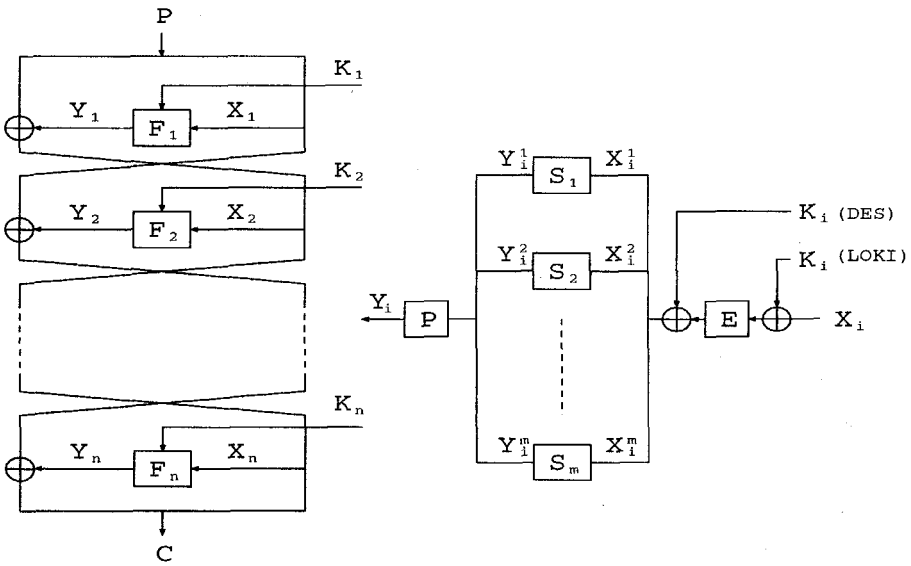

Figure 1: The data randomization part and F-function of DES-like cryptosystem.

We will discuss differential cryptanalysis and linear cryptanalysis in parallel, and for this purpose, we define the best probability of n-round cipher depending on the context as described in [3]:

[In the case of Differential Cryptanalysis]

- $P(\Delta X_i^j, \Delta Y_i^j) \stackrel{\text{def}}{=} Prob\{X_i^j \oplus \Delta X_i^j = Y_i^j \oplus \Delta Y_i^j\}$,
- $P(\Delta X_i, \Delta Y_i) \stackrel{\text{def}}{=} Prob\{F_i(X_i \oplus \Delta X_i, K_i) = Y_i \oplus \Delta Y_i\}$,
- $BEST_n^{DC} \stackrel{\text{def}}{=} \max_{\Delta X_i = \Delta X_{i-2} \oplus \Delta X_{i-1} (3 \le i \le n), (\Delta P, \Delta C) \neq (0,0)} \{ \prod_{i=1}^{n} P(\Delta X_i, \Delta Y_i) \}$,

[In the case of Linear Cryptanalysis]

- $P(\Gamma Y_i^j, \Gamma X_i^j) \stackrel{\text{def}}{=} | Prob\{ Parity(X_i^j \bullet \Gamma X_i^j) = Parity(Y_i^j \bullet \Gamma Y_i^j) \} - 1/2 |$,
- $P(\Gamma Y_i, \Gamma X_i) \stackrel{\text{def}}{=} | Prob\{ Parity(X_i \bullet \Gamma X_i) = Parity(Y_i \bullet \Gamma Y_i) \} - 1/2 |$,
- $BEST_n^{LC} \stackrel{\text{def}}{=} \max_{\Gamma O_i = \Gamma O_{i-2} \oplus \Gamma I_{i-1} (3 \le i \le n), (\Gamma P, \Gamma C) \neq (0,0)} \{ 2^{n-1} \prod_{i=1}^{n} P(\Gamma Y_i, \Gamma X_i) \}$,

where X_i^j, X_i and K_i are randomly given, and the symbol $\bullet$ represents a bitwise AND operation.

