On Matsui's Linear Cryptanalysis

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

Abstract

In [9] Matsui introduced a new method of cryptanalysis, called *Linear Cryptanalysis*. This method was used to attack DES using 2^{47} known plaintexts. In this paper we formalize this method and show that although in the details level this method is quite different from differential cryptanalysis, in the structural level they are very similar. For example, characteristics can be defined in linear cryptanalysis, but the concatenation rule has several important differences from the concatenation rule of differential cryptanalysis. We show that the attack of Davies on DES is closely related to linear cryptanalysis. We describe constraints on the size of S boxes caused by linear cryptanalysis. New results to Feal are also described.

1 Introduction

In EUROCRYPT'93 Matsui introduced a new method of cryptanalysis, called *Linear Cryptanalysis* [9]. This method was used to attack DES using 2^{47} known plaintexts.

In this paper we formalize this method and show that although in the details level this method is quite different from differential cryptanalysis[2,1], in the structural level they are very similar. For example, characteristics can be defined in linear cryptanalysis, but the concatenation rule has several important differences from the concatenation rule of differential cryptanalysis. We show that the attack of Davies[5] on DES is closely related to linear cryptanalysis. We describe constraints on the size of S boxes caused by linear cryptanalysis. New results to Feal[15,11] are also described.

2 Overview of Linear Cryptanalysis

Linear cryptanalysis studies statistical linear relations between bits of the plaintexts, the ciphertexts and the keys they are encrypted under. These relations are used to predict values of bits of the key, when many plaintexts and their corresponding ciphertexts are known.

Since all the operations in DES, except the S boxes, are linear, it suffices to derive linear relations of the S boxes. These relations are derived for each S box by choosing a subset of the input bits and the output bits, calculating the parity (exclusive-or) of these bits for each of the possible inputs of the S box, and counting the number of inputs whose subset's parity is zero. If the S box is linear in the bits of the subset, all the inputs must have a zero parity of the subset. If the S box is affine in the bits of

Table 1. The Linear Approximation Table of S5.

Input	Output subset															
subset	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2_x	0	4	-2	2	-2	2	-4	0	4	0	2	-2	2	-2	0	-4
3_x	0	0	-2	6	-2	-2	4	-4	0	0	-2	6	-2	-2	4	-4
4_x	0	2	-2	0	0	2	-2	0	0	2	2	4	-4	-2	-2	0
5_x	0	2	2	-4	0	10	-6	-4	0	2	-10	0	4	-2	2	4
6_x	0	-2	-4	-6	-2	-4	2	0	0	-2	0	-2	-6	-8	2	0
7_x	0	2	0	2	-2	8	6	0	-4	6	0	-6	-2	0	-6	-4
8_x	0	0	2	6	0	0	-2	-6	-2	2	4	-12	2	6	-4	4
9_x	0	-4	6	-2	0	-4	-6	-6	6	-2	0	-4	2	-6	-8	-4
A_x	0	4	0	0	-2	-6	2	2	2	2	-2	2	4	-4	-4	0
B_x	0	4	4	4	6	2	-2	-2	-2	-2	-2	2	0	-8	-4	0
C_x	0	2	0	-2	0	2	4	10	-2	4	-2	-8	-2	4	-6	-4
D_x	0	6	0	2	0	-2	4	-10	-2	0	-2	4	-2	8	-6	0
E_x	0	-2	-2	0	-2	4	0	2	-2	0	4	2	-4	6	-2	-4
F_x	0	-2	-2	8	6	4	0	2	2	4	8	-2	8	-6	2	0
10_x	0	2	-2	0	0	-2	-6	-8	0	-2	-2	-4	0	2	10	-20
11_x	0	2	-2	0	4	2	-2	-4	4	2	2	0	-8	-6	2	4
12_x	0	-2	0	-2	2	-4	-2	-8	4	6	4	6	-2	4	-6	0
13_x	0	-6	0	2	-2	4	2	0	4	-6	4	2	-6	4	-2	0
14_x	0	4	-4	0	0	0	0	0	-4	-4	4	4	0	4	-4	0
15_x	0	4	0	-4	-4	4	-8	-8	0	0	-4	4	8	4	0	4
16_x	0	0	6	6	2	-2	4	0	4	0	6	2	2	2	0	0
17_x	0	4	-6	-2	6	-2	-4	4	4	-4	-6	2	-2	2	0	4
18_x	0	6	0	2	4	-10	-4	2	2	0	-2	0	2	4	-2	-4
19_x	0	2	4	-6	0	-2	4	-2	6	8	6	4	10	0	2	-4
$1A_x$	0	2	2	-8	-2	4	0	2	-2	0	4	2	0	-2	-2	0
$1B_x$	0	2	6	-4	-6	0	0	2	6	8	0	-2	-4	-6	-2	0
$1C_x$	0	0	-2	2	4	0	-6	2	-2	6	-4	0	2	-2	0	0
$1D_x$	0	4	-2	6	-8	0	-2	2	10	-2	-8	-8	2	2	0	4
$1E_x$	0	-4	-8	0	-2	-2	-2	2	-2	2	-2	6	4	4	4	0
$1F_x$	0	-4	8	-8	2	-6	-6	-2	-2	2	-2	-2	-8	0	0	-4
20_x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21_x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22_x	0	-4	-2	2	-2	2	-4	8	-4	0	-6	6	2	-2	-16	-12
23_x	0	0	-2	-2	6	-2	-4	4	0	0	-2	-2	-2	6	4	-4
24_x	0	-2	6	4	0	6	-2	4	4	-6	-2	4	0	14	2	0
25_x	0	6	2	0	0	6	2	0	-4	-6	2	-8	0	-2	6	-4
26_x	0	2	4	-2	-2	0	2	-4	4	-2	-4	-2	6	0	-2	0
27_x	0	-10	0	-2	6	4	6	-4	0	6	-12	2	2	0	6	-4
28_x	0	4	-2	-2	0	4	-6	2	2	-6	4	0	6	-2	-4	0
29_x	0	0	2	6	0	0	6	2	2	-2	-8	0	-2	-6	0	0
$2A_x$	0	0	-4	-8	6	6	6	-6	6	2	-2	-2	-8	4	-4	4
$2B_x$	0	8	0	4	6	-2	-6	6	2	6	-2	6	-4	0	4	4
$2C_x$	0	2	4	-6	0	-6	0	6	-2	-4	2	-4	-2	4	6	0
$2D_x$	0	-2	-4	-2	0	-2	-8	2	-2	0	-6	-8	-2	0	-2	4
$2E_x$	0	6	2	-4	6	4	4	-2	-10	-8	0	-2	4	-2	2	0
$2F_x$	0	6	-6	-4	6	-4	4	-2	2	4	4	-6	0	2	-2	-4
30_x	0	2	-2	0	-4	-6	-2	-4	4	2	2	0	0	2	2	4
31_x	0	2	-2	0	0	-2	2	0	0	-2	-2	-4	0	2	2	4
32_x	0	6	0	-2	-2	8	2	4	0	10	0	2	-2	4	2	0
33_x	0	-6	0	10	2	0	-2	-4	0	6	0	-10	2	4	-2	0
34_x	0	0	-12	4	-4	0	4	-8	-4	0	-4	0	-4	-4	0	0
35_x	0	-8	0	0	8	-4	4	0	0	-4	-4	0	4	4	-4	4
36_x	0	4	-2	-6	-2	-2	8	0	4	-4	-2	-2	6	2	-4	0
37_x	0	-8	-6	-6	-6	6	0	4	12	0	2	-2	2	2	4	-4
38_x	0	2	4	-6	0	-2	4	-2	-6	4	-6	0	6	4	-2	0
39_x	0	-2	8	2	-4	6	-4	-6	-2	-4	2	4	-2	0	2	0
$3A_x$	0	6	-10	0	2	4	0	-2	6	-4	0	2	4	-2	-2	-4
$3B_x$	0	-2	-6	-4	-10	0	-8	-2	-10	4	4	-2	0	2	-2	4
$3C_x$	0	-8	-6	-2	0	-4	2	2	-6	2	4	0	10	-2	4	4
$3D_x$	0	4	2	2	4	4	-2	2	-2	10	0	0	2	2	4	0
$3E_x$	0	-4	4	-4	2	2	-2	2	2	-2	-2	-2	4	-4	0	4
$3F_x$	0	-4	-4	-4	14	6	-6	-2	2	-2	6	-2	0	0	-4	0

