Securing DES S-boxes against Three Robust Cryptanalysis

Kwangjo Kim Sangjin Lee Sangjoon Park Daiki Lee

Section 0710, P.O.Box 106, Yusong
Electronics and Telecommunications Research Institute
Taejon, 305-600, KOREA

Abstract

In this paper, we propose an expanded set of design criteria for the generation of DES-like S-boxes which enable DES being immunized against three known robust cryptanalysis, *i.e.,* differential, Improved Davies' and linear cryptanalysis and we also suggest a set of new 8 DES-like S-boxes generated by our proposed design criteria in order to replace with the current 8 DES S-boxes. The computer simulation leads us to conclude that the breaking complexity of the strengthened DES (we call s^5DES) by three powerful cryptanalysis is no more efficient than the key-exhaustive search.

1 Introduction

Until now, three powerful cryptanalysis have been published to break DES (Data Encryption Standard) [1] more efficiently than the 56-bit key exhaustive search. One is the DC (Differential Cryptanalysis) proposed by Biham and Shamir [2],[4] in 1990. The DC is a kind of chosen plaintext attack in a sense that an attacker has to choose 2^{47} plaintexts and their corresponding ciphertexts to find an unknown 56-bit DES key. The other attack, known as LC (Linear Cryptanalysis), is more feasible than DC and was proposed by Matsui [6] in 1993. The overall complexity to break DES by LC has been reduced [14] to be 2^{43} known plaintexts and ciphertexts pairs comparing to the initial complexity of 2^{47}. Moreover, the Improved version of Davies' attack proposed by Biham and Biryukov [13] was found to break DES with the complexity of 2^{50}. The common point of three cryptanalysis is to use the cryptanalytic properties of DES S-boxes which play an important role in making DES work as nonlinear cryptographic functions.

Two researches in [3] and [5] have been reported to strengthen DES resistant against DC by only replacing the current DES S-boxes with new S-boxes based on the different design criteria rather than the well-known 6 design criteria of DES S-box. Two DES-like cryptosystems are named as s^2DES and s^3DES, respectively. By the efficient search techniques [10],[11] evaluating on the overall strength of DES against DC and LC, the relative security of the full-round DES and s^iDES was found to be $s^2\text{DES} < DES < s^3\text{DES}$ against DC and $s^3\text{DES} < DES < s^2\text{DES}$ against LC.

In this paper, we propose an expanded set of design criteria for the generation of DES-like S-boxes which make DES be immunized against three robust attacks. We also suggest a set of DES-like S-boxes satisfying our proposed design criteria to replace the current DES S-boxes with new S-boxes. Finally, we evaluate the breaking complexity of new DES (we call s^5DES) by three powerful attacks.

2 Design Criteria of DES S-boxes

The followings are the well-known 6 design criteria of DES S-boxes :

(S-1) No S-box is a linear or affine function.

(S-2) Changing one bit in the input of an S-box results in changing at least two output bits.

(S-3) The S-boxes were chosen to minimize the difference between the number of 1's and 0's when any single bit is held constant.

(S-4) S($\mathbf{x}$) and S($\mathbf{x} \oplus (001100)$) differ at least two bits.

(S-5) S($\mathbf{x}$) $\neq$ S($\mathbf{x} \oplus$ (11ef00)) for any e and f.

(S-6) S($\mathbf{x}$) $\neq$ S($\mathbf{x} \oplus$ (0abcd0)) for any a, b, c, and d, abcd $\neq$ 0000.

In addition to these criteria, Coppersmith [12] has recently published additional design criteria of DES S-boxes, such as

(S-7) For a given nonzero input XOR and output XOR, no more than 8 of the outputs may exhibit the given output XOR among the 32 pairs of inputs exhibiting the given input XOR.

(S-8) Similar to (S-7), but stronger restrictions in the case zero output XOR, for the case of 3 active S-boxes on round i.

(S-9) Other criteria dealt with other issue, such as ease of implementation.

He has described that *most of the criteria are aimed at increasing the number of active S-boxes (against DC) involved over the 12 or 16 rounds of the "probable pattern", say this total number is k. Then (S-7), along with the simplifying assumption of independence, puts an upper bound of* $(1/4)^k$ *on the overall probability of this "probable pattern".*

In other words, (S-7) means that the maximal entry in a XOR distribution table of any DES S-boxes is 16 and (S-8) means that nonzero input XOR with 3 active S-boxes resulting the same output always exists with some probability. From all criteria, we can see that the DES designers might initially put in mind the strength of DES against DC.

