J. Cryptology (1997) 10: 195–205

Journal of
CRYPTOLOGY

An Improvement of Davies' Attack on DES

Eli Biham
Computer Science Department, Technion—Israel Institute of Technology, Haifa 32000, Israel

Alex Biryukov
Applied Mathematics Department, Technion—Israel Institute of Technology, Haifa 32000, Israel

Communicated by Don Coppersmith

Received 24 April 1995 and revised 28 February 1996

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} known plaintexts and 2^{50} complexity of analysis. If independent subkeys are used, a variant of this attack can find 26 bits out of the 768 key bits using 2^{52} known plaintexts. All the 768 bits of the subkeys can be found using 2^{60} known plaintexts. The data analysis requires only several minutes on a SPARC workstation. 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.

Key words. Data Encryption Standard (DES), Cryptanalysis.

1. Introduction

In 1987, Davies [2] described a potential attack on DES [6] that is based on the nonuniform distribution of outputs from adjacent S-boxes, which theoretically allows a cryptanalyst to determine 16 parity bits of the key. However, the direct application of Davies' attack is impractical since the resulting distribution is too close to uniform. The variant based on the best pair $S7/S8$ requires about $2^{56.6}$ known plaintexts and finds two parity bits of the key with a 95.5% success rate (each bit with a 97% 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. If independent subkeys are used, a variant of this attack can find 26 bits out of the 768 key bits using 2^{52} known plaintexts. All the 768 bits of the subkey can be found using 2^{60} known plaintexts. It is interesting to note that the data analysis phase is independent of the number of rounds and runs only several minutes on a SPARC workstation. We also suggest how to make the S-boxes immune to our new 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 16 data bits, so that each pair of adjacent S-boxes shares two data bits. These bits are XORed with 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 a nonuniform 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 and for some $d_1(x, y)$.[1] 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 (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, and for some $d_n(x, y)$. Note that $d_n(x, y)$ can be easily computed as a convolution of $d_{n-1}(x, y)$ and $d_1(x, y)$.

Davies suggested collecting many known plaintexts and calculating their empirical distribution $D'(x, y, p_n)$. Given sufficiently many known plaintexts, the sign in the D_n distribution can be identified, along with one parity bit of the key, using the indicator

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

whose sign observes the parity bit of the key: if $I > 0$ the parity is zero and if $I < 0$ the parity is one.

Davies estimated the required amount of data for his attack as

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

[1] $d_1(x, y)$ is an extension of Davies' product $d(x) \cdot e(y)$, since for pairs of DES S-boxes it can be factored into the two one-variable functions $d(x)$ and $e(y)$. In [3] $D_n(x, y, p_n)$ is denoted by $S_{X,Y}(s, t)$.

Table 1. The complexities of Davies' attack.

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	$2^{66.0}$	$2^{69.3}$	$2^{85.6}$	$2^{70.6}$	$2^{71.6}$	$2^{66.0}$	$2^{56.6}$	$2^{77.3}$

With this amount of data a 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 an even number of rounds, and one bit for an odd number of 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.

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. 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 off one round of DES—we do that by guessing all the possible values of the key bits of the pair of S-boxes in the last round, and calculating the distribution which results for each of the guessed values (by XORing the plaintext and ciphertext bits with the output of the S-boxes in the last round). 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

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

	Success rate for m key bits found (%)							
Complexity	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

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 decryption is performed, the complexity of this attack could have been more than $4 \cdot 2^{49.74} \cdot 2^{12}/64 \approx 2^{58}$. Later we will describe an efficient algorithm to solve this problem. Once we get 4096 distributions we use a statistical technique (see Appendix) to distinguish the right distribution from the 4095 other (random-looking) 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 0.72 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 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 $(S'(E'(\alpha) \oplus K) \oplus \beta)$ in 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 numbers of key bits are 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 remaining 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 expected success rate.

4. Independent Subkeys

In this section we show a method of attack on the independent subkeys variant of DES (768 key bits), that finds all the 768 bits of the subkeys using 2^{60} known plaintexts and 2^{50} complexity of analysis.