the subset, all the inputs must have parity 1. Usually, a subset will have many inputs with parity 0 and many inputs with parity 1. As the number of zeroes is closer to the number of ones, we will say that the subset is more non-linear. The least linear subset under this definition is one whose half of the inputs have parity zero, and the other half inputs have parity 1.

Matsui has calculated the number of zero parities for each of the $64 \cdot 16 = 1024$ possible subsets of the input and the output bits of each S box. To represent the subsets' linearity in a simple manner, he subtracts from these numbers the number of half of the inputs. This way, zero values denote non-linear subsets, and high absolute values denote linear/affine or close to linear/affine subsets. A table which describes all these values for all the possible subsets of an S box is called a *linear approximation table* of the S box. Table 1 is the linear approximation table of S5 of DES. In this linear approximation table, we can see that 30% of the entries have value zero.

The highest absolute value in the linear approximation table of S5 is -20 in entry $(10_x, F_x)$. Therefore, only in 12 out of the 64 inputs, the parity of the four output bits is the same as the value of the second input bit! This entry was actually described by Shamir[14] in 1985, but it was later described as a necessity from the design criteria of DES, and nobody knew to point out whether it weakens DES. This specific entry, which is the most linear entry of all the S boxes of DES, is actually one of the three entries used in Matsui's attack.

Matsui's solution was to find a statistical linear expression consisting of a parity of subsets of the plaintext, ciphertext and the key, which is derived from similar expressions of the various rounds. Thus, the parity of some set of data bits in each round is known as a function of the parity of the previous set of bits in the previous round and the parity of several key bits. The round-linearization is based on the linearization of the S boxes. If we would XOR the same value to the two halves of the data, we would remain with the same parity as before the XOR. Since the subset of the input bits is statistically linear/affine to the subset of the output bits, the parity of the data after the XOR is usually the parity before the XOR XORed with a particular key-dependent constant.

The probability that the approximation in an S box is valid is given as the distance from half; for example the probability of the above entry with value -20 is $p' = 12/64 = 1/2 - 20/64$. An entry with value 0 has probability $p' = 1/2$; such an entry is useless to attack an cryptosystem. Any other non-zero value (either positive or negative) can be used in attacks. An approximation may involve more than one S box. We will follow Coppersmith[4] and call the S boxes involved in the linearization *active* S boxes. The probability of an approximation with two active S boxes is $p'_1 \cdot p'_2 + (1 - p'_1) \cdot (1 - p'_2)$, since the parity is even if either both parities of the approximations of the two S boxes are zero, or both are one. For simplicity we denote the probabilities with the notation p_i by their distance from half $p'_i = 1/2 + p_i$. Then, the combined probability is $1/2 + p = 1/2 + 2 \cdot p_1 \cdot p_2$. In general, if an approximation consists of l S boxes, the combined probability is $1/2 + p = 1/2 + 2^{l-1} \cdot \prod_{i=1}^{l} p_i$.

When a linear approximation with probability $1/2 + p$ is known to the attacker, he can mount an attack which requires about p^{-2} known plaintexts; these plaintexts can be randomly chosen, but all of them must be encrypted under the same key, and the ciphertexts should be known to the attacker as well.

The basic method of linear cryptanalysis finds only one bit of the key, which is a parity of a subset of the key bits. Auxiliary techniques of reducing the number of rounds of the approximations, by eliminating the first and/or last rounds, and counting on all the key bits affecting the data at the rounds not in the approximation can reduce the number of plaintexts required, and increase the number of key bits that the attack finds.

3 A Study of Linear Cryptanalysis

Before we formalize the linear approximations by defining characteristics, we feel it is very important to mention that the bits we set in the characteristics are *not* the actual values of bits (or bit-differences as in differential cryptanalysis); the bits we set denote the subset of bits whose parity is approximated. The expected parity itself is not directly denoted; however, the reader can easily identify the expected parity from the probability of the characteristic: if the probability is more than half, the expected parity is zero, and if the probability is less than half, the expected parity is one.

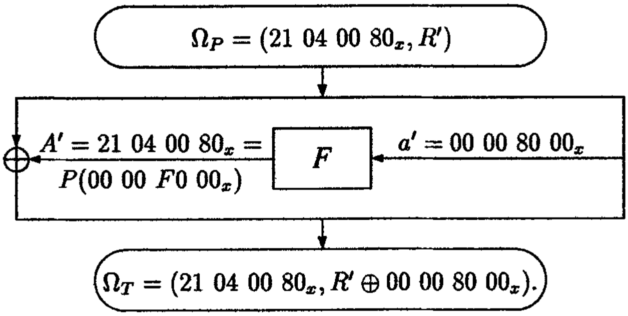
Another very important topic is the key space used in the analysis of linear cryptanalysis. There is a difference between the key space of the analyzed cryptosystem and the key space that the attack can handle. In differential cryptanalysis it was mentioned that the attacks assume that independent keys are used. The independent keys were defined as follows[1]:

Definition 1 An *independent key* is a list of subkeys which is not necessarily derivable from some key via the key scheduling algorithm.