2.2 LOKI89/91 and s^2DES

LOKI is a 64-bit key/64-bit block cryptosystem similar to DES. The main difference between LOKI and DES is the F-function and the key-scheduling part. The input of the F-function of LOKI is XORed with the 32-bit subkey, and expanded to 48 bits, which enter into four 12-bit input/8-bit output S-boxes. The 12-bit input of the S-box is partitioned into two segments: a 4-bit row value '*row*' and an 8-bit column value '*col*'. The row value '*row*' is used to select one of 16 S-functions $Sfn(row, col)$, which then take as input the column value '*col*' and produce an 8-bits output value. The structure of $Sfn(row, col)$ depends on versions of LOKI as follows [6]:

$$[LOKI89] : Sfn(row, col) = (col \oplus row)^{31} mod\ g_{row},$$
$$[LOKI91] : Sfn(row, col) = (col + ((row * 17) \oplus ff_{16}) \& ff_{16})^{31} mod\ g_{row},$$

where g_{row} is an irreducible polynomial over $GF(2^8)$, which is used in forming the $\{row\}$-th S-box. We omit the detail of their key-scheduling part and the initial and final permutations, since our analysis is independent of them. (Note: ROL12 and ROL13 shown in Figure 5 in [6] must be exchanged.) s^2DES is a 56-bits key/64-bits block cryptosystem, which has the same structure as DES except its S-box tables. They are based on Boolean functions satisfying the Strict Avalanche Criterion (SAC) [7].

3 Statistical Properties of LOKI and s^2DES

3.1 Differential and Linear Characteristics of the S-boxes

In this section, we discuss the strength of LOKI and s^2DES in regard to differential and linear cryptanalysis from viewpoints of differential and linear characteristics of their S-boxes, respectively.

Figure 2 illustrates frequency distribution of differential characteristics of the S-boxes using a line graph, where the ordinate axis denotes probability p and the abscissa axis shows the ratio of the number of pairs $(\Delta X_i^j, \Delta Y_i^j)$ such that $p{=}P(\Delta X_i^j, \Delta Y_i^j)$. To normalize the size of the S-boxes, we have considered, in the case of DES and s^2DES, a 12-bit input/8-bit output table that consists of two neighboring S-boxes: S_1 and S_2.

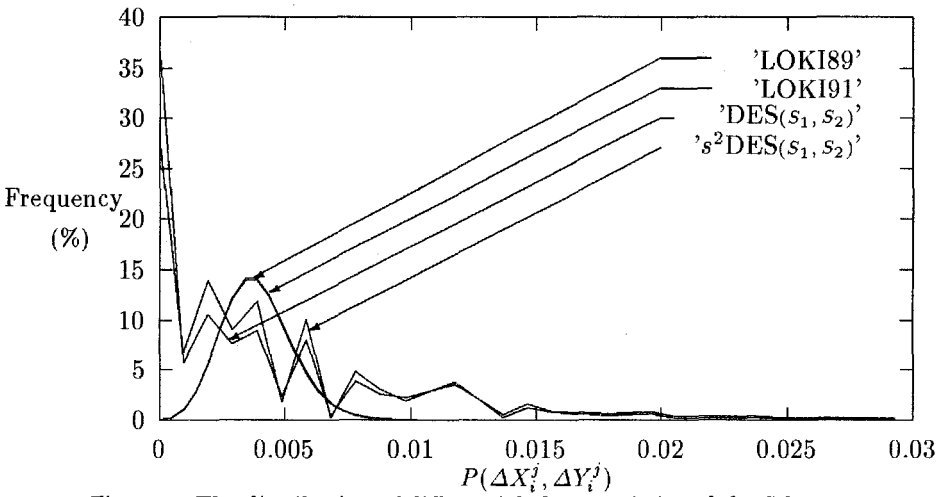

Figure 2: The distribution of differential characteristics of the S-boxes.

