J. Cryptology (2002) 15: 207–222
DOI: 10.1007/s00145-002-9839-y

Journal of
CRYPTOLOGY

The Security of Feistel Ciphers with Six Rounds or Less*

Lars R. Knudsen
Department of Mathematics, Technical University of Denmark,
Building 303, DK-2800 Kgs. Lyngby, Denmark
lars@ramkilde.com, www.ramkilde.com

Communicated by Bart Preneel

Received November 1998 and revised January 2002
Online publication 14 June 2002

Abstract. This paper considers the security of Feistel networks where the round functions are chosen at random from a family of 2^k randomly chosen functions for any k. Also considered are the networks where the round functions are themselves permutations, since these have applications in practice. The constructions are attacked under the assumption that a key-recovery attack on one round function itself requires an exhaustive search over all 2^k possible functions. Attacks are given on all three-, four-, five-, and six-round Feistel constructions and interesting bounds on their security level are obtained. In a chosen text scenario the key recovery attacks on the four-round constructions, the analogue to the super pseudorandom permutations in the Luby and Rackoff model, take roughly only the time of an exhaustive search for the key of one round. A side result of the presented attacks is that some constructions, which have been proved super pseudorandom in the model of Luby and Rackoff, do not seem to offer more security in our model than constructions which are not super pseudorandom.

Key words. Feistel ciphers, Luby–Rackoff permutations, Cryptanalysis, Data Encryption Standard.

1. Introduction

In their celebrated paper [16] Luby and Rackoff showed how to construct $2n$-bit pseudorandom permutations from n-bit pseudorandom functions. The constructions use three and four rounds in Feistel networks [11] with a randomly chosen function in the round function. An interpretation of Luby and Rackoff's result is, that in order to be able to distinguish the three-round construction from a randomly chosen $2n$-bit function with probability close to one, an attacker needs at least $2^{n/2}$ chosen plaintexts and their

[*] Part of the work in this article was done whilst visiting the Department of Computer Science and Engineering, University of California at San Diego, on leave from the Department of Informatics, University of Bergen, supported by the Norwegian Research Council.

corresponding ciphertexts. Such a permutation is called *pseudorandom* [16]. However, if an attacker can mount a chosen plaintext and a chosen ciphertext attack, he is able to distinguish the construction from a randomly chosen $2n$-bit function using two chosen plaintexts and one chosen ciphertext. Luby and Rackoff also showed that even in a combined chosen plaintext and chosen ciphertext attack for the four-round construction, an attacker will need roughly $2^{n/2}$ chosen texts to win with probability close to one. Such a permutation is called *super pseudorandom*.

Since [16] much research has been done in that direction and many other (super) pseudorandom constructions have been suggested, see, e.g., [21] for a survey. The security of all these constructions is measured in terms of the complexity of distinguishing the outputs from the outputs of a truly random function.

Aeillo and Venkatesan [1] showed that with q chosen plaintexts one can distinguish the three-round construction from a random function with probability close to $q^2/2^n$. (A similar but weaker result was previously shown by Patarin [24].) Patarin [24] showed that with roughly $2^{n/2}$ chosen plaintexts there is an algorithm A which distinguishes the four-round construction from a random function with "good probability", more precisely, A outputs "1" with a probability twice as high when the four-round construction is considered. (This was later restated in [1].) Thus, these results show that the inequalities by Luby and Rackoff are tight, that is, to distinguish three rounds from a randomly chosen function with probability close to one, an attacker needs at least but not much more than $2^{n/2}$ chosen plaintexts and their corresponding ciphertexts and similarly for four rounds.

Patarin [26] showed that to distinguish a six-round construction from a random $2n$-bit function with a high probability, an attacker would need to see the encryptions of at least $2^{3n/4}$ plaintexts. Also, in [1] and [24] it was mentioned that with 2^n chosen plaintexts it is possible to distinguish constructions with r rounds for any r from a random function. This follows from the trivial fact that the Feistel constructions are permutations and with 2^n chosen distinct plaintexts, the resulting ciphertexts will all be distinct, whereas a collision is likely to occur for a truly random function.

In this paper we consider a model different from that of Luby and Rackoff. Instead of choosing the round functions at random from the set of all functions, it is assumed that the round functions in the Feistel network are chosen at random from a subset of 2^k randomly chosen functions. Each round function is specified by a k-bit key. We then try to cryptanalyse such constructions, more precisely, we try to determine the complexity of finding all the keys of the cipher with r rounds. Also, constructions where the round function in the Feistel network is itself a permutation are considered. Thus, given a family of pseudorandom n-bit permutations, the strength of the resulting $2n$-bit permutations with respect to key recovery attacks is investigated.

For the remainder of this paper, the time complexity is measured in the required number of round function evaluations of the attacked cipher and memory requirements are measured in the number of n-bit words.

This paper is organised as follows. In Section 2 we define the Feistel ciphers considered in the rest of the paper. These constructions are analysed in Section 3 with respect to key recovery attacks. Section 4 discusses the security of some constructions for which analogue constructions in the Luby–Rackoff model have been proved pseudorandom and some which have been proved super pseudorandom. In Section 5 applications for the DES are given, related work is discussed in Section 6 and conclusions and open problems are given in Section 7.

2. Feistel Ciphers with Ideal Round Functions

Let $\{0, 1\}^n$ be the set of all 2^n binary strings of length n, and let $\mathcal{F}^n$ and $\mathcal{P}^n$ denote the set of all functions, respectively permutations, mapping $\{0, 1\}^n$ to itself. Also, we let $\mathbf{F}^n$ and $\mathbf{P}^n$ denote sets of 2^k functions, respectively 2^k permutations, chosen independently and uniformly at random from $\mathcal{F}^n$, respectively $\mathcal{P}^n$. The round functions $\mathbf{f}_i$ and permutations $\mathbf{p}_i$ are chosen uniformly at random from $\mathbf{F}^n$, respectively $\mathbf{P}^n$. Note that $\mathcal{P}^n \subset \mathcal{F}^n$ and that the probability that a randomly chosen function is a permutation is $2^n!/2^{n2^n}$, which using Stirling's approximation is roughly $\sqrt{2\pi}2^{n/2}/e^{2^n}$ for large n. Clearly this probability decreases rapidly with n. As an example, for $n = 6$ the probability is about 2^{-88}. Therefore, in the following, when considering a function from $\mathcal{F}^n$ it is assumed that it is not a permutation.

