10

Analysis of DES Double Key Mode

G.Carter[‡], A.Clark[†], E.Dawson[†] and L.Nielsen[†]

[†] Information Security Research Centre
[‡] School of Mathematics

Queensland University of Technology, GPO Box 2434, Brisbane, Australia

Abstract: In this paper we examine closely a new mode of the Data Encryption Standard (DES), which is included in a new chip called SuperCrypt. This mode allows for a 112-bit key which encrypts at the same speed as DES. Initially, we give some background on the development of the cipher, and then proceed to cryptanalyse it using differential cryptanalysis and a combination of linear and differential cryptanalysis. We present results for the four, six and eight-round versions and comparisons with the DES. We theoretically extend this to the full sixteen-round version. Finally, we look at exhaustive key search in light of the fact that it has been proven feasible to construct a machine at realistic cost to find the DES key in a matter of hours.

1 INTRODUCTION

Three recent attacks on the DES algorithm over the past four years have raised serious doubts about the security of this algorithm.

The first of these attacks uses the method of differential cryptanalysis by Biham and Shamir [1]. Using this method it was shown that it may be possible to derive the 56-bit DES key using 2^{47} chosen plaintext pairs of blocks.

The second attack uses the method of linear cryptanalysis by Matsui [2]. At CRYPTO'94 [4] Matsui reported the first experimental, publicly reported cryptanalysis of the DES algorithm using 2^{43} known plaintext blocks. This attack recovered the entire key in fifty days using twelve HP9735/PA-RISC 99mhz computers operating in parallel.

The final method is a brute force attack by Wiener. At SAC'94 [5] Wiener proposed the construction of special DES hardware consisting of many DES chips operating in parallel using 1993 technology. This device could conduct an exhaustive key search requiring on the average testing 2^{55} keys and a couple of known plaintext-ciphertext block pairs. The estimated time required for this attack varied according to how many chips were used. Wiener's estimate for the costs in US $ and the time to complete the attack are given in Table 1.

Machine Cost	Time
$100,000	35 hours
$1,000,000	3.5 hours
$10,000,000	21 minutes

Table 1: Wiener's Time-Cost Tradeoffs

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

Recently, a new high speed encryption chip called SuperCrypt has been designed by the company Computer Elecktonic Infosys from Germany [7]. This chip incorporates the DES algorithm and allows for high speed encryption rates at twelve megabytes per second for the various standard modes of operation of the DES algorithm. As well, this chip allows for a special extended mode of operation of DES using a 112-bit key in place of the standard 56-bit key.

Briefly, the 112-bit mode key operation used in the SuperCrypt chip consists of the standard DES algorithm with two 56-bit keys, Key 1 and Key 2, which operate on odd and even rounds respectively. Each of these 56-bit keys is expanded into sixteen subkeys of length forty-eight bits using the DES key schedule. On the odd rounds forty-eight bits of Key 1 are used as per the odd round DES key schedule, and on the even rounds forty-eight bits of Key 2 are used as per the even round DES key schedule. All the other operations are as per the DES algorithm. Figure 1 shows the algorithm. We shall call this encryption procedure the *double-key* mode of DES. This procedure allows the SuperCrypt chip to encrypt at the same speed of twelve megabytes per second using a 112-bit key, as with a 56-bit key.

The natural question to ask is how much have we increased the security of the standard DES algorithm by using a 112-bit key in place of a 56-bit key as described above? In this paper we will examine this question in relation to differential and linear cryptanalysis as well as exhaustive key search.

2 DIFFERENTIAL CRYPTANALYSIS

Differential cryptanalysis is a powerful cryptanalytic tool developed by Biham and Shamir [1]. The method applies a chosen plaintext attack on many ciphers which use an iterated round operation as originally proposed by Feistel [6]. The attack is based on using chosen plaintext pairs of blocks whose difference is fixed. This difference is called the characteristic. On this basis, it is possible to approximate the round operation, F, of the cipher by determining, probabilistically, the output differences of the F-function for any given input difference. This can be done for each round of the cipher and thus for a given plaintext difference the output difference of any number of rounds can be determined probabilistically.

2.1 Differential Cryptanalysis of DES

Differential cryptanalysis is a chosen plaintext attack which firstly defines the 'difference' of two plaintext blocks P and P^* as $P \oplus P^* (= P')$, where $\oplus$ indicates the bitwise exclusive-or (XOR) operation. In any round of this cipher, the inputs to the round function, F, will be $P_{Li} \oplus K_i$ and $P^*_{Li} \oplus K_i$, where P_{Li} is the right-most 32-bits of the plaintext block, P_{Hi} is the left-most 32-bits of the plaintext block and K_i is the secret key used in Round i. The input 'difference' to any round is independent of the key, since $(P_{Li} \oplus K_i) \oplus (P^*_{Li} \oplus K_i) = (P_{Li} \oplus P^*_{Li})$.

