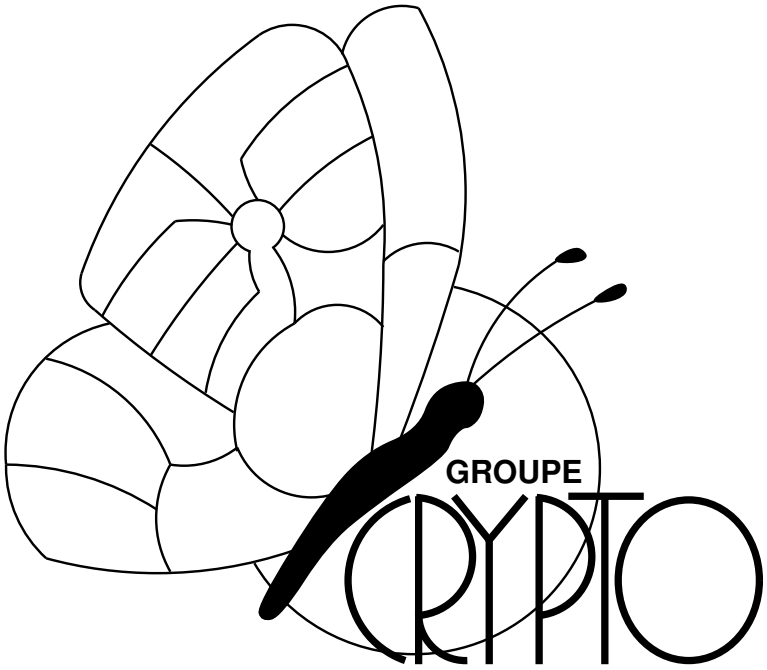
UCL
Université
catholique
de Louvain

REGARDS

UCL Crypto Group Technical Report Series

Cryptanalysis of Block Ciphers: A Survey

Francois-Xavier Standaert, Gilles Piret,
Jean-Jacques Quisquater



http://www.dice.ucl.ac.be/crypto/

Technical Report
CG–2003/2

Place du Levant 3
B-1348 Louvain-la-Neuve, Belgium

Phone: (+32) 10 472541
Fax: (+32) 10 472598

Cryptanalysis of Block Ciphers: A Survey

Francois-Xavier Standaert, Gilles Piret, Jean-Jacques Quisquater

UCL Crypto Group
Laboratoire de Microelectronique
Universite Catholique de Louvain
Place du Levant, 3, B-1348 Louvain-La-Neuve, Belgium
standaert,piret,quisquater@dice.ucl.ac.be

Abstract. This report summarizes readings in the area of the cryptanalysis of block ciphers. Historically, the academic field started in 1981 with the first CRYPTO conference and observations on some undesirable properties of the DES. Practically, most cryptanalytic techniques were developed in the 1990s. A number of them are variants of two decisive progresses in the field. Differential cryptanalysis was found by Biham and Shamir and presented at CRYPTO 90. Linear cryptanalysis was developed by Matsui and presented at EUROCRYPT 93. From these times plenty of papers tried to take advantage of these techniques in different attempts to break public ciphers and some of these papers introduced original improvements. These two techniques also led to the development of criteria for security evaluation of block ciphers. Recently designed block ciphers like the Advanced Encryption Standard Rijndael have been based on the idea of provable security against these two attacks and their improvements. This work tries to list and give an intuitive description of the most important cryptanalytic techniques published up to 2002. No technical details are given and the interested reader is referred to the bibliography if exhaustive information is requested.

Introduction

Cryptanalysis is a fast moving area of research and its most important results were presented during conferences. As a consequence, very few reports are dedicated to the presentation and survey of cryptanalytic results. Although this report is not complete and it could also be largely improved, it seemed to us that it could be a useful tool for students interested in the design and cryptanalysis of block ciphers.

Practically, the report is structured into different sections that present some of the most important cryptanalytic techniques published up to 2002. Sections are presented as reading notes as they practically result from the readings of different students and researchers in UCL Crypto Group. For every section, we tried to give an intuitive description of the attack, illustrate how it can be a threat for block ciphers security, give some examples of practical implementations and describe possible countermeasures. For these purposes, we assume that the reader is familiar with the basics of block cipher theory.

The different sections are (with no chronological significance):

1. Linear cryptanalysis.
2. Differential cryptanalysis.
3. Characteristics vs differentials, multiple approximations and key independence.
4. Extensions of differential and linear cryptanalysis:
   (a) Differential-linear cryptanalysis.
   (b) Non-linear cryptanalysis.
   (c) Chosen-plaintext linear cryptanalysis.
   (d) Partial or truncated differential.
   (e) Higher order differentials.
5. Miss in the middle attacks - impossible differentials.
6. Boomerang - rectangle attacks.
7. Interpolation attacks.
8. Square saturation - integral - multiset attacks.
9. Related key attacks.
10. Slide attacks - secret s-box cryptanalysis.
11. Complementation property attacks and weak keys.
12. Conclusion: future work in cryptanalysis.

Finally, the reader should be aware that this report is "just" reading notes. It probably includes mistakes and imprecisions. As a consequence, we would be grateful to any reader for sending comments, corrections, ... of the text.

1 Linear cryptanalysis

Introduction: In its basic version, linear cryptanalysis is a known plaintext attack that uses a linear relation between inputs and outputs of an encryption algorithm that holds with a certain probability. This approximation can be used to assign probabilities to the possible keys and locate the most probable one.

Analysis of components: The first part of a linear cryptanalysis is a systematic analysis of the components of the cipher. Usually, the only non-linear part of a block cipher is the substitution layer composed of a number of S-boxes. The basic idea is to approximate these boxes with an expression that is linear. Such an expression is of the form:

$$X_{i1} \oplus X_{i2} \oplus X_{i3} \oplus X_{i4} \oplus ... \oplus Y_{i1} \oplus Y_{i2} \oplus Y_{i3} \oplus Y_{i4} = 0 \quad (1)$$

Where X_i, Y_i respectively are the S-box inputs and outputs. For a n-bit input, m-bit output S-box, there are $(2^n - 1) \times (2^m - 1)$ possible linear approximations of the box. The cryptanalyst will investigate every possible linear approximations and the probabilities that these approximations hold. As S-boxes have 2^n possible inputs, if x is the number of times a linear approximation holds, the resulting probability is computed by $p = \frac{x}{2^n}$ and the corresponding *bias* is defined as $\epsilon = p - \frac{1}{2}$.

Combining the linear approximations through the cipher: Once linear approximations of the S-boxes have been found, the problem is to find a way to combine them so that a final approximation of the cipher only involves plaintext bits, ciphertext bits and key bits.
Such a combination will propagate a single linear approximation through the cipher, involving a number of S-boxes and therefore, a number of linear approximations. The following lemma allows deriving the probability of a linear approximation through several S-boxes.

