A Chosen-Plaintext Linear Attack on DES

Lars R. Knudsen and John Erik Mathiassen

Department of Informatics, University of Bergen, N-5020 Bergen, Norway
{lars.knudsen,johnm}@ii.uib.no

Abstract. In this paper we consider a chosen-plaintext variant of the linear attack on DES introduced by Matsui. By choosing plaintexts in a clever way one can reduce the number of plaintexts required in a successful linear attack. This reduces the amount of plaintexts to find key bits to a factor of more than four compared to Matsui's attack. To estimate the probabilities of success in the attack we did extensive experiments on DES reduced to 8 and 12 rounds. We believe that the results in this paper contain the fastest attack on the DES reported so far in the open literature. As an example, one attack needs about 2^{42} chosen texts, finds 12 bits of key information and succeeds with a probability of about 86%. An additional 12 key bits can be found by similar methods. For comparison, Matsui's attack on the DES needs about 2^{44} known texts, finds 13 bits of the key and succeeds with a probability of 78%. Of independent interest is a new approach searching for "pseudo-keys", which are secret key bits added an unknown but fixed value. These bits can be used to find the secret key bits at a later stage in the analysis.

1 Introduction

The DES is one of the most important cryptosystems that has been around in the open literature. Although it has seen the end of its days, this is mainly because of the short keys in the algorithm and not because any damaging intrinsic properties have been detected. In fact, today, about 25 years after the development of the DES, the most realistic attack is still an exhaustive search for the key. Several attacks have been developed which can find a DES-key faster than this, but all attacks reported require a huge amount of known or chosen plaintext-ciphertext pairs.

In 1992 Matsui introduced the linear cryptanalytic attack by applying it to FEAL [6] and one year later to the DES [3]. His attack on the DES using 2^{44} known texts, finds 13 bits of the key and succeeds with a probability of 78%. An additional 13 key bits can be found by a similar method. Subsequently, the remaining 30 bits can be found by exhaustive search. In [4] Matsui also considers "key-ranking", where one considers the attack successful if the correct key is amongst the q most likely keys. Clearly, with key-ranking the success rates will be higher or the text requirements decrease for the same success probability. If we assume that the number of key bits found by the attack is k, one does an exhaustive search for the remaining $56 - k$ bits for each of the q candidates

B. Schneier (Ed.): FSE 2000, LNCS 1978, pp. 262–272, 2001.

of the first k bits. Thus, key-ranking can be used to decrease the number of texts needed but wil increase the computational effort in the final key search. Matsui implemented this attack in January 1994 and successfully recovered one DES-key after the encryption of 2^{43} plaintext blocks.

In this paper, if not stated otherwise, all the reported success rates are measured as the number of times the correct value of the key is the most likely candidate suggested by the attack. Clearly, with key-ranking the success rates will be higher.

In the year following Matsui's publications, several reports were publicised which modify and improve on his results e.g., [1,2,7,8]. However until now these approaches have led to only small improvements for attacks on the DES. One exception is the chosen-plaintext differential-linear attack which led to a big reduction in the number of texts needed, however the attack as reported is applicable to only up to 8 rounds of the DES.

In this paper another chosen-plaintext variant of the linear attack on the DES is studied. It is shown that in this scenario it is possible to reduce the number of required texts (the main obstacle in the attack) to a factor of more than four less than that required by Matsui's attack. We use what we believe is a new idea in cryptanalytic attacks, namely in a first-phase of the attack we search for "pseudo-keys", which are the secret keys added some unknown, but fixed value. In a later stage these pseudo-key bits can be used to reduce an exhaustive key search.

In § 2 we introduce the most important concepts and results of the linear attack on the DES. In § 3 we outline three possible chosen-plaintext variants. All but the second variant can be used to attack the DES up to 16 rounds. The second one is limited to attack DES up to 12 rounds.