3 Resistance against DC

The important properties of DES-like S-boxes are derived through an analysis of tables showing a group of particular distributions—called the pairs XOR distribution—defined as follows:

Definition 1 (XOR distribution table) *A table that shows the distribution of input XORs and output XORs of all possible pairs of an S-box is called the pairs XOR distribution table of the S-box. In this table, each row corresponds to a particular input XOR, each column corresponds to a particular output XOR, and the entries in the table count the number of possible pairs with such an input XOR and an output XOR.*

Since the pairs XOR distribution in any DES S-box are used for DC, some intuitive definitions which measures the level of its resistance against DC are necessary. We can consider how many entries appear in the pairs XOR distribution–% of entry, denoted by μ_d.

$$\mu_d = \frac{nz}{64 \times 16} \times 100 \tag{1}$$

where nz denotes the number of non-zero entries in a pairs XOR distribution table. In order to measure how well the values of all entries are distributed from the ideal (uniform) value of entry, the standard deviation, σ_d of all entries can be checked by

$$\sigma_d = \sqrt{\sum_{i=0}^{63}\sum_{j=0}^{15}(e_{ij}-4)^2/64\times 16.} \quad (2)$$

where e_{ij} is a measured number of entry in pairs XOR distribution table. We can also check the nontrivial[1] maximum value of entries, denoted by λ_d, in DES S-boxes since the relatively higher valued entries are directly employed for DC. We simply call these three parameters differential characteristics of an S-box. Differential characteristics of DES S-boxes are measured in Table 2.

Up to now, the 2-round iterative characteristics ($\Phi \rightarrow 0$ with some prob. p) have ever been known to be the basic tool in breaking DES by DC. The 2-round iterative characteristic $\Phi = 1960000_x$ with probability $\frac{1}{234}$ is found to be close to the best characteristic for attacking the full 16-round DES. We discuss cases where 2-round iterative characteristics occur in DES and suggest an efficient design criterion of DES-like S-boxes which guarantees to exhibit 2-round iterative characteristics with very low probability, *i.e.,* the method to immunize DES against DC is to find any necessary condition such that 2-round iterative characteristics exist with more than 3 active S-boxes.

The careful examination of E-expansion of DES F-functions leads us to the following theorem.

Theorem 1 *For a given DES-like S-box satisfying 6 design criteria, the possibilities that nonzero input XOR with 3 active S-boxes results in the nonzero output XOR is one of the followings :*

(A-1) $S(\mathbf{x}) \neq S(\mathbf{x} \oplus (00ef11))$ *for any* e *and* f.

(A-2) $S(\mathbf{x}) \neq S(\mathbf{x} \oplus (10ef00))$ *for any* e *and* f.

(A-3) $S(\mathbf{x}) \neq S(\mathbf{x} \oplus (11ef10))$ *for any* e *anf* f.

If we combine 6 design criteria with A-3, we can obtain the following important theorem to immunize DES against DC.

Theorem 2 *If nonzero input XOR* $\underbrace{00a_1a_2a_3a_4}_{1}\ \underbrace{a_3a_4a_5a_6a_7a_8}_{2}\ \cdots\ \underbrace{a_{n-7}a_{n-6}a_{n-5}a_{n-4}a_{n-3}a_{n-2}}_{l-1}$ $\underbrace{a_{n-3}a_{n-2}a_{n-1}a_n00}_{l}$ *for each* $n = 4i+2, (i = 1, \ldots, l)$ *is given to* l *neighbouring DES S-boxes satisfying 6 criteria and (A-3), output XOR will never be zero.*

The above theorem means that we can only find 2-round iterative characteristics with 8 active S-boxes, *i.e.,* we cannot find any 2-round iterative characteristics with less than 7 active S-boxes. Combining (A-3) and (S-5), the necessary condition to immunize DES against DC is :

Condition 1 (D-1) $S(\mathbf{x}) \neq S(\mathbf{x} \oplus (11efg0))$ *for any* efg.

Note that if DES-like S-boxes meet **(D-1)**, DES whose S-boxes are replaced with new S-boxes can be resistant against Improved Davies' attack [13],[17].

[1]It is trivial that the entry always has a value of 64 when the input XOR and output XOR of any DES-like S-box are zero.

4 Resistance against LC

The following notations are used hereinafter.

- I_i : The input value of *i-th* round in DES F-function.
- O_i : The output value of *i-th* round in DES F-function.
- K_i : The key value of *i-th* round in DES F-function.
- $X[Z] = \oplus_{k \in Z} X[k]$, where $Z \subset \{0, 1, \ldots, 47\}$ and $X[k]$ is the *k-th* bit of X which is one of I_i, O_i and K_i.
- a_x : The hexadecimal value of a.
- $W(\alpha)$: The Hamming weight of α.
- For $x, y \in GF(2)^n$, $x \bullet y$ denotes the dot product of x and y.