Piling-Up Lemma: Let X_i be independent random variables of which the values are 0 with probability p_i and 1 with probability $1-p_i$. Then the probability that $X_1 \oplus X_2 \oplus X_3 \oplus X_4 \oplus ... \oplus X_n = 0$ is

$$\frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} (p_i - \frac{1}{2}) \tag{2}$$

If the number of active S-boxes (i.e. involved in the linear approximation of the cipher) is n, and the probability that these active S-boxes hold is p_i, we can easily derive the probability of a global linear approximation of the cipher. Equation (2) shows the importance of considering the *bias* of a linear approximation. We will see that the bigger the bias is, the better the attack works.

The attack: If R is the number of rounds of the algorithm, linear cryptanalysis needs a $R-1$ rounds linear approximation of the cipher. Then, only some bits of K_R are needed to expand the linear approximation to R rounds, corresponding to the "active" boxes of round $R-1$; let us denote these bits by k_R. The linear approximation used can thus be written as:

$$X[i_1, ..., i_m] \oplus F^{-1}(Y, k_R)[j_1, ..., j_n] = K[l_1, ..., l_p] \tag{3}$$

where X represents the plaintext, Y the ciphertext, and K the key. $X[i_1, ..., i_m]$ denotes the sum of bits i_1, ..., i_m of X. For example, $X[i_1, ..., i_m] := X_{i_1} \oplus ... \oplus X_{i_m}$.

We implement this last round for every possible k_R. Then for each key candidate k_R^i, let T_i be the number of plaintexts such that the linear approximation of the cipher holds, T_{max} the maximal T_i, T_{min} the minimum T_i and N the number of computed plaintexts.

1. If $|T_{max} - \frac{N}{2}| > |T_{min} - \frac{N}{2}|$, then adopt the key candidate corresponding to T_{max}.
2. If $|T_{max} - \frac{N}{2}| < |T_{min} - \frac{N}{2}|$, then adopt the key candidate corresponding to T_{min}.

If enough plaintexts are computed, we will probably recover k_R. As the linear approximation involves plaintext bits, ciphertext bits and key bits, an additional XOR relation between key bits can be obtained.

Key guess: The procedure to expand a $r-1$ approximations to r rounds by trying all possible keys involved in this expansion is called key guess and is often used in cryptanalysis. We can usually guess the key on the first and last rounds but sometimes also on the second and $r-1$ ones.

Complexity of the attack: Let ϵ represent the bias corresponding to the probability that the linear expression for the cipher holds. In his paper, Matsui shows that the number of known plaintexts required in the attack (let us denote it by N) is proportional to ϵ^{-2}, so it is reasonable to approximate N by

$$N \simeq \frac{1}{\epsilon^2} \tag{4}$$

The probability of success of the attack (i.e. the probability that the key recovered is indeed the right one) increases with the number N of plaintexts considered. In practice, it is generally reasonable to expect some small multiple of ϵ^{-2} known plaintexts are required.

Countermeasures: The effectiveness of linear cryptanalysis depends on the probability that a global approximation of a cipher holds. Therefore, to provide resistance against linear cryptanalysis:

1. The bias of the linear approximations of the single S-boxes or other possible non-linear elements in the cipher must be as low as possible.
2. The number of active S-boxes or other non-linear elements in any approximation of the cipher must be as high as possible. In this respect the diffusion layer plays an important role.

It is important to note that resistance against linear cryptanalysis gives no proofs of security because similar attacks could be imagined using other approximations of the cipher (higher order approximations for example). Other attacks could also be imagined.

2 Differential cryptanalysis

Introduction: In its basic version, differential cryptanalysis is a method that analyses the effect of particular differences in plaintext pairs on the difference of the resultant ciphertexts. These differences can be used to assign probabilities to the possible keys and to locate the most probable key.

Analysis of components: The first part of a differential cryptanalysis is a systematic analysis of the components of the cipher. Usually, the only non-linear part of a block cipher is the substitution layer composed of a number of S-boxes. Linear transformations like bit permutations or key additions only affect differences between 2 texts in a deterministic and bijective way. On the other hand, for a non-linear S-box, knowledge of the input difference of a pair cannot guarantee knowledge of its output difference. However, every input difference of

a substitution box suggests a probabilistic distribution of the possible output differences.
For a n-bit input, m-bit output S-box, there are 2^n possible input difference and for every possible input difference, 2^m output differences are a priori possible. The cryptanalyst will investigate every possible input difference and compute the number of occurrences of every output difference. We define a S-box differential as a pair:

$$\Delta X \xrightarrow{p} \Delta Y \tag{5}$$

which means that an input difference ΔX causes an output difference ΔY with probability p. One can tabulate the complete data for a S-box in a difference distribution table.

Constructing differential characteristics: Once the differential information has been compiled for the non-linear components of the cipher, we have the data to proceed with the determinations of a useful differential characteristic of the overall cipher. Such a differential characteristic combines single S-boxes differentials and finally involves plaintext and ciphertext bits only.

Probability that the differential characteristic holds: Assuming that occurrences of pairs of input and output differences in active S-boxes are independent from each other, the differential characteristic probability is given by:

$$\prod_{i=1}^{n} p_i \tag{6}$$

where n is the number of active S-boxes and p_i the probability of the difference propagation in S-box i.

The attack: If R is the number of rounds of the algorithm, differential cryptanalysis needs a $R-1$ rounds differential characteristic of the cipher with a suitably large enough probability. Let K_R denote the key involved in the last round. Typically, only some bits of K_R are needed to expand the differential characteristic to R rounds, corresponding to the "active" S-boxes of round R; let us denote these bits by k_R. If we implement this last round for every possible k_R, and count the number of occurrences of our differential characteristic for every k_R, after a sufficient number of plaintext pairs the correct one can be distinguished.

Complexity of the attack: We denote the plaintext difference of a characteristic by Ω_P and the corresponding difference after $R-1$ rounds by Ω_C. Any pair of plaintexts with a plaintext difference of Ω_P and a difference of data after round $R-1$ of Ω_C is called a right pair. It can be shown that the number of chosen plaintext pairs required to distinguish right pairs when trying subkey candidates is

$$\frac{c}{p} \tag{7}$$

Where p is the characteristic's probability for the $R-1$ rounds and c is a small constant.

Signal to noise ratio: The attack effectiveness can be evaluated independently from the number of plaintext pairs by computing S/N. If we are looking for k key bits, then we count the number of occurrences of 2^k possible key values in 2^k counters. The counters contain an average count of $\frac{m.\alpha.\beta}{2^k}$ counts where m is the number of pairs, α is the average number of keys suggested by each pair of plaintext and β is the ratio of non-discarded pairs to all pairs. The right key value is counted about $m.p$ times using the right pairs where p is the characteristic probability. The signal to noise ratio of a counting scheme is therefore:

$$S/N = \frac{m.p}{m.\alpha.\frac{\beta}{2^k}} = \frac{2^k.p}{\alpha.\beta} \tag{8}$$

If $S/N \leq 1$, then a differential attack will not succeed.