The first phase of the attack uses 2^{60} known plaintexts and performs our improved Davies' attack for each of the three S-box pairs $S1/S2$, $S6/S7$, $S7/S8$ finding 66 key bits (30 bits of K_1, 30 bits of K_{16} and six parity bits). If we would know now all the bits of K_1 and K_{16}, we could peel off the first and the last rounds, and attack the resultant 14-round cryptosystem with the distribution D_6, and with fewer known plaintexts. However, we do not know all the bits of K_1 and K_{16}.

Since we know 30 key bits out of 48 of K_{16} we can perform the attack on the reduced 15-round DES 2^{18} times with the 2^{50} known plaintexts required for detection of distribution D_6. Nevertheless, improved attack can do better. Table 3 describes the missing and known bits entering the S-boxes in the fifteenth round after partial decryption of the sixteenth round using 30 key bits. Known bits are marked by x and unknown bits are represented by the number of the S-box of the sixteenth round they originate from. We pay attention to 32 bits: (a) the 14 input bits entering S-boxes $S3$, $S4$, $S5$ in the last round; (b) five bits of the input to pair $S7/S8$ on fifteenth round (the x bits in Table 3 are received by partial decryption); (c) eight bits resulting from XORing eight plaintext bits

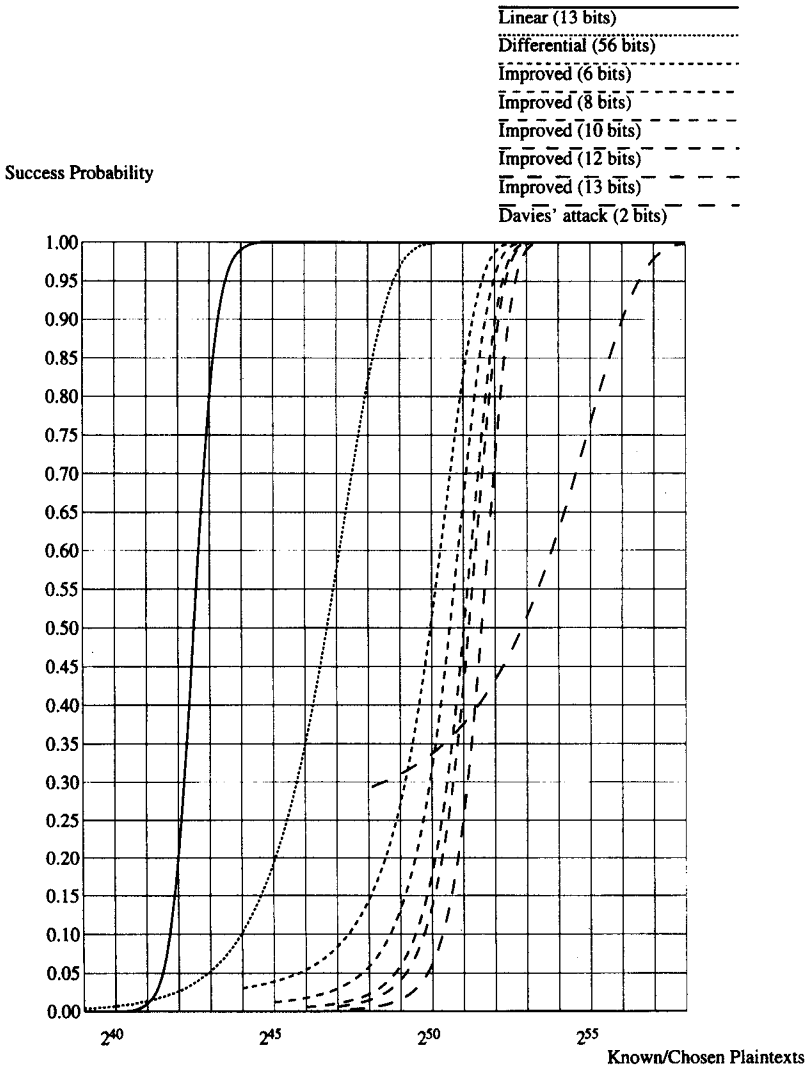

Fig. 1. Comparison of the success probability of differential cryptanalysis, linear cryptanalysis, Davies' attack, and the improved attack.

with eight ciphertext bits and eight output bits of the pair $S7/S8$ from the first round; and (d) five bits of the ciphertext which correspond to unknown five bits entering $S7/S8$ in the fifteenth round.

