Cryptanalysis of the CFB mode of the DES with a reduced number of rounds

Bart Preneel*, Marnix Nuttin, Vincent Rijmen**, and Johan Buelens

Katholieke Universiteit Leuven, Laboratorium ESAT-COSIC,
Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium
bart.preneel@esat.kuleuven.ac.be

Abstract. Three attacks on the DES with a reduced number of rounds in the Cipher Feedback Mode (CFB) are studied, namely a meet in the middle attack, a differential attack, and a linear attack. These attacks are based on the same principles as the corresponding attacks on the ECB mode. They are compared to the three basic attacks on the CFB mode. In 8-bit CFB and with 8 rounds in stead of 16, a differential attack with $2^{39.4}$ chosen ciphertexts can find 3 key bits, and a linear attack with 2^{31} known plaintexts can find 7 key bits. This suggests that it is not safe to reduce the number of rounds in order to improve the performance. Moreover, it is shown that the final permutation has some cryptographic significance in the CFB mode.

1 Introduction

The Data Encryption Standard (DES) was developed in the seventies at IBM (together with NSA) and was published by the National Bureau of Standards in 1977 [8]. Its intended application was sensitive but unclassified data. In spite of the initial controversy, it became the most widespread cryptographic algorithm. Four modes of use of the DES have been specified in national and international standards [9, 11]: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB). The DES has been the subject of several studies. One of the first properties that was discovered was the complementation property [10]; it can be exploited to halve the number of operations for an exhaustive key search. Attacks have been described in [6, 7], but the most successful techniques are differential cryptanalysis introduced by E. Biham and A. Shamir [3] and linear cryptanalysis invented by M. Matsui [13]. The first attack which is faster than exhaustive key search was the differential attack of [5]. Most attacks on the DES are applicable to the ECB mode, and some can be extended to the CBC mode [4]. Only one attack was published on the OFB mode [12]: it was shown by R. Jueneman that the size of the feedback

* N.F.W.O. postdoctoral researcher, sponsored by the National Fund for Scientific Research (Belgium).
** N.F.W.O. research assistant, sponsored by the National Fund for Scientific Research (Belgium).

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 212-223, 1994.

variable should be 64 bits. For the time being no evaluation of the DES in the CFB mode has been published [14].

In this volume, K. Ohta and M. Matsui describe a differential attack which is applicable to the m-bit CFB mode for 'large' values of m ($m \geq 24$) [15]. This paper presents attacks that are also applicable for smaller values of m.

In the first part of this paper the CFB mode is described. In Sect. 3 three basic attacks are discussed that depend only on the size of the parameters of the algorithm; they can serve as a point of reference. Section 4 shows how a meet in the middle attack can be applied in the CFB mode. In Sect. 5 the main result is discussed, namely the extension of differential cryptanalysis to the CFB mode. Section 6 discussed the applicability of linear attacks. Finally the conclusions are presented.

2 The CFB mode

This section discusses the CFB mode for a block cipher with a block length of t bits ($t = 64$ in case of the DES). The CFB mode is a stream mode, i.e., the size m of the plaintext blocks can be arbitrarily chosen between 1 and t bits. The scheme that is described here is a simplified version of the more general scheme contained in the standards.

The CFB mode makes use of an internal t-bit register. The state of this register before the encryption or decryption of the ith block is denoted with X_i. First this register is initialized with the starting variable or $X_1 = SV$. The plaintext and ciphertext blocks are denoted with P_i and C_i respectively, and the encryption operation with the secret key K is denoted with $E_K()$.

The encryption of plaintext block i consists of the following two steps:

$$C_i = P_i \oplus \mathrm{rchop}_{t-m}(E_K(X_i))$$
$$X_{i+1} = \mathrm{lchop}_m(X_i)||C_i\,.$$

Here $||$ denotes concatenation, rchop_a denotes the function that drops the a rightmost bits of its argument, and lchop_a denotes the function that drops the a leftmost bits of its argument. The decryption operates in a similar way.