Countermeasures: The effectiveness of differential cryptanalysis depends on the probability that a differential characteristic of a cipher holds. Therefore, to provide resistance against differential cryptanalysis:

1. The difference propagations inside the single S-boxes or other possible non-linear elements in the cipher have to be as low-probable as possible.
2. The number of active S-boxes or other non-linear elements in any differential characteristic of the cipher must be as high as possible.

It is important to notice that resistance against differential cryptanalysis gives no proofs of security because similar attacks could be imagined using other characteristics (higher order for truncated differentials for example). Other attacks could also be imagined.

3 Characteristics vs differentials, multiple approximations and key independence

Introduction: Predictions of linear and differential cryptanalysis are done using approximations for which the probability is hard to evaluate.

Characteristics vs differentials: In a differential characteristic, only the plaintext difference ΔP and the last ciphertext difference ΔC are relevant to the attack. This means that the intermediate differences can be arbitrary selected. The notion of differentials was introduced to account this observation:

- A *differential* is a pair formed of an input difference Δ_0 and an output difference Δ_R.
- A *characteristic* is a sequence of differences $(\Delta_0; \Delta_1; ...; \Delta_R)$ where the difference after each round is given.

The problem is that where the probability of a r-round characteristic can be easily computed as the product of the probabilities of r one-round characteristics, the probabilities of a differential $(\Delta P, \Delta C)$ seem hard to evaluate.

Even though the existence of good characteristics is sufficient to mount efficient attacks, to prove security against differential attacks, we need to ensure that there are no differentials with high enough probabilities to enable successful attacks.

Linear hulls: The concept of linear hulls was introduced to underline the same phenomenon of multiple possible intermediate patterns in linear cryptanalysis. As both linear hulls and differentials are difficult to predict, designers usually make use of approximations in order to predict an upper bound of their probabilities.

Multiple approximations: Multiple approximations usually exist inside block ciphers and it was also attempted to efficiently combine the approximations in order to improve the efficiency of cryptanalysis. However, the problem of their combination is complex because the sign of the bias of different approximations is needed if we want to combine them. As this sign depends on the key, additional guesses have to be made if we want to use multiple approximations. It practically resulted only in limited improvements and the question of the optimal combination of multiple approximations in cryptanalysis is still open.

Key independence: Another hypothesis used to compute the probabilities of linear or differential attacks is the assumption that all the round keys are uniformly random and independent. Practically, the round keys are often derived from a master key using a key scheduling algorithm. As a consequence, there are some small differences between what an attacker can expect to see and what he actually sees when performing the attacks. Nevertheless making this hypothesis remains very reasonable.

4 Extensions of differential and linear cryptanalysis

4.1 Differential-linear cryptanalysis

Introduction: A chosen plaintext attack where the linear cryptanalysis was used to provide a differential characteristic.

Interest: Basic linear or differential cryptanalysis uses prohibitive amounts of known or (worse) chosen plaintexts. The goal of differential-linear cryptanalysis is to reduce the amount of texts required. An eight round attack against DES recovers 10 bits of key with only 512 chosen plaintext. However, expansions to higher number of rounds have not been found.

The attack on DES: The key point of the attack is the observation that toggling 2 bits in the second round of the cipher will leave the output bits of Matsui's best 3-round linear relation unchanged.
If we consider this chosen pair of plaintexts and an 8-round attack using Matsui's 3-round characteristic twice, the input bits of the second 3-round approximation

are unchanged with probability 1 and its output bits are unchanged with probability $p^2 + (1-p)^2$ where p is the probability that the 3-round relation holds. Indeed these bits will not change if either:

1. The second relation holds twice: p^2.
2. The second relations fail twice: $(1-p)^2$.

Then, we extend this differential characteristic to the ciphertext bits, involving one s-box. So we have to guess 6 key bits.
The remaining problem is to find a way to toggle adequate bits in the second round. This can be done by guessing another 6 key bits (but only 4 new ones) and therefore, we can generate the adequate pair of plaintexts with a certain probability.
Finally, 10 key bits are recovered with about 512 chosen plaintexts.

Countermeasures: The attack is possible because some bits may remain unchanged after a number of rounds. Therefore, differential-linear cryptanalysis can by avoided by designing a cipher where overall diffusion is provided in a small number of rounds, so that a change in an input bit will produce a possible change of every output bit.

4.2 Non-linear cryptanalysis

Introduction: It is an improvement of linear cryptanalysis that decreases the number of texts required to cryptanalyse the cipher. One proposes to use non-linear approximations in order to get better s-boxes approximations (better probabilities).

Motivation: As a motivational example, the best linear approximation of a DES s-box holds with an absolute valued bias of $\frac{20}{64}$, yet there is a relatively simple non-linear approximation which holds with absolute bias $\frac{28}{64}$.

The problem of joining non-linear approximations: Let C_h^i be the left input bits of round i and C_l^i be the right input bits. $C_h^i[\alpha]$ denotes a general and unspecified and linear sum of bits of the data block C_h^i and $C_h^i[p(\alpha)]$ denotes a general and unspecified non-linear relation between bits of the data block C_h^i. Forming a round approximation as we have in linear cryptanalysis is difficult because it requires that we can combine bits. For example, for a Feistel cipher, we need:

$$(C_h^{i-1} \oplus C_l^i)[p(\alpha)] = C_h^{i-1}[p(\alpha)] \oplus C_l^i[p(\alpha)] \tag{9}$$

And for a non-linear $p(.)$, this will not, in general, hold.

Practically, to extend the approximation across a DES s-box to the entire round, we need to guess additional key bits. Indeed, the input bits of the s-box x_i are combined with key bits k_i to form the expansion function output bits z_i: $x_i \oplus k_i = z_i$. Therefore, the expansion of, say $x_0 x_1$ to the round input bits will

depend on key bits. For example, if $(k_0, k_1) = (0, 1)$, we have $x_0 x_1 = z_0 z_1 \oplus z_0$. This involves an additional guess on these key bits. In non-linear cryptanalysis, not only the sign of the bias depends on the key, its value does also.

The attack: Despite of difficult combination, non-linear approximations can still be used in a variety of ways:

1. The inputs (resp. outputs) to an approximation to the first (resp last) round of some ciphers need not be combined with any other approximations. Consequently, approximations of these rounds can equally be linear or non-linear if we can fix some plaintext bits, making the key-dependency of first (resp last) rounds known to the attacker.
2. Linear cryptanalysis of Feistel ciphers makes certain bits of the input to the second (or penultimate) round available to the cryptanalyst. Consequently, non-linear approximations can potentially be used in these rounds also.
3. Key dependency of non-linear approximations can be used to perform another kind of key guess in the first (resp last) rounds of block ciphers. It allows more flexibility than classical cryptanalysis.

Conclusions and countermeasures: There may be circumstances where non-linear approximations can improve linear approximations. Moreover they can be used if large S-boxes are used in order to make the key guess impractical. It is then possible to perform the key guess on a non-linear approximation of the s-box. Regarding countermeasures, remark that non-linear approximations are limited to the outer rounds of an algorithm; consequently, in a cipher using a large number of rounds, linear cryptanalysis should not be significantly improved by non-linear approximations.