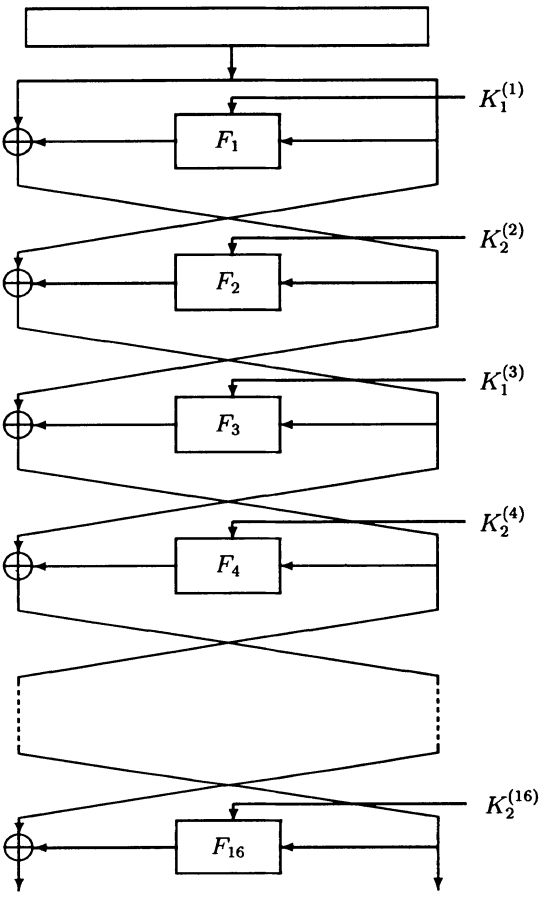

Figure 1: Double Key Mode DES, where $K_i^{(j)}$ is the jth round schedule of key K_i

The round function in DES is a series of eight substitution boxes (S-boxes). Into each of these is passed six bits, and four bits are outputted. Biham and Shamir [1] were able to show that, if the input 'difference' to each S-box was known, then, by an exhaustive search, the possible output differences and the regularity of their occurrence (i.e. their probability) could be determined. These results were published by Biham and Shamir in their so-called XOR tables [1]. There are eight such tables, one for each S-box. Table 2 is an extract from the XOR table for S-box 1.

Input	Output XOR														
XOR	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A_x	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B_x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D_x	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E_x	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F_x	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
								⋮								
30_x	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
31_x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32_x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33_x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34_x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
35_x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36_x	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
37_x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38_x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39_x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
$3A_x$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
$3B_x$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
$3C_x$	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
$3D_x$	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
$3E_x$	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
$3F_x$	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

Table 2: Partial Pairs XOR Distribution Table of S1

There are sixty-four possible input differences $P_t \oplus P_t^* = P_t'$, where P_t and P_t^* are the six bits of P and P^* respectively which go into S-box numbered t. There are sixteen possible output differences. Thus for a given input difference, P_t', the regularity of each of the possible output differences is in the row corresponding to P'. Since there are

sixty-four possible input differences the probability of any particular output difference occurring is obtained by dividing that particular entry in the table by sixty-four. For example, an input difference of 34_x (hexadecimal) will given an output difference of 2_x with probability of 0.25. Thus, the round function of DES can be approximated by these expressions. This can be done for all the rounds of DES and thus we get a string of approximations for the rounds of DES. These approximations, together with the initial plaintext difference and the final ciphertext difference constitute what is known as a *characteristic*. If the probability of this characteristic (which is just the product of the probabilities of the round approximations) is not too small, then for a given number of chosen plaintext-ciphertext pairs, key bits in the last round can be determined. By using two or more different characteristics more last round key bits can be determined until it is possible to find the remaining unknown bits by exhaustive search.

2.2 Differential Cryptanalysis of Double-Key Mode

Because this version of DES uses two distinct keys, variation of the traditional differential cryptanalysis attack on DES must be employed. Our technique is to use differential cryptanalysis to find all the last round key bits and then strip away the last round and perform the traditional attack on the double-key mode of DES with one less round. This technique is not new. Biham and Shamir [1] suggested it as a method for attacking a version of DES that employed independent keys in each round. The results of our attacks on the four-round, six-round and eight-round versions of the double-key mode are presented in Table 3, together with the theoretical extension to sixteen rounds.

