# Practically secure Feistel ciphers

Lars R. Knudsen

Århus University, Denmark**

**Abstract.** In this paper we give necessary design principles to be used, when constructing secure Feistel ciphers. We introduce a new concept, **practical security** against linear and differential attacks on Feistel ciphers. We give examples of such Feistel ciphers (practically) resistant to differential attacks, linear attacks and other attacks.

## 1 Introduction

In this paper we consider Feistel ciphers, often called DES-like iterated ciphers. Feistel ciphers are block ciphers, where the ciphertext is calculated by recursively applying a round function to the plaintext. Consider an $r$-round Feistel cipher with block size $2m$ bits. The round function is defined as follows:

$$Round_i : (L_i , R_i) \rightarrow (R_{i-1} , F(K_i, R_{i-1}) \oplus L_{i-1})$$

for $i = 1, ..., r$, where $L_i$ and $R_i$ are of length $m$ and $K_i$ are round keys derived from a (master) key using a key schedule algorithm. $F$ is a function with two arguments producing an $m$ bit value. $L_0$ and $R_0$ are the left and right halves of the plaintext and typically the two halves $L$ and $R$ are swapped after the last round, i.e. the ciphertext is defined as $(R_r||L_r)$.

The paper is organized as follows. In section 2 we give some necessary properties of secure Feistel ciphers. In section 3 we give simple ideas of how to obtain these properties. We define and construct so-called strong key schedule algorithms. We define **practical security** against differential and linear attacks and show a simple method which can be used to obtain lower bounds of the complexities of practical linear and differential attacks in accordance with the definition of practical security. Examples of (insecure) ciphers with all the properties of section 2 are given. Thus we also illustrate the danger of focusing solely on a limited set of design criteria. We expect the reader to be familiar with the concepts of differential cryptanalysis and refer to [1, 13] for further details.

## 2 Necessary design principles

In this section we give necessary design principles for secure Feistel ciphers. First we define

** This paper was written while the author was visiting the ETH, Zürich, Switzerland.

**Definition 1** *Let $E$ be a block cipher, s.t. $E_K(\cdot)$ denotes the encryption function using the key $K$ and let $f, g_1, g_2$ be 'simple' functions, such that the total complexity of one evaluation of each of $f, g_1, g_2$ is smaller than one evaluation of $E$ (one encryption). Then if*

$$E_K(P) = C \Rightarrow E_{f(K)}(g_1(P, K)) = g_2(C, K) \quad (1)$$

*$E$ is said to contain a* **simple relation** *between the encryption functions $E_K(\cdot)$ and $E_{f(K)}(\cdot)$.*

This definition is different from the definition of *linear structures* given in [7]. A set of necessary properties for a secure Feistel cipher $E$ is given in Table 1.

- There are no simple relations
- All keys are equally good
- Resistance against differential attacks
- Resistance against linear attacks

**Table 1.** Necessary properties for a secure Feistel cipher

In the following we explain the necessity of those properties. Later we illustrate that the properties are insufficient to guarantee a secure cipher.

### 2.1 Simple relations

Simple relations for which (1) holds for all plaintexts and all keys can be exploited in a chosen plaintext attack as follows

1. Denote by $PK$ the set of all potential keys.
2. Choose a random plaintext $P$.
3. Get the encryption $C = E_K(P)$ where $K$ is the secret key.
4. Choose a key $K' \in PK$
   (a) Calculate $C' = E_{K'}(P)$. If $C' = C$ output $K'$ and stop
   (b) Get the encryption $C^* = E_K(g_1(P, K'))$.
   If $g_2(C', K') = C^*$ output $f(K')$ and stop
5. Remove $K'$ and $f(K')$ from $PK$ and go to 4

Note that in step 4b we get $E_{f(K')}(g_1(P, K')) = g_2(C', K') = C^*$. That is, in general one can check two keys using one chosen plaintext and doing one encryption and one evaluation of $f$ and the $g_i$'s. The restriction to 'easy' evaluations of $f$ and the $g_i$'s is now obvious and the efficiency of this attack depends on the complexity of the evaluations of the simple functions. Furthermore if the $g_i$'s are independent on the keys a further improvement of the attack is possible as we will illustrate now. For the DES and LOKI'91 there is a well-known simple

relation known as the complementation property, where $f(K) = \overline{K}$ (the complemented value of $K$) and $g_i(X, K) = \overline{X}$ . In this case we need only ask for the chosen plaintext once in step 4b of the above attacks.