A Feistel network consists of a number of rounds, where one round is defined as follows. Denote by (L, R) the $2n$-bit input (plaintext), set $x_0 = L$ and $y_0 = R$ and let (x_{i-1}, y_{i-1}) be the input to the ith round. The output of the round is defined

$$\begin{aligned} x_i &= y_{i-1}, \\ y_i &= \psi_i(y_{i-1}) \oplus x_{i-1}, \end{aligned}$$

where ψ is called the round function. Define $EF^j(L, R) = (T, S) = (y_j, x_j)$ for $\psi_i = \mathbf{f}_i$ and similarly define $EP^j(L, R) = (T, S) = (y_j, x_j)$ for $\psi_i = \mathbf{p}_i$.

A particular round function is specified by selecting a k-bit key k_i, in a way similar to the DES being thought of as a family of 2^{56} permutations of 64 bits, where one permutation can be selected by specifying a 56-bit key. The resulting r-round block ciphers have block size $2n$ and key size $r \cdot k$. Note that there are in total 2^{n2^n} n-bit mappings, thus with $k = n2^n$ our construction equals that of Luby and Rackoff.

In the following let $\lceil x \rceil$ denote the smallest integer greater than x.

Definition 1 (Ideal Function). Let f be an n-bit function or permutation chosen from a family of 2^k functions. Then f is called ideal, if finding the key (with certainty) which specifies the function requires at least 2^k function evaluations and at least $\lceil k/n \rceil$ inputs and corresponding outputs.

It is assumed that each of the functions from the family of 2^k functions is uniquely determined by a k-bit key. A side result of the above definition is as follows. If in an r-round Feistel construction the round functions $\mathbf{f}_i$ or $\mathbf{p}_i$ are ideal, independent, and randomly chosen, then the time complexity of a key recovery attack which finds all keys is at least $r \cdot 2^k$ round function evaluations.

As mentioned earlier, it has been shown that with roughly $2^{n/2}$ chosen plaintexts, it is possible to distinguish both the three- and four-round Luby–Rackoff constructions from a randomly chosen $2n$-bit function with a high probability. These distinguishers make use of the fact that two different inputs to the functions $\mathbf{f}_i$ may yield equal outputs.

Therefore these distinguishers will not work if the round functions are permutations. However, the following result holds.

Theorem 1. *There exists an attack A (a distinguisher) which distinguishes EP^3 and EP^4 from a randomly chosen function using $2^{(n+1)/2}$ chosen plaintexts.*

Proof. EP^3: Choose $2^{(n+1)/2}$ plaintexts of the form (L_i, R) for $i = 1, \dots, 2^{(n+1)/2}$, where R is a fixed value and $L_i \neq L_j$ for $i \neq j$. Let (T_i, S_i) denote the ciphertexts after three rounds of encryption. Then it holds that $S_i \neq S_j$ for $1 \leq i < j \leq 2^{(n+1)/2}$. If the values (T_i, S_i) are output from a randomly chosen function there exists some i, j, where $i \neq j$ and $S_i = S_j$ with probability $1 - (1 - 2^{-n})^{2^n}$ which is approximately 0.63 for $n > 4$.

EP^4: Choose $2^{(n+1)/2}$ plaintexts of the form (L_i, R) for $i = 1, \dots, 2^{(n+1)/2}$, where R is a fixed value and where all L_i's are distinct. Let (T_i, S_i) denote the ciphertexts after four rounds of encryption. Form the values $\alpha_i = L_i \oplus S_i$ for $1 \leq i \leq 2^{(n+1)/2}$. Then it holds for EP^4 that $\alpha_i \neq \alpha_j$ for $1 \leq i < j \leq 2^{(n+1)/2}$. If the values (T_i, S_i) were computed by a randomly chosen function there would exist a pair i, j, such that $\alpha_i = \alpha_j$ with a probability of 0.63. □

As mentioned earlier, Luby and Rackoff showed that in a combined chosen plaintext and chosen ciphertext scenario their three-round construction can be distinguished from a randomly chosen $2n$-bit function using two chosen plaintexts and one chosen ciphertext. This result holds also for EF^3 and EP^3. The argument is reviewed here, since it will be used several times in the following. Consider Fig. 1.

An attacker chooses two plaintexts with left halves L_1 and L_2, where $L_1 \neq L_2$ and with equal right halves R. From the corresponding ciphertexts (T_1, S_1) and (T_2, S_2) he computes the ciphertext $(T_1 \oplus L_1 \oplus L_2, S_1)$ and asks for the corresponding plaintext. If the encryptions are computed with EF^3 (or EP^3) the right half of this plaintext equals $R \oplus S_1 \oplus S_2$, in which case the attacker would guess that the permutation is not randomly

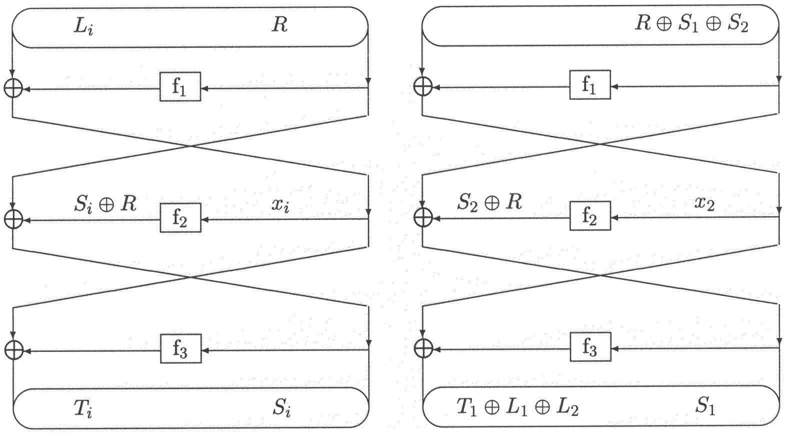

Fig. 1. Two three-round encryptions in the distinguisher. In the cipher on the left, $i = 1, 2$.

chosen. Note that $x_1 \oplus x_2 = L_1 \oplus L_2$. In the distinguisher for EF^3 one has to ensure that $S_1 \neq S_2$, since if $S_1 = S_2$ the ciphertext $(T_1 \oplus L_1 \oplus L_2, S_1)$ is equal to the ciphertext (T_2, S_2), thus the ciphertext of one of the chosen plaintexts. However, when the left halves of the inputs are chosen uniformly at random, $S_1 \neq S_2$ with probability $1 - 2^{-n}$.

First it is shown that for any three-round construction, there is an algorithm which, on input $d > 1$ chosen plaintexts and their ciphertexts, yields an algorithm which returns half of the plaintext for almost any of d^2 ciphertexts independent of the size of the keys. The method used in the proof of the following result is in essence the way Luby and Rackoff show that a three-round construction is not super pseudorandom. One exception is the case where a permutation is used in the round function.