The most important property of the CFB mode is that if m is chosen equal to the character size, this mode is *self synchronizing*. This means that if one or more m-bit characters between sender and receiver are lost, automatic resynchronization occurs after t bits. This is especially important in a communication environment, where m is typically equal to 1 or 8 bits. The price paid for this property is that the performance decreases with a factor t/m. In contrast with the OFB mode, a single bit error is propagated with a factor t.

For the m-bit CFB mode, a known plaintext and a chosen plaintext attack are equivalent: in both cases the cryptanalyst has no control over the input of the block cipher. If the cryptanalyst wants to control this input, like in a chosen plaintext attack on the ECB mode, a chosen ciphertext attack is required. In all cases the cryptanalyst can only observe m output bits. In OFB mode, the number of observable bits is also limited to m, but the most powerful attack is a known plaintext attack.

3 Three basic attacks

The simplest attack is clearly an *exhaustive search* for the key; it is a known plaintext attack. Exploitation of the complementation property requires a chosen ciphertext attack, or more precisely, a sufficient number of pairs of the form $(C_i, P_i), (\overline{C_i}, P_i')$. Even in 1976 there was a debate over the feasibility of an exhaustive search for a 56-bit DES key. It is clear that this attack is becoming more and more realistic. For more details the reader is referred to [16]. The exhaustive attack is only discussed as a reference for other attacks.

Two results will be presented. The first result is an expression for the number of plaintext/ciphertext pairs to determine the key uniquely.

Proposition 1 *Assume one has a block cipher with a k-bit key in m-bit CFB, where every ciphertext bit depends on every key bit and plaintext bit. If one knows M plaintext/ciphertext pairs, the expected number of keys that remains after an exhaustive search is equal to*

$$K_{\text{exp}} = 1 + \frac{2^k - 1}{2^{Mm}}. \tag{1}$$

From this proposition it follows that in order to determine the key uniquely M has to be slightly larger than k/m.

A second result is applicable to the DES with a reduced number of rounds. The DES has 16 rounds; the number of rounds for the reduced version of the DES will be denoted with N. Table 1 indicates how many key bits influence the ciphertext in the case of m-bit CFB with N rounds. It is clear that this depends on the selection of the bits. The standards specify that the leftmost m bits are selected. For the DES, this selection is influenced by IP^{-1}. In 1-bit CFB, the output bit is independent from the operations (and the subkey) in the last round, and for larger values of m the output bits are selected from different S-boxes. It will be shown in Sect. 5 and 6 that differential and linear attacks are very sensitive to these positions. It is remarkable that IP^{-1} has a cryptographic meaning in this context. IP and IP^{-1} were probably introduced to facilitate hardware implementations, and it is easily seen that in ECB and CBC mode they have no security implication (except for the case where the plaintext has a special structure [3]).

A second attack that is relevant is a *comparison attack* [14]: the cryptanalyst searches for t-bit matches between the ciphertext bits. If a match occurs, he knows that the output of the block cipher will be equal in both cases, and hence he knows the exor of two plaintext bits. Note that the position of these plaintext bits cannot be selected. Because of the birthday paradox, such a match will occur after about $2^{t/2+1}$ ciphertext bits. If $t = 64$, and the encryption speed is equal to 2 Mbit/s, the storage requirements are 1 Gigabyte, and it will take about 1.16 hour to find a single match. If one waits for 25 days, one can collect 512 Gigabyte, and one expects about 2^{19} matches. This attack can be thwarted by increasing the frequency of the key change. If more than 2^{42} bits are collected, even triple matches will occur.

A third attack is the *tabulation attack*, which depends only on the size of

Table 1. The number of key bits that influence the ciphertext in the case of the DES with N rounds in m-bit CFB.

	number of rounds N				
m	1	2	3	4	5
1	0	6	39	53	56
2	6	45	53	56	56
4	12	50	56	56	56
8	18	52	56	56	56
16	36	55	56	56	56

the input register (and not on the size of the key or the number of rounds). The cryptanalyst will use a huge amount of known plaintexts to build a table of the secret mapping f. After about $2^t \cdot \ln(2^t)$ encryptions of *arbitrary* plaintexts with the unknown key, the secret mapping is completely known. An important difference between this type of attack and the simple exhaustive key search attack is that in this case it is not possible to perform the computations in parallel.