In [11, 2] a chosen plaintext attack on LOKI'91 was presented, in [2] called a 'related key' attack, where $f$ is a linear function and the $g_i$'s are functions each corresponding to two rounds of encryptions of (16-round) LOKI'91. The attack reduces an exhaustive search of all keys by about a factor of four using about $2^{33}$ chosen plaintexts [11].

In [12] it is shown that there are other simple relations for the DES. It is unclear however how to exploit those relations since (1) holds only for subsets of all plaintexts and all keys.

### 2.2 All keys are equally good

For the DES and the LOKI ciphers there are a small number of keys, called weak and pairs of semi-weak keys, which should not be used for encryption. A weak key $K$ is a key for which encryption is the same function as decryption. A pair of semi-weak keys, $K$ and $K^*$, are keys for which encryption with $K$ is the same function as decryption with $K^*$ and vice versa. The keys used in a block cipher should be chosen at random. If the number of weak and pairs of semi-weak keys are small they are of no importance for the security of a block cipher, however since block ciphers are often used in hash modes where the key input can be chosen by the attacker in attempts to find collisions, one should design key schedules without any weak or semi-weak keys.

### 2.3 Resistance against differential attacks

The differential attacks on DES [1] exploit the property that the xor of two inputs to the F-function of the DES leads to a non-uniform distribution of the xor of the corresponding outputs. The concept of **characteristic** was introduced, a list of (the most) likely xors in the inputs and outputs of each round in two encryptions of the block cipher. In [13, 14] the notion of **differential** was introduced, where the xors of inputs and outputs of the intermediate rounds are not fixed. In general, an $r$-round Feistel cipher is vulnerable to a differential attack if there exist $(r-1)$-round characteristics with high probabilities. In [13, 14] a definition of **security** against a differential attack was given, in short terms, an $r$-round cipher is secure against differential attacks, if there exists no $(r-1)$-round differential with a probability higher than $\frac{1}{2^{2m}-1}$, where $2m$ is the block size of the cipher.

In general the probability of a differential will be higher than the probability of a corresponding characteristic. However for the Feistel ciphers DES, LOKI'89 and LOKI'91 it seems extremely difficult to find useful $s$-round differentials, where $s > 4$ for which the probability of the differential is higher than for a corresponding characteristic [9, 10].

In [17] it was shown that in an $r$-round iterative DES-like cipher with independent round keys, the probability of any $s$-round differential is upper bounded

by $2 \times (p_{max})^2$, where $s = 4, ..., r$ and $p_{max}$ is the maximum probability of a non-trivial one-round characteristic. This fact was used to upper bound the probability of the best differentials, thereby achieving so-called provable security. Since the round keys have to be independent a large key is required and the practical applications are limited. The following practical definition is useful.

**Definition 2** *A block cipher with dependent round keys is* **practically secure** *against a differential attack, if there exists no characteristic with a probability high enough to enable a successful attack under the assumption of independent round keys.*

The term 'high enough' can be replaced by a formal definition depending on the security required. The complexity of a differential attack is approximately the reciprocal value of the probability of the characteristic used in the attack [1, 13, 14]. As an example, for a 64-bit block cipher we may say, that if every characteristic has a probability lower than $2^{-32}$, the cipher is practically secure against a differential attack, since in this case the attack would require $2^{32}$ chosen plaintexts, which is an unrealistic attack.

In [1] it is shown how to 'pass' the first round in a characteristic by using so-called meta-structures. This means, that in general for an $r$-round Feistel cipher the existence of an $(r-2)$-round differential with a sufficiently high probability may enable a successful differential attack.

### 2.4 Linear cryptanalysis

Linear cryptanalysis [15] is a known plaintext attack in which the attacker exploits linear approximations of some bits of the plaintext, ciphertext and key. In the attack on DES (or on DES-like iterated ciphers) the linear approximations are obtained by combining approximations for each round under the assumption of independent round keys. The attacker hopes in this way to find an expression [15]

$$P_{i_1} \oplus P_{i_2} \oplus .... \oplus P_{i_a} \oplus C_{j_1} \oplus C_{j_2} \oplus .... \oplus C_{j_b} = K_{k_1} \oplus K_{k_2} \oplus .... \oplus K_{k_c} \quad (2)$$

which holds with probability $p_L \neq \frac{1}{2}$ over all keys, such that $|p_L - \frac{1}{2}|$ is maximal. The complexity of a successful attack can be approximated by [15]

$$N_P \simeq |p_L - \frac{1}{2}|^{-2}$$

As in differential cryptanalysis we can define characteristics to be used in linear cryptanalysis, see [3, 15, 16].