2 Linear Cryptanalysis on DES

In linear cryptanalysis one tries to find probabilistic linear relations between the plaintext P, the ciphertext C, and the key K. The easiest way to obtain this is to look for one-round linear relations and use these iteratively to obtain relations over more rounds. First we consider one-round relations. In the following let C_i denote the ciphertext after i rounds of encryption. Then a linear expression in the ith round has the following form.

$$(C_i \cdot \alpha) \oplus (C_{i+1} \cdot \beta) = (K_i \cdot \gamma), \tag{1}$$

where α, β and γ are bit-masks and '$\cdot$' is a bit-wise dot product operator. The masks are used to select the bits of a word used in the linear relation. The bit masks (α, β) are often called one-round linear characteristics. Since the key K_i is a constant, one looks at the probability p_i that the left side of (1) equals 0 or 1. We denote by the bias, the quantity $|p_i - \frac{1}{2}|$. For the DES one can easily calculate all linear relations for the S-boxes, combine these and get all possible linear relations for one round of the cipher. Subsequently, one can combine the one-round relations to get linear relations for several rounds under the assumption of independent rounds. To calculate the probabilities one usually uses the Piling-up Lemma:

Lemma 1. *Let Z_i, $1 \leq i \leq n$ be independent random variables in $\{0,1\}$. If $Z_i = 0$ with probability p_i we have*

$$Pr(Z_1 \oplus Z_2 \oplus \ldots \oplus Z_n = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} (p_i - \frac{1}{2}) \tag{2}$$

For most ciphers the one-round linear relations involved in a multi-round relation are not independent. For the DES the relations are dependent, but our experiments, as well as Matsui's experiments [3,4], show that Piling-up Lemma gives a good approximation for the DES.

For the DES, Matsui has provided evidence [5] that the best linear characteristics over 14 rounds or more are obtained by iterating 4-round characteristics.

Four-round iterative characteristics. The four-round characteristic used in Matsui's attack on the DES is shown in Fig. 1. Let X_i denote the input to the F-function in the ith round. For convenience we shall write $F(X_i)$ instead of $F(X_i, K_i)$. The masks A, D and B are chosen to maximise the probabilities of following linear relations.

$$\begin{aligned} F(X_1) \cdot A &= X_1 \cdot D \qquad \text{with prob. } p_1, \\ F(X_3) \cdot B &= X_3 \cdot D \qquad \text{with prob. } p_3, \text{ and} \\ F(X_2) \cdot D &= X_2 \cdot (A \oplus B) \qquad \text{with prob. } p_2. \end{aligned}$$

Then it follows from the Piling-Up Lemma and by easy calculations that the relation $(X_0 \cdot A) \oplus (X_4 \cdot B) = 0$ holds with probability

$$P_L = \frac{1}{2} - 4(p_1 - \frac{1}{2})(p_2 - \frac{1}{2})(p_3 - \frac{1}{2}).$$

This 4-round characteristic can be iterated to a 14-round characteristic, which in a short, space-consuming notation is

2: - - -

3: A ← D

4: D ← A⊕B

5: B ← D

6: - - -

7: B ← D

8: D ← A⊕B

9: A ← D

10: - - -

11: A ← D

12: D ← A⊕B

13: B ← D

14: - - -

15: B ← D

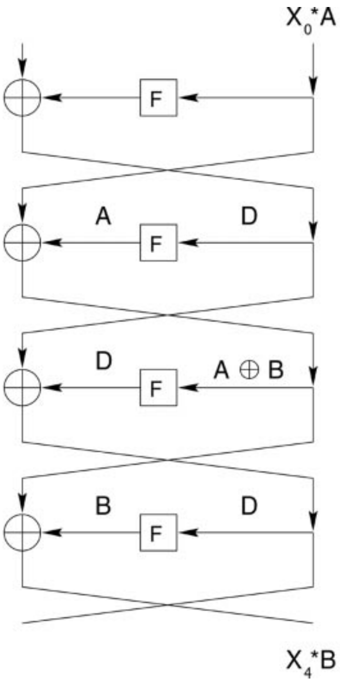

Fig. 1. 4-round linear characteristic of DES.

Here 'n:' denotes that the expression occurs in round no. n and '- - -' means that no approximation is made in the round. Notice that A and B are interchanged for every 4-round iteration. This leads to the equation for 16-round DES:

$$(P^L \cdot A) \oplus (F(P^R, K_1^*) \cdot A) \oplus (C^L \cdot D) \oplus (F(C^R, K_{16}^*) \cdot D) \oplus (C^R \cdot B) = 0 \quad (3)$$

The probability for this equation is

$$P_L^{15} = \frac{1}{2} + 2^{14-1} \prod_{i=2}^{15} (p_i - \frac{1}{2}) \quad (4)$$

where

$$\begin{aligned} p_i &= 1, \quad i \in \{2, 6, 10, 14\}, \\ p_i &= 42/64, \quad i \in \{3, 9, 11\}, \\ p_i &= 30/64, \quad i \in \{4, 8, 12\}, \\ p_i &= 12/64, \quad i \in \{5, 7, 13, 15\} \end{aligned}$$

For the correct guesses of K_1^* and K_{16}^* the equation (3) will have probability P_L^{15}. For other keys, the equation will look random. In the attack one keeps a counter

Table 1. Complexities of Matsui's linear attack on 8-round DES and full DES, where 13 key bits are found.

