with a high probability $P_1(N)$.

Our goal is to calculate the success rate of our attack $P_1(N)$. The density function of I_K is:

$$f_K(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-m)^2}{2\sigma^2}} = \frac{2^4}{\sqrt{2\pi N}} \exp\left\{-\frac{1}{2}\left(\frac{2^4}{\sqrt{N}}x - \frac{S\sqrt{N}}{2^4 E(D_n)}\right)^2\right\}. \qquad (13)$$

The density function of the other indicators are:

$$f_{R_i}(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}} = \frac{2^4}{\sqrt{2\pi N}} \exp\left\{-\frac{2^3 x^2}{N}\right\} = f_R(x). \qquad (14)$$

Then:

$$P_1(N) = P(|I_K| > \max_{i=1\ldots4095} |I_i|) = \int_0^{+\infty} f_K(x) \cdot P_R(|r| < x)^{4095} dx \qquad (15)$$

where

$$P_R(|r| < x) = \int_{-x}^{x} f_R(y) dy. \qquad (16)$$

The probability that $|I_K|$ is one of the n highest indicators (rather than the maximal one) is:

$$P_n(N) = \int_0^{+\infty} f_K(x) \sum_{i=0}^{n-1} \binom{4095}{i} P_R(|r| < x)^{4095-i} (1 - P_R(|r| < x))^i dx. \qquad (17)$$

Table 2 shows $P_n(N)$ for $n = 2^k, k = 0, \ldots, 7$ for $N = 2^{40}, \ldots, 2^{54}$ (note that in the table $m = 13 - k$). Figure 1 shows $P_n(N)$ for $n = 1, 2, 8, 32, 128$.

6 Appendix

In this appendix we present the details of the calculations of the success rate of our attack versus its data complexity. These calculations were used to generate Table 2 and Figure 1.

The data analysis phase of our attack calculates 4096 distributions – one for each possible value of the 12 key bits. 4095 distributions correspond to the incorrect values of the key bits and are assumed to be multinomial with $P_{x,y} = 1/256$. One distribution corresponds to the actual values of the 12 key bits, and is thus distributed as D_7. We calculate the indicator I (equation (3)) for each of the 4096 distributions. Given sufficiently many known plaintexts, the absolute value of the indicator corresponding to the right value of the key should be the largest.

We start with the calculation of the mean and the standard deviation of the indicators of the right distribution I_K, and of the indicators of the other multinomial distributions $I_{R_1} \ldots I_{R_{4095}}$. We assume that all the indicators have normal distributions. We denote the measure of non-uniformity of D_n by:

$$S = \sqrt{\sum_{x,y} d_n(x,y)^2}. \tag{10}$$

The empirical distribution $D'_K(x,y,p_n)$ is multinomial with the probabilities $P_{x,y} = \frac{D_n(x,y,p_n)}{2^8 \cdot E(D_n)}$. Thus the mean of I_K is:

$$\begin{aligned} E(I_K) &= E\left(\sum_{x,y}\left(D'_K(x,y,p_n) - \frac{N}{2^8}\right)\cdot\frac{d_n(x,y)}{S}\right) \\ &= \sum_{x,y}\frac{d_n(x,y)}{S}\left(E(D'_K(x,y,p_n)) - \frac{N}{2^8}\right) \\ &= \frac{N}{2^8}\sum_{x,y}\frac{d_n(x,y)}{S}\left(\frac{D_n(x,y,p_n)}{E(D_n)} - 1\right) = (-1)^{p_n}\frac{N\cdot S}{2^8\cdot E(D_n)}. \end{aligned}$$

The variance of I_K is (we assume independence of $D'(x,y,p_n)$ for the different x,y):

$$\begin{aligned} Var(I_K) &\approx \sum_{x,y}\left(\frac{d_n(x,y)}{S}\right)^2 Var(D'_K(x,y,p_n)) \\ &\approx \sum_{x,y}\left(\frac{d_n(x,y)}{S}\right)^2 \frac{N\cdot D_n(x,y,p_n)}{E(D_n)\cdot 2^8} \approx \frac{N}{2^8}. \end{aligned}$$

The other multinomial distributions satisfy: $E(D'_{R_i}(x,y,p_n)) = N/2^8$, $Var(D'_{R_i}(x,y,p_n)) \approx N/2^8$ and thus:

$$E(I_{R_i}) = 0 \quad , \quad Var(I_{R_i}) \approx \frac{N}{2^8} \quad i = 1\ldots 4095. \tag{11}$$