**Definition 3** *A one-round linear characteristic is a list of input, key and output bits of one round of the block cipher and a probability* p, *s.t. the boolean value obtained by adding (modulo 2) the input and key bits equals the boolean value obtained by adding (modulo 2) the output bits with probability* p. *An* r*-round* **linear characteristic** *is the concatenation of* r *one-round linear characteristics.*

In some rounds of a linear characteristic linear approximations are not needed. We call these rounds **trivial** one-round linear characteristics. Certainly, more work has to be done in the area of linear cryptanalysis. For instance, is there a similar useful definition of differentials versus characteristics as for differential cryptanalysis? Or can we conclude that a cipher is resistant to linear cryptanalysis if no linear expressions can be found by combining expressions from each round? These questions are left open. In [3] it is mentioned that the collection of characteristics which form a differential might cancel the effect of each other. As in differential cryptanalysis, to be able to build an $r$-round linear characteristic from one-round characteristics in a block cipher with dependent round keys we have to assume independent round keys. We are led to the following definition.

**Definition 4** *A block cipher with dependent round keys is* **practically secure** *against a linear attack, if there exists no linear characteristic with a probability high enough to enable a successful attack under the assumption of independent round keys.*

In [16] the DES is attacked in a linear attack using a 14 round linear characteristic. This is possible by counting on all key bits affecting the linear expressions in the first and in the last rounds, see [15, 16] for further details. This means, that in general for an $r$-round Feistel cipher the existence of a highly probable $(r-2)$-round linear characteristic may enable a successful linear attack. Notice the resemblance between differential and linear attacks.

## 3 Measures

In this section we show how to obtain the properties of the previous section by means of

- Strong key schedules
- Highly nonlinear and differentially uniform round functions

The strong key schedules give the first two properties of Table 1 and complicate differential and linear attacks. The resistance to those attacks can be further improved using highly nonlinear and differentially uniform round functions.

### 3.1 Strong key schedules

In [20] ideas of how to improve the resistance of DES to an exhaustive key search attack were given. The ideas given in this section are inspired by [20]. In [1] it is shown that DES with independent round keys, i.e. a 768 bit key, is not essentially stronger than DES with a 56 bit key. An attack using $2^{59}$ pairs of encryptions is presented, which finds the secret 768 bit key in time about $2^{61}$ encryptions. The improved attack on DES [1, Sect. 5] exploits the dependencies in the round keys and is not directly applicable to DES with independent round keys. The complexity of an improved differential attack on DES with independent round

keys is not known to us. It seems, however, to require more than the $2^{47}$ chosen plaintexts used to attack the DES with dependent round keys as in [1].

In [15, 16] a linear attack on the full 16-round DES is outlined. It finds 26 bits of the 56-bit key using $2^{45}$ known plaintexts. It is suggested to find the remaining 30 bits by exhaustive search. [15, 16] contain no estimates of linear attacks on DES with independent round keys. It is obvious that the existence of a linear attack finding the full round key of the last round would enable a possible attack on DES with independent round keys, since the ciphertexts can then be decrypted one round with the obtained round key and a linear attack on DES with 15 rounds can be performed. It seems though, that a linear attack on the round key in the last round of DES will require many linear expressions [15, 16], including expressions with a probability that requires many known plaintexts for the key to be uniquely determined.

The above speaks in favor of independent round keys in DES-like iterated ciphers. However, as an example, a 768 bit key for DES is of no practical interest. The security gained seems, after all, to be small compared to the big increase in the key size. We introduce new properties of a key schedule in a Feistel cipher.

**Definition 5** *Consider an $r$-round iterated $2m$-bit block cipher with $r$ round keys, each of length $n$ bits. A* **strong key schedule** *has the following properties*

1. *Given any $s$ bits of the $r$ round keys, derived from an unknown master key, where $s < rn$, it is* 'hard' *to find any of the remaining $rn - s$ key bits from the $s$ known bits.*
2. *Given some relation between two master keys it is* 'difficult' *to predict the relations between any of the round keys derived by the two master keys.*

The terms 'hard' and 'difficult' can be replaced by more precise definitions depending on the applications. Of course 'hard' cannot be harder than performing the key schedule for all keys, and 'difficult' cannot more difficult than performing the key schedule for the two master keys.
The above properties will complicate differential and linear attacks and thwart the attacks based on simple relations discussed earlier.

