Enhancing Differential-Linear Cryptanalysis*

Eli Biham[1], Orr Dunkelman[1], and Nathan Keller[2]

[1]Computer Science Department, Technion.
Haifa 32000, Israel
{biham,orrd}@cs.technion.ac.il
[2]Mathematics Department, Technion.
Haifa 32000, Israel
nkeller@tx.technion.ac.il

Abstract. Differential cryptanalysis analyzes ciphers by studying the development of differences during encryption. Linear cryptanalysis is similar but is based on studying approximate linear relations. In 1994, Langford and Hellman showed that both kinds of analysis can be combined together by a technique called *differential-linear cryptanalysis*, in which the differential part creates a linear approximation with probability 1. They applied their technique to 8-round DES. In this paper we present an enhancement of differential-linear cryptanalysis in which the inherited linear probability is smaller than 1. We use this extension to describe a differential-linear distinguisher for a 7-round reduced-version of DES, and to present the best known key-recovery attack on a 9-round reduced-version of DES. We use our enhanced technique to attack COCONUT98 with time complexity $2^{33.7}$ encryptions and $2^{27.7}$ chosen plaintexts.

1 Introduction

Differential cryptanalysis [2] analyzes ciphers by studying the development of differences during encryption. Linear cryptanalysis [11] is similar but is based on studying approximate linear relations.

In 1994, Langford and Hellman [10] showed that both kinds of analysis can be combined together by a technique called *differential-linear cryptanalysis*, in which the differential part creates a linear approximation with probability 1. Using their new technique they have succeeded to analyze up to 8-round reduced variants of DES [12] using only 512 chosen plaintext in a few seconds on a personal computer. This attack is so far the best known attack on 8-round DES.[1]

The differential-linear technique was later applied to analyze the IDEA cipher [9]: a reduced version of IDEA was analyzed by a differential-linear attack in [6], and differential-linear weak keys of the full IDEA (along with a related-key

* The work described in this paper has been supported by the European Commission through the IST Programme under Contract IST-1999-12324.

[1] From now on we will use the shorthand *r-round DES* for an r-round reduced version of DES.

differential-linear attack on reduced IDEA) were found in [7]. It was also shown that the ciphertext-only extension of differential and linear cryptanalysis works also with differential-linear cryptanalysis [5].

Langford and Hellman's technique is an example for devising the "distinguisher" used in the attack as a combination of two much simpler parts; in this case a combination of a differential characteristic and a linear approximation. Such combinations were later used in other kinds of cryptanalysis, e.g., cryptanalysis using impossible differentials [4, 3] (miss in the middle), and boomerang attacks [15], both use combinations of differential characteristics.

In this paper we present an extension of differential-linear cryptanalysis in which the linear probability induced by the differential characteristic is smaller than 1. We use this extension to describe a differential-linear distinguisher for 7-round DES, and then present a differential-linear key-recovery attack on 8-round and 9-round DES. This extension can attack DES with up to 10 rounds, where the 9-round variant of the attack is by far the best known attack against 9-round DES. We also apply the technique to the full COCONUT98.

This paper is organized as follows: In Section 2 we describe Langford and Hellman's differential-linear attacks. In Section 3 we present our differential-linear extension. In Section 4 we present the distinguishing attack on 7-Round DES. In Sections 5 and 6 we present the key recovery attacks on 8-Round and 9-Round DES, respectively. In Section 7 we present a key recovery attack on COCONUT98. Finally, Section 8 summarizes the paper.

2 Differential-Linear Cryptanalysis

Langford and Hellman [10] show that a concatenation of a differential characteristic and a linear characteristic can be performed. They select a 3-round characteristic of DES, which predicts the differences of a few bits after three rounds with probability 1 (the probability for the whole block difference after three rounds is much lower). So, given a pair of plaintexts with the required plaintext difference, they know the difference of a few bits after three rounds for certain. They use a 3-round linear approximation for rounds 4–6. If the difference in the intermediate data before the linear approximation can be predicted, then we can obtain information about the parities. More precisely, if the difference in the input subset can be predicted, then we know whether the input subset parity in both encryptions is the same or differ. As the linear approximation predicts the output subset parity, we can now predict whether the output subset parities of the two ciphertexts are more likely to be the same or not. Fortunately, they found differential and linear characteristics in which the subset required for the parity is predicted with probability 1 by the differential characteristic. Thus, the differential characteristic actually tells them the difference of the two parities. Both difference and parity are linear operations (they both use XOR). Thus, the two linear approximations in rounds 4–6 in both encryptions can be combined into a six-round approximation of rounds

$$6_1\text{–}5_1\text{–}4_1\text{–differential–}4_2\text{–}5_2\text{–}6_2,$$

where the subscript denote whether the round is in the first encryption or the second, and "differential" refers to the differential combiner that ensures that the parities of the data before round 4 in both encryptions are always equal (or always differ).