The method used was to find enough different characteristics to completely determine the last round key, and then, as explained earlier, attack the second-last round (and hence the other key) using standard differential techniques. To find a number of different characteristics we used the dynamic programming algorithm as introduced by Matsui [3]. We adapted this algorithm in that, instead of finding the characteristic with best probability, characteristics whose probabilities were above a certain threshold were determined. As well sufficient characteristics were required in order that the six key bits for each of the eight S-boxes could be determined.

In the four-round version, we were able to determine all forty-eight bits of the last (even) round key with two characteristics (see Table 3). The second-last (odd) round key was determined completely by a single characteristic (see Table 3). In all, forty-eight plaintext-ciphertext pairs were used to find ninety-six bits of the 112-bit key. We were then able to find the remaining eight bits of the odd-round key and the eight remaining bits of the even-round key by exhaustive search. Such an attack on the DES would yield forty-eight bits of the 56-bit DES key with thirty-two plaintext-ciphertext pairs.

We noted that, in the four-round version, each key was used twice. If the DES key scheduling algorithm is employed not all fifty-six bits of either key are used, so the effective length of each key will shorten. However, this could be easily overcome by altering the key schedule to ensure that all key bits are used by the fourth round.

To break the six-round version, three characteristics (see Table 3) were used to determine the last round key. In each case, one hundred and sixty pairs were required. All forty-eight bits of the penultimate round key were found using two characteristics (see Table 3), each with one hundred and sixty pairs. Thus in six rounds of the double-key mode, ninety-six bits of the 112-bit key were found using eight hundred plaintext-ciphertext pairs. Once again, the sixteen remaining unknown bits were found by exhaustive search. The forty-eight bits of the last round key can be found using four hundred and eighty plaintext-ciphertext pairs.

The eight-round version was broken using three characteristics (see Table 3) to determine the complete last round key. Since each has a different probability, different numbers of pairs were required. The maximum required was three million. To attack the seventh round key three characteristics (see Table 3) were used. This retrieved forty-two bits used in the seventh round key. Hence, for eight rounds of the double-key mode, ninety bits of the 112-bit key were found using 6.65 million plaintext-ciphertext pairs. The twenty-two remaining key bits were found by exhaustive search. For eight rounds of DES forty-two bits of the 56-bit key can be found using 2.15 million pairs.

Version	Round Number	*Bits* Found	Characteristic (hexadecimal)	No.ofPairs Double − Key	DES
4−round	4	42	2000 0000 0000 0000	16	16
		6	0222 2222 0000 0000	16	16
	3	48	0222 2222 0000 0000	16	n/a
6−round	6	30	4008 0000 0400 0000	160	160
		12	0020 0008 0000 0400	160	160
		6	4000 4010 0200 0000	160	160
	5	36	4008 4000 0400 0000	160	n/a
		12	0020 0008 0000 0400	160	n/a
8−round	8	30	405C 0000 0400 0000	150 000	150 000
		12	0404 0780 0020 2000	2 000 000	2 000 000
		6	1960 0000 0000 0000	3 000 000	n/a
	7	24	405C 0000 0400 0000	100 000	n/a
		12	0200 0401 0000 0020	100 000	n/a
		6	0000 0820 0000 0006	100 000	n/a
16−round	16	18	1960 0000 0000 0000	2^{57}	2^{57}
		18	0000 1D40 0000 0000	$2^{59.3}$	$2^{59.3}$
		6	0019 6000 0000 0000	2^{57}	n/a
		6	2000 001d 0000 0000	2^{61}	n/a
	15	48	1960 0000 0000 0000	2^{57}	n/a

Table 3: Double-Key - DES Comparison Table

2.3 Extension to Sixteen Rounds

Biham's initial proposed attack on the sixteen-round version of DES required more

plaintext-ciphertext pairs than exhaustive search of the key space. However, in 1992 [11], he proposed a modification to his initial sixteen-round attack and was able to reduce the number of pairs required from 2^{57} to 2^{47}, analysing these in 2^{37} time, without the need for huge memory. In this theoretical attack, all fifty-six bits of the key were obtained. Thus, the DES was rendered theoretically vulnerable to differential cryptanalysis.

However, this new attack is not feasible against a DES-like algorithm that has independent keys. Double-key mode DES falls into this category and, hence, remains out of reach of differential cryptanalysis for the time being.

We can talk theoretically about breaking the double-key mode DES using standard differential cryptanalysis techniques, and compare it with the standard differential attack on the DES, using iterative characteristics. The entries in Table 3 which refer to sixteen-round attacks, reflect such a comparison.