4 A meet in the middle attack

One of the first attacks on the DES with a reduced number of rounds in ECB mode was the meet in the middle attack proposed by D. Chaum and J.-H. Evertse [6]. The attack is faster than exhaustive search for $N \leq 6$. The basic idea is to look for r data bits in a middle round that depend on a limited number s of key bits. First an exhaustive search is performed for these bits, and subsequently the remaining key bits are determined.

In the case of the CFB mode, the probability that a key can be eliminated is significantly smaller, as only a small part of the ciphertext is known. If $N = 3$ and $m = 1$, one can show that the optimal choice is $r = 4$ bits in the middle (namely bits 18, 19, 20, and 21 of the right half of the register in the second round). In this case the subkey has $s = 27$ bits. The probability that a bad subkey survives in one trial is not equal to $1/2^r$ as for the ECB mode, but $h/2^r$, where h is a constant that has to be determined with a computer program (yielding $h = 0.5$). If it is assumed that the probability of survival for different plaintext/ciphertext pairs is independent, one can determine the expected number of remaining keys if M pairs are known:

$$\tilde{K} = 1 + (2^s - 1)\left(1 - \frac{h}{2^r}\right)^M . \tag{2}$$

The expected number of encryptions is equal to $M + (2^r \cdot 2^s)/h \approx 2^{32}$ if $M \ll 2^{32}$. The search for the remaining key bits requires $M + (2^{k-s}\tilde{K})/(1 - 2^{-m})$ encryptions, where k denotes the total number of key bits that influences the output (in this case one finds in Table 1 that $k = 39$). If $M = 256$, the number

of operations in the second step is small compared to the first step. The total number of encryptions is a factor 2^7 smaller than for exhaustive search, but about 5 times more plaintext/ciphertext pairs are necessary.

For larger values of m, more ciphertext bits are known, but more key bits come into play as well. If $m = 8$, one can extend the previous approach in a straightforward way. One can however also try to reduce the number of required plaintext/ciphertext pairs by looking to bits 3 and 5 of the output (hence $r = 2$). These bits only depend on $s = 37$ key bits. The number of operations for the first and second step are equal to [6]:

$$M + \frac{2^s}{1 - 2^{-r}} \quad \text{and} \quad M + \frac{2^{n-s} + 2^{n-Mr}}{1 - 2^{r-m}}.$$

The first term corresponds to 2^{36} 3-round DES encryptions, and the second term is equal to 2^{32} if $M = 12$. This means that this is a factor 2^{20} faster than exhaustive search. A comparable improvement was obtained in [6] for $N = 4$ in ECB mode.

These results can be extended partially to 4 or 5 rounds, but the attack becomes more complicated: one cannot simply go backwards, because one has to guess some key bits and part of the ciphertext bits. Note that in ECB mode the improvement for 6 rounds is limited to a factor 4. As these attacks are known plaintext attacks, they are also applicable to m-bit OFB.

5 A differential attack

First it will be explained why a differential attack cannot be applied directly to the CFB mode. Subsequently the required modifications will be discussed, and an attack on 4, 5, and more rounds will be presented. Finally some extensions will be discussed, and several modifications to enhance the security of the DES in the CFB mode will be proposed.

5.1 Why does the conventional differential approach not work?

A differential attack in ECB mode is based on the following principle. The actual values of the input bits of the last round are known (because they are the right half of the ciphertext before IP^{-1}). The output exor of the last round is known with a certain probability (if the input pair is a right pair, the exor can be predicted). Subsequently the exor table and some additional information on the S-boxes allow to determine part of the subkey of the last round.