This enlarged linear characteristic has twice as many rounds as the original, thus its probability is much closer to 1/2 than the original. However, it is still usable, and in various cases it leads to the best known attacks against the analyzed cipher, as in the case of the differential-linear attack on 8-round DES described by Langford and Hellman.

The differential-linear distinguisher is based on encrypting many pairs with some known input difference. Each pair is encrypted, and the output subset parity is computed for both ciphertext. The fraction of times when the two parities are agree differ from 1/2 for a good differential-linear characteristic. Thus, it can be used to distinguish the cipher from a random permutation. A key recovery attack can be mounted using standard techniques (guessing the following round subkey, etc.).

3 Our Differential-Linear Extension

We observed that in the above approximation

$$6_1\text{–}5_1\text{–}4_1\text{–differential–}4_2\text{–}5_2\text{–}6_2$$

all the rounds are approximated with probabilities which may be different than $1/2 \pm 1/2$, except for the connection by the differential characteristic, which has probability 1.

From now on, we use notations based on [1, 2] for differential and linear cryptanalysis, respectively. In our notations Ω_P, Ω_T are the input and output differences of the differential characteristic, and λ_P, λ_T are the input and output subsets (denoted by bit masks) of the linear characteristic.

In this paper we propose using a differential connection with fractional probabilities. Let the probability of the linear characteristic be denoted by $1/2 + q$, and the probability of the differential characteristic be denoted by p' (in the case of Langford and Hellman, $p' = 1$ and $q = 0.195$).

Given the probabilities of the differential characteristic p', we approximate the linear probability $1/2+p$ of the relations of the parities of the subsets of bits λ_P between both encryptions (in the particular case of $p' = 1$ certainly $p = 1/2$ as in Langford and Hellman's analysis), and then compute the probability of the total relation (from the last round of the linear characteristic through all its rounds backward in the first encryption, through the differential approximation of the parity, through the linear characteristic in the second encryption to its last round). This probability is computed by the usual rule for probabilities of concatenation of linear characteristics. Thus, the total probability is

$$1/2 + 4pq^2.$$

Note that the differential probability p' is the probability for the expected difference in the required subset of bits, which is usually different (higher) than the probability of the differential characteristic with the full block output difference, so the best characteristic for our purposes may be different than the best ordinary characteristic. For example, in Langford and Hellman's case the characteristic predicts with probability 1 only 36 bits of the 64 bits of the output difference; these 36 bits include all the 5 bits of λ_P. Given an ordinary differential characteristic with probability p_Ω, we know that the full block output difference Ω_T appears with probability p_Ω, and that with probability $1 - p_\Omega$ the difference is different. When considering only the subset of bits in λ_P, the probability of the characteristic on these bits becomes p'. The probability $1/2 + p$ can now be approximated by

$$1/2 + p \approx p' + (1 - p')/2 = 1/2 + p'/2,$$

assuming that the parity in the rest of the cases is uniformly distributed. This assumption is not necessarily accurate, for example, there might be other high-probability differential characteristics with the same plaintext difference, but with different (or same) parity of the subset of bits of the difference. Thus, this approximated probability should be verified by the designer of an attack, and if possible, he should perform a more accurate computation of the probability, or check it experimentally.