Each key in the cryptosystem's key space has an equivalent independent key derived by the key scheduling algorithm. We observe that linear cryptanalysis also assumes the use of independent keys. The theoretical analysis of systems with dependent keys are much harder. However, in practice it can be very well estimated by the analysis of the independent key variants. Therefore, Matsui's method to find 14 bits of the subkeys still hold even if independent keys are used. Other auxiliary methods can then be used to find the other bits of the first and the last subkeys (possibly using additional characteristics), and to reduce the cryptosystem to a cryptosystem with a smaller number of rounds, which is easier to analyze.

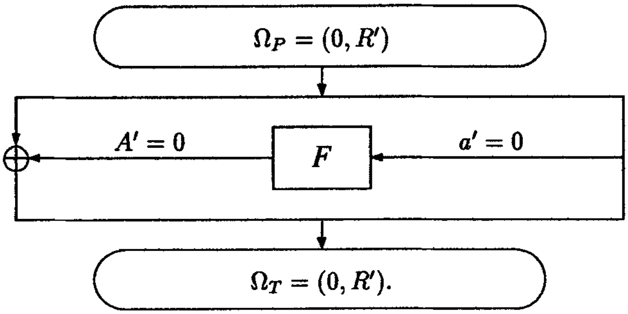
Definition 2 A *one-round characteristic* is a tuple $(\Omega_P, \Omega_T, \Omega_K, 1/2+p)$, in which $(\Omega_P)_L = (\Omega_T)_L = A$, $(\Omega_P)_R \oplus (\Omega_T)_R = a$, and in which $1/2+p$ is the probability that a random input block P, and its one-round encryption C under a random subkey K satisfies $P \cdot \Omega_P \oplus C \cdot \Omega_T \oplus K \cdot \Omega_K = 0$, where '$\cdot$' denotes binary scalar product of two binary vectors, Ω_P is the subset of bits of the data before the round, Ω_T is the subset of bits of the data after the round, and Ω_K is the subset of bits of the key whose parity is approximated.

As in differential cryptanalysis, it is quite easy to derive one-round characteristics with one active S box: we only have to choose a non-zero entry in one of the S boxes, and choose the subsets Ω_P, Ω_T, Ω_K as the round-function requires. The following one-round characteristic has only one active S box, and it was chosen to maximize the probability, thus it uses the maximal entry in S5:


$\Omega_P = (21\ 04\ 00\ 80_x, R')$
$A' = 21\ 04\ 00\ 80_x =$
$P(00\ 00\ F0\ 00_x)$
F
$a' = 00\ 00\ 80\ 00_x$
$\Omega_T = (21\ 04\ 00\ 80_x, R' \oplus 00\ 00\ 80\ 00_x).$

with probability $1/2 - 20/64$
one affected key bit

The best one-round characteristic does not have any active S box. This characteristic has probability 1:



with probability 1
no affected key bits

We can also derive one-round characteristics with more than one active S boxes: in this case we should choose the entries in two or more S boxes. However, unlike in differential cryptanalysis, we do not need to have the same values in common input bits of both S boxes (due to the E expansion), so if we affect bits common to two S boxes, it is not necessary that both S boxes would be active. Moreover, if both S boxes are active, the value of the common input bits becomes the XOR of their values from both S boxes, since we use the same bit twice in a linear equation, and thus it cancels itself. Note that in theory, the probability we receive in that way is the average between all the possible random keys. In practice, in DES the probability holds for all the keys, due to the design rules of the S boxes[4].

We can also concatenate characteristics (and define n-round characteristics recursively):

Definition 3 An n-round characteristic $\Omega^1 = (\Omega^1_P, \Omega^1_T, \Omega^1_K, 1/2 + p_1)$ *can be concatenated with* an m-round characteristic $\Omega^2 = (\Omega^2_P, \Omega^2_T, \Omega^2_K, 1/2 + p_2)$ if Ω^1_T equals the swapped value of the two halves of Ω^2_P. The *concatenation* of the characteristics Ω^1 and Ω^2 (if they can be concatenated) is the $(n+m)$-round characteristic $\Omega = (\Omega^1_P, \Omega^2_T, \Omega^1_K \oplus \Omega^2_K, 1/2 + 2 \cdot p_1 \cdot p_2)$.

When we concatenate l characteristics (that can be concatenated) the probability of the resultant characteristic is $1/2 + p = 1/2 + 2^{l-1} \cdot \prod_{i=1}^{l} p_i$.

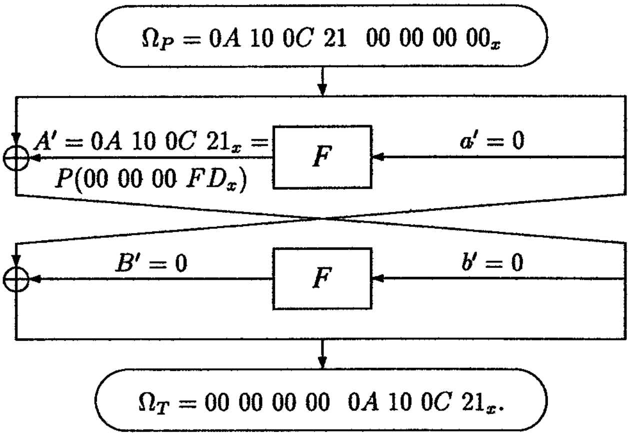
A strange situation occurs for n-round characteristics: Whenever an XOR operation exists in the cryptosystem (excluding XORs with subkeys within the F-function), the values of both its arguments in the characteristic must be the same, and this value is also the output of the "XOR operation". Whenever the data is duplicated (when the right half of the data is input to the F-function and also becomes the left half of the next round), both "duplicated" outputs may not be the same as the input, only their XOR value should be the same as the input. This phenomena is just the opposite to the usual operations in the cryptosystem, where an XOR operation XORs the inputs and duplications duplicates the input; in our case, an XOR operation duplicates the input, and duplications XOR the input with one of the original outputs to form the second output. This phenomena causes a basic difference between linear cryptanalysis and differential cryptanalysis, which can be easily viewed in the one-round characteristic with probability 1: the free variable in the linear cryptanalysis characteristic is at the right half, while in differential cryptanalysis it is at the left half.

This phenomena is easily understood when we remind the meaning of the values in the characteristics: they are not actual values, neither XORs of actual values; They only describe the subset of bits whose parity is statistically known. In order to know the parity of bits of the output of an XOR operation, we should know the parities of the same subsets of bits both inputs, and then we known the parity of the same subset of the output.