Theorem 2. *Consider* (*any*) *three-round* $2n$*-bit Feistel construction and assume that* $2 \leq d \leq 2^n$ *chosen plaintexts and their corresponding ciphertexts are available. Then there exists an algorithm which*, *on input any of about* d^2 *chosen ciphertexts*, *returns the right half of the corresponding plaintext without the knowledge of any of the secret keys. If the round function is a permutation and* $d = 2^n$ *one obtains an algorithm which*, *on input any of the* 2^{2n} *ciphertexts*, *returns the right half of the plaintext.*

Proof. Choose $2 \leq d \leq 2^n$ plaintexts (L_i, R) for $L_i = 0, \ldots, d-1$, such that $L_i \neq L_j$ for $0 \leq i < j < d$, and get the corresponding ciphertexts (T_i, S_i). Then the right halves of the plaintexts of the d^2 ciphertexts $(T_i \oplus L_i \oplus L_j, S_i)$ are $S_i \oplus S_j \oplus R$ for $0 \leq i, j < d$. This fact was used by Luby and Rackoff [16] to distinguish a three-round Feistel construction from a random function with two chosen plaintexts and one chosen ciphertext. It remains to show how many of these ciphertexts are different. For any $i = 0, \ldots, d-1$ the ciphertexts $(T_i \oplus L_i \oplus L_j, S_i)$ for $j = 0, \ldots, d-1$ are all different. When the round function is not a permutation it can happen that $S_i = S_j$ for $i \neq j$ and consequently there can be two ciphertexts such that $(T_i \oplus L_i \oplus L_l, S_i) = (T_j \oplus L_j \oplus L_k, S_j)$, thus, the d^2 ciphertexts are not distinct. It holds that d randomly chosen n-bit values will be pairwise distinct with probability $(1 - 2^{-n})^{d(d-1)/2^{n+1}}$. This means that the number of distinct S_i's will be close to d for $d < 2^{n/2}$ and for $d = 2^n$ the number of distinct values S_i is about $0.63 \cdot 2^n$. If the round function is a permutation all S_i's are different, from which the last claim follows. □

It should be stressed the above result is no contradiction to the results of Luby and Rackoff. In the next section Feistel networks with three to six rounds are analysed with respect to key recovery attacks.

3. Key-Recovery Attacks on the Feistel Ciphers

The attacks presented in this section first find the key in one of the outer rounds, that is, in the last round or in the first round; subsequently the remaining keys can be found by attacking a cipher one round shorter. Note that an attack which distinguishes an $(r-1)$-round Feistel construction from a random function using x chosen texts with some probability p, can be extended into a key recovery attack on an r-round cipher. Repeat the distinguishing attack for all values of the key in the last (or first) round by decrypting all ciphertexts (or plaintexts) for all values of the particular round key. The complexity of the attack depends on n, k, x, and p. However, as we shall see, this attack is not always the best possible attack.

As mentioned earlier it has been shown [1], [24] that with 2^n chosen plaintexts it is possible to distinguish EF^r from a random function for any r. This is due to the fact that EF^r is a permutation. This, however, cannot be used directly in key recovery attacks on EF^r. The key recovery attacks considered here are different, since we are trying to distinguish between sets of permutations. Also note that the $2^{3n/4}$ result for EF^6 in [26] is only a lower bound, and thus cannot be used directly in a key recovery attack as described in the previous paragraph.

The notion of a *characteristic* by Biham and Shamir [4], [5] is used in the following. That is, $((l_0, r_0), \ldots, (l_s, r_s))$ specifies that for a pair of plaintexts of exclusive-or difference l_0 in the left halves and r_0 in the right halves the difference after s rounds of encryption is expected to be (l_s, r_s). To help the reader the following notation is used for a one-round characteristic:

$$(l_0, r_0) \;{}^{r_0 \to l_0 \oplus r_1}\; (l_1, r_1),$$

where the middle part specifies the input difference and output difference of the nonlinear function in the round function of the Feistel cipher. In a traditional characteristic one predicts the exact values of (l_i, r_i). A broader definition is that of *differentials* by Lai et al. [15], where the intermediate values (l_i, r_i), $1 \leq i < s$, of a characteristic may vary. A yet broader definition is that of truncated differentials by Knudsen [13], where only parts of the output differences are predicted. In this paper only characteristics are used.

3.1. *Three-Round Constructions*

Proposition 1. *For all $2n$-bit three-round Feistel constructions EF^3 and EP^3 there exist key recovery attacks which find the secret key in time $4 \cdot 2^k$ using $\lceil k/n \rceil + 1$ chosen plaintexts.*

Proof. It is straightforward to perform a meet-in-the-middle attack for the keys in the first and third rounds. This attack requires $\lceil k/n \rceil$ known plaintexts and about 2^k words of memory. There exist time–memory tradeoffs for this attack by van Oorschot and Wiener [28], [29]. Once k_1 and k_3 have been found, k_2 can be found. There is another attack which on input $\lceil k/n \rceil + 1$ chosen plaintexts finds the secret key with only small memory. Choose plaintexts (L_1, R) and (L_2, R). From the ciphertexts (T, S) and (T', S') check whether $\mathbf{f}_3(S) \oplus \mathbf{f}_3(S') = L_1 \oplus L_2 \oplus T \oplus T'$ for all values of the key in the third round. This will always be the case for the correct value of the key, but will only hold with probability 2^{-n} for an incorrect value of the key. With $\lceil k/n \rceil + 1$ chosen plaintexts the above test can be performed at least $\lceil k/n \rceil$ times and with a high probability only the correct value of k_3 is left. Once k_3 has been found, it is straightforward to find the other keys by exhaustive search. Finding k_3 takes the time of $2 \cdot 2^k$ round function evaluations. The two remaining keys can be found in the time of $2 \cdot 2^k$ round function evaluations. □

Since the round functions are assumed to be ideal, see Definition 1, the time complexities of the attacks of Proposition 1 are close to optimal.

3.2. *Four-Round Constructions*

It is possible to attack a four-round construction by a simple extension of Luby–Rackoff's method which distinguishes a three-round construction from a random permutation. Simply guess the key in the last round and execute the distinguishing algorithm described earlier. The guesses of the last-round key for which the distinguisher succeeds are candidates. Repeat the attack until only one value of the key remains a candidate. In total this attack requires $3 \cdot 2^k$ chosen texts and time $3 \cdot 2^k$. For $k > n/2$ there are faster attacks.

Proposition 2. *For all* $2n$*-bit four-round Feistel constructions* EF^4 *there exist key recovery attacks which find the secret key in time* $6 \cdot 2^k$ *using* $c \cdot 2^{n/2}$ *chosen plaintexts and* $c \cdot 2^{n/2}$ *words of memory, where* $c = \sqrt{2\lceil k/n \rceil}$.