4.3 Chosen plaintext linear cryptanalysis

Introduction: It is an improvement of the linear cryptanalysis based on an adequate choice of the plaintext, in order to reduce the number of active s-boxes and therefore, reduce the number of required plaintexts. The resulting attack is the fastest attack reported on DES.

Basic idea: In Matsui's original linear cryptanalysis, one performs a key guess in the first and last rounds of the cipher, corresponding to 12 key bits in DES. By fixing the 6 input bits to the first active s-box, the key guess is reduced to 6 key bits in the last round. Since the noise of 63 wrong keys is less than the one of 4095 wrong keys, the attack is expected to be of lower complexity than that of Matsui.

Improvement: In addition to fixing the 6 key bits of the input to the active s-box in the first round, one can try to do the same for a possible active s-box in the second round, so that the probability of the characteristic is improved. Practically, we just fix the inputs to all s-boxes in the first round which output bits are input to the active s-boxes in the second round. Consequently, the probability of the linear characteristic is computed considering one round less.

Conclusions and countermeasures: Moving to the chosen plaintext context, we can improve Matsui's linear cryptanalysis significantly (a factor of $\simeq 2.6$ is gained). However, this improvement is limited to the outer rounds of a cipher because one tries to fix the input bits of active s-boxes and we can only access input bits of outer rounds. Fixing bits is possible as long as the diffusion process is not complete. In a cipher using a large number of rounds with good diffusion, linear cryptanalysis should not be significantly improved by chosen-plaintext attacks.

4.4 Partial or Truncated differentials

Introduction: In a conventional differential attack, (a, b) is a differential if a difference a in the plaintext block yields a difference b in the ciphertext after some rounds of encryption. Actually, it is not always necessary to predict the full difference.

Interest: For some ciphers, secure against differential cryptanalysis, it is possible to build truncated differentials with significant probabilities. Typically, these differentials predict that some parts of the output difference is 0, while other parts are non-0 (without more precision). For example, there is a 24-round truncated differential for SKIPJACK that holds with probability one and the function $f(x) = x^{-1}$ in $GF(2^n)$ has 2-round truncated differential with probability one.

Countermeasures: Truncated differentials are efficient mainly against ciphers for which all the layers operate on well aligned blocks, for example transformations operating on bytes rather than individual bits. Using binary permutations (that are optimal in hardware) is the adequate tool to provide resistance against it.

4.5 Higher order differentials

Introduction: It is possible to expand the notion of differential characteristic to higher degrees. There exist ciphers that are secure against differential cryptanalysis but susceptible to be broken by higher order attacks.

Derivative of a boolean function: The derivative of a function f at the point a is defined as:

$$\Delta_a f(x) = f(x \oplus a) - f(x) \tag{10}$$

Higher order derivatives: The i'th derivative of a function f at the point $a_1, ..., a_i$ is defined as:

$$\Delta^i_{a_1,...,a_i} f(x) = \Delta_{a_i}(\Delta^{(i-1)}_{a_1,...,a_{i-1}} f(x)) \tag{11}$$

Note that the characteristics and differentials used by Biham and Shamir correspond to a first order derivative.

Attacks using higher order differentials: There exist round functions resistant against first order differentials but not against second order differentials. For example, let $f(x,k) = (x+k)^2 \mod p$ (where p is prime) be the round function of a cipher of block size $2 \cdot log_2 p$. Then every non-trivial one round differential of f has a probability of $\frac{1}{p}$ and the second order derivative is a constant.
Another example is the round function $f(x) = x^{2^k+1}$ in $GF(2^n)$ described by Nyberg. Higher order differentials allow performing improved attacks on (up to) 6-rounds ciphers. However, higher order differentials seem to be limited to this low number of rounds. The problem is to find a method to iterate higher order differentials to more than two rounds in the same way as first order differentials.

Computing the non-linear order: The following test using higher order differentials can be used to compute the non-linear order of a block cipher:

Input: $E_K(.)$ a block cipher, a key K and plaintexts $x_1 \neq x_2$.
Output: A minimum non-linear order of E_K.
Let $a_1, ..., a_i$ be linearly independant.

1. Set $i = 1$.
2. Compute $y_1 = \Delta_{a_1,...,a_i} E_K(x_1)$ and $y_2 = \Delta_{a_1,...,a_i} E_K(x_2)$.
3. If $y_1 = y_2$, output i and stop.
4. Set $i = i + 1$ and go to step (2).

In general, a cipher with five rounds (or less) using round functions of nonlinear order r can be attacked by an r'th order differentials.

Countermeasures: Basically two types of countermeasures can be considered:

1. As the process of combining higher order differentials seem to be limited to a small number of rounds, use large number of rounds.
2. Use round functions with a high non-linear order.

5 Miss in the middle attack - impossible differentials

Introduction: It is a variant of truncated differential cryptanalysis in which a differential predicts that some particular differences should never occur.

Principle: The fact that impossible events can be useful in cryptanalysis is an old idea. Miss in the middle attacks, also called impossible differentials attacks, are about systematic analysis on how to identify an impossible behavior in a block cipher and how to exploit it in order to derive the key.
The general technique to construct impossible events is called *miss in the middle*, and the way to exploit it in order to cryptanalyze block ciphers is a *sieving* attack that finds the correct keys by eliminating all the keys which lead to contradictions (or impossible events).

Miss in the middle technique: Let B be a 64-bit block cipher with 4 rounds. The construction of impossible differentials is related to the existence of differentials with probability 1 for some rounds.
Imagine the input difference $(a, 0, a, 0)$ causes the difference $(b, b, 0, 0)$ with probability 1 after round 1. Moreover the output difference $(c, c, 0, 0)$ causes[1] a difference $(0, d, 0, d)$ at the same place. Therefore, if input and output differences are as above, the difference at the middle is constrained by both ways (encryption and decryption) which leads to a contradiction. Consequently, no pairs simultaneously satisfy the input and output difference.

Using impossible differentials: First, impossible differentials allows distinguishing a block cipher from a random permutation. Identification only requires to feed the black box with enough plaintexts with input differences involved in an impossible differential and check whether the output difference is possible.

Impossible differentials can also be used to attack block ciphers by adding some rounds to the impossible differential characteristic. The basic attack requires to choose enough plaintexts with input differences corresponding to the impossible differential and collect ciphertexts. Then, by partially decrypting the additional rounds with all possible subkeys, we can reject all those which give rise to impossible differentials.

Conclusions: Impossible differentials exist for various block ciphers. Moreover, cryptanalysis with impossible differentials can be used with low-probability (rather than zero probability) differentials or combined with linear cryptanalysis.
Designers of block ciphers usually try to show that their schemes are resistant to differential cryptanalysis by providing an upper bound of characteristics and differentials in their schemes. A consequence of impossible differentials is that they also have to consider lower bounds.
Another general belief is that large s-boxes offer increased security against differential attacks. However, the difference distribution table of such s-boxes contains very few possible entries and a lot of input/output differences are impossible. This could facilitate the construction of impossible differentials and can thus make such schemes more vulnerable to these attacks.