When we duplicate the data, we may know parity of a subset of bits. However, since we do not wish to use these bits twice (in which case one use will cancel the other use by the parity), we should use each set bit once, either in one output or in the other output. It is also possible to use a bit which is not set in the input to the duplication, in which case a zero bit become one in both outputs. In this case, both usages cancel each other by their parity, and thus the same effect as of the original zero remains.

An important difference between linear cryptanalysis and differential cryptanalysis is the ability to use differentials[6,7], in which only the values of Ω_P and Ω_T matter. In differential cryptanalysis, whenever several characteristics have the same values for Ω_P and Ω_T, they are developed on top of each other: they can be viewed as one differential, and their internal information can be ignored. In linear cryptanalysis, the internal information contains the information about the subset of key bits participating in the linearization. Thus, if two characteristics with the same values of Ω_P and Ω_T and with a similar probability exist, they might cancel the effect of each other if the parity of the subset of the key bits is not the same (or if their probabilities are the complement of each other and the parity of the subset of their key bits is the same). Therefore, we should be much more careful when we claim for linear cryptanalysis' characteristics. However, if the attacker knows of all the different characteristics whose effect might be canceled, he can find one (parity) bit of the key whenever he identifies that the effect is canceled.

Davies[5] investigated an attack against DES based on the non-uniform distribution of the outputs of pairs of adjacent S boxes, when their inputs are uniformly distributed. He assumes the uniform distribution in the inputs to the even rounds (or alternatively the odd rounds), and studies the resultant distribution in the outputs of these rounds. As a result, he receives a key-dependent distribution, which depends on the parity of several key bits. Using a large sample of known plaintexts, he can find this bit. His algorithm can be applied to any pair of adjacent S boxes, and to even or odd rounds, thus he can find up to 16 potential parity bits of the key. His attack is strongly related to linear cryptanalysis[1], and has a linear cryptanalysis variant. In the even rounds (odd rounds) the characteristics have zero values in the input and non-zero values in the outputs, since the inputs are not involved in the linearization, but the output are involved. In the other rounds, both inputs and outputs have zero values. Thus, we receive the following two-round iterative characteristic for the S boxes S7/S8 (and similar characteristics for other adjacent S boxes):


$\Omega_P = 0A\ 10\ 0C\ 21\ \ 00\ 00\ 00\ 00_x$
$A' = 0A\ 10\ 0C\ 21_x =$
$P(00\ 00\ 00\ FD_x)$
F
$a' = 0$
$B' = 0$
F
$b' = 0$
$\Omega_T = 00\ 00\ 00\ 00\ \ 0A\ 10\ 0C\ 21_x.$

with probability 1/2 − 3/64
four affected key bits

always
no affected key bits

Each of the S boxes has a linear approximation between the two common bits to a subset of the four output bits. In S7: $03_x \rightarrow F_x$ with probability $1/2 + 8/64$ and in S8: $30_x \rightarrow D_x$ with probability $1/2 - 12/64$. The total probabilities of these characteristics iterated to 16 rounds and the required number of known plaintexts for the attack based on linear cryptanalysis are given in Table 2, along with the number of known plaintexts required for the original Davies' attacks based on the same pairs of S boxes[2]. Notice that the results of these two attacks are very similar.

S boxes	Probability	Known Plaintexts	Davies' Attack
S1–S2	$1/2 + 2^{-33}$	2^{66}	2^{66}
S2–S3	$1/2 + 2^{-36}$	2^{73}	2^{69}
S3–S4	$1/2 + 2^{-44}$	2^{89}	2^{86}
S4–S5	$1/2 + 2^{-36}$	2^{73}	2^{71}
S5–S6	$1/2 + 2^{-36}$	2^{73}	2^{72}
S6–S7	$1/2 + 2^{-33}$	2^{66}	2^{66}
S7–S8	$1/2 + 2^{-28}$	2^{57}	2^{57}
S8–S1	$1/2 + 2^{-40}$	2^{79}	2^{77}

Table 2. Results of Linear Cryptanalysis of DES using Davies' Characteristics.

[1] Davies studies the overall distribution of the output bits of the S boxes, while linear cryptanalysis studies only the parity of these bits. Thus, Davies' attack is not a special case of linear cryptanalysis.

[2] The number of known plaintexts required for Davies' attack were calculated using the equations given in [5].

4 Constraints on the Size of the S Boxes

In this section we show new constraints on the size of S boxes. Researchers have already studied the differential behavior of the size of S boxes. For example, Luke O'connor[12,13] analyzed the differential behavior of bijective S boxes and of composite S boxes, and concluded that for large enough S boxes, even random S boxes are immune against differential cryptanalysis. However, there was no result on required relationships between the input size of the S boxes and their output size. In this section we show such a relationship.

In differential cryptanalysis we can easily reduce the probability of all the entries in the difference distribution tables of the S boxes by increasing the number of output bits of the S boxes. Whenever the number of output bits of an S box is (sufficiently) larger than the number of its input bits, it is very likely that the entries in the difference distribution table will have only values 0 and 2; thus all the possible entries have the same low probability.

Examples of cryptosystems which use such S boxes are Khufu and Khafre[10]. The attack on Khafre[3,1] used exactly these properties, but still it used the specific structure of Khafre.

Linear cryptanalysis adds a new criteria for this relationship. We identified that whenever the number of output bits is large enough, there *must* be linear and affine relations between these bits, which hold for all the possible inputs of the S box. Denote the number of input bits by m, and the number of output bits by n. We can now describe the S box by a binary matrix $\mathcal{M}$ with 2^m rows, corresponding to the 2^m inputs of the S box, and with $m+n$ columns, which contain the input values themselves (in the first m columns), and the output values of the S box (in the other n columns).

Each column of $\mathcal{M}$ contains one bit from each input/output pair of the S box. Linear combinations of subsets of the input/output bits of the S box are represented by linear combinations of the columns. We say that a subset of bits of the input and output of the S box form a linear combination if for all inputs the linear combination of these bits is zero. We say that a subset of bits of the input and output of the S box form an affine combination if for all inputs the linear combination of these bits is a constant (either all zero, or all one). Equivalently, a subset of the bits of the input and output of the S box form a linear combination if the columns of $\mathcal{M}$ are linearly dependent, and a subset of the bits of the input and output of the S box form an affine combination if the columns of $\mathcal{M}$ and the all one vector are linearly dependent.