Characteristics of the S-boxes of LOKI89 and LOKI91 are densely distributed from $p = 0$ to $p \cong 2^{-5}$, while those of DES and s^2DES are widely distributed from $p = 0$ to $p \cong 2^{-2}$ and have many '0' entries. Note that though the distribution of LOKI89 is almost the same as that of LOKI91, their maximum values are different.

Table 1 shows the best differential characteristics of the S-boxes. The best probability of LOKI91 is lower than that of LOKI89, as the designers intended. Each of LOKI89 and LOKI91 has a unique characteristic that attains the best probability, whereas DES and s^2DES have 60 and 9 best characteristics, respectively.

	LOKI89	LOKI91	DES	s^2DES
The best probability	1.00×2^{-4}	1.03×2^{-5}	1.00×2^{-2}	1.00×2^{-2}
The best characteristic $(\Delta X_i^j, \Delta Y_i^j)$	$(004_{16}, 01_{16})$	$(004_{16}, 01_{16})$	$(34_{16}, 2_{16})of S1$ *etc.*	$(0C_{16}, D_{16})of S5$ *etc.*

Table 1. The best differential characteristic of the S-boxes.

Figure 3 illustrates frequency distribution of linear characteristics of the S-boxes using a line graph, where the ordinate axis denotes probability p and the abscissa axis shows the ratio of the number of pairs $(\Gamma Y_i^j, \Gamma X_i^j)$ such that $p=P(\Gamma Y_i^j, \Gamma X_i^j)$.

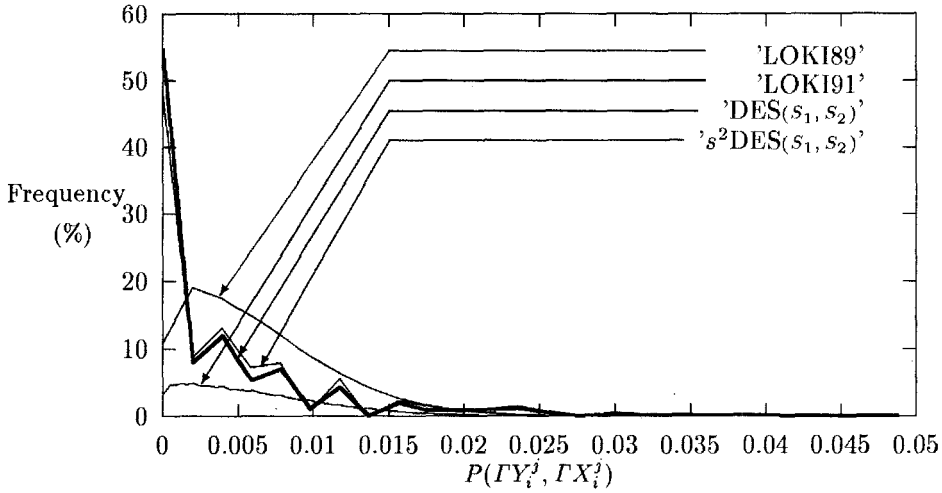

Figure 3: The distribution of linear characteristics of S-box.

Linear characteristics of the S-boxes of DES and s^2DES are widely distributed and again have many '0' entries. However, as opposed to the case of differential characteristics, the distribution of linear characteristics of LOKI89 is different from that of LOKI91, while their maximum values are almost the same.

Table 2 shows the best linear characteristics of the S-boxes. Each cryptosystem has a unique characteristic that attains the best probability. LOKI89 and LOKI91 are hence expected to be resistant to linear cryptanalysis from the viewpoint of the characteristics of their S-boxes.

	LOKI89	LOKI91	DES	s^2DES
The best probability	$\frac{1}{2} + 1.25 \times 2^{-5}$	$\frac{1}{2} - 1.28 \times 2^{-5}$	$\frac{1}{2} - 1.25 \times 2^{-2}$	$\frac{1}{2} + 1.13 \times 2^{-2}$
The best characteristic $(\Gamma Y_i^j, \Gamma X_i^j)$	$(61_{16}, F4A_{16})$	$(8D_{16}, 41F_{16})$	$(F_{16}, 10_{16})$ of S5	$(E_{16}, 1F_{16})$ of S5

Table 2. The best linear characteristic of the S-boxes.