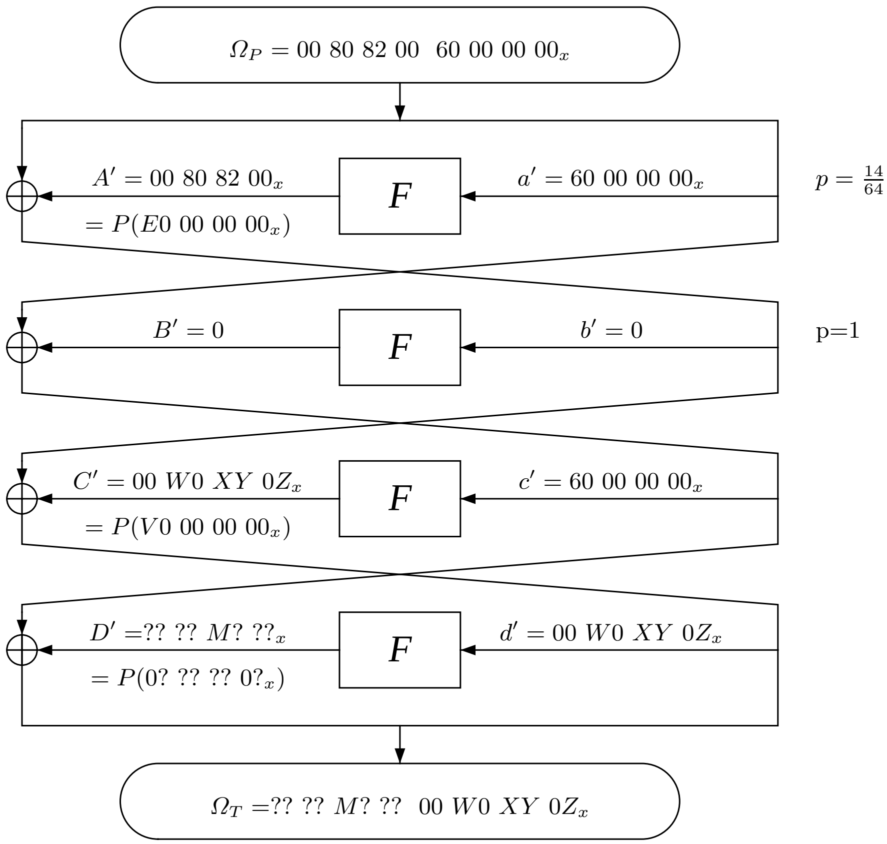
It is worth mentioning that the attack works even if the differential characteristic predicts that there are differences in some of the bits in the subset λ_P. All we need is to know the parity of the differences of the bits in λ_P (rather than fixing the differences to 0). For example, assume that $\Omega_T =$ 10 ?0 ?0 67 80 D7 6? 11_x (where the ? denotes an unpredicted hex digit) and assume that $\lambda_P =$ 00 00 08 D7 00 00 00 01_x. Then, the 8 bits selected by λ_P are known in Ω_T, of which 5 have value 1 and 3 have value 0. Therefore, the expected parity of the differences of the two runs is $\Omega_T \cdot \lambda_P = 1$. Note that even if $\Omega_T \cdot \lambda_P$ is unknown but constant, the attack still succeeds.

4 A Distinguishing Attack on 7-Round DES

We now present an attack that distinguishes whether a cipher (given in a form of a black box) is a 7-round DES, or a random permutation, using the differential-linear technique. We use the following 4-round extended differential characteristic with probability $p_\Omega = 14/64 = 0.21875$, which is an extension by one round of the 3-round characteristic used by Langford and Hellman. This extended characteristic is presented in Figure 1.

The 3-round differential was concatenated with the 3-round linear approximation with probability $1/2 + 0.195$ presented in Figure 2. This 3-round linear approximation is also the best 3-round linear approximation for DES.

We use our 4-round differential characteristic to build a distinguisher with a probability of $1/2 + p \approx 1/2 + \frac{14/64}{2} \approx 1/2 + 0.109$ (recall, that for a random permutation this value is 1/2). This approximation assumes that the behavior of



(where $V \in \{1, \ldots, F_x\}$, $W \in \{0, 8\}$, $X \in \{0, 8\}$, $Y \in \{0, 2\}$, $Z \in \{0, 2\}$, $M \in \{0, \ldots, 7\}$, and any ? is any arbitrary value)

Fig. 1. The Extended 4-Round Differential Characteristic Used in Our Distinguisher

the remaining fraction of $1 - 14/64 = 50/64$ of the pairs induces uniform linear distribution. We have verified the value of p experimentally, and confirmed this probability using hundreds of different keys, and millions of encrypted pairs. The linear characteristic has probability $1/2 + q = 1/2 + 2(\frac{-20}{64})^2 \approx 1/2 + 0.195$. The total probability of the approximation is thus

$$1/2 + 4pq^2 = 1/2 + 4 \cdot 0.109 \cdot 0.195^2 = 1/2 + 0.0167 = 1/2 + 2^{-5.91}.$$

The distinguishing attack is as follows:

1. Select $N = 2^{11.81}$ plaintext pairs with the plaintext difference $\Omega_P = 00\,80\,82\,00\ \ 60\,00\,00\,00_x$.
2. Request the ciphertexts of these plaintext pairs (encrypted under the unknown key K).