	8-round DES			16-round DES		
Plaintexts	2^{18}	2^{19}	2^{20}	2^{43}	2^{44}	2^{45}
Success rate	49.4%	93.2%	100%	32.5%	77.7%	99.4%

for each value of the secret key $(K_1^{'}, K_{16}^{'})$ which keeps track of the number of times the left side of the equation is 0. With N (P, C)-pairs, the key $(K_1^{'}, K_{16}^{'})$ with counter value T farthest from $\frac{N}{2}$ is taken as the correct value of the key. The sum of the key bits involved in the approximation can also be found [3]. The probability of success can be calculated by a normal approximation of the binomial distribution. Under the assumptions that $|P_L - \frac{1}{2}|$ is small, it can be shown that if one chooses $N = (P_L - \frac{1}{2})^{-2}$, one gets a probability of 97.72% that the value T of the counter for the correct value of key is more than $N/2$ when $P_L > \frac{1}{2}$ and less otherwise. However, there will be noise from the wrong keys also which have to be considered. It has been conjectured and confirmed by computer experiments that the left side of (3) will look random when wrong values of the keys are used [3]. It was also estimated by experiments that the complexity Np for the attack on DES is

$$Np \approx c|p_L - \frac{1}{2}|^{-2}$$

where $c \leq 8$. To confirm the theory we implemented tests on DES reduced to 8 rounds. The equation (3) for 8 rounds is the same as for 16 rounds except for the index of the key in the last round. For 8 rounds $Np = c \times 0.95 \times 2^{16}$. Our experimental results for 8-rounds DES can be found in Table 1.

This attack finds 13 bits of the key. It is possible to find a total of 26 key bits by using the same linear characteristic on the decryption operation. In this case the probabilities in Table 1 must be squared.

The complexity of the attack on the DES can be estimated from the complexity of the attack on 8-round DES. If one lets the complexity for the attack on 8-round DES be Np_8, the expected complexity Np_{16} for 16-round DES can be calculated such that the success probabilities are approximately the same. The formula is [4]

$$Np_8 = Np_{16}|P_{L16} - 1/2|^2/|P_{L8} - 1/2|^2.$$

With $Np_{16} = 2^{45}$ one gets

$$Np_8 = 2^{45} \times |1.19 \times 2^{-21}|^2/|1.95 \times 2^{-9}|^2 = 1.49 \times 2^{19}.$$

Thus, the success probability of the attack on 8-round DES with $N = 1.5 \times 2^{19}$ will be the same as the attack on 16-round DES with $N = 2^{45}$. The estimates of the complexity of the linear attack by Matsui, where 13 key bits are found, can be found in Table 1.

Table 2. Complexities of the first chosen-plaintext variant of the linear attack on 8-round and 12-round DES finding 7 key bits.

	8-round DES			12-round DES		
Plaintexts	2^{18}	2^{19}	2^{20}	2^{28}	2^{29}	2^{30}
Success rate	68%	99%	100%	46%	72%	94%

3 Chosen-Plaintext Attacks

In this section we consider chosen-plaintext variants of the linear attack on the DES. The time complexity of the reported attacks is always less than the data complexity, that is, the number of needed texts, and is therefore ignored in the following.