Kim et al. [8],[9] have already suggested the necessary condition to design DES-like S-boxes which can be resistant to LC. In this section, we will summarize those conditions and revise them by the computer experiments.

4.1 Uniformity of a Linear Distribution Table

It is necessary to precompute the linear distribution table of DES-like S-boxes defined as below like DC in order to break DES by LC.

Definition 2 (Linear distribution table) *For a given DES S-box S, we define $NS(\alpha, \beta)$ as the number of times minus 32 out of 64 input patterns of S, such that an XORed value of the input bits masked by α coincides with an XORed value of the output bits masked by β, i.e.,*

$$NS(\alpha, \beta) \quad = \quad \#\{x \in GF(2)^6 | x \bullet \alpha = S(x) \bullet \beta\} - 32$$

where $\alpha \in GF(2)^6$ and $\beta \in GF(2)^4$. We refer the complete table for every α and β to the linear distribution table.For a specific S-box, S_i $(i = 1, \ldots, 8)$, we denote its linear distribution table as $NS_i(\alpha, \beta)$.

In order to check the uniformity of a linear distribution table of any S-box, let us denote % of the entry by μ_l and the maximal entry by λ_l as the same way to check the uniformity of XOR distribution table.

Based on the computer experiments and theoretical analysis, the first necessary condition [9] to make DES-like S-boxes to be immunized against LC is :

Condition 2 (L-1) *The λ_l of any S-box should be less than 16.*

4.2 Iterative Linear Approximation

The following definitions are necessary to understand the concept of LC.

Definition 3 (Linear approximation) *For a given expression $I[Z_1] \oplus O[Z_2] = K[Z_3]$ with probability $p + 1/2$, this linear approximation is denoted as $A: I[Z_1], K[Z_3] \longrightarrow O[Z_2]$ with p. We denote this expression as $A, B, C, \cdots$ and sometimes omit the term $K[Z_3]$. Also $\delta(A)$ denotes the set of S-boxes necessary to express A and $\#\delta(A) = |\delta(A)|$.*

Definition 4 (nR iterative linear approximation) *The n-round (simply, nR) iterative linear approximation is defined by* $I_1[Z_1] \oplus I_n[Z_n] = K_2[Z_2] \oplus \cdots \oplus K_{n-1}[Z_{n-1}]$. *For the consecutive n-rounds, the XORed values of n-2 keys in an (n-2)-round can be expressed by its input and output XORed values. When this expression holds with probability* $q = p+1/2$, *the probability of this linear approximation is to be p. Also, we denote nR iterative linear approximation as* $-A_1 \cdots A_{n-2}-$ *and its concatenated expression as* $-A_1 \cdots A_{n-2} - A_{n-2} \cdots A_1 -$.

To cryptanalyze n-round DES by LC in general, we need to find an useful linear approximation of $(n-1)$-round DES. When the linear approximation of $(n-1)$-round DES holds with probability $q = p + \frac{1}{2}$, the number of plaintexts which the attacker needs are about $|p|^{-2}$ by Lemma 2 in [6]. Thus, a linear approximation of 15-round DES is necessary to break the full 16-round DES. When this approximation holds with probability p_{15}, the necessary condition that LC is no more efficient than key-exhaustive search is $p_{15}^{-2} \geq 2^{56}$, *i.e.*, $|p_{15}| \leq 2^{-28}$. Thus, in order that DES can be resistant to LC, the main idea is to find some necessary conditions such that DES-like S-boxes should have any linear approximation with the small probability.

By Lemma 3 in [6], if we find an nR iterative linear approximation with probability p, then we can also obtain $(k \cdot (n-1)+1)$R linear approximation with probability $2^{k-1}p^k$ when nR iterative linear approximation is applied k times. We discuss the necessary condition how to lower the probability of 3R, 4R, and 5R iterative linear approximations to prevent DES from being broken by a successful LC.

4.2.1 3R Iterative Linear Approximation

The 3R iterative linear approximation has a form of $I_1[Z_1] \oplus I_3[Z_1] = K_1[Z_2]$, *i.e.*, there exists a linear correlation between key and output subblocks without input subblock as $O_i[Z_1] = K_i[Z_2]$. This case always occurs when two outer bits of a DES S-box are given to two neighbouring S-boxes. Thus, we can build the 3R iterative linear approximation from this case.