In the CFB mode only part of the output is known, as indicated in Table 2. The information on the output bits is restricted to exor information. It is clear that a differential attack requires that information on both input and output bits of a single S-box is available. This means that in 1-bit CFB this approach is restricted to the trivial case of 2 rounds. If 3 rounds or more are used, it follows from Table 2 that m has to be at least 3. In the following the differential attack will be described for 8-bit CFB. In this case most information is available

on S-box 3, namely 1 input bit and 2 output bits. A reduced exor table can be produced for the bits that are known by adding columns and rows of the original exor table. One could hope to determine information on key bit K_{44} that is exored with input bit a of $S3$. However, it is easy to show that in this situation the output bits will not suggest a particular value for this single key bit (i.e., all values in the reduced exor table are equal).

Table 2. Input bits of S-boxes that are known and output bits that are accessible in the case of m-bit CFB ($m \leq 8$); the 6 inputs bits of an S-box are denoted with a through f, the 4 outputs are denoted with α through δ, and the CFB bits are denoted with the digits 1 through 8.

S-box	known inputs	accessible outputs	S-box	known inputs	accessible outputs
1	$a = 7$		5	$a = 3$	$\alpha = 2$
2	$e = 1$		6	$e = 5$	
3	$a = 1$	$\alpha = 4$, $\beta = 6$	7	$a = 5$	$\alpha = 8$
4	$e = 3$		8	$e = 7$	

5.2 An extended differential attack

The differential attack can be extended to the CFB mode if one also uses the characteristic to predict the input exor of the last round (at least partially). This implies that the reduced exor table is obtained by adding only the columns of the original exor table.

A second property which can be exploited is that if an input bit exor of an S-box equals 0, the output exor reveals some information on the corresponding key bit. Denote the pair of intermediate ciphertext bits corresponding to bit a of $S3$ with (c, c'); the cryptanalyst knows both bits. The corresponding key bit is K_{44}. The unknown input bits to the S-box are $(c \oplus K_i, c' \oplus K_i)$. If $c = c'$, or $c \oplus c' = 0$, these input bits will be equal to $(0, 0)$ if $K_i = c = c'$ and will be equal to $(1, 1)$ otherwise. One can now divide the reduced exor table into two parts, and distinguish between these two cases. This will reveal some information on key bit K_{44}. If $c \neq c'$, no information can be obtained on K_{44}. Indeed, the input bits to the S-box will be different, and the key bit K_{44} only determines whether they are equal to $(0, 1)$ or $(1, 0)$. Table 3 gives part of the new exor table for $S3$. The input and output exors of S-box i are denoted with Si'_E and Si'_O respectively, x denotes an unknown bit, and the subscript $_x$ indicates hexadecimal notation.

Information on the key bits can be obtained as follows. The probability that the corresponding key bit K_{44} is equal to 1 can be determined from the observed

Table 3. Part of the reduced exor table for $S3$ where the entries are split based on the actual value of input bits a. Only the most useful input exors are listed.

input exor $S3'_E$	output exor $S3'_O$				quality H
	00xx	01xx	10xx	11xx	
01_x	2	18	18	26	0.719
with $0 \oplus 0$	2	14	10	6	
with $1 \oplus 1$	0	4	8	20	
02_x	2	10	26	26	0.688
with $0 \oplus 0$	0	8	16	8	
with $1 \oplus 1$	2	2	10	18	
04_x	4	8	24	28	0.688
with $0 \oplus 0$	4	8	8	12	
with $1 \oplus 1$	0	0	16	16	
10_x	4	24	12	24	0.625
with $0 \oplus 0$	0	8	8	16	
with $1 \oplus 1$	4	16	4	8	

output exor by applying Bayes' rule[1]. For a right pair, one obtains that :

$$q = \Pr(K_{44} = 1 \mid S3'_O = \alpha\beta xx) = \frac{\Pr(K_{44} = 1) \cdot \Pr(S3'_O = \alpha\beta xx \mid K_{44} = 1)}{\Pr(S3'_O = \alpha\beta xx)}. \tag{3}$$

It is clear that $\Pr(K_{44} = 1) = 1/2$. Both input and output exor are only known with a certain probability. The probability that the input exor is correct is slightly larger, and it is clear that both probabilities are not independent.