The second phase of the attack uses 2^{50} known plaintexts and for each plaintext/ciphertext pair increments one of the $2^{14+5+5+8} = 2^{32}$ counters which corresponds to the 32 bits of (a), (b), (c), (d).

The third phase analyzes each counter in the resultant array for each of the possible values of the 18 key bits (denoted by k) entering the S-boxes $S3$, $S4$, $S5$ in the last

Table 3. Known and unknown bits, entering S-boxes in the fifteenth round.

S-box	Bits
$S1$	$x4x5xx$
$S2$	$xx3x5x$
$S3$	$5x4xxx$
$S4$	$xx5x3x$
$S5$	$3xxx4x$
$S6$	$4xxx35$
$S7$	$354xxx$
$S8$	$xx3xx4$

round. It translates them to counters corresponding to: (1) those 18 key bits (k); and (2) five unknown bits of the input of $S7/S8$ in the fifteenth round (calculated in inaccurate notation by $F(a, k) \oplus d$), and the $5+8$ bits of (b), (c). This phase performs $2^{18} \cdot 2^{32} = 2^{50}$ counterincrements and results with a new array containing $2^{18+5+5+8} = 2^{36}$ counters.[2]

In the fourth phase we create 2^{30} distributions by trying all the possible values of the 12 key bits entering $S7/S8$ with 2^{48} operations. Note that in this attack we use a lot more known plaintexts than required in the attack on D_6 (2^{50} instead of the approximation of (4) $N = 2^{42.8}$), thus the success rate is very high although we should identify the right distribution from a large set of 2^{30} distributions. In the fourth phase of the attack we find 18 bits of K_{16} and 12 key bits of K_{15}. Similarly, in the attack on the even rounds, we find 18 bits of K_1 and 12 bits of K_2. Thus K_1 and K_{16} are fully known and we can reduce the attacked cryptosystem to 14 rounds and know 120 actual bits of the subkeys and 8 parity bits out of the 768 independent bits of the subkeys.

In the fifth phase, a similar method is used to find the rest of the subkeys, using the reduction to a fewer number of rounds. This phase is much faster and does not require additional known plaintexts.

5. Protecting Design Criteria

DES was not optimized against Davies' attack: even a simple reordering of the S-boxes can increase the complexity of the attack by a factor of about 600. In this section we show that S-boxes can be chosen to be immune against this attack, by eliminating the properties that it uses.

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 that render DES-like S-boxes immune against Davies' attacks.

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

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

[2] Vector processors with 2^{13} vector addition operations can process groups of 2^{13} entries at once and thus increase the speed of the analysis.

In order to make DES-like S-boxes immune, it suffices to eliminate either the differential property $abcd00_b \to 0$ in the left S-box in each pair, or the differential property $00cdef_b \to 0$ in the right S-box in each pair (we denote binary numbers by the subscript b, where the letters $a, b, \ldots, f$ denote arbitrary values in $\{0, 1\}$). In DES all the patterns of the described type (except $00cd01_b$) 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 the output x of the left S-box in a pair and $E(y, k)$ be the distribution of the output y of the right S-box in the pair, when the value of the two common bits is constrained to be k ($k \in \{0 \ldots 3\}$).[3] For DES S-boxes Davies derived 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 $0bcde0_b \not\to 0$). Thus, any pair of DES-like S-boxes must have a uniform joint distributions if and only if

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

Lemma 1. *The additional differential property* $0bcd11_b \not\to 0$ *leads to uniform joint distribution.*

Proof. Let $\{pbcdq0\}$ be a set of eight entries for some fixed p and q. Since $0bcde0_b \not\to 0$ for any b, c, d, and e, the values in the eight entries $\{pbcd\bar{q}0\}$ (where $\bar{q}$ is the complement of q) are different from the eight values in the entries $\{pbcdq0\}$. Since we assume that $0bcd11_b \not\to 0$, the eight values in the entries $\{pbcd\bar{q}1\}$ are different from the eight values in the entries $\{pbcdq0\}$. Thus, $\{pbcd\bar{q}0\} = \{pbcd\bar{q}1\}$ for any p and q, which causes $D(x, 0) = D(x, 1)$. □

Lemma 2. *The additional differential property* $11cde0_b \not\to 0$ *leads to uniform joint distribution.*

The proof is similar to the proof of Lemma 1, and leads to $E(y, 0) = E(y, 2)$.