We have shown that I_K and I_{R_i} have approximately the same standard deviation which grows as a square root of the number of known plaintexts N. The mean of I_K grows linearly with N and the mean of I_{R_i} is zero. Then for sufficiently large N:

$$|I_K| > \max_{i=1\ldots 4095} |I_{R_i}| \tag{12}$$

($k \in \{0 \ldots 3\}$). For DES S-boxes Davies received the formula:

$$D_1(x,y,0) = 4 + (D(x,0) - D(x,1)) \cdot (E(y,0) - E(y,2)) \tag{6}$$

(this formula holds for any S-boxes with the differential property $0abcd0_b \not\rightarrow 0$). Thus, any pair of DES-like S-boxes must have a uniform joint distributions if and only if

$$D(x,0) = D(x,1) \quad \text{or} \quad E(y,0) = E(y,2) \tag{7}$$

The following two additional differential properties lead to uniform joint distribution:

$$01xy11_b \not\rightarrow 0 \quad , \quad 00xy11_b \not\rightarrow 0, \tag{8}$$

since they cause $D(x,0) = D(x,1)$. Alternatively, the following two additional differential properties lead to uniform joint distribution:

$$11xy00_b \not\rightarrow 0 \quad , \quad 11xy10_b \not\rightarrow 0, \tag{9}$$

since they cause $E(y,0) = E(y,2)$. Note that $11xy00_b \not\rightarrow 0$ is already a design principle of DES. The s^3DES S-boxes [4] were designed with the additional criteria $11xy10_b \not\rightarrow 0$, and are thus immune to Davies' attack and to the improved attack.

5 Summary

We improved Davies' attack on DES. We describe a tradeoff between the number of plaintexts, the success rate and the time of analysis. The best tradeoff requires 2^{50} known plaintexts and 2^{50} steps (2^{49} in average) of analysis and has about 51% success rate. An alternative attack is capable of finding 24 bits of the key with 2^{52} known plaintexts with 53% success rate. The data analysis phase of this attack is independent of the number of rounds and runs only several minutes on a SPARC. We also suggest how to make S-boxes immune to these attacks.

References

[1] Eli Biham, Adi Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag,1993.

[2] D.W. Davies, *Investigation of a Potential Weakness in the DES Algorithm*, private communications, 1987.

[3] D. Davies, S. Murphy, *Pairs and Triplets of DES S-boxes*, to appear in the Journal of Cryptology.

[4] Kwangjo Kim, Sangjun Park, Sangjin Lee, *How to Strengthen DES Against Differential Attacks*, private communications, 1994.

[5] Mitsuru Matsui, *Linear Cryptanalysis Method for DES Cipher*, Abstracts of EUROCRYPT'93, pp. W112-W123, May 1993.

[6] National Bureau of Standards, *Data Encryption Standard*, Federal Information Processing Standards Publication 46, January 1977.