Using a standard differential attack, eighteen bits of the last round key of sixteen-round DES can be found using 2^{57} plaintext-ciphertext pairs. The characteristic used is $1960\,0000\,0000\,0000_x$, the iterative characteristic with largest probability ($\frac{1}{234}$). Another iterative characteristic, $0000\,1D40\,0000\,0000_x$, with probability $\frac{1}{293}$ can be used with approximately $2^{59.3}$ pairs to find another eighteen bits of the last round key. The remaining twelve unknown key bits could be found by exhaustive search. With double-key DES the remaining twelve bits of the last round key would need to be determined by methods other than exhaustive search. This could be done using iterative characteristics $0196\,0000\,0000\,0000_x$, requiring 2^{57} pairs, and $2000\,001D\,0000\,0000_x$, requiring 2^{61} pairs.

Thus the total number of plaintext-ciphertext pairs required to get all forty-eight bits of the last round key is $2^{61.5}$. All forty-eight bits of the fifteenth round key can be found using the characteristic $1960\,0000\,0000\,0000_x$ with 2^{51} plaintext-ciphertext pairs. Thus we will require approximately $2^{51} + 2^{61.5} \approx 2^{61.5}$ plaintext-ciphertext pairs to get ninety-six bits of the 112-bit key. The remaining bits can be found by exhaustive search. Thus the order of magnitude of additional pairs required to break the double-key mode of DES is $\frac{2^{61.5}}{2^{59.6}} \approx 4$.

3 LINEAR CRYPTANALYSIS

Linear cryptanalysis as introduced by Matsui [2] is a known plaintext attack which exploits probabilistic linear relationships between the plaintext P, ciphertext C and key K. The relationship can be expressed in the form

$$P[i_1, i_2, \cdots, i_a] \oplus K[j_1, j_2, \cdots, j_b] = C[k_1, k_2, \cdots, k_c],$$

where $P[i_1, i_2, \cdots, i_a]$ is the XOR sum of plaintext bits $i_1, i_2, \cdots, i_a$ and $K[j_1, j_2, \cdots, j_b]$ and $C[k_1, k_2, \cdots, k_c]$ are similar XOR sums of key and ciphertext bits respectively.

If the above equation holds with probability $p \neq \frac{1}{2}$ then we can exploit this linear relationship to determine some key bits. The further the value of p is from $\frac{1}{2}$, the more efficiently we can find these key bits.

For each round of a cipher an approximation similar to the one above can be

determined which relates the input of the round to the output. These approximations can be XOR summed, and if they are chosen carefully, only plaintext, ciphertext and key bits will remain, with bits of intermediate rounds cancelling. This then produces a linear expression for the cipher.

3.1 Linear Cryptanalysis of DES

In the DES, probabilistic linear approximations for a round are determined by examining the linear relationship between the XOR sum of input bits and the XOR sum of output bits for each S-box. Thus, we can produce a table for each S-box which displays this relationship and its probability. Table 4 is an extract of the S-box 5 table.

α/β	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
02	4	−2	2	−2	2	−4	0	4	0	2	−2	2	−2	0	−4
03	0	−2	6	−2	−2	4	−4	0	0	−2	6	−2	−2	4	−4
04	2	−2	0	0	2	−2	0	0	2	2	4	−4	−2	−2	0
05	2	2	−4	0	10	−6	−4	0	2	−10	0	4	−2	2	4
06	−2	−4	−6	−2	−4	2	0	0	−2	0	−2	−6	−8	2	0
07	2	0	2	−2	8	6	0	−4	6	0	−6	−2	0	−6	−4
08	0	2	6	0	0	−2	−6	−2	2	4	−12	2	6	−4	4
09	−4	6	−2	0	−4	−6	−6	6	−2	0	−4	2	−6	−8	−4
10	4	0	0	−2	−6	2	2	2	2	−2	2	4	−4	−4	0
11	4	4	4	6	2	−2	−2	−2	−2	−2	2	0	−8	−4	0
12	2	0	−2	0	2	4	10	−2	4	−2	−8	−2	4	−6	−4
13	6	0	2	0	−2	4	−10	−2	0	−2	4	−2	8	−6	0
14	−2	−2	0	−2	4	0	2	−2	0	4	2	−4	6	−2	−4
15	−2	−2	8	6	4	0	2	2	4	8	−2	8	−6	2	0
16	2	−2	0	0	−2	−6	−8	0	−2	−2	−4	0	2	10	−20
							⋮								
48	2	−2	0	−4	−6	−2	−4	4	2	2	0	0	2	2	4
49	2	−2	0	0	−2	2	0	0	−2	−2	−4	0	2	2	4
50	6	0	−2	−2	8	2	4	0	10	0	2	−2	4	2	0
51	−6	0	10	2	0	−2	−4	0	6	0	−10	2	4	−2	0
52	0	−12	4	−4	0	4	−8	−4	0	−4	0	−4	−4	0	0
53	−8	0	0	8	−4	4	0	0	−4	−4	0	4	4	−4	4
54	4	−2	−6	−2	−2	8	0	4	−4	−2	−2	6	2	−4	0
55	−8	−6	−6	−6	6	0	4	12	0	2	−2	2	2	4	−4
56	2	4	−6	0	−2	4	−2	−6	4	−6	0	6	4	−2	0
57	−2	8	2	−4	6	−4	−6	−2	−4	2	4	−2	0	2	0
58	6	−10	0	2	4	0	−2	6	−4	0	2	4	−2	−2	−4
59	−2	−6	−4	−10	0	−8	−2	−10	4	4	−2	0	2	−2	4
60	−8	−6	−2	0	−4	2	2	−6	2	4	0	10	−2	4	4
61	4	2	2	4	4	−2	2	−2	10	0	0	2	2	4	0
62	−4	4	−4	2	2	−2	2	2	−2	−2	−2	4	−4	0	4
63	−4	−4	−4	14	6	−6	−2	2	−2	6	−2	0	0	−4	0