Countermeasures: Avoid differentials with probabilities 0 (impossible) and 1 (that allows mounting impossible differentials using the miss in the middle technique). Practically, these impossible differentials should not exist over a large number of rounds.

6 Boomerang - rectangle attacks

Introduction: The boomerang attack is a differential-style attack in which the attacker does not try to cover the whole cipher with a single highly-probable

[1] In the decryption way.

differential pattern. Instead, the attacker tries to find two high-probability patterns that are not necessarily related to each other but together cover the whole cipher. In its basic version, it requires the ability to make chosen-plaintext and chosen-ciphertext queries.

Interest: Algorithm designers usually compute an upper bound p on the probability of any differential characteristic for the cipher. Then the designer invokes an often repeated "folk theorem" to justify that any successful differential attack will require at least $\frac{1}{p}$ texts to break the cipher. Boomerang attacks show that this folk theorem is wrong.

Principle: Let us denote the encryption operation by E and its decomposition into two parts as $E = E_1 \circ E_0$. Suppose that we start with two plaintexts P_1, P_2, such that $P_1 \oplus P_2 = \Delta$. Suppose that we have a differential pattern $\Delta \rightarrow \Delta^*$ propagating through the E_0 part of the cipher with probability p. Now consider the corresponding ciphertexts C_1, C_2 and their shift by a difference ∇ as follows: $C_3 = C_1 \oplus \nabla$, $C_4 = C_2 \oplus \nabla$. As ∇ we use a pattern that goes up through E_1^{-1} with high probability q, i.e. $\nabla \rightarrow \nabla^*$. We decrypt the new ciphertexts C_3, C_4 to obtain their corresponding plaintext P_3 and P_4. If the previous two difference patterns happened as predicted, between E_0 and E_1, we obtain a difference $P_3 \oplus P_4 = \Delta$ with probability p^2q^2.
As a consequence, algorithm having good approximations through half the cipher can be efficiently attacked by this kind of attacks. The real weakness of such an attack is that, in its basic version, the boomerang requires adaptative-chosen-ciphertext queries.

Amplified boomerang attacks and rectangle attacks: Improvements of the boomerang attacks propose moving to a more familiar chosen-plaintext context attack. Basically, the question that rises then is: "If we generate differential quartets (a, b, c, d) such that $a \oplus b = c \oplus d = \Delta$, with Δ the first required difference, what will be the amount of right quartets with all the difference patterns needed?". In the amplified boomerang attack, the probability of a quartet to be right is claimed to be $2^{-(n-1)/2}pq$. In the paper about the rectangle attack, it is shown that several degrees of freedom exist in the difference patterns between E_0 and E_1, which significantly increases the proportion of right quartets.

Countermeasures and conclusions: Boomerang and rectangle techniques illustrate interesting ways to combine differentials. The resulting attack can be very efficient, specially against ciphers having no good differentials through the whole algorithm but well through some parts of it. Precise countermeasures are hard to determine but we observe that:

1. Ciphers that does not have a well distributed security are dangerous. Iterative block ciphers repeating always the same round are preferred.
2. Ciphers of which the security is weak if we divide them are susceptible to be broken by these attacks. Complete diffusion and low probable differentials are needed in a short number of rounds.

7 Interpolation attacks

Introduction: This attack is applicable to ciphers for which the round function can be written as a reasonably simple algebraic expression. It relies on the application of the *Lagrange interpolation formula*:

Definition 1. *Let K be a field. Given $2n$ elements $x_1, ..., x_n, y_1, ..., y_n \in R$, where the x_i's are distinct, define:*

$$f(x) = \sum_{i=1}^{n} y_i \prod_{1 \leq j \leq n, j \neq i} \frac{x - x_j}{x_i - x_j}$$

Then $f(x)$ is the only polynomial over K of degree at most $n-1$ such that $f(x_i) = y_i$ for $i = 1 \dots n$. This equation is called ***Lagrange interpolation formula****.*

The principle: Consider a cipher for which the round function can be written as a polynomial (possibly with several variables) with a reasonable number of terms. Then the whole cipher can be written as a polynomial too, in which the coefficients are key-dependent. By considering sufficiently many plaintext-ciphertext pairs, and using the Lagrange interpolation formula, all coefficients may be computed. It is a *global deduction* attack, in the sense that an equivalent expression for the cipher is constructed, but the key is not recovered. However, the last round key guess technique allows it ro be converted into a key recovery attack. Note that combining this attack with a meet-in-the-middle approach allows reducing the number of terms of the polynomial, and thus the number of plaintexts needed. Also, the attack is easily adaptable to ciphers that can be expressed as a rational expression (quotient of two polynomials).

8 Square - saturation - integral - multiset attacks

Introduction: The multiset cryptanalysis has first been presented as a dedicated attack when J. Daemen, V. Rijmen, and L. Knudsen published the algorithm Square (hence the alternative name "Square attack"). Since then, it has been applied to many others algorithms: Twofish, IDEA, Camellia, Skipjack, Misty,... It is a chosen plaintext attack studying the propagation of well chosen sets of plaintexts through the cipher. It has the particularity that we can get information only by considering the whole group of plaintexts (contrary to linear or differential cryptanalysis, for example, for which each plaintext (resp. each pair of plaintexts) potentially brings some pieces of information). Also, the particular characteristics of some components of the cipher such as S-boxes, do not affect the efficiency of this attack (only the fact that these S-boxes are bijective may be important).

Principle: Consider the data at the input of a bijective S-box, corresponding to some sets of plaintexts. Let us assume that all possible values appear the same number of times (i.e., if $k \cdot 2^n$ plaintexts are considered, where n is the size of the S-box (in bits), then each value appears k times). Then trivially, all values will still appear the same number of times at the output of the S-box. Even more trivial, if the input to an S-box is constant, then so is the output. Multiset attacks trace this type of features through as many rounds as possible. The following terminology is currently used in multiset attacks:

- A **multiset** is, roughly speaking, a set of which the elements may appear several times. A **n-bit multiset** is a multiset of which the elements belong to the set $\{0,1\}^n$.
- A n-bit multiset with $k \cdot 2^n$ entries is said **active** or **saturated** if any value in $\{0,1\}^n$ is found exactly k times.
- A multiset is said **passive** if it contains only one fixed value.
- A multiset is said **garbled** if it is neither active nor passive.

Consider for example a byte-oriented cipher with a block size of $8 \cdot n_b$. Typically, a multiset distinguisher for this cipher will require a group of 2^{8a} plaintexts, of which the $n_b - a$ bytes are constant, the others forming a $8a$-bit active multiset. Key-recovery is possible using this distinguisher by doing a classical last round key guess.