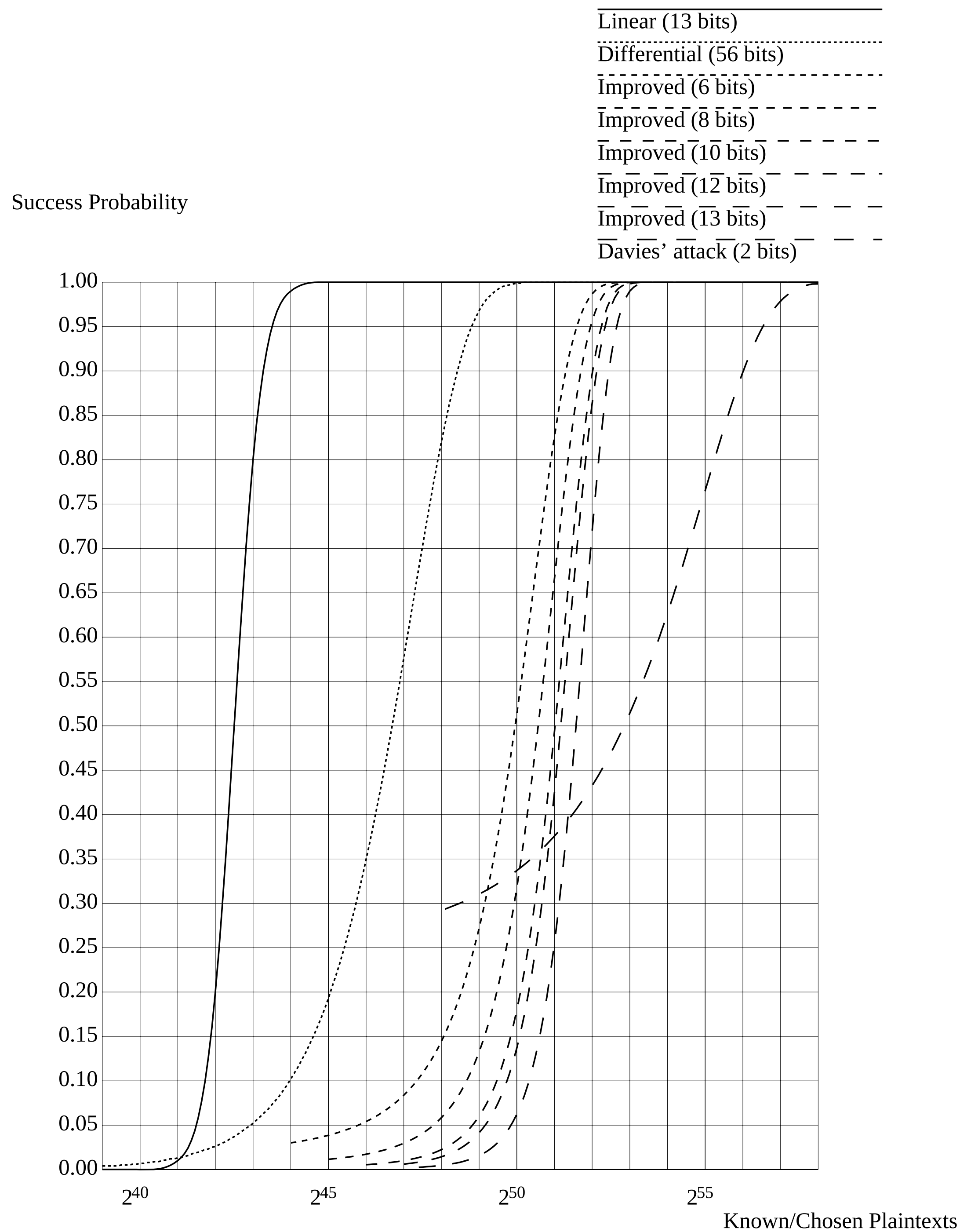

Figure 1: Comparison of the success probability of differential cryptanalysis, linear cryptanalysis, Davies' attack, and the improved attack.

the distribution generated with the particular value of the key is increased by the value of the corresponding counter (α, β). We get 2^{12} distributions which we analyze (as described above) to find the right value of the key. We receive 12 key bits of the subkey K_{16} of the last round plus one parity bit of the key. The cost of the data analysis phase is about $2^{12} \cdot 2^{10} \cdot \frac{1}{64} = 2^{16}$ DES encryptions, plus 2^{30} counter increments. It runs only several minutes on a SPARC station.

This attack is repeated twice, once for the even rounds and once for the odd rounds (with the only difference that one round encryption of the first round is applied, guessing 2^{12} bits of subkey K_1). The data collection phase counts simultaneously into the two counting arrays, and the data analysis phase is applied for each array. Among the 24 actual key bits found during the attack two bits are common to both rounds and are used to discard some wrong keys that are left after the data analysis phase. Finally we obtain 24 bits of the key. The other 32 key bits can be found by exhaustive search.

Figure 1 compares the known attacks on DES. It shows the success rate of each attack versus the number of known/chosen plaintexts it requires. Our attack is represented by the five curves corresponding to the different numbers of effective bits found. We have cut the success curves when they reach the probability of a random guess. These cut points differ for each curve, since the number of key bits is different. There is a tradeoff between the number of bits the attack finds, and the data complexity of the attack for particular success rate. We found that the best tradeoff is reached when the attack finds six effective bits with 2^{50} known plaintexts and success rate 51.3% and the rest 50 key bits are found by exhaustive search.

We wrote a program that implements our improved attack and finds 13 bits of the key of reduced round variants of DES. In tests we made, this program found the key with the success rate expected by our probabilistic calculations (from which the Figure 1 was generated).