Proof. Consider the following four-round characteristic:

$$(\alpha, 0) \overset{0 \to 0}{} (0, \alpha) \overset{\alpha \to 0}{} (\alpha, 0) \overset{0 \to 0}{} (0, \alpha) \overset{\alpha \to \beta}{} (\alpha, \beta),$$

where $\alpha \neq 0$ and β can take any value. That is, the inputs to **f** in the first and third rounds are equal. The inputs in the second and fourth rounds have difference α, and the outputs of **f** in the second round are equal. Consider a set of $\sqrt{2 \cdot \lceil k/n \rceil 2^{n/2}}$ plaintexts (L_i, R), where R is a fixed value and the L_i's are randomly chosen, and where the corresponding ciphertexts are (T_i, S_i). One expects to find $\lceil k/n \rceil$ pairs i, j such that $L_i \oplus L_j = S_i \oplus S_j$, that is, pairs of texts in accordance with the above characteristic, where $\alpha = L_i \oplus L_j$. For all values of the key in the fourth round, decrypt these pairs of ciphertexts one round and check whether equal values are obtained in the inputs to the round function in the third round. For one such pair of ciphertexts, a wrong value of the key will be suggested with probability 2^{-n}, thus with $\lceil k/n \rceil$ such pairs the probability that a key is suggested every time is at most 2^{-k}. Therefore it can be expected that only a few values of the key including the correct one will be left as candidates for the secret key. Note that for most (wrong) values of the key in the fourth round, only one pair of ciphertexts needs to be decrypted. Thus, finding k_4 takes the time of $2 \cdot 2^k$ round function evaluations. Subsequently, the attack of Proposition 1 on the three-round construction can be mounted to find the remaining keys. □

The attack in the following proposition is less effective than the attack of Proposition 2, however, it applies to both EF^4 and EP^4 whereas the result of Proposition 2 applies to only EF^4.

Proposition 3. *For all* $2n$*-bit four-round Feistel constructions* EP^4 *and* EF^4 *there exist key recovery attacks which find the secret key in time* $8 \cdot 2^k$ *using* $c \cdot 2^{n/2}$ *chosen plaintexts,* $c \cdot 2^{n/2}$ *chosen ciphertexts, and* $c \cdot 2^{n/2}$ *words of memory, where* $c = \lceil k/n \rceil$.

Proof. The proof is the same for EP^4 and EF^4. Consider Fig. 2. Let R_1, R_2 be two n-bit constants, such that $R_1 \neq R_2$. Choose $2^{n/2}$ plaintexts of the form (L_i, R_1) for $i = 0, \ldots, 2^{n/2} - 1$, and $2^{n/2}$ plaintexts of the form (L_i, R_2) for $i = 2^{n/2}, \ldots, 2^{n/2+1} - 1$, such that the set $\{L_u \oplus L_v\}$ for $u = 0, \ldots, 2^{n/2} - 1$, and $v = 2^{n/2}, \ldots, 2^{n/2+1} - 1$, is exactly the set of all n-bit strings. Denote the resulting ciphertexts (T_i, S_i).

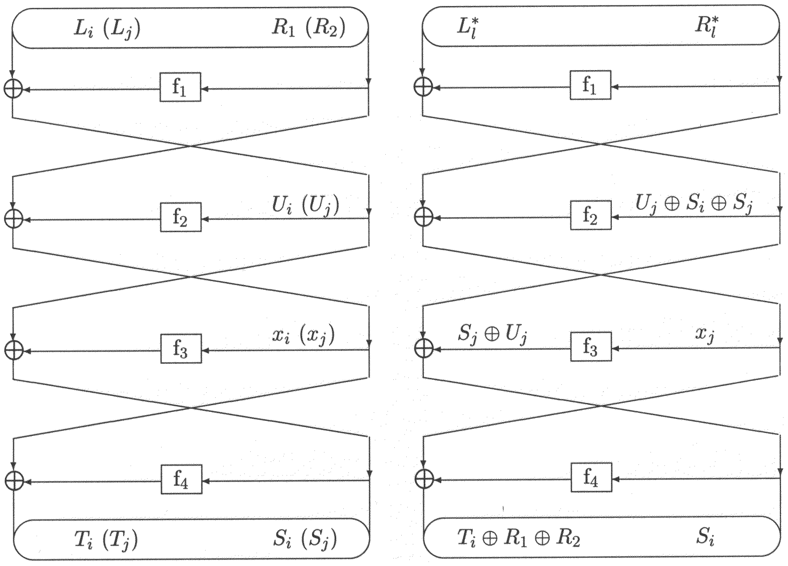

Fig. 2. The four-round encryptions in the attack of Proposition 3.

Get the plaintexts (L_l^*, R_l^*) of the $2^{n/2+1}$ ciphertexts $(T_i \oplus R_1 \oplus R_2, S_i)$. Consider the left half of Fig. 2. For each possible value of the key k_1 in the first round, find the two plaintexts (L_i, R_1) and (L_j, R_2) such that the inputs to the second round are equal $(U_i = U_j)$. Since R_1 and R_2 are fixed, this requires only two round function evaluations. Note also that the attacker has such a pair of plaintexts, since the set $\{L_u \oplus L_v\}$ is all n-bit strings. Also, if $U_i = U_j$, then $x_i \oplus x_j = R_1 \oplus R_2$. Let (T_i, S_i) and (T_j, S_j) be the two corresponding ciphertexts. From the plaintexts of the chosen ciphertexts $(T_i \oplus R_1 \oplus R_2, S_i)$ and $(T_j \oplus R_1 \oplus R_2, S_j)$ find the inputs to the second round using the guess of k_1. It follows from the rightmost construction in Fig. 2 that for the correct guess of k_1 the two inputs are $U_i \oplus S_i \oplus S_j$ and $U_j \oplus S_i \oplus S_j$. The two inputs are equal, since $U_i = U_j$. If it is assumed that for wrong values of k_1 these two inputs are equal with probability 2^{-n}, after one iteration of the attack about 2^{k-n} keys will remain candidates. Repeating the attack $\lceil k/n \rceil$ times will identify the correct value of k_1. This part of the attack takes the time of $4 \cdot 2^k$ round function evaluations. Once k_1 has been determined, k_4 can be determined from the pairs considered. For the correct value of k_1, pairs of texts are known for which $U_i = U_j$ and consequently it is known that $x_i \oplus x_j = R_1 \oplus R_2$. This can be used to test the value of k_4 using $2 \cdot 2^k$ round function evaluations, which is also the time to find the remaining two keys. □

Assuming that the round functions are ideal the time complexities of the attacks of Propositions 2 and 3 are close to optimal. It is further conjectured that any key recovery attack on EF^4 and EP^4 needs at least 2^l, $l = \min(k, n/2)$, known or chosen texts.