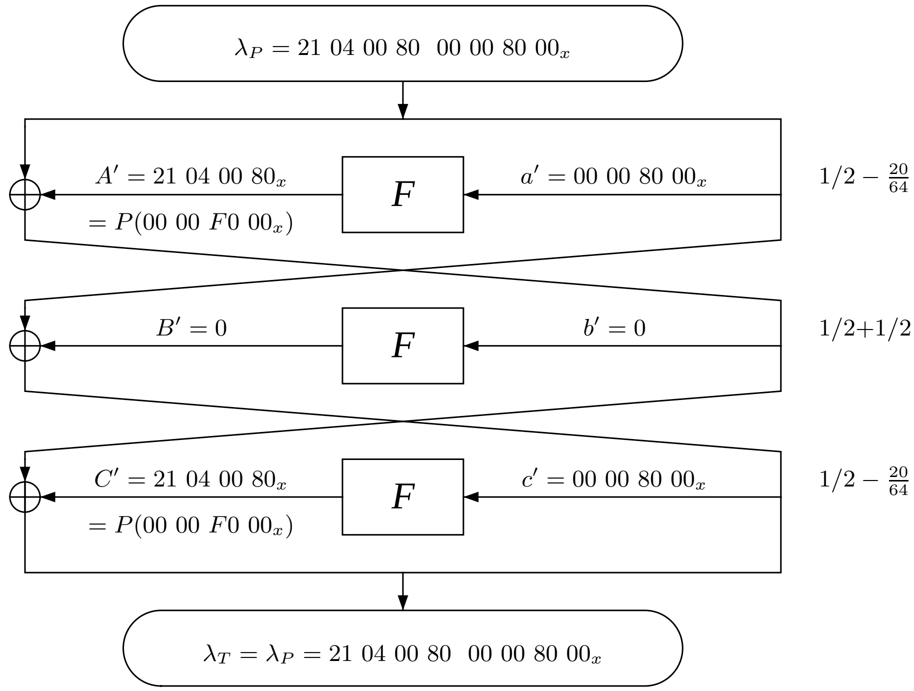


Fig. 2. The 3-Round Linear Approximation Used in [10]

3. For each ciphertext pair, compute the parity of the bits masked by $\lambda_T = 21\ 04\ 00\ 80\ \ 00\ 00\ 80\ 00_x$ in each of the plaintexts, and count for how many pairs both parities are equal. Let the number of such pairs be denoted by m.
4. If
$$\frac{m}{N} > \frac{1}{2} + \epsilon, \qquad \text{where } \epsilon = \frac{4pq^2}{2} = 2^{-6.90},$$
(i.e., $m > 2^{10.81} + 2^{4.91}$) conclude that the cipher is 7-round DES.
5. Otherwise, conclude that the cipher is not 7-round DES.

The parameters N and ϵ are selected as to maximize the success rate of the attack while requiring the lowest data complexity. For $N = 2^{11.81}$ and $\epsilon = 2^{-6.90}$ the attack succeeds with probability higher than 84.13%, and has data and time complexities of $2^{12.81}$.

We point out that unlike most linear attacks (and most differential-linear attacks) it suffices in this case to test whether $\frac{m}{N} > \frac{1}{2} + \epsilon$ rather than whether $|\frac{m}{n} - 1/2| \geq \epsilon$. This follows from the fact that in this specific attack the bias is always positive and is unaffected by any key bit (as all the affected key bits are used twice and thus cancelled).

In order to show that for these parameters we get this success rate we use the following statistical reasoning (see [13]): For a random permutation each pair behaves randomly, and thus in half of the pairs the two parities of the subset of the ciphertext bits are equal. Therefore, the number of equal parities behaves like a binomial random variable $X \sim Bin(2^{11.81}, 1/2)$. It is easy to see that such random variable can be approximated according to the normal distribution, and thus we conclude that the probability that this random variable (counting the number of pairs with equal parities) is higher than $2^{10.81} + 2^{4.91}$ is at most 15.87%. We conclude that for a random permutation the probability that the above algorithm outputs 'this is a random permutation' is 84.13%.

Repeating this analysis for 7-round DES with $X \sim Bin(2^{11.81}, 1/2 + 2^{-5.91})$ the probability that the algorithm outputs 'this is a random permutation' is 15.87%.

5 A Key Recovery Attack on 8-Round DES

This attack can be extended to a key-recovery attack by adding one round for the analysis, and using the 7-round distinguisher, as follows

1. Select $N = 2^{13.81}$ plaintext pairs with the plaintext difference $\Omega_P = 00\ 80\ 82\ 00\ \ 60\ 00\ 00\ 00_x$.
2. Request the ciphertexts of these plaintext pairs (encrypted under the unknown key K).
3. Initialize an array of 64 counters to zeroes.
4. For each ciphertext pair
   (a) Try all the 64 possible values of the 6 bits of the subkey $K8$ that enter the S Box S1 in round 8.
   (b) For each value of the subkey, compute the output of S1 in the last round, and use its output to compute the parity of the subset of bits in λ_T after round 7. Now we can compute the output subset parity, as we know 4 of the subset bits from the ciphertext, and the remaining one from the the output of $S1$ and the ciphertext.
   (c) If the parities in both members of the pair are equal, increment the counter in the array which relates to the 6 bits of the subkey.
5. The highest entry in the array should correspond to the six bits of $K8$ entering S1 in round 8.
6. The rest of the key bits can be recovered by auxiliary techniques.