3.2 The Best Probabilities of LOKI and s^2DES

In this section, we discuss the strength of LOKI and s^2DES in regard to differential and linear cryptanalysis from viewpoints of the best differential characteristic probability and the best linear approximate probability, respectively.

In [3] Matsui has proposed a practical algorithm for determining the best differential characteristic and linear approximate expression of DES-like cryptosystems on the basis of duality between differential cryptanalysis and linear

cryptanalysis. His program works by induction of the number of rounds n. In other words, it derives the best n-round probability $BEST_n$ from knowledge of the best i-round probability ($1 \leq i \leq n-1$). The framework of the algorithm is established by the following procedure including essentially recursive routines [3]:

Procedure Round-i:

For each candidate for ΔX_i and ΔY_i, do the following:

- $p_i = (\Delta X_i, \Delta Y_i)$,
- If $p_1 \cdot p_2 \cdot \ldots \cdot p_i \cdot BEST_{n-i}^{DC} \geq \overline{BEST_n^{DC}}$ then
  If $i = n$ then $\overline{BEST_n^{DC}} = p_1 \cdot p_2 \cdot \ldots \cdot p_n$,
  else Call *Procedure Round-(i+1)*.

If $i = 1$, then Exit the program,
else Return to *Procedure Round-(i-1)*.

We first define $\overline{BEST_n^{DC}}$ as any positive number smaller than $BEST_n^{DC}$ and then begin with *Procedure Round-1*. The program rewrites the initial value $\overline{BEST_n^{DC}}$ while running and when it completes the search, $\overline{BEST_n^{DC}}$ is equal to the actual best probability $BEST_n^{DC}$. Using this algorithm, Matsui found the best probability of DES and better orders of its S-boxes in regard to differential and linear cryptanalysis.

We have implemented this algorithm to determine the best differential characteristic probability of LOKI89, LOKI91, s^2DES and dcDES, where dcDES is a DES-variant whose S-boxes are rearranged in the strongest order against differential cryptanalysis [3]. Figure 4 summarizes our computational results.

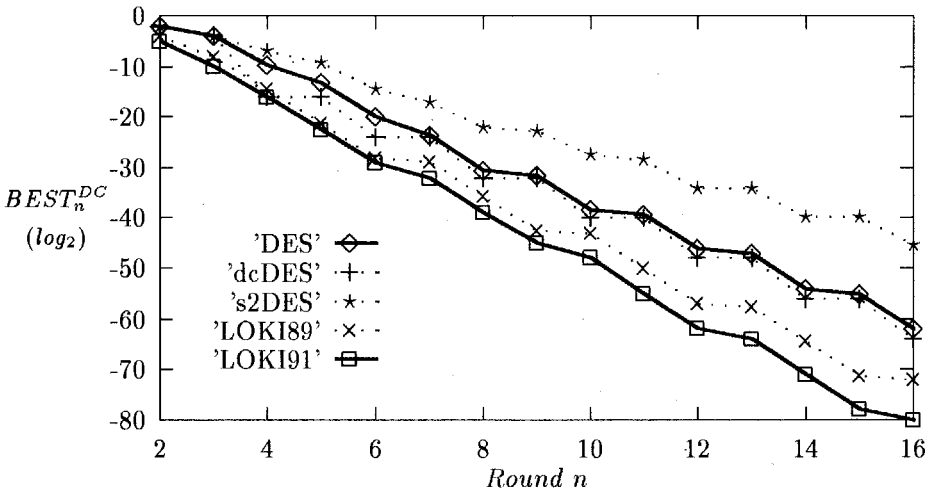

Figure 4: The best probability of differential cryptanalysis.