### A simple design of a strong key schedule

Let $E_K(\cdot)$ be an $r$-round Feistel cipher using master key $K$ with block length $2m$ bits and where the $r$ round keys are of length $n$ bits each and $n \leq 2m$.

1. Define an initial key schedule, which on input a master key $K$ outputs $r$ dependent round keys $\{K_i\} = K_1, ..., K_r$, s.t.
   (a) $E_{\{K_i\}}(\cdot)$ is secure against a known plaintext attack using encryptions of at most $r$ known plaintexts.
   (b) $E_{\{K_i\}}(\cdot)$ contains no simple relations as defined in Definition 1, where $g_1(P, K) = P \oplus \alpha$, $\alpha$ a constant.

2. Define the round keys $\{RK_l\} = RK_1, ..., RK_r$ used for encryption as

$$RK_l = nMSB(E_{\{K_i\}}(IV \oplus l)),$$

where $IV$ is a fixed value and $nMSB(X)$ denotes the $n$ most significant bits of $X$.

At a first glance it may seem strange and difficult to construct an initial key schedule yielding a cipher secure against a known plaintext attack and with no simple relations. However for a 16 round cipher, as an example, it does not seem difficult to prove or at least be strongly convinced that the obtained cipher is secure against an attack using only 16 encryptions of known plaintexts and the condition on the simple relations is weak. For a 16 round cipher the relation in 1b will be $g_1(P) = P \oplus h$, $h$ a hex digit, so this relation would not even hold for a cipher with the complementation property, the most well-known simple relation. As an example of such an initial key schedule, see the key schedules of the DES [6] and the LOKI ciphers [4, 5]. We can prove

**Theorem 1** *The key schedule just defined is a strong key schedule, where 'hard' means as hard as a brute force attack on $E_{\{K_i\}}(\cdot)$ and 'difficult' means as difficult as one encryption of $E_{\{K_i\}}(\cdot)$. Furthermore the absence of weak keys is guaranteed and pairs of semi-weak keys are very unlikely to occur.*

Proof: By contradiction. Assume that property 1 of Definition 5 can be compromised faster than exhaustive search for all keys of $E_{\{K_i\}}(\cdot)$. This means, that given $s$ bits of the set $\{RK_l\}$, which are ciphertext bits corresponding to less than $r$ encryptions $E_{\{K_i\}}(IV \oplus l)$, it is possible in time less than brute force to find (bits of) ciphertexts, which were not given to us. But that yields a contradiction because of 1a.

Assume that property 2 of Definition 5 can be compromised faster than one encryption of $E_{\{K_i\}}(\cdot)$. This means, that we can find some relation between two master keys, $K$ and $K^*$, s.t. $f(K) = K^*$ and some relation between two round keys, $RK_l$ and $RK_n^*$, s.t. $g_2(RK_l) = RK_n^*$, where the total complexity of $f$ and $g_2$ is less than that of one encryption of $E_{\{K_i\}}(\cdot)$. But that yields a contradiction because of 1b and Definition 1, since then

$$E_{\{K_i\}}(P) = C \;\Rightarrow\; E_{f(\{K_i\})}(P \oplus (l \oplus n)) = g_2(C),$$

where $P = IV \oplus l$ and $C = RK_l$.

To prove the final statements we note that $RK_l \neq RK_n$ for $l \neq n$, i.e. there are no weak keys. Furthermore it seems very unlikely that we can find $K$ and $K^*$, s.t. $E_K(IV \oplus l) = E_{K^*}(IV \oplus (r + 1 - l))$ for all $l = 1, ..., r$. □

The above method applied to the DES may yield a DES-version with improved immunity to differential, linear and other attacks. However, this DES-version is only 16 times harder to break than the DES by exhaustive search of all keys and in view of [21] a larger master key is needed. A possibility would be to define the round keys as follows:

$$RK_i = 48MSB(DES_{K1}(DES_{K2}^{-1}(DES_{K1}(IV \oplus i)))),$$

i.e. use two-key triple DES to calculate the new round keys.

The above method involves encryptions in the generation of the round keys, but note that encryption with these ciphers is as fast as encryption with the same cipher using a conventional key schedule when the key is held constant (see also [20]).