The next problem is how to combine the outcome of M pairs in an efficient way. Assume that it follows from pair j that the probability that $K_{44} = 1$ is equal to q^j. Then one defines

$$Q^j = \frac{q^j \cdot Q^{j-1}}{q^j \cdot Q^{j-1} + (1 - q^j) \cdot (1 - Q^{j-1})} \quad \text{for } j = 1, 2, \ldots, M \text{ and } Q^0 = 0.5. \tag{4}$$

It can be shown that this corresponds to a repeated application of Bayes' rule. If $Q^M > 0.5$, one decides that $K_{44} = 1$. In practice one expects that, after a sufficient number of experiments, Q^M will form a reliable estimate for K_{44} and will be close to 1 (or 0) with high probability.

An important issue is the choice of the characteristic in order to maximize $|q - 0.5|$. This depends on the probability p of the characteristic, the possibility of filtering, and on the difference between the $0 - 0$ and $1 - 1$ entries in the reduced exor table. Let q_i denote the value of q corresponding to a given input and output exor (the same numbering is used as for the values e_i in Table 4).

One can now prove this proposition (the proof will be given in the full paper):

[1] One obtains in fact the exor of the key bit with the corresponding input bit of $S3_E$.

Table 4. A reduced exor table.

input exor S'_E	output exor S'_O			
	00xx	01xx	10xx	11xx
	$e_1 + e_5$	$e_2 + e_6$	$e_3 + e_7$	$e_4 + e_8$
with $0 \oplus 0$	e_1	e_2	e_3	e_4
with $1 \oplus 1$	e_5	e_6	e_7	e_8

Proposition 2 *The number M' of right pairs required to predict a key bit with a probability of error equal to $1 - z$ satisfies the following inequality:*

$$M' \leq 64 \cdot \frac{\ln\left(\frac{1}{z} - 1\right)}{\ln(\rho)} \qquad \text{with } \rho = \prod_{i=1}^{4} \left(\frac{1}{q_i} - 1\right)^{e_i - e_{i+4}}.$$

Note that Proposition 2 can be extended to the case where certain output exors are filtered: one can simply modify the corresponding table entries such that $e_i = e_{i+4}$, yielding $q = 0.5$.

The optimization of the attack, or equivalently the minimization of M is not easy, since M also depends on the properties of the characteristic. A good heuristic measure for the differences in the exor table for a given input exor S'_E is the expression

$$H = \sum_{i=1}^{4} \Pr(S'_O \mid S'_E) \, \frac{\max(e_i, e_{i+4})}{e_i + e_{i+4}}.$$

Here i indexes the 4 columns corresponding to the 4 possible output exors S'_O. This measure is indicated in Table 3.

5.3 An attack on 4 rounds

It follows from the previous section that the value of $S3'_E = 01_x$ in the last round is optimal. The input exor to the first round is equal to $(40\,08\,00\,00_x, 04\,00\,00\,00_x)$. Then the characteristic has a probability of $1/4$ in the first round. In the third round, it is sufficient that the input exor to $S3$ is correct. If the pairs with output exor $00xx$ for $S3$ are filtered, only a fraction of $\frac{2}{64}$ of the right pairs is lost. From this it follows that the fraction $\tilde{p}$ of right pairs after filtering is equal to

$$\frac{\frac{3}{16} \cdot \frac{62}{64}}{\frac{3}{16} \cdot \frac{62}{64} + \frac{12}{16} \cdot \frac{3}{8}} = 0.392.$$

One obtains then with (3) the following equation for q:

$$q = \frac{1}{2} \cdot \frac{\tilde{p} \cdot \frac{14}{30} + (1 - \tilde{p}) \cdot \frac{1}{3}}{\tilde{p} \cdot \frac{18}{62} + (1 - \tilde{p}) \cdot \frac{1}{3}}. \tag{5}$$