The attack of Proposition 3 applies to Ladder-DES [2], which is EP^4 where DES is used in the round function. The attack requires about 2^{58} encryptions with about 2^{33}

chosen texts. This is faster than the attack given in [2], although it should be pointed out that the latter uses only chosen plaintexts and no chosen ciphertexts.

3.3. *Five-Round Constructions*

For five-round constructions there is a simple meet-in-the-middle attack which finds the secret keys in time 2^{2k} using 2^{2k} words of memory. There are variants of such meet-in-the-middle attacks with a tradeoff between memory and time [28], [29]. However, there are faster, non-trivial attacks.

Proposition 4. *For all* $2n$*-bit five-round Feistel constructions* EF^5 *there exist key recovery attacks which find the secret key in time* $c \cdot 2^{(k+n/2)}$, *using* $c \cdot 2^{n/2}$ *chosen plaintexts and* $c \cdot 2^{n/2}$ *words of memory, where* c *is a function of* k, *and* $c \leq 30$ *for* $k \leq 128$.

Proof. Choose $c \cdot 2^{n/2}$ different plaintexts (L_i, R) and denote the resulting ciphertexts (T_i, S_i). Consider the following four-round characteristic:

$$(\alpha, 0) \ {}^{0\to 0}\ (0, \alpha) \ {}^{\alpha\to 0}\ (\alpha, 0) \ {}^{0\to 0}\ (0, \alpha) \ {}^{\alpha\to\beta}\ (\alpha, \beta),$$

where $\alpha \neq 0$ and β can take any value. Only the value of α after four rounds of encryption is of interest. Patarin points out in [24] that the following characteristic also provides the desired result after four rounds:

$$(\alpha, 0) \ {}^{0\to 0}\ (0, \alpha) \ {}^{\alpha\to\gamma}\ (\alpha, \gamma) \ {}^{\gamma\to 0}\ (\gamma, \alpha) \ {}^{\alpha\to\beta\oplus\gamma}\ (\alpha, \beta),$$

where γ can take any value. The first characteristic has a probability of 2^{-n} and the second characteristic a probability of $(1 - 2^{-n})2^{-n}$, since γ can take any value except for zero. For all keys in the fifth round decrypt all ciphertexts (T_i, S_i) one round and count the number of pairs that yield the desired difference $\alpha = L_i \oplus L_j$ after four rounds. It follows that the probability of success for this test is about 2^{-n+1} for the correct value of the key and 2^{-n} for a wrong value of the key. With $c \cdot 2^{n/2}$ texts the expected number of matches for a wrong value of the key is about $c(c-1)/2$. The expected number of matches for the correct value of the key is about $c(c-1)$. Thus by using sufficiently many plaintexts a unique key will be suggested significantly more often than other keys. In the attack only keys suggested more than a certain number of times are stored. The necessary number of plaintexts depends on k. Using the Central Limit Theorem, see, e.g., p. 244 of [10], it can be shown that, if $c(c-1) = 720$, the probability that the number of times a wrong value of the key is suggested is larger than for the correct value of the key is 2^{-136}. Thus, if $k \leq 128$ (which will be the case for all practical applications) it suffices to choose $c = 30$ so that with a high probability the correct value of the key will be the most suggested value. If $k \leq 64$, $c = 20$ is sufficient. Subsequently, the attack of Proposition 2 can be applied to find the remaining keys. □

Note that for the values of c above, the value of the counter for the correct value of the key is the largest with a high probability. There exist variants of this part of the attack, e.g., using "key-ranking" as proposed by Matsui in [18]. Here one would choose c such that with a high probability the value of the counter for the correct value of the key will be among the t, e.g., $t = 100$, highest values. Subsequently, the attack on the four-round construction can be performed for each of these t values.

Proposition 5. *For all $2n$-bit five-round Feistel constructions EP^5 there exist key recovery attacks which find the secret key in time $2^{k+(n+3)/2}$ using $\sqrt{2k} \cdot 2^{n/2}$ chosen plaintexts requiring $\sqrt{2k} \cdot 2^{n/2}$ words of memory.*

Proof. Choose $\sqrt{2k} \cdot 2^{n/2}$ different plaintexts (L_i, R) and denote the resulting ciphertexts (T_i, S_i). Consider the following four-round characteristic:

$$(\alpha, 0) \ {}^{0 \to 0} \ (0, \alpha) \ {}^{\alpha \to \beta} \ (\alpha, \beta) \ {}^{\beta \to \alpha \oplus \gamma} \ (\beta, \gamma) \ {}^{\gamma \to \beta \oplus \varphi} \ (\gamma, \varphi),$$

where $\alpha \neq 0$. Only the value of γ after four rounds of encryption is of interest. Since the round function is a permutation, $\beta \neq 0$ and thus the outputs of the third round are not equal and consequently $\gamma \neq \alpha$. For all values of k_5 decrypt all ciphertexts (T_i, S_i) one round. Denote the inputs to the round function in the fourth round by U_i. Subsequently, find i, j such that $L_i \oplus L_j = U_i \oplus U_j$. It follows from above that for the correct value of k_5 such pairs do not exist. For a wrong value of k_5 there exist such pairs with some positive probability. Thus by running the attack with sufficiently many plaintexts the probability that such pairs exist for (almost) every wrong value of the key can be made large. With $\sqrt{2d} \cdot 2^{n/2}$ chosen texts one can expect d such pairs for all wrong values of the key, since $\binom{\sqrt{2d} \cdot 2^{n/2}}{2} / 2^n \simeq d$. With $d = 1$ one can expect half of the values of k_5 to be left suggested, thus with $d = k$ with a high probability only a few candidates (including the correct value of k_5) are left. The time complexity of this attack is roughly $2^{k+n/2+1}$. Observe that for a wrong value of k_5 one can expect to find pairs satisfying $L_i \oplus L_j = U_i \oplus U_j$ after examining $2^{n/2+1/2}$ texts. Thus for half of the values of k_5, only $2^{n/2+1/2}$ decryptions are needed. With $2^{n/2+1}$ texts one can expect two pairs yielding the desired α, thus hereafter three-quarters of the keys are discarded, etc. The time complexity therefore is at most $2^{n/2+1/2} \cdot (2^k + 2^{k-1} + 2^{k-2} + \cdots + 2 + 1) \simeq 2^{n/2+1/2} 2^{k+1} = 2^{k+(n+3)/2}$. Subsequently, the attack of Proposition 3 can be applied to find the remaining keys. □

The attacks of Propositions 4 and 5 show an upper bound of the strength of the constructions. However, the fact that an attacker will need at least $2^{n/2}$ chosen texts to distinguish a four-round construction from a random function, gives an indication of the strength of our attacks. For $k > (n + 3)/2$ the time complexity is less than 2^{2k} (the complexity of a meet-in-the-middle attack).