4 Discussion

Davies estimates that the correlations of the outputs of the pairs of the S-boxes were reduced in DES. He claims that much stronger reductions are possible. In this section we suggest additional design principles to immune DES-like S-boxes against Davies' attacks.

S-boxes immune to Davies' attack must have uniform joint distribution:

$$D_1(x, y, 0) = D_1(x, y, 1) = E(D_1). \tag{5}$$

In order to make DES-like S-boxes immune, either the differential property $abcd00_b \not\rightarrow 0$ or the differential property $00efgh_b \not\rightarrow 0$ suffices (we denote binary numbers by the subscript b). In DES all the patterns of the described type (except for $00xy01_b$) are impossible, or were intentionally lowered by the designers to prevent differential cryptanalysis.

Following Davies we define $D(x, k)$ to be the distribution of x and $E(y, k)$ be the distribution of y, when the value of the two common bits is constrained to be k

Complexity	Success rate for m key bits found (%)							
	13	12	11	10	9	8	7	6
2^{40}	0.0	0.0	0.1	0.1	0.2	0.5	0.9	1.9
2^{41}	0.0	0.0	0.1	0.1	0.3	0.5	1.0	2.0
2^{42}	0.0	0.0	0.1	0.2	0.3	0.6	1.1	2.2
2^{43}	0.0	0.0	0.1	0.2	0.4	0.7	1.3	2.5
2^{44}	0.0	0.1	0.1	0.2	0.4	0.9	1.6	3.0
2^{45}	0.1	0.1	0.2	0.3	0.6	1.1	2.1	3.9
2^{46}	0.1	0.2	0.3	0.5	1.0	1.7	3.1	5.4
2^{47}	0.2	0.3	0.6	1.0	1.7	3.0	5.0	8.4
2^{48}	0.5	0.8	1.4	2.2	3.6	5.9	9.3	14.5
2^{49}	1.5	2.5	3.9	6.0	9.0	13.2	19.2	27.2
2^{50}	6.2	9.1	13.0	17.9	24.1	31.7	40.9	51.3
2^{51}	25.5	32.9	40.9	49.3	57.9	66.6	75.0	82.6
2^{52}	71.9	79.2	85.0	89.6	93.0	95.6	97.5	98.7
2^{53}	99.0	99.5	99.8	99.9	99.9	100.0	100.0	100.0
2^{54}	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

Table 2: The complexity and the success rate of the improved Davies' attack for different number of key bits found.

decryption is performed, the complexity of this attack is more than $2^{49.74} \cdot 2^{12}/64 \approx 2^{56}$. Later we will describe an efficient algorithm to solve this problem. Once we get 4096 distributions we use a statistical technique (see the Appendix) to distinguish the right distribution from the 4095 random distributions. Since we should distinguish the right distribution, we require about four times the number of plaintexts than if the distribution is known. We identify the actual distribution and the 13 bits of the key with 0.73 probability of success. The mean of the indicator should be greater than four times the standard deviation. With probability 0.53 we find 24 key bits by applying the method twice. There is a tradeoff between the number of bits that the attack finds and the number of known plaintexts it requires, since we can consider the n maximal indicators rather than only one indicator. This is equivalent to finding of the $m = 13 - \log_2 n$ bits of the key. Table 2 summarizes this tradeoff.

In the efficient algorithm the attack incorporates a data collection phase and a data analysis phase. Only 10 ciphertext bits are required for the partial decryption. The data collection phase counts the number of occurrences of each possible value of the eight distribution bits (which are received as XOR of plaintext and ciphertext bits) together with these ten ciphertext bits (entering the pair of S-boxes in the last round), and outputs an array of the 2^{18} counters. Note that the data collection phase only increments one counter for each plaintext that it encrypts.