Table 4: Partial Linear Approximate Probabilities for S-box 5

The entry -20 is at the conjunction of row 16 and column 15. In 6-bit binary notation 16 is 010000, and in 4-bit binary notation 15 is 1111. This indicates that the second most significant bit of input to S-box 5, XOR'd with the corresponding key bit, will be equal to the XOR sum of all output bits on twelve occasions out of a possible sixty-four. The entry -20 in the table is obtained by subtracting thirty-two from twelve. In fact, all entries in the table have had thirty-two subtracted. This gives a better appreciation of how far from $\frac{1}{2}$ the probability for each expression is. By combining approximations of this kind, it is possible to determine a linear expression for any number of rounds of DES, and from this, some of the key bits in the first and last rounds can be found. Remaining key bits can then be determined by exhaustive search.

4 COMBINED DIFFERENTIAL AND LINEAR CRYPTANALYSIS

In this section, we use a combination of differential and linear cryptanalysis (Differential-Linear cryptanalysis) to break four, six and eight rounds of double-key DES. We also present a theoretical extension to sixteen rounds.

Our method is to use differential cryptanalysis to determine the last round key and, hence, forty-eight bits of Key 2. We then use linear cryptanalysis to attack one fewer round. Our reason for preferring differential cryptanalysis to linear cryptanalysis in determining the last round key is that, in general, differential cryptanalysis will determine more key bits for a give characteristic than will a linear cryptanalysis expression and, as we require *all* the key bits in the last round, the fewer characteristics we can use the better.

To illustrate this, note that in the previous section all forty-eight bits of the last round key were found using, at most, three characteristics in the cases of four, six and eight rounds. If we were to use Matsui's algorithm 2-A [2], then we would require a minimum of four linear expressions as this algorithm finds at most thirteen distinct bits per expression. However, each expression rarely finds thirteen distinct bits so it is certain that more than four expressions will be required and, hence, more pairs will be needed.

Thus, we will use linear cryptanalysis to attack three, five and seven rounds of double-key DES assuming that the fourth, sixth and eighth round keys respectively have been determined by differential cryptanalysis.

4.1 Differential-Linear Cryptanalysis of Double Key Mode

We attacked three rounds of the double-key DES and obtained forty-four bits of Key 1 using five different approximations to Round 2, and using algorithm 2-A as produced by Matsui. Each approximation has the form

$$X_2[m] \oplus F_2(X_2, K_2^{(2)})[a, b, c, d] = K_2^{(2)}[t],$$

where X_2 is the input to Round 2, F_2 is the output of the S-boxes and $K_2^{(2)}$ is the

second-round key. Each approximation required no more than two hundred plaintext-ciphertext pairs. The linear expression for three rounds of DES, obtained from each of these approximations has the form

$$P_H[m] \oplus F_1(P_L, K_1^{(1)}[m] \oplus C_H[m] \oplus F_3(C_L, K_1^{(3)})[m] = 0,$$

where P_H and C_H represent the left-most thirty-two bits of plaintext and ciphertext respectively, and P_L and C_L represent the right-most thirty-two bits of plaintext and ciphertext respectively. With the forty-eight bits of $K_2^{(4)}$ obtained by differential cryptanalysis, we were able to determine ninety-two bits of the key. The other twenty bits were found by exhaustive search. The results are summarised in Table 5.