3.4. *Six-Round Constructions*

For $2n$-bit six-round constructions a simple meet-in-the-middle attack will find the secret keys in time 2^{3k} using 2^{2k} words of memory. As mentioned already, there are variants of the attacks with a tradeoff between memory and time [28], [29]. However, there are faster attacks.

Proposition 6. *For all six-round Feistel constructions EF^6 there exist key recovery attacks which find the secret key in time $c \cdot 2^{k+n}$ using $c \cdot 2^n$ chosen plaintexts with $c \cdot 2^n$ words of memory, where c is a function of k, and $c \leq 720$ for $k \leq 128$.*

Proof. Consider the following five-round characteristic:

$$(\alpha, 0) \ {}^{0\to 0}\ (0, \alpha) \ {}^{\alpha\to 0}\ (\alpha, 0) \ {}^{0\to 0}\ (0, \alpha) \ {}^{\alpha\to 0}\ (\alpha, 0) \ {}^{0\to 0}\ (0, \alpha),$$

where $\alpha \neq 0$. The probability of the characteristic is 2^{-n} in both the second and the fourth rounds, the overall probability is 2^{-2n}. Also consider the following five-round characteristic:

$$(\alpha, 0) \ {}^{0\to 0}\ (0, \alpha) \ {}^{\alpha\to \gamma}\ (\alpha, \gamma) \ {}^{\gamma\to 0}\ (\gamma, \alpha) \ {}^{\alpha\to \gamma}\ (\alpha, 0) \ {}^{0\to 0}\ (0, \alpha),$$

where $\alpha \neq 0$ and $\gamma \neq 0$. The probability of the characteristic is $1 - 2^{-n}$ in the second round, since γ can take any value except for zero, and 2^{-n} in both the third and fourth rounds. The overall probability is thus about 2^{-2n}. In total a pair of plaintexts of difference $(\alpha, 0)$ leads to ciphertexts after five rounds of difference $(0, \alpha)$ with a probability of about 2^{-2n+1}, while for a randomly chosen permutation this would happen with probability 2^{-2n}, the probability taken over all possible functions and over all plaintexts.

The attack goes as follows. Choose all 2^n plaintexts with a fixed right half and variable left half, $P_i = (L_i, R)$ for $i = 1, \ldots, 2^n$. Let (T_i, S_i) denote the corresponding ciphertexts. Compute $L_i \oplus S_i$ and find matches $L_i \oplus S_i = L_j \oplus S_j$ for $i \neq j$. Pairs of plaintexts with no such match are discarded and not considered in the attack. One can expect about 2^{n-1} such matches, since $\binom{2^n}{2}/2^n \simeq 2^{n-1}$. Let $\alpha = L_i \oplus L_j = S_i \oplus S_j$. For all the matching pairs and for all values of k_6 decrypt the ciphertexts one round. If the differences in the ciphertext halves after five rounds are α and zero, the value of the key k_6 is a candidate for the correct value. With 2^n plaintexts one can form 2^{2n-1} pairs and would expect to get one pair which follows one of the above two characteristics. A pair which does not follow any of the characteristics will suggest any wrong value of the key with an average probability of 2^{-n}. It follows that with 2^n chosen plaintexts, the expected number of times the correct value of the key will be suggested in the attack is one, while the expected number of times a wrong value of the key will be suggested is 0.5. From the proof of Proposition 4 it follows that by repeating the above attack about 720 times the probability that the correct value of the key is suggested the most is very high, provided that $k \leq 128$. Once k_6 has been found, the remaining five keys can be found using the attack of Proposition 4. □

As in the attack on EP^5 from the previous section, the "key-ranking" technique can be used in this attack.

The following lemma is used in a next attack on EP^6.

Lemma 1. *Consider the five-round Feistel construction EP^5. It holds that a pair of inputs with difference $\alpha \neq 0$ in the left halves and equal values in the right halves, never results in ciphertexts with difference α in the left halves and equal values in the right halves.*

Proof. Consider the following five-round characteristic:

$$(\alpha, 0) \ {}^{0\to 0}\ (0, \alpha) \ {}^{\alpha\to 0}\ (\alpha, 0) \ {}^{0\to 0}\ (0, \alpha) \ {}^{\alpha\to 0}\ (\alpha, 0) \ {}^{0\to 0}\ (\alpha, 0),$$

where $\alpha \neq 0$. Note that the halves are not swapped after the last round. We shall show that the probability of this characteristic is zero. Consider a pair of plaintexts with difference $\alpha \neq 0$ in the left halves and with equal right halves. Assume that the ciphertexts after five rounds have a difference of α in the left halves and zero in the right halves. This implies that the two inputs to the round function are equal both in the first and the fifth rounds. Subsequently, the differences in the inputs to the round function in the second and fourth rounds are both α. This means also that the outputs of the round function in the third rounds are equal, which again means that the inputs to the third rounds are equal. This leads to a contradiction, since this means that different inputs to the round function in the second rounds lead to equal outputs (and similarly for the fourth rounds), which is not possible since the round function is a permutation. So the assumption that the difference in the ciphertexts after five rounds $(0, \alpha)$ was wrong. In other words, a five-round characteristic with probability zero has been defined. □

This lemma was used by the author in a different context in the proof of Theorem 7.4.7 of [12]. Now we can prove the following result.

Proposition 7. *For all six-round Feistel constructions EP^6 there exist key recovery attacks which find the secret key in time 2^{k+n+1} using $k \cdot 2^n$ chosen plaintexts with $k \cdot 2^n$ words of memory.*

Proof. Consider the five-round characteristic of Lemma 1. The attack goes as follows. Choose all 2^n plaintexts with a fixed right half and variable left half, say $P_i = (L_i, R)$ for $i = 1, \ldots, 2^n$. Let (T_i, S_i) denote the corresponding ciphertexts. Compute $L_i \oplus S_i$ and find matches $L_i \oplus S_i = L_j \oplus S_j$ for $i \neq j$. One can expect about 2^{n-1} such matches (see previous proposition). Let $\alpha = L_i \oplus L_j = S_i \oplus S_j$. For all these matching pairs of plaintexts and for all values of k_6 decrypt the ciphertexts one round. If the differences in the ciphertext halves after five rounds are α and zero, the guess of the key is wrong. Note that for the correct value of k_6 one never obtains these differences after the fifth round, since the characteristic has probability zero. However, for wrong values of the key this will happen with probability 2^{-n} for each analysed pair. Thus with 2^{n-1} pairs about half of the keys will have been discarded. By repeating the attack k times, only a few values of k_6 will be left suggested. In total the attack requires $k \cdot 2^n$ chosen plaintexts, $(2^k + 2^{k-1} + 2^{k-2} + \cdots + 2 + 1) \cdot 2^n \simeq 2^{k+1} \cdot 2^n = 2^{k+n+1}$ encryptions, and $k \cdot 2^n$ words of memory. Once k_6 has been found, the remaining five keys can be found using the attack of Proposition 5. □

It is possible to perform the above attack with a smaller memory at the cost of a slight increase in the time complexity.