For $N = 2^{13.81}$ this attack succeeds with probability 77.27% or more. The complexity of the attack is $2^{14.81} \cdot 2^6/64 = 2^{14.81}$ time (in units of 8-round DES encryptions; 2^6 subkeys tried, each trial takes about one S box computation out of the 64 S boxes of a full encryption), requiring $2^{14.81}$ chosen plaintexts.

6 A Key Recovery Attack on 9-Round DES

Similarly, the attack can be extended to 9 rounds by analyzing two rounds in addition to the 7-round distinguisher.

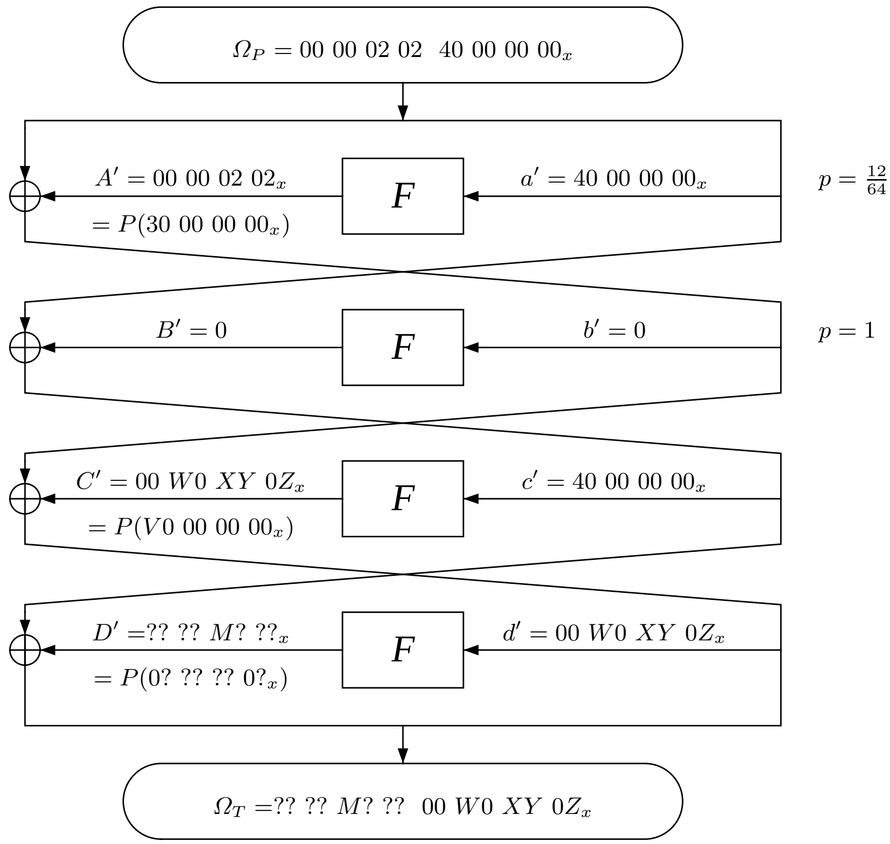


Fig. 3. The Modified 4-round Differential Characteristic Used in the 9-Round Attack

In this case we use the slightly modified differential characteristic presented in Figure 3.

This characteristic is similar to the original, except that its first round is replaced. This replacement is done to reduce the number of active S boxes in the round preceding the characteristic. This characteristic induces a linear probability of $1/2+p = 1/2+0.09375$ (again, we experimentally verified this probability). With this change, the 7-round distinguisher with 84.13% success rate would require $N = 2^{12.25}$ pairs (for $\epsilon = 2^{-7.13}$).

To mount a 9-round key recovery attack, we set the differential and linear characteristics combination at rounds 2–8, and analyze rounds 1 and 9.

The attack is as follows

1. Select $N = 2^{15.75}$ plaintexts, consisting of $2^{6.75}$ structures, each is chosen by selecting:

   (a) Any plaintext P_0
   (b) The plaintexts $P_1,\ldots,P_{255}$ which differ from P_0 by all the 255 possible subsets of the eight bits masked by 18 22 28 28 00 00 00 00_x (these are the output bits of S6 and S8 in round 1).
   (c) The plaintexts $P_{256},\ldots,P_{511}$ selected as $P_i = P_{i-256} \oplus 40\ 00\ 00\ 00\ \ 00\ 00\ 02\ 02_x$.
2. Request the ciphertexts of these plaintext pairs (encrypted under the unknown key K).
3. At this stage we do not know which pairs in the structure have the difference Ω_P before round 2. Instead, we guess these pairs by trying all the possible values of the 12 bit of the subkey K1 which enter S6 and S8.
4. For each value of the 12 bits of K1 entering S6 and S8
   (a) Partially encrypt S6 and S8 in the first round of each plaintext and find the pairs which satisfy the difference Ω_P before round 2 (assuming the guessed value is correct)
   (b) Given all the pairs, apply the 8-round attack on these pairs (the attack is on the 8 rounds from round 2 to round 9).
5. Each trial of the key gives us $12 + 6 = 18$ bits of the subkeys (12 bits in round 1 and 6 bits in round 9), along with a measure for correctness (which is the number of times it is suggested in the 8-round attack). The correct value of the 18 bits is expected to be the most frequently suggested values (with over 88.80% success rate).
6. The rest of the key bits are then recovered by auxiliary techniques.