### 3.2 Nonlinear and differentially uniform round functions

We consider as before an $r$-round Feistel cipher. In [11] a method to upper bound the probability of characteristics in Feistel ciphers was given. The basic idea is to find the minimum number of trivial one-round characteristics that one can have in an $(r-2)$-round characteristic. Then the maximum probability of a non-trivial one-round characteristic gives an upper bound of the probability of the best possible $(r-2)$-round characteristic.

Assume that the only way to attack a Feistel-cipher by linear and differential attacks, is by finding the best (linear) characteristics, i.e. that (linear) differentials are too hard to find, then

- the probability of the best non-trivial one-round (linear) characteristic and
- the number of rounds in the characteristic

give a lower bound on the complexities of these two attacks. This lower bound may be sufficient to prove resistance for all practical implementations of these two attacks, if the probability of the best non-trivial characteristic can be arranged to be sufficiently small. One way of obtaining this is by constructing the round functions based on the differentially uniform mappings from [18]. As the name indicates, for these functions the probabilities of non-trivial one round characteristics are low. And because of their high nonlinearity they are also well-suited for the construction of ciphers resistant against linear attacks as we will illustrate in the next section. Finally it follows from the results in [19] that round functions build from big random S-boxes are resistant to differential attacks. A similar result for linear attacks is not known to us.

### 3.3 Examples

In this section we give two examples of iterated block ciphers practically resistant to both linear and differential attacks. The examples are based on the differentially uniform mappings from [18]. Consider an $r$-round Feistel cipher with block size $2m$ defined as in the introduction of this paper. For simplicity, let $F(K,R) = f(R \oplus K)$, a function producing an $m$ bit value.

**Example 1:** Let $r = 8$ and $m = 34$. Divide the input $X$ to the $f$-function into two halves $X_1$ and $X_2$. Define the output $f(X) = f_1(X_1) \,||\, f_2(X_2)$, where $f_i(x) = x^3$ in $GF(2^{17})$ over $GF(2)$.

**Example 2:** Let $r = 16$ and $m = 32$. Divide the input $X$ to the $f$-function into four eight bit values $X_1, X_2, X_3, X_4$. Define the output

$$f(X) = f_1(X_1) \,||\, f_2(X_2) \,||\, f_3(X_3) \,||\, f_4(X_4)$$

where $f_i(x) = x^{-1}$ in $GF(2^8)$ over $GF(2)$.

In Table 2 we give the estimated number of known and chosen plaintexts needed for successful linear and differential attacks. We transformed the estimates for the complexity of the linear attacks on SP networks from [8] to Feistel-ciphers obtaining

$$|p_\epsilon - 1/2| \leq \frac{2^{m-1} - NL(f)}{2^m} \quad \text{and} \quad |p_L - 1/2| \leq 2^{\alpha-1} \times |p_\epsilon - 1/2|^\alpha$$

where $\alpha$ is the number of non-trivial one round linear characteristics needed and $NL(f)$ is the nonlinearity for the above functions given in [18].

| | Example 1 | Example 2 | DES |
|---|---|---|---|
| Rounds | 8 | 16 | 16 |
| Block size (bits) | 68 | 64 | 64 |
| Practical security ($log_2$) | | | |
| - Linear attack (known pl.texts) | 66 | 56 | 14 (45) |
| - Differential attack (chosen pl.texts) | 48 | 48 | 12 (47) |
| Space (for $f$) | $O(1)$ | 1Kbyte table | |
| Speed (one encr.) | $O$(500 xors) | $O$(64 look ups) | |

**Table 2.** Estimates of complexity

It can be shown that the minimum number of non-trivial one round linear characteristics needed for a linear characteristic of a Feistel cipher is two for every three rounds. By stripping off the first and last round, where we count on key bits, it follows that we need at least 4 and 9 non-trivial one round linear characteristics for the above Feistel ciphers with 8 and 16 rounds respectively.

Similarly it can be shown that the number of non-trivial one-round characteristics needed for the above Feistel ciphers is two for every three rounds, since the round functions are permutations. By using meta-structures and performing 2R attacks (see [1]) it follows that we need at least 3 and 8 non-trivial one-round characteristics for example 1 and 2 respectively.

For comparison we use these estimates to obtain lower bounds on the complexities of linear and differential attacks on DES. The numbers in parentheses in Table 2 are the complexities of the best known practical attacks.