Though various characteristics of LOKI89, LOKI91 and s^2DES have been studied in recent works [1][9][10][11], our results first give a complete proof that some of them are actually best. For instance, the best 13-round probability of LOKI91 is 2^{-64}, which corresponds to four time repetitions of type B characteristic showed in [10]. Figure 4 indicates that LOKI91 is stronger than LOKI89, and s^2DES is weak in regard to differential cryptanalysis, as stated in [9][10][11].

The program for deriving the best differential characteristics is also applicable to calculating the best linear approximate equations. We have then derived the best linear approximate probabilities of LOKI89, LOKI91 and s^2DES, which are showed in Figure 5 with those of the original DES and lcDES, where lcDES is a DES-variant whose S-boxes are rearranged in the strongest order against linear cryptanalysis [3].

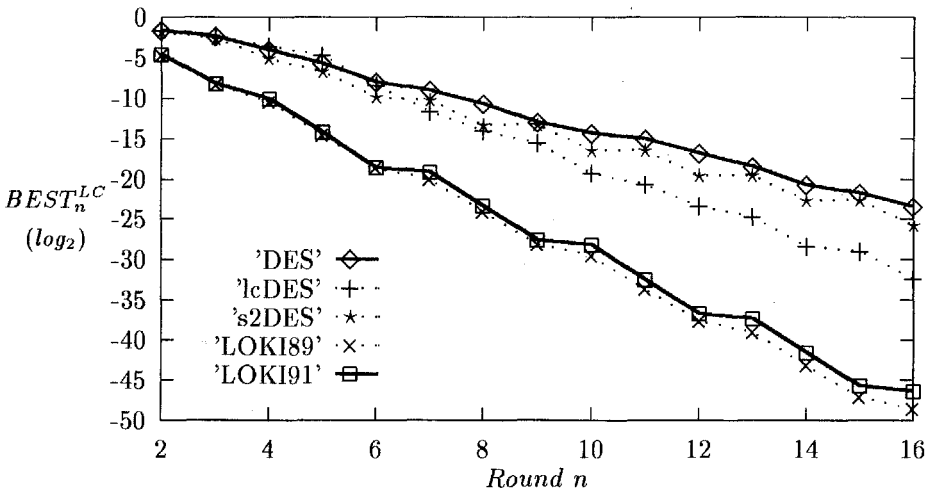

Figure 5: The best probability of linear cryptanalysis.

Figure 5 shows that LOKI89 and LOKI91 are much stronger than lcDES, and hence resistant to linear cryptanalysis. Note that LOKI89 is slightly better than LOKI91. Since s^2DES is slightly stronger than DES, it is breakable by a known-plaintext attack. Therefore, we conclude that LOKI is resistant to both differential and linear cryptanalysis from viewpoints of the best differential and linear probabilities, respectively.

The following is the best 16-round linear approximate equation of each cryptosystem, where we omit the initial and final permutations (see [2] for notations):

The best 16-round linear expression of LOKI89 holds with $BEST_{16}^{LC} = 1.37 \times 2^{-49}$:

$$P_L[30] \oplus C_L[19] = K_2[19] \oplus K_3[30] \oplus K_5[19] \oplus K_6[30] \oplus K_8[19]$$

$$\oplus K_9[30] \oplus K_{11}[19] \oplus K_{12}[30] \oplus K_{14}[19] \oplus K_{15}[30]. \quad (1)$$

The best 16-round linear expression of LOKI91 holds with $BEST_{16}^{LC} = 1.51 \times 2^{-47}$:

$$\begin{aligned} & P_L[18,22,26] \oplus C_L[18,22,26] \\ &= K_2[18,22,26] \oplus K_3[18,22,26] \oplus K_5[18,22,26] \oplus K_6[18,22,26] \\ &\quad \oplus K_8[18,22,26] \oplus K_9[18,22,26] \oplus K_{11}[18,22,26] \oplus K_{12}[18,22,26] \\ &\quad \oplus K_{14}[18,22,26] \oplus K_{15}[18,22,26]. \end{aligned} \quad (2)$$