Table 1 lists the complexities of the attacks on three-, four-, five-, and six-round constructions. It is interesting to note that the complexities of the attacks on EP^i and EF^i are roughly the same for $i = 3, 4, 5, 6$. It is stressed that all the attacks of this section prove only an upper bound for the strength of the constructions and the reader is invited to improve the attacks.

Table 1. Complexities of the attacks on $2n$-bit Feistel constructions with k-bit round keys, where c is a function of k and $c \leq 30$ for $k \leq 128$.

Scheme	Time	Number of texts	Memory
EF^3	$4 \cdot 2^k$	$\lceil k/n \rceil + 1$	$\lceil k/n \rceil$
EP^3	$4 \cdot 2^k$	$\lceil k/n \rceil + 1$	$\lceil k/n \rceil$
EF^4	$6 \cdot 2^k$	$\sqrt{2\lceil k/n \rceil} \cdot 2^{n/2}$	$\sqrt{2\lceil k/n \rceil} \cdot 2^{n/2}$
EP^4	$8 \cdot 2^k$	$2\lceil k/n \rceil \cdot 2^{n/2}$	$2\lceil k/n \rceil \cdot 2^{n/2}$
EF^5	$c \cdot 2^{k+n/2}$	$c \cdot 2^{n/2}$	$c \cdot 2^{n/2}$
EP^5	$2^{k+(n+3)/2}$	$\sqrt{2k} \cdot 2^{n/2}$	$\sqrt{2k} \cdot 2^{n/2}$
EF^6	$c^2 \cdot 2^{k+n}$	$c^2 \cdot 2^n$	$c^2 \cdot 2^n$
EP^6	2^{k+n+1}	$k \cdot 2^n$	$k \cdot 2^n$

4. Pseudorandom versus Super Pseudorandom

Patarin [25], Sadeghiyan and Pieprzyk [27], and others have shown that for the super pseudorandom properties it is not necessary that all four functions in a four-round Luby–Rackoff construction are different. Let now $(\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4)$ denote a four-round construction. This notation will be used to show explicitly the relation between the functions $\mathbf{f}_i$. It has been shown that four-round super pseudorandom permutations can be constructed from only one or two pseudorandom functions. The constructions with one function will not be discussed any further, because for the key recovery attacks considered here these constructions can be attacked by the same trivial exhaustive key search attack. Table 2 lists the possible constructions with two different functions, see [25]. In the following we analyse these constructions in our model: it is assumed that the round functions are chosen randomly from a set of 2^k randomly chosen n-bit functions. It is easy to see that for constructions (1) and (2) from Table 2 the keys can be found in time 2^k using a few known plaintexts. The third construction can be attacked using only a few chosen plaintexts. Choose two plaintexts such that the inputs to $\mathbf{f}_1$ in the first round are equal. For all values of k_2 decrypt the ciphertexts two rounds. Since the difference in the inputs to $\mathbf{f}_2$ in the second round can be predicted from the plaintexts, k_2 will be identified. The best known attack on constructions (4) and (5) is that of Proposition 2. Also for (4) the "slide-attack" [6] applies with roughly the same complexity.

Table 2. Four-round permutations constructed from two functions.

Super pseudorandom		Not super pseudorandom
(1) $(\mathbf{f}_1, \mathbf{f}_1, \mathbf{f}_1, \mathbf{f}_2)$	(2) $(\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_1, \mathbf{f}_1)$	(5) $(\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_2, \mathbf{f}_1)$
(3) $(\mathbf{f}_1, \mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_2)$	(4) $(\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_1, \mathbf{f}_2)$	

For similar constructions with a permutation in the round function, (1), (2), and (3) can be attacked as before and (4) or rather $(\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_1, \mathbf{p}_2)$ can be attacked using only few chosen texts. To see this, note that by guessing the value of k_2 one can compute the outputs of $\mathbf{p}_2$ in the second round from the ciphertexts and plaintexts. If it is assumed that if $\mathbf{p}_2$ is known, then the inverse to $\mathbf{p}_2$ is also known, then one can find also the inputs to $\mathbf{p}_2$ in the second round. By choosing plaintexts equal in the right halves and different in the left halves, and thereby predicting the difference in the inputs to the second round one can identify k_2 in time roughly 2^{k+1} with $\lceil k/n \rceil$ texts. For (5) the best attack we have found has a complexity similar to that of Propositions 2 and 3. The attacks on (1)–(4) are all (close to) optimal under the assumptions of the constructions.

The point to make here is that a construction which is super pseudorandom in Luby and Rackoff's model is not necessarily stronger than a construction which is (only) pseudorandom when translated into our model.

5. Applications for DES

The keys of the DES have become too small as was illustrated in [9], [30], and [31]. Therefore, it is often recommended using a triple encryption scheme with the DES. However, the block size of the DES has become too small as well. It is well known that for an n-bit block cipher when about $2^{n/2}$ blocks are encrypted with the same key, with a high probability an attacker can deduce information about the plaintext blocks [8], [12]. The more blocks encrypted under the same key the more serious this attack is. Since $n = 64$ for the DES, some concern must be expressed regarding the matching ciphertext attacks. These attacks do not depend on the size of the keys and are therefore also applicable to a triple encryption scheme.

Next we discuss the 128-bit block ciphers obtained from Feistel networks where the DES is used in the round function. It follows that with 2^{64} ciphertext blocks information about the plaintext blocks is leaked. For key recovery attacks this paper shows that if the time complexity for the best known attacks of such a cipher is to be more than 2^{100}, then at least six rounds are needed. Using the DES in the round function the time complexity of the attack of Proposition 7 is about 2^{121} using about 2^{70} chosen plaintexts. The scheme encrypts a 128-bit block in the average time of that of three encryptions and is as fast as the triple encryption schemes on 64-bit blocks. In [14] the author proposes the block cipher DEAL, which is EP^6 using the DES in the round function. DEAL was submitted as a candidate for the AES block cipher competition initiated by the U.S. National Institute of Standards and Technology (NIST), see [23].

6. Related Work

In [7] Coppersmith analysed EF^4 where the round functions are randomly chosen from the set of all n-bit functions. He has shown that with $n2^n$ chosen plaintexts the round functions can be identified up to symmetry. With 8×2^n texts 99.9% of the functions are identified. The attack on DEAL by Knudsen in [14] uses for the first time a characteristic of probability zero. In [3] Biham et al. use similar structures under the name of "impossible differentials". In [17] Lucks offers a tradeoff between the number of text pairs and the time needed in the attack on DEAL.