The data analysis phase starts by calculating the 2^{12} distributions. For each possible value of the 12 key bits and 10 ciphertext bits (α) entering the pair of S-boxes, the output of the pair of S-boxes is calculated. The result (eight bits) is XORed to each possible 8-bit value (β) and the corresponding entry ($f_K(\alpha) \oplus \beta$) in

Rounds	Distribution	S1/2	S2/3	S3/4	S4/5	S5/6	S6/7	S7/8	S8/1
2,3	D_1	$2^{6.4}$	$2^{6.1}$	$2^{8.8}$	$2^{6.7}$	$2^{7.4}$	$2^{7.1}$	$2^{6.2}$	$2^{7.7}$
4,5	D_2	$2^{16.3}$	$2^{15.7}$	$2^{20.4}$	$2^{16.7}$	$2^{17.6}$	$2^{16.8}$	$2^{14.5}$	$2^{18.5}$
6,7	D_3	$2^{25.2}$	$2^{24.9}$	$2^{31.4}$	$2^{26.0}$	$2^{27.0}$	$2^{25.4}$	$2^{21.8}$	$2^{28.6}$
8,9	D_4	$2^{33.6}$	$2^{33.9}$	$2^{42.3}$	$2^{35.1}$	$2^{36.1}$	$2^{33.7}$	$2^{28.9}$	$2^{38.5}$
10,11	D_5	$2^{41.8}$	$2^{42.8}$	$2^{53.1}$	$2^{44.1}$	$2^{45.0}$	$2^{41.8}$	$2^{35.9}$	$2^{48.2}$
12,13	D_6	$2^{49.9}$	$2^{51.6}$	$2^{64.0}$	$2^{52.9}$	$2^{53.9}$	$2^{49.9}$	$2^{42.8}$	$2^{57.9}$
14,15	D_7	$2^{57.9}$	$2^{60.5}$	$2^{74.8}$	$2^{61.8}$	$2^{62.8}$	$2^{57.9}$	$2^{49.7}$	$2^{67.6}$
16	D_8	$2^{66.0}$	$2^{69.3}$	$2^{85.6}$	$2^{70.6}$	$2^{71.6}$	$2^{66.0}$	$2^{56.6}$	$2^{77.3}$

Table 1: The complexities of Davies' attack.

3 The Improved Attack

In this section we present an improved version of Davies' attack which breaks the full 16-round DES faster than exhaustive search.

We observed that the distribution D_7 can be used instead of D_8 (a similar observation was made independently by H. Gilbert and mentioned in [3]). D_7 is much less uniform than D_8 and thus a smaller number of known plaintexts is required. In order to use D_7 we should peel up one round of DES — we do that by guessing all the possible values of the key bits of the pair of S-boxes, and calculating the distribution that results for each value of the key bits entering the pair of S-boxes in the last round after XORing the plaintext and ciphertext bits with the output of the S-boxes. We receive 2^{12} distributions, of which the one which corresponds to the right value of the 12 key bits should be similar to D_7. The analysis of this distribution is similar to the original analysis of the 15-round variant. Still we should identify the right distribution out of the 2^{12} distributions. We select the distribution which has the highest absolute value of the indicator I. This analysis recovers both a parity bit of the key and additional 12 actual key bits entering the pair of adjacent S-boxes. We study only the distribution of the S-box pair $S7/8$ which is the least uniform (see Table 1). All other pairs of adjacent S-boxes result with complexity higher than exhaustive search.

Davies' attack on the 15-round DES uses D_7 and finds one parity bit of the key in $2^{49.74}$ steps. Our improved attack adds one round to this attack and can find 24 bits of the key of the 16-round DES by applying the analysis twice: both to the even rounds (with the additional last round) and to the odd rounds (with the additional first round) (the 24 bits are two parity bits of subsets of the key bits plus $12+12-2=22$ actual key bits: two key bits are common to the first and the last rounds).

We calculate the output of the pair of S-boxes in the last round by performing one-round partial decryption of the pair of S-boxes. The value of the 12 bits of the key entering these S-boxes is unknown. We try all the 2^{12} possibilities, doing the counting for 4096 different distributions (each distribution has 2^8 counters) — a distribution for each possible value of the 12 key bits. Since for each ciphertext about 1/64 of a DES different key bits before they serve as inputs to the S-boxes. As a result, the output of adjacent pairs (and triplets, etc.) of S-boxes has non-uniform distribution. Davies found that this distribution depends only on the parity of the four key bits which are mixed with the shared data bits. We denote this parity by p_1 and the mean value of the various values of the distribution by $E(D_1)$. The distribution of the output of a pair of S-boxes can be written as:

$$D_1(x, y, p_1) = E(D_1) + (-1)^{p_1} \cdot d_1(x, y), \tag{1}$$

where x is the output of the left S-box of the pair and y is the output of the right S-box. The XOR of the outputs of the F-functions in the eight even (odd) rounds can be calculated by XORing of the right (left) half of the plaintext with the left (right) half of the ciphertext and applying the inverse permutation P^{-1}. Davies found that the n-fold XOR distributions of the outputs of adjacent pairs of S-boxes have a form similar to equation (1):