It is easily seen that none of the above prototypes are secure ciphers as they are described. The ciphers can be described as the concatenation of small ciphers, since the bits going in and out of the functions $f_i$ are not mixed. However by combining the above round functions with an appropriate linear mapping $L$, s.t. $F = L \circ f$ , strong ciphers may be obtained [18].

For the cubing function in example 1, there are possible trade offs between space and speed, one extreme is given in Table 2, the other extreme would be to pre-compute a table (an S-box) of $2^{17}$ 17 bit values, in that case the space for $f$ would be about 300 Kbytes and the speed would be $O$(2 look ups) per round. We believe that some useful method in between these two extremes can be

found. Using the cubing function alone with linear mappings might be dangerous because of the low degree of the output bit functions, i.e. only quadratic terms. The inverse function from example 2 has degree $n-1$ [18], in the above example the output bits would be of degree 7, however there seems to be no way of implementing the inverse function efficiently in $GF(2^n)$ for large $n$. We believe that a combination of the cubing and the small inverse functions from our two examples together with some linear mapping will be a good choice for a round function of a DES-like iterated cipher resistant to both linear and differential cryptanalysis.

## 4 Acknowledgements

The author would like to thank Kenneth Paterson, Shirlei Serconek and Gerhard Krämer for useful comments.

## References

1. E. Biham, A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard.* Springer Verlag, New York, 1993.
2. E. Biham. *New Types of Cryptanalytic Attacks Using Related Keys.* Proceedings of EuroCrypt'93, Springer Verlag, LNCS 765, 1994.
3. E. Biham. Private Communication.
4. L. Brown, J. Pieprzyk, J. Seberry. *LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications.* Proceedings of AusCrypt '90. Springer Verlag, LNCS 453, 1990.
5. L. Brown, M. Kwan, J. Pieprzyk, J. Seberry. *Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI.* Proceedings of AsiaCrypt'91, Springer Verlag, LNCS 739, 1993.
6. *Data Encryption Standard,* Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.
7. J.H. Evertse. *Linear Structures in Blockciphers.* Proceedings of EuroCrypt'87, Springer Verlag, LNCS 304, 1988.
8. H.M. Heys, S. E. Tavares. *The Design of Product Ciphers Resistant to Differential and Linear Cryptanalysis.* Technical Report, Aug. 19, 1993, Queen's University at Kingston, Ontario, Canada.
9. L.R. Knudsen. *Cryptanalysis of LOKI.* Proceedings of AsiaCrypt'91, Springer Verlag, LNCS 739, 1993.
10. L.R. Knudsen. *Iterative Characteristics of DES and $s^2$-DES.* Proceedings of Crypto'92, Springer Verlag, LNCS 740, 1993.
11. L.R. Knudsen. *Cryptanalysis of LOKI'91.* Proceedings of AusCrypt'92, Springer Verlag, LNCS 718, 1993.
12. L.R. Knudsen. *New potentially weak keys for DES and LOKI.* Unpublished manuscript.
13. X. Lai, J. L. Massey, S. Murphy. *Markov Ciphers and Differential Cryptanalysis.* Proceedings of EuroCrypt'91. Springer Verlag, LNCS 547, 1991.
14. X. Lai. *On the Design and Security of Block Ciphers.* Thesis, 1992.

15. M. Matsui. *Linear Cryptanalysis Method for DES Cipher.* Proceedings of EuroCrypt'93, Springer Verlag, LNCS 765, 1994.
16. M. Matsui. *Linear Cryptanalysis Method of DES Cipher (I).* Private Communications.
17. K. Nyberg, L.R. Knudsen. *Provable Security Against a Differential Attack.* To appear in the Journal of Cryptology. A preliminary version appears in the Proceedings of Crypto'92, Springer Verlag, LNCS 740, 1993.
18. K. Nyberg. *Differentially uniform mappings for cryptography.* Proceedings of EuroCrypt'93, Springer Verlag, LNCS 765, 1994.
19. L. J. O'Connor. *On the distribution of characteristics in bijective mappings.* Proceedings of EuroCrypt'93, Springer Verlag, LNCS 765, 1994.
20. J.-J. Quisquater, Y. Desmedt, M. Davio. *The importance of 'good' key scheduling schemes.* Proceedings of Crypto'85. Springer Verlag, LNCS 218, 1986.
21. M.J. Wiener. *Efficient DES key search.* To appear in the proceedings of Crypto'93.