7. Conclusion and Open Problems

In this paper the security of Feistel ciphers with ideal round functions was studied with emphasis on key recovery attacks. The security of the four-round construction with respect to key recovery attacks was shown to be roughly only that of the round function in a chosen text scenario. Attacks were presented also on five- and six-round constructions with a moderate increase in the complexity compared with the four-round attacks. It was further shown that a construction which is super pseudorandom in Luby and Rackoff's model is not necessarily stronger than a construction which is pseudorandom when translated into our model. Finally, using the DES as the round function in a Feistel construction was suggested. These constructions have some superior properties compared with the existing multiple schemes using the DES.

It is left as an open problem to extend the attacks in this paper to constructions with more than six rounds in a non-trivial manner. It would be interesting also to consider the class of Feistel networks where the round functions are fixed, and where the key material is inserted via a simple operation, e.g., exclusive-ors. Also, it would be interesting to analyse Matsui's MISTY networks [19], [20] in a model similar to the one used in this paper.

Acknowledgments

The author thanks Don Coppersmith, Stefan Lucks, Bart Preneel, Matt Robshaw, and David Wagner together with three anonymous referees for valuable comments on this paper.

References

[1] W. Aiello and R. Venkatesan. Foiling birthday attacks in length-doubling transformations. In U. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96*, LNCS 1070, pages 307–320. Springer-Verlag, Berlin, 1996.

[2] E. Biham. Cryptanalysis of Ladder-DES. In E. Biham, editor, *Fast Software Encryption*, *Fourth International Workshop*, *Haifa*, *Israel*, *January* 1997, LNCS 1267, pages 134–138. Springer-Verlag, Berlin, 1997.

[3] E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In J. Stern, editor, *Advances in Cryptology*: *EUROCRYPT '99*, LNCS 1592, pages 12–23. Springer-Verlag, Berlin, 1999.

[4] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

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

[6] A. Biryukov and D. Wagner. Slide attacks. In L.R. Knudsen, editor, *Fast Software Encryption*, *Sixth International Workshop*, *Rome*, *Italy*, *March* 1999, LNCS 1636, pages 245–259. Springer-Verlag, Berlin, 1999.

[7] D. Coppersmith. Luby–Rackoff: four rounds is not enough. Technical Report RC 20674, IBM, December 1996.

[8] D. Coppersmith, D.B. Johnson, and S.M. Matyas. A proposed mode for triple-DES encryption. *IBM Journal of Research and Development*, 40(2):253–261, March 1996.

[9] Electronic Frontier Foundation. *Cracking DES — Secrets of Encryption Research*, *Wiretap Politics & Chip Design*. O'Reilly, Cambridge, MA, 1998. ISBN 1-56592-520-3.

[10] W. Feller. *Probability Theory and its Applications*, Vol. I. Wiley, New York, 1950.

[11] H. Feistel, W.A. Notz, and J.L. Smith. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of IEEE*, 63(11):1545–1554, 1975.

[12] L.R. Knudsen. Block Ciphers – Analysis, Design and Applications. Ph.D. thesis, Aarhus University, 1994.

[13] L.R. Knudsen. Truncated and higher order differentials. In B. Preneel, editor, *Fast Software Encryption – Second International Workshop*, *Leuven*, *Belgium*, LNCS 1008, pages 196–211. Springer-Verlag, Berlin, 1995.

[14] L.R. Knudsen. DEAL – a 128-bit block cipher. Technical Report 151, Department of Informatics, University of Bergen, February 1998. Submitted as an AES candidate by Richard Outerbridge.

[15] X. Lai, J.L. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. In D.W. Davies, editor, *Advances in Cryptology - EUROCRYPT '*91, LNCS 547, pages 17–38. Springer-Verlag, Berlin, 1992.

[16] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal of Computing*, 17(2):373–386, 1988.

[17] S. Lucks. On the security of the 128-bit block cipher DEAL. In L.R. Knudsen, editor, *Fast Software Encryption*, *Sixth International Workshop*, *Rome*, *Italy*, *March* 1999, LNCS 1636, pages 60–70. Springer-Verlag, Berlin, 1999.

[18] M. Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In Y.G. Desmedt, editor, *Advances in Cryptology - CRYPTO '*94, LNCS 839, pages 1–11. Springer-Verlag, Berlin, 1994.

[19] M. Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. In D. Gollman, editor, *Fast Software Encryption*, *Third International Workshop*, *Cambridge*, *UK*, *February* 1996, LNCS 1039, pages 205–218. Springer-Verlag, Berlin, 1996.

[20] M. Matsui. New block encryption algorithm MISTY. In E. Biham, editor, *Fast Software Encryption*, *Fourth International Workshop*, *Haifa*, *Israel*, *January* 1997, LNCS 1267, pages 54–68. Springer-Verlag, Berlin, 1997.

[21] M. Naor and O. Reingold. On the construction of pseudorandom permutations: Luby–Rackoff revisited. *Journal of Cryptology*, 12(1):29–66, 1999.

[22] National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC, January 1977.

[23] National Institute of Standards and Technology. Advanced encryption algorithm (AES) development effort. `http://www.nist.gov/aes`.

[24] J. Patarin. New results on pseudorandom permutations generators based on the DES scheme. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO '*91, LNCS 576, pages 301–312. Springer-Verlag, Berlin, 1992.

[25] J. Patarin. How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function. In R.A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT '*92, LNCS 658, pages 256–266. Springer-Verlag, Berlin, 1993.

[26] J. Patarin. About Feistel schemes with six (or more) rounds. In S. Vaudenay, editor, *Fast Software Encryption*, *Fifth International Workshop*, *FSE '*98, *Paris*, *France*, *March* 1998, LNCS 1372, pages 103–121. Springer-Verlag, Berlin, 1998.

[27] B. Sadeghiyan and J. Pieprzyk. A construction for super pseudorandom permutations from a single pseudorandom function. In R.A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT '*92, LNCS 658, pages 267–284. Springer-Verlag, Berlin, 1993.

[28] P.C. van Oorschot and M.J. Wiener. Improving implementable meet-in-the-middle attacks of orders of magnitude. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO '*96, LNCS 1109, pages 229–236. Springer-Verlag, Berlin, 1996.

[29] P.C. van Oorschot and M.J. Wiener. Parallel collision search with cryptanalytic applications. *Journal of Cryptology*, 12(1):1–28, 1999.

[30] M.J. Wiener. Efficient DES key search. Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, May 1994. Presented at the Rump Session of CRYPTO '93.

[31] M.J. Wiener. Efficient DES key search – an update. *CryptoBytes*, 3(2):6–8, 1998.