Note that due to the mass of 2^{12} applications of the 8-round attack, and the need to identify which application uses the correct guess of the 12 bits of the first subkey, we need more data than for a single application of the 8-round attack.

This attack requires $2^{15.75}$ chosen plaintexts, and finds the key in time $2^{15.75} \cdot 2^{12} \cdot 2^6 \cdot 3/72 \approx 2^{29.17}$ (in units of 9-round DES encryptions). This time complexity of this attack can be further reduced using auxiliary techniques and reordering of the operations.

7 Attack on COCONUT98

We can use our results to present the best known attack against the COCONUT98 block cipher. COCONUT98 is a 64-bit blocksize 256-bit keysize block cipher, that was designed using the decorrelation theory [14].

The cipher is composed of 4 Feistel rounds, a decorrelation module, and 4 additional Feistel rounds. The decorrelation module is $M(xy) = (xy \oplus K_5K_6) \times K_7K_8 \bmod GF(2^{64})$, where x, y are the 32-bit data word, xy denotes their concatenation. K_5, K_6, K_7, K_8 are four 32-bit values supplied by the user key, and where $K_7K_8 \neq 0$. The multiplication is over the finite field $GF(2^{64})$ defined by the polynomial $x^{64}+x^{11}+x^2+x+1$ over $GF(2)$. Note that the exact underlying polynomial has no effect on our results. The Feistel rounds can be described as follows:

$$\phi(x) = x + 256 \cdot S(x \bmod 256) \bmod 2^{32}$$
$$F_{k_i}(x, y) = (y, x \oplus \phi(ROL_{11}(\phi(y \oplus k_i)) + c \bmod 2^{32}))$$

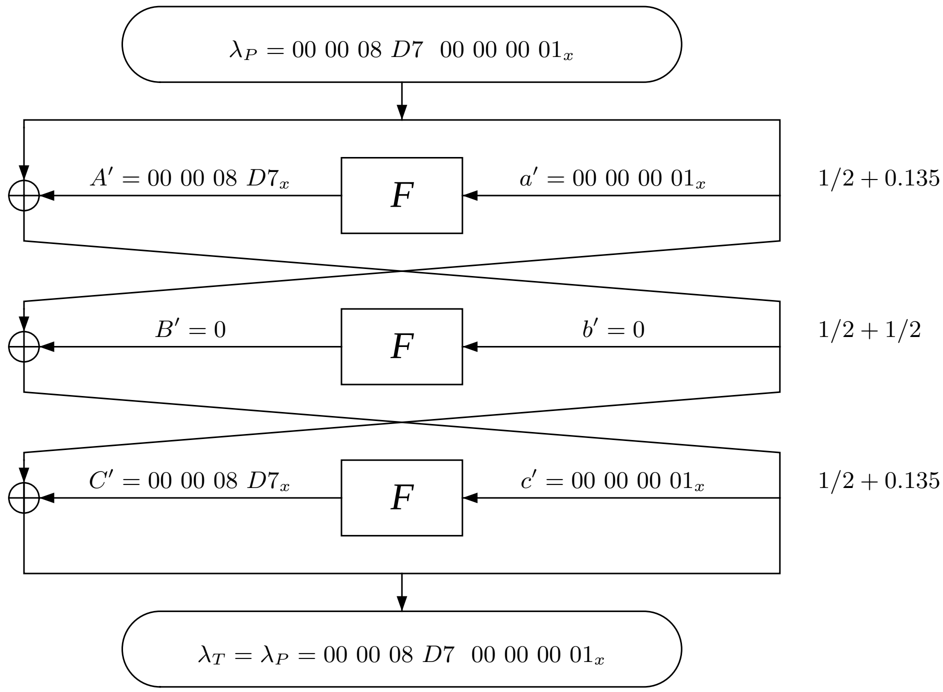


Fig. 4. A 3-round Linear Approximation of COCONUT98 with Probability 1/2+0.0364

where $c = B7\ E1\ 51\ 62_x$ is a known constant and k_i is the round subkey.