The Integral attack: We can define one useful property more for a multiset: namely, a multiset G is said **balanced** with respect to some group operation if: $\sum_{x \in G} x = 0$. For the group operations usually used in a block cipher($\oplus$ or addition $\mod 2^n$), it holds that an active multiset is also balanced. Using the property that the sum of two balanced multisets is still balanced, a multiset distinguisher can sometimes be pushed a few rounds further. It is then called **integral** distinguisher (the term"integral" referring to the sum).

Countermeasures: As multiset and integral attacks are targeting the diffusion layer, strong such layers must be devised to counter them.

Extensions The following two papers do not present "pure" multiset/integral attacks, but exploit some of their principles: the Gilbert-Minier attack on Rijndael exploits collisions between some partial functions introduced by the cipher. The SASAS cryptanalysis from Biryukov and Shamir exploits the multiset principle combined with some linear algebra to attack whatever cipher with structure $S \cdot A \cdot S \cdot A \cdot S$, with S and A respectively denoting a layer of parallel invertible S-boxes and an invertible affine mapping over $GF(2)$.

9 Related key attacks

Introduction: A *related key attack* is an attack under the particular hypothesis that the attacker is able to learn the encryption of some plaintexts not only under the original (unknown) key K, but also under some derived keys $K^* = f(K)$.

Biham's related keys: Block ciphers usually make use of a master key from which round keys (or subkeys) are derived and used in different rounds. Let K_i be the subkey in round i. Two keys K, K^* are said to be *related* if there is a defined relation $K^* = f(K)$ that holds. In the specific related key attack we present here, 2 keys K, K^* are said to be *related* if $K_{i+1} = K_i^*$ during several rounds (typically $n-1$, with n the number of rounds of the cipher).

Biham's related key attack: This related key attack is based on the following property: for two related keys, if the data before the second round in an encryption under the key K equals the data before the first round under the key K^*, then the data and the inputs to the rounds are the same in both executions with a difference of one round. If furthermore $K_1 = K_n^*$, finding such a pair P, P^* is sufficient to retrieve K_1. It is a known-plaintext attack.
In case of a n-bit Feistel cipher, we can turn it into a chosen-plaintext attack by taking $P_R = P_L^*$. $2^{n/4}$ chosen plaintexts are required. By the birthday paradox, there is a high probability that we find the expected pair. It is easy to identify this pair by checking whether $C_L = C_R^*$.
Then we use relations holding between P, P^*, C, C^* and the secret key to recover secret key bits in less tests than an exhaustive key search.
A similar known-plaintext attack uses $2^{n/2}$ known-plaintexts.

Another weak key schedule: Knudsen found a weakness in the key schedule of SAFER. It has the effect that for virtually every key K, there exists at least one different key K^*, such that for a non-negligible fraction of all plaintexts, the outputs after 6 rounds of an encryption are equal.
The weakness is caused by:

1. A key byte j affects only S-box j directly in every round.
2. A key is applied to the text before and just after the S-box, thus enabling collisions considering one byte isolated in every round.

From this, we can find a large number of keys that equally encrypt a plaintext with a fixed probability. We call them related keys. This allows mounting a related key chosen plaintext attack against the cipher. It also greatly reduces the security of the algorithm when used in hashing modes.

Interest: One interest is purely theoretical: a cipher that succumbs a related-key attack can be distinguished from a random family of permutations, which is an undesirable property.
But although the condition to mount related key attacks (having plaintexts encrypted under related keys) needs to use related key queries and therefore does not lead to the most realistic attacks, related key cryptanalysis is not a strictly theoretical attack. Examples of communication protocols exist where (too) simple key management makes the attack practical.
The security of the cipher used in hashing mode can also be affected.

Extensions: The related-keys attack principle can be combined with other cryptanalytic techniques such as to obtain new attacks.

1. Differential related key attack: it consists in a differential attack in which the keys as well as the plaintexts are chosen with specific differences.
2. Related key differential timing attack: it breaks cryptosystems by timing their operations. For example, it was measured that increasing the number of zero multiplicative subkeys by one decreases the time required to carry out 1 000 000 block encryptions (IDEA) by an average of 3 seconds.

Countermeasures: To provide resistance against related key cryptanalysis and its expansions:

1. DES is not vulnerable to Biham's attack because the number of shifts in the key schedule is not the same in all the rounds. Generally, sliding techniques like Biham's one can be avoided by making the key schedule different in every round. The use of round constants efficiently solves this problem.
2. Avoid linear key schedules.
3. Maximize avalanche in the subkeys to avoid key-bytes affecting only one text-byte. Provide a good diffusion of the key.

Optimal key schedules should resist differential attacks and possess some form of collision-freedom which is a standard property of hashing functions as well.

10 Slide attacks

10.1 Basic slide attack and extensions

Introduction: Slide attacks exploit the degree of self-similarity of a block cipher and thus are applicable to iterative block ciphers with a periodic key schedule.

Slid pair: Let F be the round function of an iterated block cipher. If a pair of known plaintexts $(P, C), (P', C')$ satisfies $F(P) = P'$, then due to the self-similarity of both the rounds and the key schedule, the corresponding ciphertexts also satisfy $F(C) = C'$. Such a pair is called a *slid pair*.

Principle: In a basic slide attack, the only requirement on F is that it is *weak* against known plaintext attacks with two plaintext-ciphertext pairs: given two equations $F(x_1, k) = y_1$ and $F(x_2, k) = y_2$, it is easy to extract the key k.
If we suppose that all rounds of a block cipher are identical, by the birthday paradox it is possible to find a slid pair in $O(2^{\frac{n}{2}})$ known texts with a high probability. Furthermore, slid pairs can often be recognized relatively easily, by checking whether it is possible that $F(P) = P'$ and $F(C) = C'$ both hold for some key. Because F is weak, we can recover the secret key with one slid pair.
In the case of Feistel ciphers, the round function modifies only half of its input. Therefore, the condition $F(x) = x'$ can be recognized by simply comparing the left half of x against the right half of x'.

Interest: The slide attack is a generic attack that is applicable independently of the number of rounds. It is important to remark that it is the counterpart of Biham's related-key attack in a classical context.

Examples: The slide attack is applicable to TREYFER, because of its trivial key scheduling algorithm: it simply uses its 64-bit key K byte by byte.
The slide attack is also applicable to 2K-DES, a "strengthened" DES with an increased number of rounds (64) and key bits (2×48). One use K_1 in the odd rounds and K_2 in the even rounds instead of DES subkeys. This cipher can be viewed as a cascade of $\frac{r}{2}$ identical fixed permutations, making it susceptible to slide attacks.
Finally, slide attacks are applicable to ciphers with key dependant S-boxes, showing that the attack is not restricted to ciphers with weak key scheduling algorithms.

Advanced slide attacks against Feistel ciphers: Advanced techniques can be used to apply slide attacks to a larger class of Feistel ciphers. Notably p-rounds self-similar block ciphers, where a generalized round consisting of p rounds of the original cipher is iterated, are vulnerable to advanced slide attacks, provided that $p = 2$ or 4.