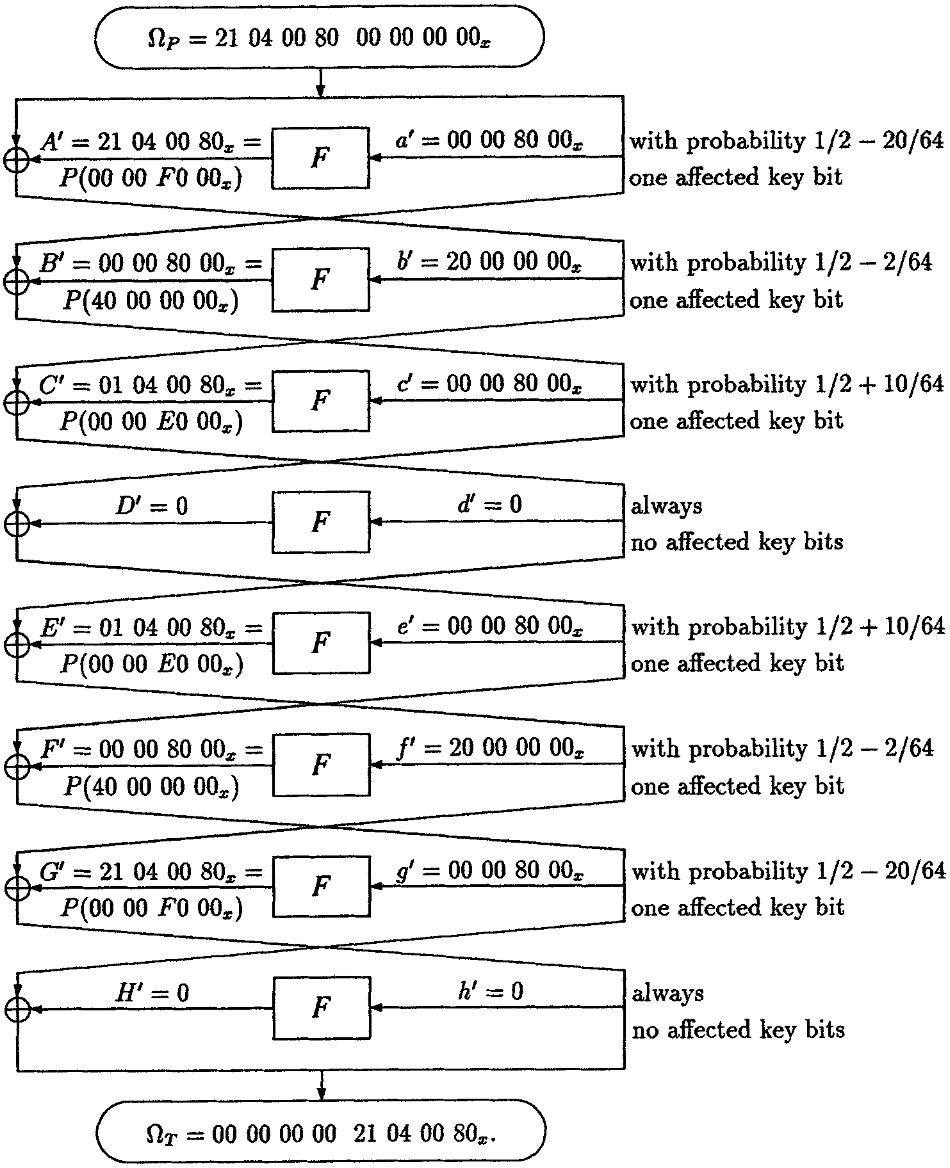
Define $\mathcal{M}'$ to be the matrix formed by $\mathcal{M}$ with one additional column with all the values ones: $\mathcal{M}' = [\mathcal{M}|1]$. Thus, if the rank of $\mathcal{M}$ equals the number of its columns $m+n$, there are no linear combinations in the S box, and if the rank of $\mathcal{M}'$ equals the number of its columns $m+n+1$, there are no affine combinations in the S box. The S box has an affine combination of its input and output bits if $\text{rank}(\mathcal{M}') < m+n+1$.

Since the number of rows of $\mathcal{M}$ and $\mathcal{M}'$ is 2^m, the maximal rank is 2^m. Therefore, if $n \geq 2^m - m$ the S box *must* have an affine combination of the input/output bits. These affine combinations cause entries with probability $1/2 \pm 1/2$ in the linear approximation table, which can be a major threat to the security of the cryptosystem. Similarly, if $n \geq 2^m$ the S box must have an affine combination of a subset of *only* output bits, which does not depend on the input bits at all! Such combinations cause (in many cases of DES-like cryptosystems) the existence of a two-round iterative characteristic with probability 1/2 ± 1/2 (of the form $0 \rightarrow X$), and thus enable attacks which require only a few known plaintexts!

These affine combinations also hold as affine combinations of the bits of the differences predicted in differential cryptanalysis. We do not know whether in differential cryptanalysis these linearities also pose a major threat.

5 Application to DES

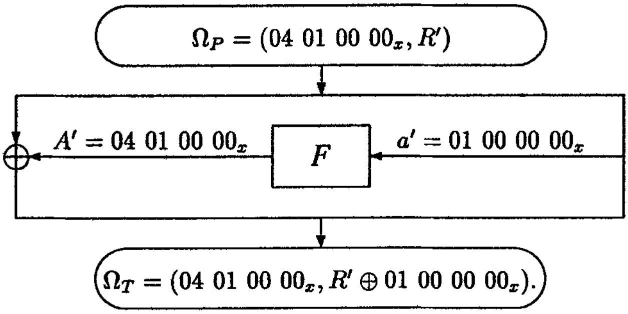
Matsui's 16-round linear approximation can be viewed as a 16-round characteristic. This characteristic is based on the following eight-round iterative characteristic:


$\Omega_P = 21\ 04\ 00\ 80\ \ 00\ 00\ 00\ 00_x$
$A' = 21\ 04\ 00\ 80_x = P(00\ 00\ F0\ 00_x)$
F
$a' = 00\ 00\ 80\ 00_x$
with probability 1/2 − 20/64
one affected key bit
$B' = 00\ 00\ 80\ 00_x = P(40\ 00\ 00\ 00_x)$
F
$b' = 20\ 00\ 00\ 00_x$
with probability 1/2 − 2/64
one affected key bit
$C' = 01\ 04\ 00\ 80_x = P(00\ 00\ E0\ 00_x)$
F
$c' = 00\ 00\ 80\ 00_x$
with probability 1/2 + 10/64
one affected key bit
$D' = 0$
F
$d' = 0$
always
no affected key bits
$E' = 01\ 04\ 00\ 80_x = P(00\ 00\ E0\ 00_x)$
F
$e' = 00\ 00\ 80\ 00_x$
with probability 1/2 + 10/64
one affected key bit
$F' = 00\ 00\ 80\ 00_x = P(40\ 00\ 00\ 00_x)$
F
$f' = 20\ 00\ 00\ 00_x$
with probability 1/2 − 2/64
one affected key bit
$G' = 21\ 04\ 00\ 80_x = P(00\ 00\ F0\ 00_x)$
F
$g' = 00\ 00\ 80\ 00_x$
with probability 1/2 − 20/64
one affected key bit
$H' = 0$
F
$h' = 0$
always
no affected key bits
$\Omega_T = 00\ 00\ 00\ 00\ \ 21\ 04\ 00\ 80_x.$