3.1 First Attack

A first chosen-plaintext extension is an attack where one does not search for the key in the first round, merely for six bits of the key in the last round, but the bias for the equation remains the same. Since the noise of 63 wrong keys is less than of 4095 wrong keys, the attack is expected to be of lower complexity than that of Matsui. The trick is that we fix the six input bits to the active S-box in the first round. Then any output mask of that function is a constant 0 or 1 with bias $\frac{1}{2}$. One then considers the following equation:

$$(P^L \cdot A) \oplus (C^L \cdot D) \oplus (F(C^R, K_n^*) \cdot D) \oplus (C^R \cdot B) = 0 \qquad (5)$$

For all guesses of the key K_n one counts the number of times the left side of the equation equals zero. Hopefully for the correct value one gets a counter with a value that differs from the mean value $\frac{N}{2}$ more than for all other counters. With a sufficient number of texts (N) this will work. Also, one can determine a seventh key bit from the bias of the equation, when searching for the rest of the key bits. The estimated number of plaintexts required, Np, is less, although only slightly less, than for Matsui's attack. The complexities of the attack on 8-round and 12-round DES are given in Table 2.

3.2 Second Attack

In addition to fixing the six bits of the input to the active S-box (no. 5) in the first round, one can try to do the same for a possible active S-box in the second round. For the 14-round characteristic used by Matsui there is no active S-box in the second round. However, if one takes the first 13 rounds of this characteristic and uses these in the rounds 3 to 15 one gets a single active S-box in both the first and second rounds. The we get the following picture.

3: - - -

4: A ← D

5: D ← A$\oplus$B

6: B ← D

7: - - -

8: B ← D

9: D ← A$\oplus$B

10: A ← D

11: - - -

12: A ← D

13: D ← A$\oplus$B

14: B ← D

15: - - -

Now we can fix the inputs to all S-boxes in the first round which output bits are input to the active S-box in the second round. To achieve this we need to fix the inputs to six S-boxes in the first round, totally 28 bits, and to fix six bits of the left half of the plaintext. Thus one needs to fix 34 bits of all plaintexts which is illustrated in Figure 2. This also means that an attacker only has 30 bits to his disposal in an attack. However, it also means that there is one round less to approximate and one would expect higher success rates.

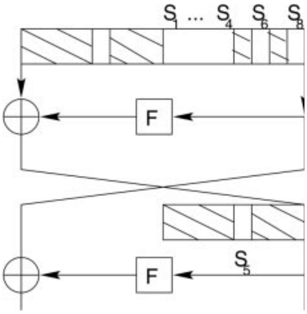

Fig. 2. The first two rounds in the linear characteristic. The bits in the striped blocks vary under the control of the attack. The bits in the white blocks are fixed.

The equation to solve in the key search is the following.

$$(P^R \cdot A) \oplus (C^L \cdot B) \oplus (F(C^R, K_n^*) \cdot B) = 0 \tag{6}$$

In this case we are able to find only six bits in the last-round key K_n, plus one key-bit from the sign of the counter T minus $\frac{N}{2}$. The probability calculation for the attack on 16-round DES is

$$P_L = \frac{1}{2} + 2^{13-1} \prod_{i=3}^{15} (p_i - \frac{1}{2}). \tag{7}$$

Table 3. Complexities of the second chosen-plaintext variant of the linear attack on 8-round DES, where we found 7 key bits.

Plaintexts	2^{16}	2^{17}	2^{18}
Success rate	78%	98%	100%
Success rate 2	90%	100%	100%

The number of chosen plaintexts needed is $Np = c|P_L - \frac{1}{2}|^{-2}$. This is a factor of $(\frac{8}{5})^2 \approx 2.6$ less than in the previous attack. By interchanging the rounds in the characteristic one can also solve for the equation

$$(P^R \cdot B) \oplus (C^L \cdot A) \oplus (F(C^R, K_{16}^*) \cdot A) = 0, \tag{8}$$

where we just flip the characteristic. Note that the involved active S-boxes and key bits are the same as for the first characteristic. This increases the success rate because for the correct key K_n we have the same sign of the bias in the two expressions. Our test results on 8-round DES of the success rate where we use one equation is shown in the first line of Table 3 and the second line is the case where we use both equations (6) and (8).

3.3 Third Attack

One problem with the previous variant is that there is a limit of 2^{30} possible texts to be used in an attack, and the attack will not be applicable to 16-round DES. In the following it is shown how more texts can be made available. This variant attack is based on two methods that we will introduce.