Note that $11cd00_b \not\to 0$ is already a design principle of DES. The s^3DES S-boxes [4] were designed with the additional criteria $11cd10_b \not\to 0$, and are thus immune to Davies' attack and to the improved attack.

6. 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} on average) of analysis and has about a 51% success rate. If independent subkeys are used, a variant of this attack can find 26 bits out of the 768 key bits using 2^{52} known plaintexts. All the 768 bits of the subkeys can be found

[3] They are denoted by $d_X(s, t)$ and $d_Y(s, t)$ in [3].

using 2^{60} known plaintext. The data analysis requires only several minutes on a SPARC workstation. We also suggest how to make S-boxes immune to these attacks.

Note. Davies has pointed out that H. Gilbert observed independently that Davies' attack can be improved, and estimated the complexity of the improvement by 2^{52} (see note in [3]).

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 Fig. 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 nonuniformity of D_n by

$$S = \sqrt{\sum_{x,y} d_n(x, y)^2}. \tag{8}$$

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

$$E(I_{R_i}) = 0, \qquad Var(I_{R_i}) \approx \frac{N}{2^8}, \qquad i = 1 \ldots 4095. \tag{9}$$

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

$$|I_K| > \max_{i=1\ldots 4095} |I_{R_i}| \tag{10}$$

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

$$f_K(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(x-m)^2/2\sigma^2} = \frac{2^4}{\sqrt{2\pi N}} \exp\left\{-\frac{1}{2}\left(\frac{2^4}{\sqrt{N}}x - \frac{S\sqrt{N}}{2^4 E(D_n)}\right)^2\right\}. \tag{11}$$

The density function of the other indicators are

$$f_{R_i}(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-x^2/2\sigma^2} = \frac{2^4}{\sqrt{2\pi N}} \exp\left\{-\frac{2^3 x^2}{N}\right\} = f_R(x). \tag{12}$$

Then

$$P_1(N) = P\left(|I_K| > \max_{i=1\ldots 4095} |I_i|\right) = \int_0^{+\infty} f_K(x) \cdot P_R(|r| < x)^{4095}\, dx, \tag{13}$$

where

$$P_R(|r| < x) = \int_{-x}^{x} f_R(y)\, dy. \tag{14}$$

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

$$P_n(N) = \int_0^{+\infty} f_K(x) \sum_{i=0}^{n-1} \binom{4095}{i} P_R(|r| < x)^{4095-i} (1 - P_R(|r| < x))^i\, dx. \tag{15}$$

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 $n = 1, 2, 8, 32, 128$.

References

[1] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, New York, 1993.

[2] D. W. Davies, Investigation of a potential weakness in the DES algorithm, Private communications, 1987.

[3] D. Davies and S. Murphy, Pairs and triplets of DES S-boxes, *Journal of Cryptology*, Vol. 8, No. 1, pp. 1–25, 1995.

[4] Kwangjo Kim, Sangjun Park, and Sangjin Lee, Reconstruction of $s^2 DES$ S-boxes and their immunity to differential cryptanalysis, *Proceedings of JW-ISC'93—Korea-Japan Joint Workshop on Information Security and Cryptology*, Seoul, Korea, October 24–26, 1993.

[5] Mitsuru Matsui, Linear cryptanalysis method for DES cipher, *Advances in Cryptology, Proceedings of EUROCRYPT '93*, Lecture Notes in Computer Science, vol. 765 (T. Helleseth, ed.), Springer-Verlag, Berlin, pp. 386–397, 1994.

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