This assumes that the wrong pairs yield a uniform distribution of output exors,

which has been confirmed by computer experiments. For $S3'_E = 01_x$ and $\tilde{p} = 0.39$ one obtains for $q = 0.609$, 0.527, and 0.383 for $S3'_O = 01xx$, $10xx$, and $11xx$ respectively. For an error probability of 5% (or $z = 0.95$), Proposition 2 predicts that $M' = 16.6$ and $M = M'/p = 89$, which has been confirmed by computer simulations.

If $m = 8$, a differential attack allows to determine 3 key bits (namely one bit corresponding to $S3$, $S5$, and $S7$). The details will only be discussed for a larger number of rounds.

5.4 An attack on 5 rounds

In order to develop an attack that is extendible to more rounds, an iterative characteristic will be used; this characteristic is probably not optimal for the 5 round case. For derivation of the key bit corresponding to $S3$, an input exor of 01_x is again the best choice. This implies that in the one but last round $S2$ has to receive a non-zero input exor. For the iterative characteristic ϕ [3] (input exor of left halve equals $1B\,60\,00\,00_x$), the probability in this round is equal to $\frac{55}{128}$, while for ψ (input exor of left halve equals $19\,60\,00\,00_x$), this probability is equal to $\frac{33}{128}$. This implies that ϕ is preferable (ψ might be used in a quartet structure).

The pairs for which the output exors of bit 1 or 7 are not equal to zero will be filtered; the same holds for the pairs for which the output exor of $S3$ is equal to $00xx$. It is assumed that pairs that do not follow the characteristic in the second round give a uniformly distributed output. For pairs that do not follow the characteristic in round 4, one can filter all those that do not follow the characteristic in $S2$, and $\frac{18}{64}$ of the pairs that do not follow the characteristic in $S1$. This yields the following fraction of right pairs among the filtered ones:

$$\tilde{p} = \frac{\frac{1}{234} \cdot \frac{55}{128} \cdot \frac{62}{64}}{\frac{1}{234} \cdot \frac{55}{128} \cdot \frac{62}{64} + \left(1 - \frac{1}{234}\right) \cdot \frac{3}{16} + \frac{1}{234} \cdot \frac{25}{128} \cdot \frac{46}{64}} = 9.40 \cdot 10^{-3}.$$

For an error probability of 5% (or $z = 0.95$), Proposition 2 predicts that 370 000 pairs are sufficient to obtain a key bit (only 1 characteristic has been used). Computer simulations show that the actual number of pairs is even smaller.

For S-boxes 6 and 7, a similar strategy can be followed. The best iterative characteristic for both S-boxes has input exor $00\,00\,1D\,40_x$ for the left halve. In the one but last round this characteristic has probability $\frac{7}{16}$ for $S5$ and $\frac{63}{256}$ for $S7$ to yield an input exor of 04_x respectively 01_x. The fraction of right pairs after filtering is equal to $5.92 \cdot 10^{-3}$ and $3.33 \cdot 10^{-3}$, from which one can estimate that the number of required pairs is equal to 12 and 8.4 million respectively. In both cases one can eliminate those pairs for which the exor of bits 3 and 5 is not equal to 0.

5.5 Six rounds and more

The same characteristics can be used as in the previous section. In order to optimize that attack one can use the ideas of [5] to get around the first round.

The problem here is that the filtering of wrong pairs will be less effective. The estimated number of pairs to find 1 and 3 key bits for 8-bit CFB are indicated in Table 5.

The attack for $N = 7$ (without the optimization to gain an additional round) was implemented as a distributed application on a heterogeneous, non-dedicated farm of 30 DEC workstations, using the PVM (Parallel Virtual Machine) software [1] for interprocess communication. The program was generated and run from the HeNCE (Heterogeneous Network Computer Environment) software [2]. The correct key bits were retrieved from $2^{35.2}$ pairs using a quartet structure; the attack took about 40 hours.