Pseudo-keys: In the first method we fix the same 28 bits in the right halves of the plaintexts as before. This gives a constant output for the six desirable bits which is output from the first round function and which affect the input to the active S-box in the second round. Let us denote these six bits by y_1. But where before we fixed also the six bits of the left halves of the plaintext that affect the active S-box in the second round we will now allow these to change. If we denote by K_2 the key affecting the active S-box in the second round, we define a "pseudo key" $K_2^{'} = K_2 \oplus y_1$. This allows us to search for and find six bits of $K_2^{'}$ in addition to the six bits of K_n. At this point we are able to generate 2^{36} different plaintexts with the desired property. We then try to solve the following equation:

$$(P^R \cdot A) \oplus (F(P^L, K_2^{'*}) \cdot B) \oplus (C^L \cdot B) \oplus (F(C^R, K_n^*) \cdot B) = 0 \tag{9}$$

When the attack terminates, the correct key K_2 can be determined from $K_2^{'}$ by simply adding $y_1 = F(P^R, K_1)$ when searching exhaustively for the remaining key bits of the key K and thereby K_1. There is also some overlap between the key bits of K_1 and the six bits of K_2. This must be taken into consideration when searching for the key.

Additional plaintexts: Here we show how to be able to control an additional six bits of the plaintexts. These must be bits in the right halves of the plaintexts, since all bits in the left halves are assumed to be under control of the attack already. However, this creates two problems. First, if we are going to vary some of the input bits to an S-box in round one, we also change the output bits of the round function, which were assumed to be fixed above. Second, changing the input bits to one S-box might affect the neighboring S-boxes, as these have overlapping, common input bits. However, the S-boxes 5 and 7 are not assumed to have a fixed input in the above attacks. (This allowed us to control and vary the middle two input bits to both S-boxes in the above attack.) Thus, if we vary the six bits input to S-box 6 in the first round, the second problem is overcome. Totally this gives the attack control over 2^{42} plaintexts. The first problem can be overcome by searching also for the affected six key bits entering S-box 6 in the first round. Note that when we vary the inputs to this S-box one of the bits of y_1 will vary. For each guess of the key to S-box 6 in the first round, we take this one bit into account when searching for K_2'. Fig. 3 illustrates which bits are fixed in the attack and which bits are not. The equation for this attack is

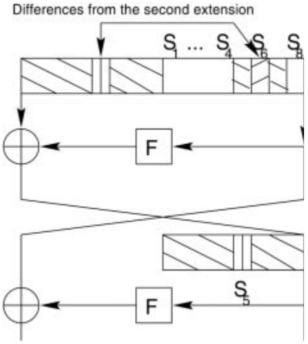
Differences from the second extension
S_1 ... S_4 S_6 S_8
F
F
S_5

Fig. 3. The first two rounds in the third attack. The inputs to the S-boxes 1,2,3,4, and 8 in the first round are fixed.

$$(P^R \cdot A) \oplus (C^L \cdot B) = (F(P^L, F(P^R, K_1^*) \oplus K_2^*) \cdot A) \oplus (F(C^R, K_n^*) \cdot B) \quad (10)$$

which has the same bias as (6). For the correct values of the three keys K_1^*, K_2^* and K_n^* observe that the equation will have probability P_L (of (7)). For wrong values the equation will look random. There are three bits in K_n and one in K_2 which overlap with key bits in K_1. Potentially the attack could find 15 key bits.

However, after implementing this attack we found that it is difficult to determine the correct value of two bits of the key K_1. The reason for this is than on the average in 50% of the cases, if the one bit of $F(P^R, K_1^*)$ that is input to S-box 5 in the second round is wrong, the masked output from S-box 5 in round 2 will still be correct. This has the effect that determining the two bits of K_1

Table 4. Complexities of the third chosen-plaintext variant of the linear attack on 8-round and 12-round DES. Here we found 12 key bits.

	8-round DES		12-round DES	
Plaintexts	2^{16}	2^{17}	2^{28}	2^{29}
Success rate	51%	94%	28%	76%

Table 5. Complexities of the known-plaintext and chosen-plaintext linear attacks on the DES. Matsui finds 13 key bits and we find 12 key bits.

	Matsui's attack			Our attack		
Plaintexts	2^{43}	2^{44}	2^{45}	2^{40}	2^{41}	2^{42}
Success rate	32%	78%	99%	6%	32%	86%

which do not overlap with bits in K_2 and K_{16} requires much effort. Because of this it is equally difficult to determine the third least significant bit in K_2. The attack finds eleven key bits much faster than all fourteen key bits. The attack can also find a 12th key bit in the similar way as in the previous attack. Simply look at the sign of the bias $|P_L - \frac{1}{2}|$ and compare with the bias of the key guessed. We implemented 100 tests with randomly chosen keys for 8-round DES and 50 similar tests for 12-round DES. The results can be found in Table 4. Thus, this variant of the attack has a poorer performance than in the previous attack, the advantage is that more plaintexts are available and a potential attack on 16-round DES is emerging.