Approximation	m	a	b	c	d	t	Probability (Round 2 approx)	Probability (Linear Expr)
1	15	7	18	24	29	22	12/64	0.6953
2	31	1	9	15	23	46	14/64	0.6582
3	3	5	11	17	27	4	16/64	0.6250
4	7	0	10	20	25	10	18/64	0.5957
5	11	3	13	21	–	16	18/64	0.5957

Table 5: Summary of Results for 3- and 5-round Double Key DES.

An attack on five rounds of double-key DES was successful using five approximations, each of which consisted of a pair of equations having the form

$$\begin{aligned} X_2[m] \oplus F_2(X_2, K_2^{(2)})[a,b,c,d] &= K_2^{(2)}[t] \\ X_4[m] \oplus F_4(X_4, K_2^{(4)})[a,b,c,d] &= K_2^{(4)}[t] \end{aligned}$$

With this type of approximation the linear expression for five rounds of double-key DES is

$$\begin{aligned} P_L[a,b,c,d] \oplus P_H[m] \oplus F_1(P_L, K_1^{(1)})[m] \oplus C_L[a,b,c,d] \oplus \\ C_H[m] \oplus F_5(C_L, K_1^{(5)})[m] = K_2^{(2)}[t] \oplus K_2^{(4)}[t], \end{aligned}$$

Again a total of forty-four bits of Key 1 was found and, together with the forty-eight bits of Key 2 found by differential cryptanalysis, a total of ninety-two bits was known. The remaining twenty were again found by exhaustive search. No more than two hundred plaintext-ciphertext pairs were required. See Table 5 for a summary.

Seven round double-key DES has been successfully attacked using three approximations, each of which consist of three equations which have the form

$$\begin{aligned} X_3[m] \oplus F_3(X_3, K_1^{(3)})[D] &= K_1^{(3)}[t_1] \\ X_4[d] \oplus F_4(X_4, K_2^{(4)})[m] &= K_2^{(4)}[t_2] \\ X_5[m] \oplus F_5(X_5, K_1^{(5)})[D^*] &= K_1^{(5)}[t_1] \end{aligned}$$

where D and D^* are sets of bits such that $D^* \subset D$, $d \epsilon D$ but D is not an element of D^*. These approximations yield a linear expression for seven rounds of

$$\begin{array}{rcccccc} P_H[D] & \oplus & F_1(P_L, K_1^{(1)})[D] & \oplus & C_H[D^*] & \oplus & F_7(C_L, K_1^{(7)})[D^*] \\ & = & K_1^{(3)}[t_1] & \oplus & K_2^{(4)}[t_2] & \oplus & K_1^{(5)}[t_1]. \end{array}$$

A total of thirty bits can be found in this way but the number of pairs required varies considerably from one hundred thousand to 2.5 million. With the forty-eight bits of key already found in round 8, we have determined a total of seventy-eight bits. The thirty-four remaining bits can be found by exhaustive search. This is summarised in Table 6.

Approximation	m	D	D*	d	Probability (linear exp)	Number of pairs
1	15	7, 18, 24, 29	7, 18, 24	29	0.5061	10^5
2	29	9, 15, 23	9, 23	15	0.4985	2×10^6
3	9	3, 21, 28	3, 21	28	0.4993	2.5×10^6

Table 6: Summary of Results for 7-round Double Key DES.

4.2 Extension to Fifteen Rounds

The extension to fifteen rounds can be made by iterating the approximations used in the seven-round attack. Hence each approximation consists of nine equations which have the form

$$\begin{array}{rcccc} X_3[m] & \oplus & F_3(X_3, K_1^{(3)})[D] & = & K_1^{(3)}[t_1] \\ X_4[m] & \oplus & F_4(X_4, K_2^{(4)})[m] & = & K_2^{(4)}[t_2] \\ X_5[m] & \oplus & F_5(X_5, K_1^{(5)})[D^*] & = & K_1^{(5)}[t_1] \\ X_7[m] & \oplus & F_7(X_7, K_1^{(7)})[D] & = & K_1^{(7)}[t_1] \\ X_8[m] & \oplus & F_8(X_8, K_2^{(8)})[m] & = & K_2^{(8)}[t_2] \\ X_9[m] & \oplus & F_9(X_9, K_1^{(9)})[D^*] & = & K_1^{(9)}[t_1] \\ X_{11}[m] & \oplus & F_{11}(X_{11}, K_1^{(11)})[D] & = & K_1^{(11)}[t_1] \\ X_{12}[m] & \oplus & F_{12}(X_{12}, K_2^{(12)})[m] & = & K_2^{(12)}[t_2] \\ X_{13}[m] & \oplus & F_{13}(X_{13}, K_1^{(13)})[D^*] & = & K_1^{(13)}[t_1] \end{array}$$