Table 5. Probability of the characteristic and number of pairs to find 1 and 3 key bits in 8-bit CFB.

# rounds N	probability p		# pairs	
	1 bit	3 bits	1 bit	3 bits
6	$9.40 \cdot 10^{-3}$	$3.33 \cdot 10^{-3}$	$2^{18.5}$	$2^{23.0}$
8	$4.05 \cdot 10^{-5}$	$1.15 \cdot 10^{-5}$	$2^{34.2}$	$2^{39.4}$
10	$1.73 \cdot 10^{-7}$	$3.93 \cdot 10^{-8}$	$2^{50.0}$	$2^{55.8}$
16	$1.35 \cdot 10^{-14}$	$1.57 \cdot 10^{-15}$	$2^{97.2}$	$2^{104.7}$

5.6 Extensions

If the number m of feedback bits increases, more key bits can be found (5 if $m \geq 15$). If $m \geq 18$ three output bits of a single S-box are known, which implies that a smaller reduction has to be applied to the exor tables, resulting in a reduction of the required number of chosen ciphertext pairs. If $m \geq 15$, two bits of $S8$ in the last round are known, and the input to the one but last round can be estimated. Only if $m \geq 28$ one obtains in this way information on both input and output of a single S-box, which allows to determine key bits in this round.

This differential attack would be impossible without IP^{-1}. In the absence of IP^{-1} only information on the output of S-boxes of the last round would be available. The security of the DES in 1-bit CFB could be improved if the bit is selected from the left half of the ciphertext. Selecting all the CFB bits from the left half of the ciphertext thwarts the proposed differential attacks for small values of m. Another way to strengthen the DES in the CFB mode against differential attacks could be a redesign of the S-boxes in the last round in order to decrease the difference between the $0-0$ and $1-1$ entries in the reduced exor table. Finally a completely different structure for the computation of the CFB bits from the inputs to the last round could be used.

6 Linear cryptanalysis

This section will summarize the most important results of a linear attack on the DES reduced to 8 rounds in the CFB mode. Additional results will be given in the full paper. The following notation will be used:

$A[i]$ = the i-th bit of A, where the most significant bit has number 1,
$A[i,j,k] = A[i] \oplus A[j] \oplus A[k]$,
$F_i(X,K)$ = the i-th round substitution.

In linear cryptanalysis of the DES [13], one tries to approximate the S-boxes by equations of the form $P[i_1,\ldots,i_p] \oplus C[j_1,\ldots,j_c] = K[l_1,\ldots,l_k]$, where $i_1,\ldots,i_p$, $j_1,\ldots,j_c$, $l_1,\ldots,l_k$ are fixed. This equation holds with probability $p \neq 0.5$. The equations of the different rounds can be combined into a relation that holds for the entire algorithm.

Unlike the differential attack, the published linear attack can be applied directly to the CFB mode. The only limitation is that there are less bits visible from the ciphertext. This reduces the number of useful linear relations. We found the following relations:

$$C[48,56] \oplus P[16,24,42] \oplus F_1(P,K)[16,24] \oplus K[2,3,11,18,35] = 0\,,$$
$$C[16,24] \oplus P[11,48,56] \oplus F_1(P,K)[11] \oplus K[17,18,19,51,52,59,60] = 0\,.$$

They hold with $p = 0.5 + 1.5 \times 2^{-15}$ and $p = 0.5 + 2^{-19}$ respectively. The output bits involved are known if $m \geq 6$. Each relation can be used to determine 7 key bits. For an accuracy of 96 %, 1.78×2^{31} texts are necessary for the first equation and 1.78×2^{39} for the second equation.