Theorem 3 *There exists a 3R iterative linear approximation if and only if the input of Si-box and the input of S(i+1)-box are* 3_x *and* 30_x, *respectively.*

If $NS_i(3_x, \beta_1)$ and $NS_{i+1}(30_x, \beta_2)$ are not equal to zero, we can build some 3R iterative linear approximations. From the 3R iterative linear approximation $-A-$ with probability p, we can build the 15-round linear approximation like $-A-A-A-A-A-A-A-$ and the total probability for this approximation to hold is 2^6p^7. Thus, the necessary condition that this attack is no more efficient than key-exhaustive search is $2^6|p|^7 \leq 2^{-28}$, *i.e.*, $|p| \leq 2^{-4.9}$. In other words,

$$|2 \cdot \frac{NS_i(3_x, \beta_1)}{64} \cdot \frac{NS_{i+1}(30_x, \beta_2)}{64}| \quad \leq \quad 2^{-4.9}. \tag{3}$$

If any DES-like S-box satisfies **(D-1)**, the values of $NS(30_x, \beta)$ and $NS(31_x, \beta)$ are always to be zero for any β. Thus the LHS of Eq. (3) is always equal to zero.

Condition 3 (L-2) $S(\mathbf{x}) \neq S(\mathbf{x} \oplus (11efg0))$ *for any* efg.

Note that **(L-2)** is a simple and common design criterion to prevent DES from being broken by successful DC, Improved Davies' attack, and special case of LC.

4.2.2 4R Iterative Linear Approximation

We discuss cases when a 4R iterative linear approximation occurs from two given linear approximations such as,

$$A \quad : \quad I_2[Z_1], K_2[Z_3] \longrightarrow O_2[Z_2] \tag{4}$$

$$B \quad : \quad I_3[Y_1], K_3[Y_3] \longrightarrow O_3[Y_2] \tag{5}$$

If we linearly approximate the 2nd round and 3rd round function of DES to A and B, respectively, $I_2[Z_1]$ should be equal to the XORed value between the 3rd round output and 4th round input, and $I_3[Y_1]$ should be equal to the XORed value between the 1st round input and 2nd round output in order to get an useful 4R iterative linear approximation.

Theorem 4 *By concatenating two linear approximations Eqns. (4) and (5) with probability p_1 and p_2, respectively, the condition for building a 4R iterative linear approximation is $Z_1 = Y_2, Z_2 = Y_1$. Also, the 4R iterative linear approximation is of the form*

$$I_1[Z_2] \oplus I_4[Z_1] \quad = \quad K_2[Z_3] \oplus K_3[Y_3] \tag{6}$$

with probability $2p_1p_2$.

If the 4R iterative linear approximation $-AB-$ with probability p is given, we can build the 15-round linear approximation as $-AB-BA-AB-BA-AB$. The necessary condition that this attack is no more efficient than key-exhaustive search is $|2^4p^5| \leq 2^{-28}$, *i.e.*, $|p| \leq 2^{-6.4}$.

Condition 4 (L-3) *The followings (18 cases in total) are necessary so that the 4R iterative linear approximation will not occur.*

- *S1-box :* $NS_1(4,4) = NS_1(2,2) = 0$, $\quad$ *S2-box :* $NS_2(4,4) = NS_2(2,1) = 0$
- *S3-box :* $NS_3(8,4) = NS_3(4,8) = 0$, $\quad$ *S4-box :* $NS_4(8,4) = NS_4(2,2) = 0$
- *S5-box :* $NS_5(16,1) = NS_5(8,8) = NS_5(2,4) = 0$
- *S6-box :* $NS_6(16,4) = NS_6(4,8) = NS_6(2,2) = 0$
- *S7-box :* $NS_7(4,8) = NS_7(2,1) = 0$, $\quad$ *S8-box :* $NS_8(16,1) = NS_8(2,4) = 0$

When DES-like S-boxes satisfying **(L-3)** are given, the necessary condition not to find 4R linear approximation is as follows:

Condition 5 (L-4) *For $W(\alpha), W(\beta) \leq 2$, $|NS(\alpha,\beta)| \leq 8$ where $\alpha \in GF(2)^6$ and $\beta \in GF(2)^4$.*

We, however, have found that it was very difficult to find a set of 8 DES-like S-boxes satisfying **(L-4)** by computer experiments. Thus we loose the maximum allowable values of $|NS(\alpha,\beta)|$ upto 10 in an empirical way but this would not disturb the strength of new DES-like S-boxes.

Condition 6 (Revised L-4) *For $W(\alpha), W(\beta) \leq 2$, $|NS(\alpha,\beta)| \leq 10$ where $\alpha \in GF(2)^6$ and $\beta \in GF(2)^4$.*

4.2.3 5R Iterative Linear Approximation

The following theorem points us cases where the possible 5R iterative linear approximations occur.