The best 16-round linear expression of s^2DES holds with $BEST_{16}^{LC} = 1.19 \times 2^{-26}$:

$$\begin{aligned} & P_L[5,10,11] \oplus C_H[5,10,11] \\ &= K_2[4,5,6,7] \oplus K_4[4,5,6,7] \oplus K_6[4,5,6,7] \oplus K_8[4,5,6,7] \\ &\quad \oplus K_{10}[4,5,6,7] \oplus K_{12}[4,5,6,7] \oplus K_{14}[4,5,6,7] \oplus K_{16}[4,5,6,7]. \end{aligned} \quad (3)$$

These linear approximate equations can be constructed by the following iterative linear approximations:

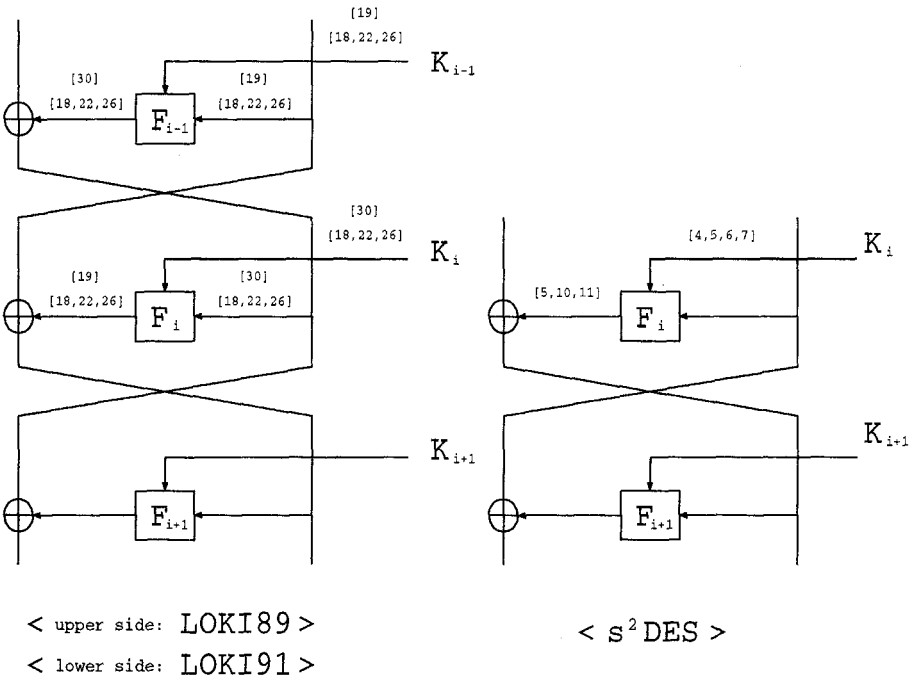

Figure 6: Iterative linear approximations establishing the best 16-round probability.

4 Experimental Results

This chapter describes our experimental results of linear cryptanalysis of 6-round LOKI91 to estimate the number of known-plaintexts required for breaking LOKI with arbitrary number of rounds.

Matsui has introduced two versions of known-plaintext attacks of n-round cryptosystems: the first method uses key equations based on the best $(n-1)$-round linear approximate expression [2], and the latter applies key equations based on the best $(n-2)$-round linear approximate expression [4].

The $(n-2)$-round method is better than the $(n-1)$-round method from the viewpoint of the probability, whereas the $(n-1)$-round method is better than the $(n-2)$-round method from a viewpoint of the size of counters and memory for the effective text/key bits. Since LOKI91 has 12-bit input/8-bit output S-boxes, the effective text/key bits are at least 12 bits in the $(n-1)$-round method, whereas they are at least 24 bits in the $(n-2)$-round method. Due to memory constraint, we have adopted the $(n-1)$-round method for linear cryptanalysis of LOKI91.