1. The complementation slide: In the conventional attack, to deal with 2-round self-similarity, one must slide by two rounds. The problem is that such an F made up of 2 rounds is probably not *weak*. The complementation slide technique consists in sliding by only one round and introducing differences $\Delta = \langle K_1 \oplus K_2, K_1 \oplus K_2 \rangle$ between rounds of encryptions of slid pairs. In other words, one chooses a slid pair so that the plaintext difference will cancel the difference between the subkeys.
2. Sliding with a twist: If we ignore the final swap, then the decryption with a Feistel cipher under key K_1, K_2 is the same as encryption with key K_2, K_1. Therefore, we can slide by one round a decryption process against an encryption process.

Complementation slide and sliding with a twist can be combined. It allows attacking Feistel ciphers with 4-round periodicity.
Finally, if the cipher is a product of stronger functions, so that multiple input/output pairs (instead of 2) are required to recover any key material, it is possible to generate different slid pairs "for free". One technique is by performing multiple encryptions $E(E(..(P)..))$ of P.

Countermeasures: Slide attacks exploit the degree of self-similarity of a block cipher. Therefore, to provide resistance:

1. Avoid periodic key scheduling algorithms.
2. Use round constants.

10.2 Secret S-boxes cryptanalysis

Introduction: Certain block ciphers like GOST or Blowfish make use of secret S-boxes. However, such secret boxes can be quite easy to cryptanalyse and do not improve the security in some contexts.

A chosen-key attack against the secret S-boxes of GOST: In a Feistel cipher using secret S-boxes, the attack proceeds in two steps. The first step search for a $\frac{n}{2}$-bit long "zero vector" $z = f(0)$, where f is the round function. This step requires no more than $2^{\frac{n}{2}}$ encryptions and is similar to the search of a slid pair in a slide attack. The second step examines one S-box at a time and extracts the content of that S-box. If S-boxes are k-bit $\times$ l-bit and $z = f(0)$, we take $a = 0$ excepted k bits corresponding to one S-box, $b = z$ excepted l bits corresponding to the same S-box and compute $b = f(a)$ with every possible S-box until we find the correct one.
Note that the chosen-key context comes from the key addition present in the round function. A comparable attack can be applied to the key-dependant S-boxes of Blowfish.

Conclusion:

1. The sliding techniques are not only applicable to ciphers with weak key scheduling algorithms.
2. Secret S-boxes do not always increase the security of an algorithm.

11 Complementation property attacks and weak keys

11.1 Complementation property attacks

Introduction: A complementation property is a relation that holds between different plaintext-ciphertext pairs of an algorithm with complementary texts or keys. It can be used to speed up exhaustive key search.

The complementation property of DES: In DES, whenever a plaintext P is encrypted under a key K into a ciphertext $C = DES(P, K)$, then the complement of P is encrypted by the complement of K into the complement of C: $\overline{C} = DES(\overline{P}, \overline{K})$.

An attack: First, we choose a pair of complementary plaintexts: $P_2 = \overline{P_1}$. Given their ciphertexts under the same key K: $C_1 = DES(P_1, K)$ and $C_2 = DES(P_2, K)$, the attacker searches for the key K by trying all the keys K' of which the most significant bit is zero (i.e. half of the key space). For each such key, he encrypts P_1 into C'. If $C' = C_1$, it is very likely that $K = K'$. Moreover if $C' = \overline{C_2}$, it is very likely that $K = \overline{K'}$, since due to the complementation property $\overline{C_2} = DES(P_1, \overline{K})$. Since comparisons are much faster than a trial encryption, this attack is twice as fast as exhaustive key search.
This attack can be carried out even under a known-plaintext attack, given about 2^{33} known plaintexts, since it is very likely that two complementary plaintexts exist within 2^{33} random plaintexts due to the birthday paradox.

Conclusion: DES present a complementation property that can be used for cryptanalytic purposes. Other block ciphers (LOKI), also present this kind of relations. In general, a cipher function should appear to be a random function of both the key and the plaintext. Any regular behavior is of interest to the cryptanalyst and should be avoided.

11.2 Weak keys

Introduction: The weak keys we are interested in here are those for which encryption is the same as decryption. We also define pairs of semi-weak keys K and K' as keys for which encryption with K is the same as decryption with K'.

Interest: Both DES and LOKI have weak keys. If the number of weak keys is relatively small, they may not compromise the cipher when used to assure confidentiality.
However, several hash modes use block ciphers where an attacker can choose the key input in an attempt to find a collision. In these modes, the cipher should not have any weak nor semi-weak keys.

Weak keys, fixed points and collisions in DES: DES weak keys are such that all 48-bit subkeys are the same for each round i, j: $K_i = K_j$, a consequence is that $E_K(E_K(X)) = X$.
For such a weak key, E_K has 2^{32} fixed points. Indeed, for some message M broken into halves M_0, M_1, with (M_{17}, M_{16}) representing the ciphertext, suppose that $M_8 = M_9$ (there are 2^{32} such messages). Then:

$$M_7 = M_9 \oplus f(K_8, M_8) = M_8 \oplus f(K_9, M_9) = M_{10} \tag{12}$$

Repeating this, we finally find $(M_0, M_1) = (M_{17}, M_{16})$ and therefore, we found a fixed point: $E_K(X) = X$.
As a result, cycles of encryptions $(E_1E_0)^l$, where E_0 and E_1 both represent an encryption using a weak key, present a short average length of about 2^{32}. Indeed, suppose that for some l we have $(E_1E_0)^l X = Y$ and Y is a fixed point of E_0. Then $E_0(E_1E_0)^l X = Y$. On the next application of E_1, we find:

$$\begin{aligned}(E_1E_0)^{l+1}X &= E_1E_0(E_1E_0)^l X = E_1Y = D_1Y \\ &= D_1E_1E_0(E_1E_0)^{l-1}X = E_0(E_1E_0)^{l-1}X\end{aligned} \tag{13}$$

Continuing for $j \leq l$, $(E_1E_0)^{l+j}X = E_0(E_1E_0)^{l-j}X$ and we are just retracing our steps until we return to the starting value X. Therefore, we found a collision in a number of steps close to 2^{32}.

Conclusion: As in the case of complementation properties, weak keys denote a regular behavior of a block cipher that can be used by the cryptanalyst. Practically, cycles of encryptions under weak keys present a short average length and this simplifies the collision search in hashing modes of a cipher.

12 Conclusion

We presented some cryptanalytic techniques developed against block ciphers in the 1990s. Historically, these techniques are closely related to the cryptanalysis of the Data Encryption Standard as well as to the design of the Advanced Encryption Standard. It seems that AES was an elegant solution to overcome the threats of attacks presented in this report. However, new directions are already considered. We mainly noticed the critical question of algebraic descriptions of block ciphers as a future trend in cryptanalysis research.

13 Bibliography

13.1 Linear cryptanalysis

1. M.Matsui, *Linear Cryptanalysis Method for DES Cipher*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'93, pp. 386-397, 1993.
2. M.Matsui, *The First Experimental Cryptanalysis of the Data Encryption Standard*, Advances in Cryptology: Proc. of CRYPTO '94, Springer-Verlag, Berlin, pp. 1–11, 1994.
3. E.Biham, *On Matsui's Linear Cryptanalysis*, Proceedings of Eurocrypt'94, LNCS 950, Springer-Verlag.