Theorem 5 *When three linear approximations are given by*

$$\begin{aligned} A &: I_2[Z_1], K_2[Z_3] \longrightarrow O_2[Z_2] \\ B &: I_3[Y_1], K_3[Y_3] \longrightarrow O_3[Y_2] \\ C &: I_4[X_1], K_4[X_3] \longrightarrow O_4[X_2], \end{aligned}$$

we can obtain a 5R iterative linear approximation only if $Z_1 = Y_2 = X_1, Y_1 = Z_2 \cup X_2 - Z_2 \cap X_2$, *and the 5R iterative linear expression* $-ABC-$ *is of the form*

$$I_1[Z_2] \oplus I_5[X_2] \quad = \quad K_2[Z_3] \oplus K_3[Y_3] \oplus K_4[X_3].$$

Using the 5R iterative linear approximation $-ABC-$, we can build 15-round linear approximation as $-ABC - CBA - ABC - DE$. The probabilities of D and E is less than 2^{-2} by **L-1**. If the probability of $-ABC-$ is p, $|p|^3$ should be less than 2^{-28}, *i.e.*, $|p| \leq 2^{-9.4}$. Some computation leads us that

Condition 7 (L-5) *For* $\alpha \in GF(2)^6$, β_1 *and* $\beta_2 \in GF(2)^4$,
$W(\alpha) = 1$ *and* $W(\beta_1 \oplus \beta_2) = 1 \Longrightarrow |NS(\alpha, \beta_1) \cdot NS(\alpha, \beta_2)| \leq 48$.

We guess that **L-2** causes $|NS(10_x, \beta_1) \cdot NS(10_x, f_x)| = 16 \times 16 = 256$ for some β_1, $W(\beta_1 \oplus f_x) = 1$. Thus we could not find any DES-like S-boxes satisfying both **(L-2)** and **(L-5)**. In order to revise **(L-5)**, we utilized the property of P-permutation in DES F-function such that :

Condition 8 (Revised L-5) *If* $\alpha \neq 10_x$,

$$|NS(\alpha, \beta_1) \cdot NS(\alpha, \beta_2)| \leq 48$$

for $W(\alpha) = 1$ *and* $W(\beta_1 \oplus \beta_2) = 1$
If $\alpha = 10_x$,

$$\begin{aligned} |NS_k(\alpha, \beta_1) \cdot NS_k(\alpha, \beta_2)| &\leq 48 \quad for \quad \beta_1 \oplus \beta_2 = 1 \\ |NS_l(\alpha, \beta_1) \cdot NS_l(\alpha, \beta_2)| &\leq 48 \quad for \quad \beta_1 \oplus \beta_2 = 4 \end{aligned}$$

for $k = 5, 8$ *and* $l = 6$.

5 Comparison

Using the same method in [3], we have successfully found a set of DES-like S-boxes satisfying additional 5 conditions described in Section 4. In the appendix, we listed a set of DES-like S-boxes for s^5DES [2] which took about three monthes to generate by Hyundai Axil HWS310 Sparc workstation (22MIPS, 33MHz).

In this section, we measure the cryptographic strength of S-boxes themselves and evaluate the breaking complexity of s^5DES.

[2] The name of s^4DES is skipped with intention since it was distributed in an informal way.

5.1 Local Properties

We compare the quantitative characteristics of S-boxes in DES and s^iDES in various points of cryptographic view and evaluate the goodness-of-fit of them.

We checked the nonlinearity of 4 Boolean functions: $Z_2^6 \to Z_2$ consisting of an S-box as shown in Table 1. In the output bit column of this table, 4 denotes the most significant location of an output vector and 1 denotes the least significant location of an output vector.

Table 1: Nonlinearity of S-boxes

Box	DES				s^2DES				s^3DES				s^5DES			
	output bit				output bit				output bit				output bit			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
S1	18	20	22	18	22	20	20	22	16	20	22	20	20	18	20	22
S2	22	20	18	18	24	22	22	22	22	22	20	22	18	20	20	20
S3	18	22	20	18	20	24	22	22	18	22	20	20	22	22	20	18
S4	22	22	22	22	20	22	22	22	18	24	20	20	20	22	18	22
S5	22	20	18	20	22	24	22	24	20	18	18	22	20	22	20	22
S6	20	20	20	20	22	22	20	22	22	20	18	12	20	22	18	20
S7	18	22	14	20	22	20	22	18	22	18	18	16	22	22	20	20
S8	22	20	20	22	22	22	22	22	20	22	22	20	22	20	18	22

It is clear that the nonlinearity of DES S-boxes ranges from 14 to 22, the nonlinearity of s^2DES and s^5DES ranges from 18 to 24, and the nonlinearity of s^3DES varies from 12 to 24. From these observation, we could say that the nonlinearity of DES-like S-boxes is required to be over 18.

We measured the differential characteristics of a S-box as shown in Table 2.