We now begin by describing 6-round LOKI91 using the following 5-round best linear approximate expression:

$$\begin{aligned} &P_L[18,22,26] \oplus C_H[18,22,26] \oplus C_L[18,19,21,23,24] \\ &= K_2[18,22,26] \oplus K_3[18,22,26] \oplus K_5[18,19,21,23,24]. \end{aligned} \tag{4}$$

It follows that we have the following expression of 6-round LOKI91 which holds with the best 5-round probability $1/2 - 1.60 \times 2^{-15}$:

$$\begin{aligned} &P_H[18,22,26] \oplus C_H[18,22,26] \oplus C_L[18,19,21,23,24] \oplus F_1(P_L, K_1)[18,22,26] \\ &\quad = K_3[18,22,26] \oplus K_4[18,22,26] \oplus K_6[18,19,21,23,24], \end{aligned} \tag{5}$$

where the following 25 bits essentially affect its left-hand side:

- (Known) text information(13bits):
  $P_L[16] \sim P_L[27]$, $P_H[18,22,26] \oplus C_H[18,22,26] \oplus C_L[18,19,21,23,24]$,
- (Unknown) subkey information(12bits):
  $K_1[16] \sim K_1[27]$.

Note that $P_H[18,22,26] \oplus C_H[18,22,26] \oplus C_L[18,19,21,23,24]$ represents one-bit information. We hence obtain a total of 13 secret key bits — unknown 12 subkey bits and one bit of the right-hand side of equation (5) — using information on known 13 text bits by the following algorithm [2]:

Data Counting Phase

(Step 1) Prepare 2^{13} counters $U_i (0 \leq i < 2^{13})$ and initialize them by zeros, where i corresponds to each value on 13 known text bits of equation (5).

(Step 2) For each plaintext P and the corresponding ciphertext C, compute the value 'i' of Step 1, and count up the U_i by one.

Key Counting Phase

(Step 3) Prepare 2^{12} counters $T_j (0 \leq j < 2^{12})$ and initialize them by zeros, where j corresponds to each value on 12 unknown subkey bits of equation (5).

(Step 4) For each j of Step 3, let T_j be the sum of U_i's such that the left side of equation (5), whose value can be uniquely determined by i and j, is equal to zero.

(Step 5) Let T_{max} be the maximal value and T_{min} be the minimal value of all T_j'.

- If $|T_{max} - N/2| > |T_{min} - N/2|$, then adopt the subkey value 'j' corresponding to T_{max} and guess that the right side of equation (5) is 0.
- If $|T_{max} - N/2| < |T_{min} - N/2|$, then adopt the subkey value 'j' corresponding to T_{min} and guess that the right side of equation (5) is 1.

Table 3 shows the success rate of our attack, where each entry shows an average of 30 trials. Generally speaking, the number of known-plaintexts required for successful linear cryptanalysis is described as $C|p-1/2|^{-2}$, where C is constant value. Table 3 tells us that we can estimate $C = 8$.

N	$2\|p-1/2\|^{-2}$	$4\|p-1/2\|^{-2}$	$6\|p-1/2\|^{-2}$	$8\|p-1/2\|^{-2}$
Success Rate	17%	53%	83%	100%

Table 3. The success rate of our experiments.

Table 4 summarizes the estimate of the number of known-plaintexts required for breaking n-round LOKI. We have applied the $(n-2)$-round method with C=8 [2] to DES and s^2DES. The sign $(-)$ shows that the number of required known-plaintexts exceeds 2^{64}.
It follows that LOKI89 and LOKI91 are resistant to linear cryptanalysis, and the strength of n-round LOKI89/91 corresponds to $2n$-round DES.