In [15] a 4-round differential (of the Feistel rounds) with probability $0.83 \cdot 2^{-4}$ was introduced. It was commented that the expected difference that enters the decorrelation module leads to some fixed but unknown difference after the decorrelation module. We denote this differential by $\Omega_{COCONUT98}$. Thus, $\Omega_{COCONUT98}$ is a differential with probability $p = 0.83 \cdot 2^{-4}$ for the first 4 Feistel rounds and the decorrelation module. Note that we have no idea what the output difference of $\Omega_{COCONUT98}$ is. Still, this does not interfere with our analysis, as we mentioned before. In case that the subset λ_P of bits of this output difference has an odd number of active bits (i.e., the scalar product $\lambda_P \cdot \Omega_T$ is 1), then there are going to be more disagreements on the output parity then agreements, and the linear bias would be negated, without affecting the analysis.

In Figure 4 we present a linear approximation for 3 Feistel rounds of COCONUT98. This approximation has a probability $1/2 + q = 1/2 + 0.0364$.

We can now use $\Omega_{COCONUT98}$ concatenated to the 3-round linear approximation to present a distinguisher for the entire COCONUT98 but the last round. The distinguisher has a bias of $4pq^2 \approx 1/3638$. Note that we do no know whether the bias is in favor of having the same parity, or having complement parities (as we have no idea what the output of the differential is; this output depends on some key that we do not know), but this does not stop us from attacking the cipher.

The attack retrieves subkey bits of the last round. As the only unknown value in the equation of the parities is the least significant bit of the right half after the 7th Feistel round (just after the approximation), we need to determine the least significant bit of the output of the function F in the last round. As this bit is unaffected by the second ϕ, and as the addition of the constant c does not change it (the least significant bit of the constant c is 0), then it is unchanged after the rotate left operation. In this operation we actually need to know bit 21 before the rotate. In order to determine this bit, we need to know the lower 22 bits that enter the first ϕ, and we conclude that we need to know the 22 lower key bits in the last round. As guessing these 22 key bits can be very time consuming, we try to look for more efficient solutions. We can approximate (with very high probability) the true value of the relevant bit, by knowing the output of the S-box in the first ϕ (i.e., look at the 8 lower subkey bits) and m bits of the subkey from bit 21 and downward. Considering only m subkey bits causes a mistake in a fraction of 2^{-m} of the cases. As this mistake appears uniformly and affects all trials similarly, we actually get a bias of $4pq^2 \cdot (1 - 2^{-m+1})$. For the value $m = 7$ this bias is $1/3700$. A slight improvement of the bias to the value $4pq^2 = 1/3638$ can be performed by discarding some mistaken data.

Our attack counts over these $7+8 = 15$ subkey bits using the following algorithm:

1. Initialize 2^{15} counters. Each corresponds to a different last round subkey.
2. Encrypt N pairs with the required input difference.
3. For each 15-bit subkey subkey value partially decrypt all ciphertext pairs and check whether the parities of the subsets are equal or different. For each ciphertext pair increment the counter of the subkey in case of equality.
4. Look for the counter with the maximal bias from $N/2$ (i.e., $|\text{counter}-N/2|$ is maximal), and suggest the related subkey as the right subkey.

The time complexity of this algorithm is $2N$ encryptions and $2 \cdot 2^{15} \cdot N$ additional last round activations (and 2^{16} additional memory accesses, which we omit). Hence, the total running time of the algorithm is $2^{16} \cdot N/8 = 2^{13} \cdot N$ COCONUT98 encryptions.

We now determine N. We associate the right key counter with the random variable X, and each of the $2^{15} - 1$ wrong subkeys with its own random variable Y_i. We assume that all of these variables have a normal distribution and that $X \sim N(N/2 + N/3700, N/4)$ and that $\forall i : Y_i \sim N(N/2, N/4)$. For $N = 8/(1/3700)^2$, the success rate of the attack is at least 75.46%. Thus, we conclude that we need $N = 8 \cdot 3700^2 = 2^{26.7}$ pairs ($2^{27.7}$ chosen plaintexts), and time complexity of $2^{39.7}$ COCONUT98 encryptions.

The rest of the key can be found with auxiliary techniques using other differentials and linear approximations with a negligible additional time and data complexities.

We can reduce the time complexity of the attack by observing that we are actually interested in 15 bits of the ciphertext. In the above analysis we perform the same operations for the same values many times. Using a precomputed table (which requires $2^{15} \cdot 2^{15} = 2^{30}$ last round activations to compute) we can reduce the time complexity of the attack to $2^{39.7}$ memory accesses, which are equivalent to at most $2^{33.7}$ COCONUT98 encryptions.

8 Summary and Conclusions

In this paper we presented an extension of differential-linear cryptanalysis that allows using a differential characteristic with probability lower than 1. We showed that this extension can attack DES reduced 7, 8, and 9 rounds. The latter is the best known method against 9-round DES.