Table 2: Differential characteristics of S-boxes

Box	DES			s^2DES			s^3DES			s^5DES		
	μ_d	σ_d	λ_d	μ_d	σ_d	λ_d	μ_d	σ_d	λ_d	μ_d	σ_d	λ_d
S1	79.49	3.76	16	84.38	3.44	14	73.54	4.09	20	74.12	4.07	18
S2	78.61	3.83	16	85.25	3.39	14	75.49	3.97	18	73.63	4.07	20
S3	79.69	3.78	16	84.38	3.34	14	73.44	4.12	18	72.85	4.06	20
S4	68.55	4.18	16	83.40	3.54	16	73.44	4.25	20	74.41	4.09	20
S5	76.56	3.86	16	82.91	3.57	16	70.61	4.41	20	74.61	4.07	20
S6	80.47	3.69	16	83.98	3.48	16	71.19	4.30	20	75.98	3.92	18
S7	77.25	3.95	16	81.93	3.62	16	75.39	3.99	20	73.54	4.08	18
S8	77.15	3.82	16	82.81	3.54	16	75.20	4.01	20	75.0	4.04	18

The uniformity of s^3DES and s^5DES in XOR distribution tables could be said to be worse than that of DES and s^2DES but s^3DES was verified to be stronger than DES and s^2DES from DC. In [7], Seberry et al. proposed a new measure of checking the robustness of S-box against DC. As defined in Section 3, let λ_d denote the largest value in the XOR distribution table of DES-like S-box and N denote the number of nonzero entries in the first column of the table. In either case the value 2^6 in the first row is not counted. R-robustness against differential cryptanalysis can be defined by $R = (1 - \frac{N}{2^6})(1 - \frac{\lambda_d}{2^6})$. We have checked the R-robustness of DES and s^iDES as shown in Table 3. All DES-like cryptosystems have

Table 3: R-robustness of S-boxes

	DES		s^2DES		s^3DES		s^5DES	
Box	N	R	N	R	N	R	N	R
S1	37	0.316	37	0.329	36	0.301	32	0.359
S2	33	0.363	42	0.269	34	0.337	34	0.322
S3	37	0.316	41	0.280	31	0.371	36	0.301
S4	24	0.469	41	0.270	35	0.312	31	0.354
S5	31	0.387	41	0.270	31	0.355	35	0.312
S6	33	0.363	40	0.281	26	0.408	32	0.359
S7	35	0.340	37	0.316	34	0.322	32	0.359
S8	36	0.328	36	0.328	35	0.312	36	0.314

the similar value of R-robustness. Thus it is difficult to decide which DES-like cryptosystem can resist harder against DC from the uniformity of XOR distribution tables and R-robustness.

The dependence matrix of a DES-like S-box are examined to check if DES-like S-boxes satisfy the SAC (Strict Avalanche Criterion). The dependence matrix $\mathbf{P} = (p_{i,j})$ of the S-box is defined as follows: The element $p_{i,j}$ of $\mathbf{P}$ is the probability that the output variable $\mathbf{y_j}$ of the S-box changes when the input variable $\mathbf{x_i}$ is complemented. The average values, *i.e.*, $(p_{i,1} + p_{i,2} + p_{i,3} + p_{i,4})/4$ of $(p_{i,j})$ of S-boxes in DES and s^iDES are compared in Table 4. Whenever one bit of input in s^2DES is complemented, every

Table 4: Average $(p_{i,j})$ values of S-boxes

Box	DES	s^2DES	s^3DES	s^5DES
S1	0.620	0.495	0.609	0.633
S2	0.633	0.510	0.609	0.625
S3	0.661	0.505	0.617	0.620
S4	0.615	0.521	0.617	0.617
S5	0.633	0.516	0.617	0.641
S6	0.651	0.516	0.620	0.628
S7	0.656	0.516	0.638	0.630
S7	0.625	0.508	0.625	0.625

output bits can be said to change with close to the probability $\frac{1}{2}$. But, the probability of dependence matrix in DES, s^3DES and s^5DES is found to have greater value than 0.6. Therefore we can infer that Boolean functions consisting of DES, s^3DES and s^5DES do not satisfy the SAC.

Finally we checked the uniformity of linear distribution table of a S-box as shown in Table 5. We can see that there was no design criteria of DES against LC but the maximal entry in s^5DES is restricted being under 16.

Thus we cannot tell which measure is the best one to check the immunity of DES-like S-boxes against DC and LC.