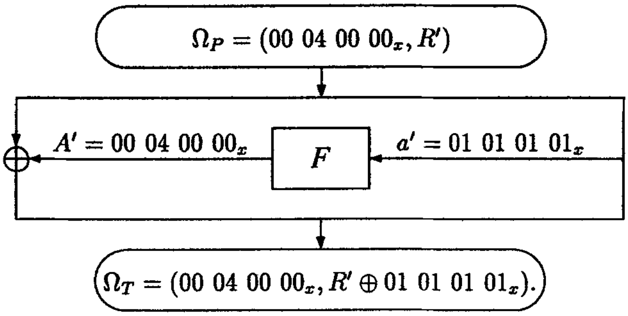
This characteristic has probability about $1/2 + 2^{-27}$. By iterating it to 16 rounds and replacing the first and last rounds by locally better ones, Matsui got a 16-round characteristic with probability about $1/2 + 2^{-24}$. We have exhaustively verified that this iterative characteristic is the best among all the characteristics with at most one active S box at each round, and that Matsui's 16-round characteristic is the best characteristics under the same restriction (Matsui claims that his characteristic is the best without any restriction).

6 Application to Feal

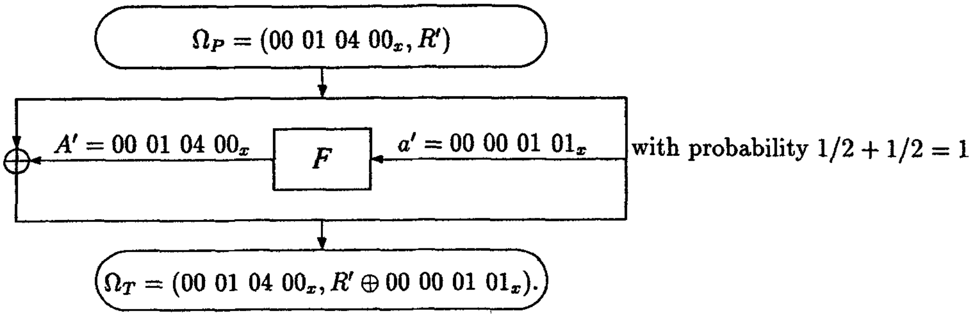
In [8] Matsui described a preliminary version of linear cryptanalysis and used it to attack Feal[15,11]. For Feal there are 15 (non-trivial) one-round characteristics with probability $1/2 \pm 1/2$, based on the linearity of the least significant bits in the addition operation (a similar effect occurs also in differential cryptanalysis of Feal, in which characteristics with probability 1 are based on the elimination of the carry from the most significant bit). The Four basic one-round characteristics with probability $1/2 \pm 1/2$ are:


$\Omega_P = (04\ 01\ 00\ 00_x, R')$
$A' = 04\ 01\ 00\ 00_x$
F
$a' = 01\ 00\ 00\ 00_x$
$\Omega_T = (04\ 01\ 00\ 00_x, R' \oplus 01\ 00\ 00\ 00_x)$.

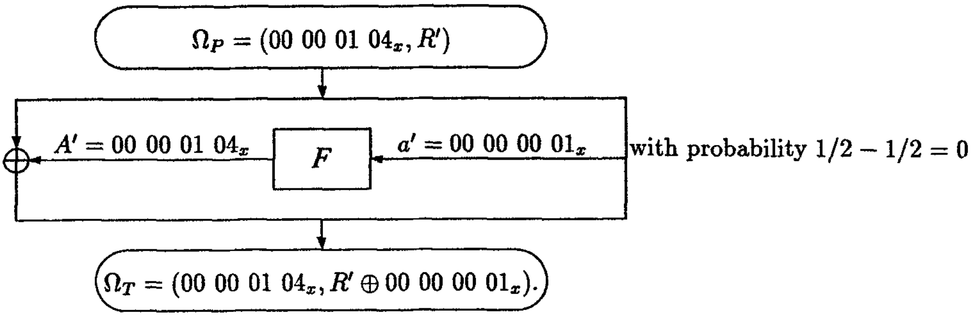
with probability $1/2 + 1/2 = 1$


$\Omega_P = (00\ 04\ 00\ 00_x, R')$
$A' = 00\ 04\ 00\ 00_x$
F
$a' = 01\ 01\ 01\ 01_x$
$\Omega_T = (00\ 04\ 00\ 00_x, R' \oplus 01\ 01\ 01\ 01_x)$.

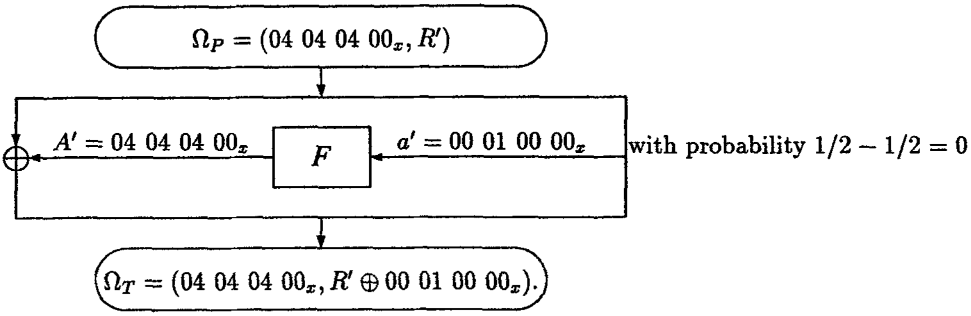
with probability $1/2 - 1/2 = 0$


$\Omega_P = (00\ 01\ 04\ 00_x, R')$
$A' = 00\ 01\ 04\ 00_x$
F
$a' = 00\ 00\ 01\ 01_x$
with probability $1/2 + 1/2 = 1$
$\Omega_T = (00\ 01\ 04\ 00_x, R' \oplus 00\ 00\ 01\ 01_x)$.