where D, D^*, m, t_1 and t_2 are as for the 7-round version. The linear expression for fifteen rounds obtained from these approximations is

$$
\begin{array}{rcccccccc}
P_H[D] & \oplus & F_1(P_L, K_1^{(1)})[D] & \oplus & C_H[D^*] & \oplus & F_{15}(C_L, K_1^{(15)})[D^*] & & \\
 & = & K_1^{(3)}[t_1] & \oplus & K_2^{(4)}[t_2] & \oplus & K_1^{(5)}[t_1] & \oplus & K_1^{(7)}[t_1] \\
 & & & \oplus & K_2^{(8)}[t_2] & \oplus & K_1^{(9)}[t_1] & \oplus & K_1^{(11)}[t_1] \\
 & & & \oplus & K_2^{(12)}[t_2] & \oplus & K_1^{(13)}[t_1]. & &
\end{array}
$$

Again, thirty bits of Key 2 can be found in this way and, as before, we now have a total of seventy-eight bits of key known. The remaining bits can be found by exhaustive search. These results are summarised in Table 7. Note that only the probabilities and number of pairs are produced in this table as the other quantities m, D, D^* and d are as in Table 6.

Approximation	Probability	Number of Pairs
1	0.500000909	1.2×10^{12} ($\sim 2^{40}$)
2	0.499999987	6.4×10^{15} ($\sim 2^{53}$)
3	0.499999987	6.4×10^{15} ($\sim 2^{53}$)

Table 7: Summary of Results for 15-round DES.

5 COMPARISON OF DIFFERENTIAL-LINEAR AND DIFFERENTIAL CRYPTANALYSIS

Table 8 shows the comparison between the linear and differential attacks.

Version	Cryptanalysis	BITS Found	Number of PAIRS
4–round	Differential – Linear	92	1032
	Differential	96	48
6–round	Differential – Linear	92	1320
	Differential	96	800
8–round	Differential – Linear	78	9 750 000
	Differential	90	5 450 000
16–round	Differential – Linear	78	$\sim 2^{61}$
	Differential	96	$\sim 2^{61}$

Table 8: Comparison between Linear and Differential Attacks.

It appears that in all versions, differential cryptanalysis is better than a combination of diffential-linear cryptanalysis both in terms of the number of pairs required and bits found. However, there may be better linear approximations which would improve the aspects of the combined attack.

6 EXHAUSTIVE SEARCH

The 56-bit DES key has long been considered inadequate. Exhaustive search attacks on the 56-bit key have supported the call for a longer DES key. As well, various

methods to extend the key length to 112 bits have been proposed.

6.1 Proposed Hardware Attack

As mentioned in Section 1, Wiener [5] has proposed a machine that could be built at reasonable cost which would determine the 56-bit key of DES in hours using 1993 technology only. The time taken to complete the search is a function of the number of processors employed. It is highly unlikely that a machine along the lines of that described by Wiener [5] will be feasible in the near future to exhaustively search all 2^{112} possible keys of the double-key mode.

6.2 Multiple Encryption

Multiple encryption of DES using two or more keys has been proposed. In particular, two methods have been proposed using a 112-bit key, namely double-encryption with two 56-bit keys and two-key triple encryption also using 56-bit keys (see Figures 2 and 3).

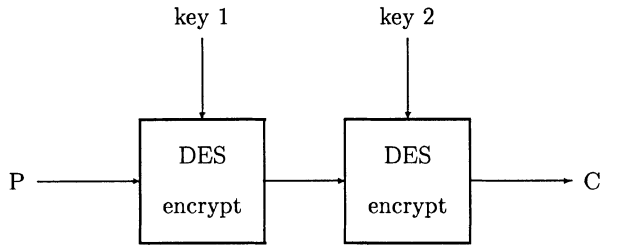

Figure 2: Double-DES Encryption

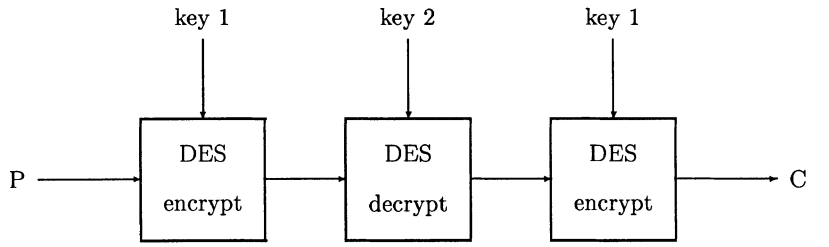

Figure 3: Triple-DES Encryption

Both of these have been extensively studied, [5] [8] [9] [10], and the complexity of the attack reduced from the brute force 2^{112} operations to an order of 2^{56} operations by 'meet-in-the-middle' type attacks using a time-memory trade-off. It should be noted that this method is still not very practical, in that is requires storage of 2^{56}

64-bit blocks. This is infeasible, even with main frame computers.