Table 5: Uniformity of Linear distribution table

Box	DES		s^2DES		s^3DES		s^5DES	
	μ_l	λ_l	μ_l	λ_l	μ_l	λ_l	μ_l	λ_l
S1	75.87	18	77.46	14	62.22	16	68.15	16
S2	69.95	16	77.67	14	68.57	16	68.68	16
S3	77.14	16	79.15	14	68.78	16	71.43	16
S4	58.84	16	75.45	14	65.08	24	71.64	16
S5	75.77	20	74.39	18	71.01	24	72.91	16
S6	76.51	14	78.62	14	69.95	20	72.49	16
S7	75.56	18	76.83	16	73.33	20	71.32	16
S8	73.12	16	77.57	14	70.69	16	71.32	16

5.2 Global Properties

5.2.1 Breaking Complexity by DC

Since the 2-round iterative differential characteristics are directly employed for the successful DC, we compare the probability of 2-round differential characteristics and the breaking complexity of 13-round DES-like cryptosystems by using them as shown in Table 6. This table tells us that the breaking com-

Table 6: Breaking complexity by DC

	Best Char.	Complexity
DES	19600000_x with $1/234$	2^{47}
s^2DES	00000580_x with $1/51$	2^{33}
	$07e00000_x$ with $1/68$	2^{35}
	$5c000000_x$ with $1/68$	2^{35}
s^3DES	11173737_x with 1.42576×10^{-5}	2^{96}
s^5DES	75175117_x with 1.15513×10^{-5}	2^{96}
	75175317_x with 1.15513×10^{-5}	2^{96}
	75177117_x with 1.02678×10^{-5}	2^{96}
	75377317_x with 1.02678×10^{-5}	2^{96}

plexity of DES and s^2DES by DC is more efficient than by key-exhaustive search. However, the attacking by DC is not useful to break s^3DES and s^5DES. Also the Improved Davies' attack cannot be applicable to break s^3DES and s^5DES due to their design criteria.

5.2.2 Breaking Complexity by LC

In [18], Lee et al. proposed an efficient method to find the linear approximation of DES-like cryptosystems by LC. By their method, we have checked the best probability of linear approximation of 4 DES-like cryptosystems as shown in Table 7.

From this table, we can see that the breaking s^5DES by LC needs $(1.94 \times 10^{-9})^{-2} \simeq 2^{57.88}$ complexity which is greater than the breaking complexity of key exhaustive search.

Table 7: Best linear approximation

Round	10	12	14	16
DES	4.66×10^{-5}	9.07×10^{-6}	5.67×10^{-7}	8.88×10^{-8}
s^2 DES	3.62×10^{-6}	2.09×10^{-7}	1.59×10^{-8}	9.17×10^{-10}
s^3 DES	5.15×10^{-5}	1.20×10^{-5}	6.03×10^{-7}	7.07×10^{-8}
s^5 DES	8.89×10^{-7}	6.94×10^{-8}	1.94×10^{-9}	1.82×10^{-10}

6 Concluding Remarks

Our systematic approach to immunize DES against three robust attacks is not only verified to enhance the security of DES, but also is very simple since the current DES S-boxes can be substituted with new S-boxes without changing other components of DES. We can conclude that three attacks to s^5DES are no more efficient than the key exhaustive search attack. In [17], Biham and Biryukov proposed some methods to strengthen the power of DES replaced by DES-like S-boxes of s^3DES in a switched order against the key exhaustive search attack. Their methods can also be applicable directly without changing the location of 8 DES-like of s^5DES to enhance the security of s^5DES against the key exhaustuve search attack.

Finally, further works are left as open problems to evaluate that s^5DES is resistant against differential-linear attack [15] and multiple linear attack [16].

References

[1] "Data Encryption Standard", FIPS-Pub. 46, National Bureau of Standards (former NIST), 1977.

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", J. of Cryptology, Vol.4, pp.3–72, 1991.

[3] K. Kim, "Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC", Advances in Cryptology-Asiacrypt'91, Springer-Verlag, pp.59–72, Fujiyoshida, Japan, 1991.

[4] E. Biham and A. Shamir, "Differential Cryptanalysis of the full 16-round DES", Advances in Cryptology-Crypto'92, Springer-Verlag, pp.487–496, 1992.

[5] K. Kim, S. Park and S. Lee, "Reconstruction of s^2DES S-boxes and their Immunity to Differential Cryptanalysis", Proc. of 1993 Korea-Japan Joint Workshop on Information Security and Cryptology (JW-ISC'93), Oct.24-26, Seoul, 1993.

[6] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology-Eurocrypt'93, Springer-Verlag, pp.386–397, 1993.

[7] J. Seberry, X. Zhang, and Y. Zheng, "Systematic Generation of Cryptographically Robust S-boxes", Proc. of the 1st ACM Conf. on Comp. and Comm. Security, pp.172–182, ACM, 1993.

[8] K. Kim, S. Lee, and S. Park, "Necessary Conditions to Strengthen DES S-boxes against Linear Cryptanalysis", Proc. of SCIS'94, Biwako, Japan, pp.15D.1-11, Jan.27–29, 1994.