Rounds	4	5	6	7	8	9	10	11	12	13	14	15	16
LOKI89	$2^{19.7}$	$2^{24.0}$	$2^{32.2}$	$2^{40.2}$	$2^{43.0}$	$2^{51.2}$	$2^{59.2}$	$2^{62.0}$	$(-)$	$(-)$	$(-)$	$(-)$	$(-)$
LOKI91	$2^{19.6}$	$2^{23.2}$	$2^{31.7}$	$2^{40.1}$	$2^{41.3}$	$2^{49.8}$	$2^{58.3}$	$2^{59.5}$	$(-)$	$(-)$	$(-)$	$(-)$	$(-)$
DES	$2^{6.4}$	$2^{7.7}$	$2^{11.1}$	$2^{14.4}$	$2^{19.1}$	$2^{21.1}$	$2^{24.4}$	$2^{29.1}$	$2^{31.8}$	$2^{33.1}$	$2^{36.5}$	$2^{39.9}$	$2^{44.5}$
s^2DES	$2^{6.6}$	$2^{8.3}$	$2^{13.1}$	$2^{16.5}$	$2^{22.7}$	$2^{23.6}$	$2^{29.8}$	$2^{29.8}$	$2^{35.9}$	$2^{35.9}$	$2^{42.1}$	$2^{42.1}$	$2^{48.3}$

Table 4. The required number for known-plaintext attack of LOKI89,LOKI91 and s^2DES.

NOTE:
Recent researches [12] [13] have revealed that multiple differential/linear paths should be taken into consideration for strict evaluation of block ciphers. Though their effects do not seem to be 'visible' in our cases, more detailed investigation is a future topic.

References

1. Biham,E.,Shamir,A.: Differential Cryptanalysis of the Data Encryption Standard. Springer Verlag (1993)
2. Matsui,M.: Linear Cryptanalysis Method for DES cipher. Advances in Cryptology – Eurocrypt'93, Lecture Notes in Computer Science, Springer-Verlag **765** (1993) 386–397
3. Matsui,M.: On correlation between the order of S-boxes and the strength of DES. Pre-proceedings of Eurocrypt'94 (1994) 375-387
4. Matsui,M.: The First Experimental Cryptanalysis of the Data Encryption Standard. Advances in Cryptology – Crypto'94, Lecture Notes in Computer Science, Springer-Verlag **839** (1994) 1–11
5. Brown,L.,Pieprzyk,J.,Seberry,J.: LOKI–A Cryptographic Primitive for Authentication and Secrecy Applications. Advances in Cryptology – Auscrypt'90, Lecture Notes in Computer Science, Springer-Verlag **453** (1990) 229–236
6. Brown,L.,Kwan,M.,Pieprzyk,J.,Seberry,J.: Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI. Advances in Cryptology – Asiacrypt'91, Lecture Notes in Computer Science, Springer-Verlag **739** (1993) 36–50
7. Kim,K.: Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. Advances in Cryptology – Asiacrypt'91, Lecture Notes in Computer Science, Springer-Verlag **739** (1993) 59–72
8. Biham,E.,Shamir,A.: Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. Advances in Cryptology – Crypto'91, Lecture Notes in Computer Science, Springer-Verlag **576** (1992) 156–171
9. Knudsen,L.: Cryptanalysis of LOKI. Advances in Cryptology – Asiacrypt'91, Lecture Notes in Computer Science, Springer-Verlag **739** (1993) 22–35
10. Knudsen,L.: Cryptanalysis of LOKI91. Advances in Cryptology – Auscrypt'92, Lecture Notes in Computer Science, Springer-Verlag **718** (1993) 196–208
11. Knudsen,L.: Iterative Characteristics of DES and s^2-DES. Advances in Cryptology – Crypto'92, Lecture Notes in Computer Science, Springer-Verlag **740** (1993) 497-511
12. Lai,X.,Massey,J.,Murphy,S.: Markov ciphers and differential cryptanalysis. Advances in Cryptology – Eurocrypt'91, Lecture Notes in Computer Science, Springer-Verlag **547** (1991) 17–38
13. Nyberg,K.: Linear Approximation of Block Ciphers. Presented at Rump Session in Eurocrypt'94