7 Conclusions and open problems

Several attacks on the DES in the ECB mode can be extended to the m-bit CFB mode. They are only faster than exhaustive key search if the number of rounds is reduced. A meet in the middle attack on the DES with 3 rounds yields an improvement with a factor 2^{20} over exhaustive search in case of 8-bit CFB or OFB mode. A modified differential attack has been presented that works in m-bit CFB with $m \geq 3$. The most important modifications are that the exor of the input to the S-boxes of the last round are determined based on the characteristic and that the exor table is reduced. Moreover additional information on actual input values is taken into account. The attack is 8 times faster than exhaustive search for 9 rounds or less and 2 times faster for 10 rounds. A linear attack for $m \geq 6$ has been discussed. When the number of rounds of the DES is reduced to 8, 2^{31} known plaintexts are required to determine 7 key bits.

These attacks are completely theoretical in the sense that they pose no threat for the DES with 16 rounds in the m-bit CFB mode (for 'small' m). However, they are of some interest because for small values of m the m-bit CFB mode is very slow: this is an argument to reduce the number of rounds in order to obtain an acceptable performance. An interesting result is that the DES with 8 rounds

in 8-bit CFB mode is less secure against these attacks than the DES with 16 rounds in ECB mode, while the first scheme is 4 times slower. It has been shown that in the CFB mode (and the OFB mode) IP^{-1} has a cryptographic meaning.

It would be interesting to extend all these attacks to other iterated block ciphers like IDEA and LOKI91. One of the important differences will be that the known bits are concentrated in a few S-boxes.

References

1. A. Beguelin, J. J. Dongarra, G. A. Geist, R. Mancheck, and V. Sunderam, *"A users' guide to PVM parallel virtual machine"*, Technical report ORNL/TM-11826, Oak Ridge National Laboratory, July 1991.
2. A. Beguelin, J. J. Dongarra, R. Manchek, K. Moore, R. Wade, J. Plank, and V. Sunderam, *"HeNCE: a user's guide"*, Version 1.2, December 1992.
3. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, Vol. 4, No. 1, 1991, pp. 3–72.
4. E. Biham and A. Shamir, "Differential cryptanalysis of Feal and N-hash," *Advances in Cryptology, Proc. Eurocrypt'91, LNCS 547*, D.W. Davies, Ed., Springer-Verlag, 1991, pp. 1–16.
5. E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," *Technion Technical Report # 708*, December 1991.
6. D. Chaum and J.-H. Evertse, "Cryptanalysis of DES with a reduced number of rounds," *Advances in Cryptology, Proc. Crypto'85, LNCS 218*, H.C. Williams, Ed., Springer-Verlag, 1985, pp. 192–211.
7. D. Davies, "Investigation of a potential weakness in the DES algorithm," July 1987 (revised January 1990), preprint.
8. FIPS 46, *"Data Encryption Standard,"* Federal Information Processing Standard, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.
9. FIPS 81, *"DES Modes of Operation,"* Federal Information Processing Standard, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., December 1980.
10. M. Hellman, R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohlig and P. Schweitzer, *"Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard,"* Information Systems Lab., Dept. of Electrical Eng., Stanford Univ., 1976.
11. ISO/IEC 10116, *"Information technology - Security techniques - Modes of operation of an n-bit block cipher algorithm,"* 1991.
12. R.R. Jueneman, "Analysis of certain aspects of Output Feedback Mode," *Advances in Cryptology, Proc. Crypto'82*, D. Chaum, R.L. Rivest, and A.T. Sherman, Eds., Plenum Press, New York, 1983, pp. 99–127.
13. M. Matsui, "Linear cryptanalysis method for DES cipher," *Advances in Cryptology, Proc. Eurocrypt'93, LNCS*, Springer-Verlag, to appear.
14. U.M. Maurer, "New approaches to the design of self-synchronizing stream ciphers," *Advances in Cryptology, Proc. Eurocrypt'91, LNCS 547*, D.W. Davies, Ed., Springer-Verlag, 1991, pp. 458–471.
15. K. Ohta and M. Matsui, "Differential attack on message authentication codes," *This Volume.*
16. M. Wiener, "Efficient DES key search," *This Volume.*