[9] K. Kim, S. Lee, S. Park, and D. Lee, "DES can be Immune to Linear Cryptanalysis", Workshop Record of SAC'94 (Selected Areas in Cryptography), May 5–6, Queen's Univ., Canada, 1994.

[10] T. Sorimachi, T. Tokita, and M. Matsui, "On a Cipher Evaluation Method Based on Differential Cryptanalysis (in Japanese) ", Proc.of SCIS'94, SCIS94-4C, Lake Biwa, Japan, Jan.27–29, 1994.

[11] T. Tokita, T. Sorimachi, and M. Matsui, "An Efficient Search Algorithm for the Best Expression on Linear Cryptanalysis (in Japanese) ", Technical Report on Information SECurity of IEICE, ISEC93-97, Mar., 1994.

[12] D. Coppersmith, "The Data Encryption Stanadard (DES) and its strength against attacks", IBM J. , Vol.38, No.3, pp.243–250,1994

[13] E. Biham and A. Biryukov, "An Improvement of Davies' Attack on DES", Proc. of Eurocrypt'94, to apprear,

[14] M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard", Advances in Cryptology-Crypto'94, Springer-Verlag, pp.1–11, 1994.

[15] S.K. Langford and M.E. Hellman, "Differential-Linear Cryptanalysis", Advances in Cryptology-Crypto'94, Springer-Verlag, pp.17–25, 1994.

[16] B.S. Kaliski and M.J.B. Robshaw, "Linear Cryptanalysis Using Multiple Approximations", Advances in Cryptology-Crypto'94, Springer-Verlag, pp.26–39, 1994.

[17] E. Biham and A. Biryukov, "How to Strength DES Using Existing Hardware", Pre-Proc. of Asiacrypt'94, pp.339–353, Univ. of Wollongong, Australia, 1994.

[18] S. Lee, S. Sung, and K. Kim "An Efficient Method to Find the Linear Expressions for Linear Cryptanalysis", Proc. of JW-ISC'95. Jan.24-27, Inuyama, Japan, 1995.

Appendix: 8 DES-like S-boxes of s^5DES

S1-box

9	10	15	1	4	7	2	12	6	5	3	14	8	11	13	0
2	13	8	4	11	1	14	7	12	3	15	9	5	6	0	10
10	12	4	7	9	2	15	1	3	6	13	8	14	5	0	11
4	11	1	13	14	7	8	2	10	0	6	3	9	12	15	5

S2-box

6	3	5	0	8	14	11	13	9	10	12	7	15	4	2	1
9	6	10	12	15	0	5	3	4	1	7	11	2	13	14	8
5	8	3	14	6	13	0	11	10	15	9	2	12	1	7	4
6	3	15	9	0	10	12	5	13	8	2	4	11	7	1	14

S3-box

11	5	8	2	6	12	1	15	7	14	13	4	0	9	10	3
7	8	1	14	11	2	13	4	12	3	6	9	5	15	0	10
8	11	1	12	15	6	2	5	4	7	10	9	3	0	13	14
13	2	4	7	1	11	14	8	10	9	15	0	12	6	3	5

S4-box

13	11	8	14	3	0	6	5	4	7	2	9	15	12	1	10
10	0	3	5	15	6	12	9	1	13	4	14	8	11	2	7
6	5	11	8	0	14	13	3	9	12	7	2	10	1	4	15
9	12	5	15	6	3	0	10	7	11	2	8	13	4	14	1

S5-box

12	6	2	11	5	8	15	1	3	13	9	14	0	7	10	4
15	0	12	5	3	6	9	10	4	11	2	8	14	1	7	13
1	12	15	5	6	11	8	2	4	7	10	9	13	0	3	14
6	3	10	0	9	12	5	15	13	4	1	14	7	11	8	2

S6-box

14	8	2	5	9	15	4	3	7	1	12	6	0	10	11	13
1	13	11	8	2	4	7	14	10	6	0	15	5	9	12	3
4	2	9	15	14	8	3	5	10	7	0	12	13	1	6	11
8	11	7	4	13	1	14	2	5	0	9	10	6	15	3	12

S7-box

4	13	10	3	7	0	9	14	2	1	15	6	12	11	5	8
9	0	15	10	12	6	5	3	14	7	1	13	11	8	2	4
13	10	3	9	0	7	14	4	8	6	5	12	11	1	2	15
10	3	12	6	5	9	0	15	4	8	11	1	14	7	13	2

S8-box

1	10	2	12	15	9	4	7	14	3	5	0	8	6	11	13
14	13	7	11	2	4	1	8	0	10	9	6	5	15	12	3
10	15	12	1	9	2	7	4	13	0	6	11	3	5	8	14
4	8	1	2	7	11	13	14	10	5	15	12	0	6	3	9