and

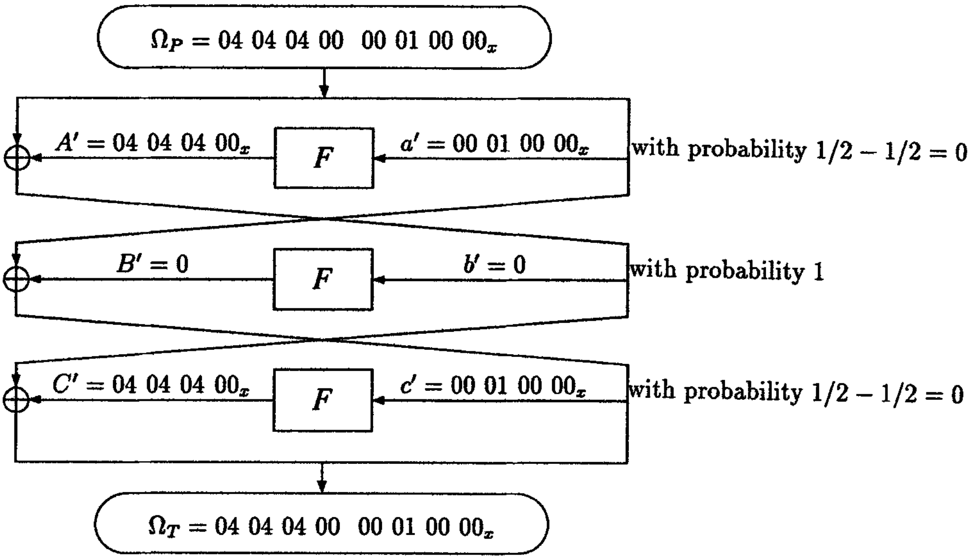

$\Omega_P = (00\ 00\ 01\ 04_x, R')$
$A' = 00\ 00\ 01\ 04_x$
F
$a' = 00\ 00\ 00\ 01_x$
with probability $1/2 - 1/2 = 0$
$\Omega_T = (00\ 00\ 01\ 04_x, R' \oplus 00\ 00\ 00\ 01_x)$.

The other 11 one-round characteristics with probability $1/2 \pm 1/2$ can be derived by combining any number of these four characteristics by XORing the values of their a' into the new a' and XORing the values of their A' into the new A'. For example, the following characteristics results from a combination of the first three of the above four characteristics:

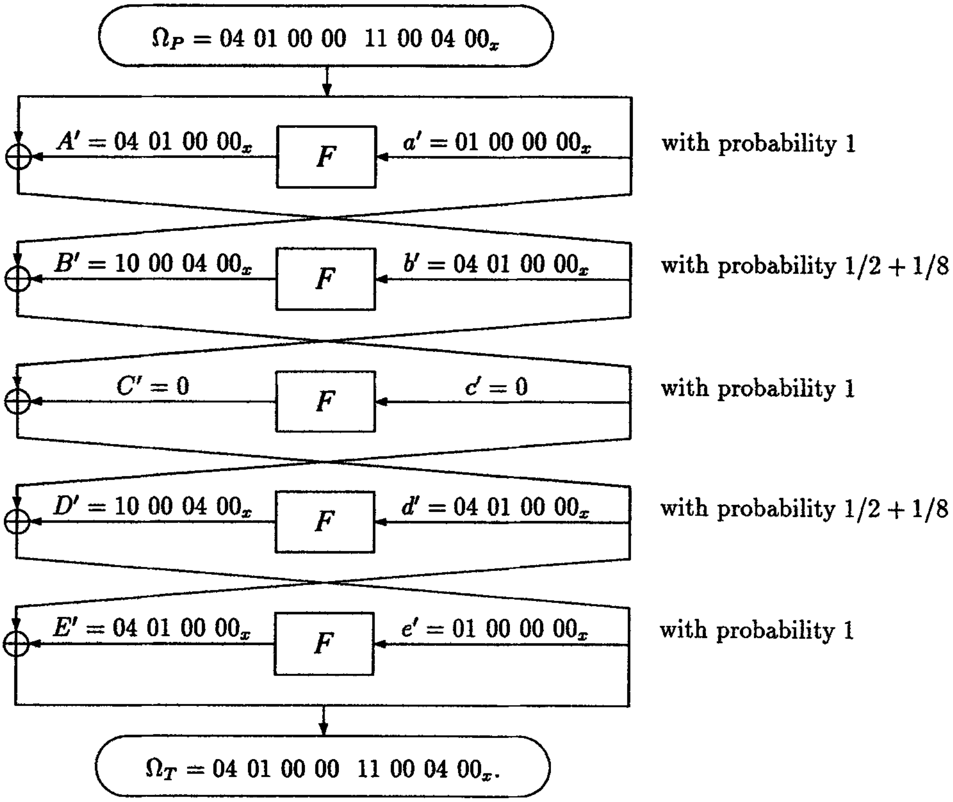

$\Omega_P = (04\ 04\ 04\ 00_x, R')$
$A' = 04\ 04\ 04\ 00_x$
F
$a' = 00\ 01\ 00\ 00_x$
with probability $1/2 - 1/2 = 0$
$\Omega_T = (04\ 04\ 04\ 00_x, R' \oplus 00\ 01\ 00\ 00_x)$.

These combinations are valid since no S box is active in two or more of the original characteristics. Such combinations are also applicable in differential cryptanalysis, whenever they do not involve the same S box active in more than one characteristic. We have also found several additional linear characteristics of Feal with smaller probabilities, among them at least eight one-round characteristics with probability $1/2 \pm 1/4$.

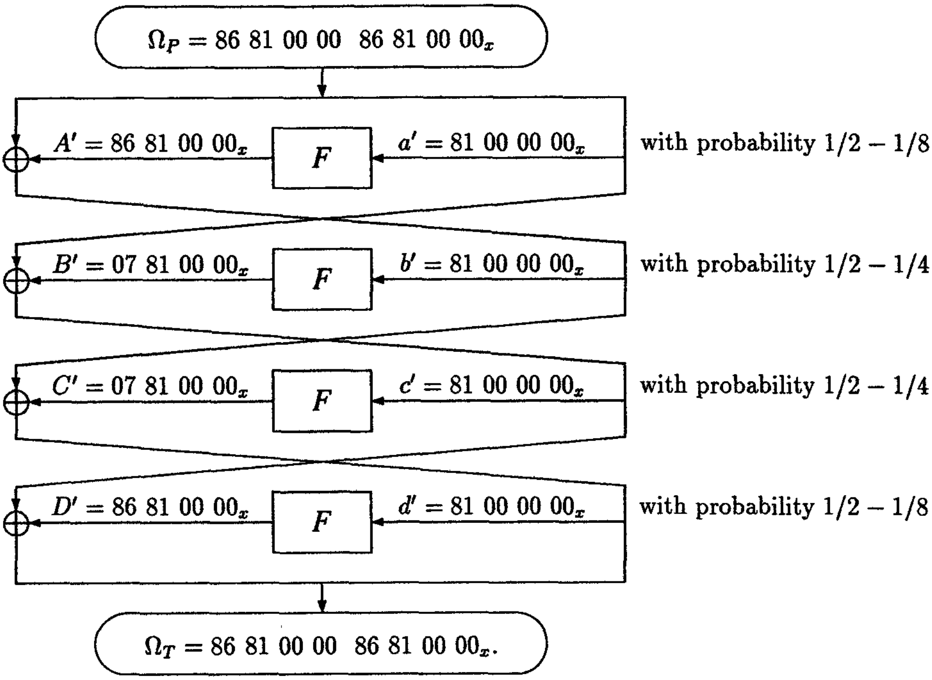
In his attack[8] Matsui uses linearities which can be formalized by the following three-round characteristic with probability 1:


$\Omega_P = 04\ 04\ 04\ 00\ \ 00\ 01\ 00\ 00_x$
$A' = 04\ 04\ 04\ 00_x$
F
$a' = 00\ 01\ 00\ 00_x$
with probability $1/2 - 1/2 = 0$
$B' = 0$
F
$b' = 0$
with probability 1
$C' = 04\ 04\ 04\ 00_x$
F
$c' = 00\ 01\ 00\ 00_x$
with probability $1/2 - 1/2 = 0$
$\Omega_T = 04\ 04\ 04\ 00\ \ 00\ 01\ 00\ 00_x$

In his attack he sets this characteristic in rounds 3–5 and tries exhaustively values of bits of the subkeys in rounds 1–2 and 6–8, with some auxiliary techniques. We have found two five-round characteristic with probability $1/2 + 1/32$. One of them is:



We have found several iterative characteristics of Feal, which can be used to attack Feal-8 using about 2^{24} known plaintexts with a smaller computation complexity. This is a much better tradeoff than in Matsui's attacks on Feal-8, which required either 2^{28} known plaintexts, for which the complexity of the analysis is 2^{50}, or 2^{15} known plaintexts, for which the complexity of the analysis is 2^{64}. One of these iterative characteristics is:


$\Omega_P = 86\ 81\ 00\ 00\ \ 86\ 81\ 00\ 00_x$
$A' = 86\ 81\ 00\ 00_x$
F
$a' = 81\ 00\ 00\ 00_x$
with probability 1/2 – 1/8
$B' = 07\ 81\ 00\ 00_x$
F
$b' = 81\ 00\ 00\ 00_x$
with probability 1/2 – 1/4
$C' = 07\ 81\ 00\ 00_x$
F
$c' = 81\ 00\ 00\ 00_x$
with probability 1/2 – 1/4
$D' = 86\ 81\ 00\ 00_x$
F
$d' = 81\ 00\ 00\ 00_x$
with probability 1/2 – 1/8
$\Omega_T = 86\ 81\ 00\ 00\ \ 86\ 81\ 00\ 00_x.$

The iteration of this characteristic to seven rounds have probability $1/2 - 2^{-11}$. A similar characteristic exist with a reverse order of the bytes in each word. From the tables in [9] we can see that about $4 \cdot 2^{11 \cdot 2} = 2^{24}$ known plaintexts are required to attack Feal-8, with success rate about 78% and that 2^{25} known plaintexts are required for success rate about 97%. This characteristic can be used to attack Feal-N with up to 20 rounds, with a complexity (and known plaintexts) smaller than of exhaustive search. The attack on Feal-8 was applied successfully on a personal computer. It takes about 10 minutes to encrypt the 2^{24} required known plaintexts and to find the key.

7 Summary

In this paper we studied Matsui's linear cryptanalysis. We showed that the formalism of differential cryptanalysis can be adopted to linear cryptanalysis. In particular, we showed that characteristics can be defined, concatenated, and used in a very similar manner as in differential cryptanalysis. Constraints on the size of S boxes were described. Matsui's characteristic used to attack DES in his paper is shown to be the best characteristic which has only up to one active S box at each round; on the other hand, we improved his results on Feal. We attack Feal-8 using 2^{24} known plaintexts with linear cryptanalysis. Davies' attack on DES[5] was shown to be closely related to linear cryptanalysis. We also described how to sum up characteristics (which also hold in differential cryptanalysis).

8 Acknowledgments

Acknowledgment: This research was supported by the fund for the promotion of research at the Technion. Some of the results in this paper were found using variants of programs, whose originals were written by Ishai Ben-Aroya.

References

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

[2] Eli Biham, Adi Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, Vol. 4, No. 1, pp. 3–72, 1991.

[3] Eli Biham, Adi Shamir, *Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer*, technical report CS91-18, Department of Applied Mathematics and Computer Science, The Weizmann Institute of Science, 1991. The extended abstract appears in Lecture Notes in Computer Science, Advances in Cryptology, proceedings of CRYPTO'91, pp. 156–171, 1991.

[4] Don Coppersmith, *The Data Encryption Standard (DES) and its Strength Against Attacks*, technical report, IBM Thomas J. Watson Research Center, RC 18613 (81421), December 1992.

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

[6] Xuejia Lai, James L. Massey, Sean Murphy, *Markov Ciphers and Differential Cryptanalysis*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'91, pp. 17–38, 1991.

[7] Xuejia Lai, *On the Design and Security of Block Ciphers*, Ph.D. thesis, Swiss Federal Institue of Technology, Zurich, 1992.

[8] Mitsuru Matsui, Atsuhiro Yamagishi, *A New Method for Known Plaintext Attack of FEAL Cipher*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'92, pp. 81–91, 1992.

[9] M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Abstracts of EUROCRYPT'93, pp. W112–W123, May 1993.

[10] Ralph C. Merkle, *Fast Software Encryption Functions*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of CRYPTO'90, pp. 476–501, 1990.

[11] Shoji Miyaguchi, Akira Shiraishi, Akihiro Shimizu, *Fast Data Encryption Algorithm FEAL-8*, Review of electrical communications laboratories, Vol. 36, No. 4, pp. 433–437, 1988.

[12] Luke O'Connor, *On the Distribution of Characteristics in Bijective Mappings*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'93, to appear.

[13] Luke O'Connor, *On the Distribution of Characteristics in Composite Permutations*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of CRYPTO'93, to appear.

[14] Adi Shamir, *On the Security of DES*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of CRYPTO'85, pp. 280–281, 1985.

[15] Akihiro Shimizu, Shoji Miyaguchi, *Fast Data Encryption Algorithm FEAL*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'87, pp. 267–278, 1987.