$$D_n(x, y, p_n) = E(D_n) + (-1)^{p_n} \cdot d_n(x, y), \tag{2}$$

where p_n is the parity of the $4n$ subkey bits which are mixed with the data bits in the n even (odd) rounds, and $E(D_n) = 2^{10n-8}$ is the mean of the distribution. $D_n(x, y, p_n)$ can be calculated by the recurrent formulae:

$$\begin{aligned} D_n(x, y, 0) &= \sum_{\substack{x_1 \oplus x_2 = x \\ y_1 \oplus y_2 = y}} D_{n-1}(x_1, y_1, 0) \cdot D_1(x_2, y_2, 0) \quad n = 2 \ldots 8, \\ D_n(x, y, 1) &= 2E(D_n) - D_n(x, y, 0). \end{aligned}$$

Davies suggested to use the indicator function:

$$I = \sum_{x,y} (D'(x, y, p_n) - E(D_n)) \cdot \frac{d_n(x, y)}{\sqrt{\sum_{x,y} d_n(x, y)^2}}, \tag{3}$$

whose sign observes the parity bit of the key: if $I > 0$ the parity is zero and if $I < 0$ the parity is one. $D'(x, y, p_n)$ is the empirical distribution received from the data collection phase of Davies' attack. Given sufficiently many known plaintexts, the sign in the D_n distribution can be identified, along with one parity bit of the key.

Davies estimated the required amount of data for his attack as:

$$N = \frac{2^{10} \cdot E(D_n)^2}{\sum_{x,y} d_n(x, y)^2} = \frac{2^{20n-6}}{\sum_{x,y} d_n(x, y)^2}. \tag{4}$$

With this amount of data 97% success rate is achieved. Table 1 summarizes the complexities of Davies attack on different S-box pairs and different numbers of rounds (to find two bits for the even rounds, and one bit for the odd rounds). The best pair of S-boxes $S7/8$ requires $2^{56.6}$ known plaintexts [2, 3] to find two parity bits. Therefore, Davies' attack is not practical and is only of theoretical interest.

An Improvement of Davies' Attack on DES

Eli Biham* Alex Biryukov†

Abstract

In this paper we improve Davies' attack [2] on DES to become capable of breaking the full 16-round DES faster than the exhaustive search. Our attack requires 2^{50} complexity of the data collection and 2^{50} the complexity of analysis. An alternative approach finds 24 key bits of DES with 2^{52} known plaintexts and the data analysis requires only several minutes on a SPARC. Therefore, this is the third successful attack on DES, faster than brute force, after differential cryptanalysis [1] and linear cryptanalysis [5]. We also suggest criteria which make the S-boxes immune to this attack.

1 Introduction

Davies [2] described a potential attack on DES[6] that is based on the non-uniformity of the distribution of the outputs of pairs of adjacent S-boxes. Theoretically one can gain up to 16 parity bits of the key with this attack. However the direct application of Davies' attack is impractical since the resulting distribution is too uniform. The variant based on the best pair $S7/S8$ requires $2^{56.6}$ known plaintexts and finds two parity bits of the key with 95.5% success rate.

In this paper we improve Davies' attack to break the full 16-round DES faster than brute force. We describe a tradeoff between the number of plaintexts, the success rate and the time of analysis. The best tradeoff requires 2^{50} known plaintexts and 2^{50} steps (2^{49} in average) of analysis. An alternative attack finds 24 key bits for which it requires 2^{52} known plaintexts. The data analysis phase is independent of the number of rounds and runs only several minutes on a SPARC. We also suggest how to make S-boxes immune to this attack.

In all further discussions we ignore the existence of the initial permutation IP and the final permutation IP^{-1}, since they have no influence on the properties of DES that are studied in this paper.

2 Davies' attack

The expansion operation of DES duplicates data bits to enter into two adjacent S-boxes. Each pair of adjacent S-boxes share two data bits. These bits are XORed with

*Computer Science Department, Technion - Israel Institute of Technology, Haifa 32000, Israel.
†Applied Mathematics Department, Technion - Israel Institute of Technology, Haifa 32000, Israel.