This attack can be extended to analyze the 10-round reduced-variant of DES with time complexity about 2^{50} and using about 2^{20} chosen plaintexts.

We also presented the fastest attack on the full COCONUT98. Our attack requires about $2^{27.7}$ chosen plaintexts and time complexity of about $2^{33.7}$ COCONUT98 encryptions. Previous results [15] required 2^{16} adaptive chosen plaintexts and ciphertexts and 2^{38} COCONUT98 encryptions.

We summarize our results along with previously known results in Table 1.

Cipher	Attack	Complexity		Success
		Data	Time	Rate
8-round DES	Differential [2]	2^{14}CP	2^{9}	53%
	Linear [11]	2^{18}KP	2^{25}	49.4%
	Linear [11]	2^{19}KP	2^{26}	93.2%
	Differential-Linear [10]	512CP	2^{14}	80%
	Differential-Linear [10]	768CP	$2^{14.6}$	95%
	C.P. Linear Cryptanalysis [8]	2^{16}CP	2^{23}	51%
	C.P. Linear Cryptanalysis [8]	2^{17}CP	2^{24}	94%
	Enhanced Differential-Linear – this paper	$2^{14.8}$ CP	$2^{14.8}$	77.3 %
9-round DES	Differential [2]	2^{24}CP	2^{32}	99.97%
	Enhanced Differential-Linear – this paper	$2^{15.8}$ CP	$2^{29.2}$	88.8%
COCONUT'98	Boomerang [15]	2^{16}ACPC	2^{38}	99.96%
(full cipher)	Enhanced Differential-Linear – this paper	$2^{27.7}$CP	$2^{33.7}$	75.5%

Complexity is measured in encryption units.
CP - Chosen Plaintexts, KP - Known Plaintexts
ACPC - Adaptive Chosen Plaintexts and Ciphertexts

Table 1. Summary of Our Results and Previously Known Results

References

1. Biham Eli, *On Matsui's Linear Cryptanalysis*, Advances in Cryptology, proceedings of EUROCRYPT '94, Lecture Notes in Computer Science 950, pp. 341–355, 1994.
2. Eli Biham, Adi Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
3. Eli Biham, Alex Biryukov, Adi Shamir, *Miss in the Middle Attacks on IDEA and Khufu*, proceedings of Fast Software Encryption 6, Lecture Notes in Computer Science 1636, pp. 124–138, 1999.
4. Eli Biham, Alex Biryukov, Adi Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials*, Advances in Cryptology, proceedings of EUROCRYPT '99, Lecture Notes in Computer Science 1592, pp. 12–23, 1999.
5. Alex Biryukov, Eyal Kushilevitz, *From Differential Cryptoanalysis to Ciphertext-Only Attacks*, Advances in Cryptology, proceedings of CRYPTO '98, Lecture Notes in Computer Science 1462, pp. 72–88, 1998.
6. Johan Borst, Lars R. Knudsen, Vincent Rijmen, *Two Attacks on Reduced Round IDEA*, Advances in Cryptology, proceedings of EUROCRYPT '97, Lecture Notes in Computer Science 1233, pp. 1–13, 1997.
7. Philip Hawkes, *Differential-Linear Weak Keys Classes of IDEA*, Advances in Cryptology, proceedings if EUROCRYPT '98, Lecture Notes in Computer Science 1403, pp. 112-126, 1998.
8. Lars R. Knudsen, John Erik Mathiassen, *A Chosen-Plaintext Linear Attack on DES*, proceedings of Fast Software Encryption 7, Lecture Notes in Computer Science 1978, pp. 262–272, 2001.
9. Xuejia Lai, James L. Massey, *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology, proceedings if EUROCRYPT '91, Lecture Notes in Computer Science 547, pp. 17-38, 1992.
10. Suzan K. Langford, Martin E. Hellman, *Differential-Linear Cryptanalysis*, Advances in Cryptology, proceedings of CRYPTO '94, Lecture Notes in Computer Science 839, pp. 17–25, 1994.
11. Mitsuru Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology, proceedings of EUROCRYPT '93, Lecture Notes in Computer Science 765, pp. 386–397, 1994.
12. US National Bureau of Standards, *Data Encryption Standard*, Federal Information Processing Standards Publications No. 46, 1977.
13. Jim Pitman, *Probability*, Springer-Verlag, 1993.
14. Serge Vaudenay, *Provable Security for Block Ciphers by Decorrelation*, proceedings of STACS '98, Lecture Notes in Computer Science 1373, pp. 249–275, 1998.
15. David Wagner, *The Boomerang Attack*, proceedings of Fast Software Encryption 6, Lecture Notes in Computer Science 1636, pp. 156–170, 1999.