We may estimate the success rate for 16-round DES as follows. One can calculate the expected number of plaintexts for 8-round DES, Np_8, and for 16-round DES, Np_{16}, which will have the same success rate. The ratio is the same as for Matsui's attack, because in these two attacks the bias differ with the same factor for both 8 and 16 rounds. E.g., we have that the success rate for 16-round DES using 2^{42} texts is the same as for the attack on 8-round DES with

$$Np_8 = 2^{42} \times |1.91 \times 2^{-21}|^2 / |1.56 \times 2^{-8}|^2 = 1.49 \times 2^{16}$$

texts. Similar, one gets from the attack on 12-round DES that with

$$Np_{12} = 2^{42} \times |1.91 \times 2^{-21}|^2 / |1.21 \times 2^{-14}|^2 = 1.25 \times 2^{29}$$

texts the success rate is the same as for the attack on 16-round DES with 2^{42} texts. From the experiments on 8-round and 12-round DES one gets the complexities of the chosen-plaintext linear attack on the DES of Table 5.

In total the attack finds 12 bits of key information. By repeating the attack on the decryption operation of DES an additional 12 bits of key information can be found. Subsequently, it is easy to find the remaining 32 bits by an exhaustive search. Using key-ranking the reported rates of success will be even higher. As an example, in the tests of Table 4 on 8-round DES using 2^{16} texts, the correct key appeared as one of the 8 highest ranked keys in 90 of the 100 tests, and using 2^{17} texts, the correct key was ranked 2,2,2,3,3, and 4 in the tests where it was not the first.

4 Conclusion

In this paper we presented what we believe is the fastest attack reported on the DES. The attack requires 2^{42} chosen plaintexts and finds 12 bits of the secret key with a probability of success of 86%. This should be compared to Matsui's attack, which finds one more key bit using a factor of four more plaintexts. Subsequently, in our attack, the remaining 44 bits of a DES key can be found by an exhaustive search or alternatively, an additional 12 key bits can be found by repeating the attack on the decryption routine. A new approach in our attacks is the search for "pseudo-key bits", which are secret key bits added with some unknown but fixed value. In a subsequent key search these pseudo-keys can be used to find real key bits. This approach might be applicable to similar attacks on other ciphers.

References

1. B.S. Kaliski and M.J.B. Robshaw. Linear cryptanalysis using multiple approximations. In Y. Desmedt, editor, *Advances in Cryptology: CRYPTO'94, LNCS 839*, pages 26–39. Springer Verlag, 1994.
2. L.R. Knudsen and M.P.J. Robshaw. Non-linear approximations in linear cryptanalysis. In U. Maurer, editor, *Advances in Cryptology: EUROCRYPT'96, LNCS 1070*, pages 224–236. Springer Verlag, 1996.
3. M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93, LNCS 765*, pages 386–397. Springer Verlag, 1993.
4. M. Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In Y.G. Desmedt, editor, *Advances in Cryptology - CRYPTO'94, LNCS 839*, pages 1–11. Springer Verlag, 1994.
5. M. Matsui. On correlation between the order of S-boxes and the strength of DES. In A. De Santis, editor, *Advances in Cryptology - EUROCRYPT'94, LNCS 950.* Springer Verlag, 1995.
6. M. Matsui and A. Yamagishi. A new method for known plaintext attack of FEAL cipher. In R. Rueppel, editor, *Advances in Cryptology - EUROCRYPT'92, LNCS 658*, pages 81–91. Springer Verlag, 1992.
7. T. Shimoyama and T. Kaneko. Quadratic relation of s-box and its application to the linear attack of full round DES. In H. Krawczyk, editor, *Advances in Cryptology: CRYPTO'98, LNCS 1462*, pages 200–211. Springer Verlag, 1998.
8. S. Vaudenay. An experiment on DES - statistical cryptanalysis. In *Proceedings of the 3rd ACM Conferences on Computer Security, New Delhi, India*, pages 139–147. ACM Press, 1995.