13.2 Differential cryptanalysis

1. E.Biham, A.Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer Verlag, 1993, ISBN: 0-387-97930-1, 3-540-97930-1.
2. E.Biham, A.Shamir, *Differential Cryptanalysis of DES-Like Cryptosystems (Extended Abstract)*, Proceedings of Crypto'90, LNCS 537, Springer-Verlag.
3. E.Biham, A.Shamir, *Differential Cryptanalysis of the Full 16-Round DES*, Proceedings of Crypto'92, LNCS 740, Springer-Verlag.

13.3 Linear Hulls, differentials, multiple approximations

1. X.Lai and J.L.Massey, *Markov ciphers and differential cryptanalysis*, Advances in Cryptology EuroCrypt '91, Springer Verlag.
2. K.Nyberg, *Linear approximation of block ciphers*, Advances in Cryptology EuroCrypt '94, Springer Verlag.
3. L.Keliher, H.Meijer, and S.Tavares, *New Method for Upper Bounding the Maximum Average Linear Hull Probability for SPNs*, EuroCrypt 2001, LNCS 2045, p. 420 ff.
4. B.S.Kaliski and M.J.B.Robshaw, *Linear Cryptanalysis using Multiple Approximations*, in the proceedings of CRYPTO 94, LNCS 0839, pp 26-39, Springer-Verlag.

13.4 Extensions of differential and linear cryptanalysis

Differential-linear cryptanalysis

1. M.E.Hellman and S.K.Langford, *Differential–linear cryptanalysis*, Advances in Cryptology - Proc. Crypto'94, LNCS 839, pages 26–39. Springer Verlag, 1994.

Non-linear cryptanalysis

1. L.R.Knudsen and M.J.B.Robshaw, *Non-linear approximations in linear cryptanalysis*, In Ueli Maurer, editor, Advances in Cryptology – EUROCRYPT 96, volume 1070 of Lecture Notes in Computer Science, pages 224-236. Springer-Verlag, 12-16 May 1996.

Chosen plaintext linear cryptanalysis

1. L.R.Knudsen,J.M.Mathiassen, *A chosen plaintext linear attack on DES*, Fast Software Encryption, Seventh International Workshop, New York, USA, April 2000. Springer Verlag.

Partial or truncated differentials

1. L.Knudsen, *Truncated and Higher Order Differentials*, Proceedings of the Second International Workshop on Fast Software Encryption, Leuven, Belgium, 1995, LNCS 1008, Springer, pp.196-211.
2. L.R.Knudsen,M.J.B.Robshaw,D.Wagner, *Truncated Differentials and Skipjack*, Proceedings of CRYPTO 1999: 165-180, Springer-Verlag.

Higher order differentials

1. L.R.Knudsen, *Partial and higher order differentials and its application to the DES*, BRICS report series, RS-95-9, ISSN 0909-0878, February 1995.
2. T.Jakobsen, *Higher order cryptanalysis of block ciphers*, Phd thesis, Department of mathematics, University of Denmark, 1999.

13.5 Impossible differentials and miss in the middle attacks

1. E.Biham,A.Biryukov,A.Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials*, In J. Stern, editor, Advances in Cryptology: EUROCRYPT'99, LNCS 1592, pp. 12-23. Springer Verlag, 1999.
2. E.Biham,A.Biryukov,A.Shamir, *Miss in the Middle Attacks on IDEA, Khufu, and Khafre*, in Proceedings of FSE 1999, LNCS 1636, pp. 124-138, Springer-Verlag 1999.

13.6 Boomerang - Rectangle attacks

1. D.Wagner, *The Boomerang Attack*, in the Proceedings of FSE999, LNCS 1636, p. 156 ff, Springer-Verlag.
2. E.Biham, O.Dunkelman, N.Keller, *The Rectangle Attack, Rectangling the Serpent*, in the proceedings of EUROCRYPT 2001, Lecture Notes in Computer Science 2045 p.340-ff, Springer-Verlag.

13.7 Interpolation attack

1. Thomas Jakobsen and Lars R. Knudsen, *The Interpolation Attack on Block Ciphers*,in the proceedings of Fast Software Encryption (FSE '97), Lecture Notes in Computer Science Volume 1267, pages 28-40, Springer-Verlag.

13.8 Square - Integral - Saturation attacks

1. Daemen, J. and Knudsen, L. and Rijmen, V., *The Block Cipher SQUARE*, in the proceedings of Fast Software Encryption 1997, Lecture Notes in Computer Science Volume 1267, pp 149-165, Springer-Verlag.
2. J. Nakahara Jr et al., *Square attacks on Reduced-Round PES and IDEA Block Ciphers*, Available at http://eprint.iacr.org/2001/068/.
3. P. S.L.M. Barreto et al., *Improved Square attack against reduced-round Hierocrypt*, Available at http://www.cryptonessie.org.
4. Gilbert, H. and Minier, M., *A collision attack on 7 rounds of Rijndael*, in the proceedings of The Third AES Candidate Conference, pp 230-241, 2000.
5. Biryukov, A. and Shamir, A., *Structural Cryptanalysis of SASAS*, Proceedings of Eurocrypt'01, pp 394-405, Lecture Notes in Computer Science, volume 2045, Springer-Verlag.

13.9 Related key attacks

1. E.Biham, *New types of cryptanalytic attacks using related keys*, Journal of Cryptology, 7(4):229-246, Fall 1994.
2. J.Kelsey,B.Schneier and D.Wagner, *Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA*, ICICS '97 Proceedings, Springer-Verlag, November 1997, pp. 233-246.

13.10 Slide attacks

1. A.Biryukov and D.Wagner, *Slide attacks*, in proceedings of Fast Software Encryption 1999, LNCS 1636, pp 245-259, Springer-Verlag.
2. A.Biryukov and D.Wagner, *Advanced Slide attacks*, in proceedings of EUROCRYPT 2000, LNCS 1807, pp 589-600, Springer-Verlag.
3. M.-J.Saarinen, *A chosen key attack against the secret S-boxes of GOST*,1998.

13.11 Complementation property attacks and weak keys

1. E.Biham, *New types of cryptanalytic attacks using related keys*, Journal of Cryptology, 7(4):229-246, Fall 1994.
2. D.W.Davies, *Some regular properties of the DES*, In Allen Gersho, editor, Advances in Cryptology: A Report on CRYPTO 81, page 41, 24-26 August 1981.

13.12 Conclusion

1. Nicolas Courtois and Josef Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, in the proceedings of Asiacrypt 2002, LNCS, Springer-Verlag.
2. S.Murphy and M.Robshaw, *Essential Algebraic Structure within the AES*, Advances in Cryptology, CRYPTO 2002, Lecture Notes in Computer Science 2442, pp. 1-16. Springer-Verlag.