The 'meet-in-the-middle' attacks on multiple encryption rely on the fact that each key is used in one complete DES encryption. The double-key mode of DES is different in that both keys are used alternately in the rounds of a single DES encryption.

Thus it appears that a 'meet-in-the-middle' attack of the type described in [5] [8] [9] [10], is not possible on the double-key mode.

7 CONCLUSION AND FURTHER RESEARCH

The double-key mode of DES does indeed have increased security over that of the DES. This increased security is very marginal in relation to standard differential cryptanalysis, but quite substantial if the modified differential attack on the DES is used for comparison. The order of magnitude of additional pairs required to break the double-key mode of DES using this modified differential attack is $\frac{2^{61.5}}{2^{47}} \approx 2^{14.5}$. We believe that the resistance of double-key mode DES to differential cryptanalysis can be further improved if the key is scheduled in a different way.

Matsui was able to break the standard mode of DES using 2^{43} known plaintext-ciphertext pairs. A differential-linear attack will break double-key DES with approximately 2^{61} plaintext-ciphertext pairs. This represents a factor of 2^{18} increase in the number of pairs required, which is very substantial. Once again it can be seen that double-key mode DES is far more secure than DES against this attack.

Exhaustive search appears to be the most likely attack to succeed against the DES in reasonable time. Despite Matsui's efforts [4] in using linear cryptanalysis to break the DES in fifty days and Biham's proposed modified differential attack [11], only exhaustive search, at the moment, appears capable of reducing this to a matter of hours rather than days. Clearly, this is not the case for double-key DES. While both differential cryptanalysis and linear cryptanalysis are currently technically incapable of breaking double-key DES, they are faster than exhaustive search.

The use of a 112-bit key either through multiple encryption or the double-key mode described in this paper will prevent exhaustive key attacks in the forseeable future.

The major strengths of the double-key mode are its apparent invulnerability to 'meet-in-the-middle', differential, linear and combined differential-linear attacks which have been used to reduce the complexity of attacks against other DES-like encryption systems, to the point where they are approaching vulnerability. As well, the double-key mode offers the same encryption/decryption speed as the standard operation of DES.

It is worth noting that the key schedule of double-key DES means that not all key bits are used until after the seventh round of the algorithm. This is in contrast to the DES where all bits are used after two rounds. We are still investigating this aspect. However, for the time being, the double-key mode of DES appears to be very secure.

References

[1] E.Biham and A.Shamir.*Differential Cryptanalysis of DES-like Cryptosystems*

Journal of Cryptology, 4(1):3-72, 1991.

[2] M.Matsui. *Linear Cryptanalysis Method for DES Cipher* Advances in Cryptology: Proceedings of EUROCRYPT '93, Springer-Verlag, Berlin, pp 386-397, 1994.

[3] M.Matsui. *On Correlation Between the Order of S-Boxes and the Strength of DES* Preproceedings of EUROCRYPT '94, pp 375-387, 1994.

[4] M.Matsui. *The First Experimental Cryptanalysis of the Data Encryption Standard* Advances in Cryptology: Proceedings of CRYPTO '94, Springer-Verlag, Berlin, pp 1-11, 1994.

[5] M.J.Wiener. *Efficient DES Key Search* Workshop on Selected Areas in Cryptography (SAC '94), Queen's University, Canada, p 1, 1994.

[6] H.Feistel. *Cryptography and Computer Privacy* Scientific American, Vol.228, No.5, May 1973, pp 15-23.

[7] *SuperCrypt - High Speed Cryptographic Data Security Element* CE Infosys 99C003 Preliminary Data Sheet Vers 1.01, Computer Elecktonic Infosys GmbH, Germany.

[8] R.C.Merkle and M.Hellman. *On the Security of Multiple Encryption* Communications of the ACM, v.24,n.7, 1981, pp 465-467.

[9] W.Tuchman. *Hellman Presents No Shortcut Solutions to DES* IEEE Spectrum, v.16, n.7, July 1979, pp 40-41.

[10] P.C.van Oorschot and M.J.Wiener. *A Known-Plaintext Attack on Two-Key Triple Encryption* Advances in Cryptology - EUROCRYPT'90 Proceedings, Berlin: Springer-Verlag, 1991, pp 318-325.

[11] E.Biham and A.Shamir. *Differential Cryptanalysis of the Full 16-round DES* Advances in Cryptology - CRYPTO'92, Springer-Verlag, Berlin, pp 487-496, 1993.