On the Role of Key Schedules in Attacks on Iterated Ciphers

Lars R. Knudsen[1] and John E. Mathiassen[2]

[1] Department of Mathematics, Technical University of Denmark
[2] Department of Informatics, University of Bergen, Norway

Abstract. This paper considers iterated ciphers and their resistance against linear and differential cryptanalysis. In the theory of these attacks one assumes independence of the round keys in the ciphers. Very often though, the round keys are computed in a key schedule algorithm from a short key in a nonrandom fashion. In this paper it is shown by experiments that ciphers with complex key schedules resist both attacks better than ciphers with more straightforward key schedules. It is well-known that by assuming independent round keys the probabilities of differentials and linear hulls can be modeled by Markov chains and that for most such ciphers the distribution of the probabilities of these converge to the uniform distribution after some number of rounds. The presented experiments illustrate that some iterated ciphers with very simple key schedules will never reach this uniform distribution. Also the experiments show that ciphers with well-designed, complex key schedules reach the uniform distribution faster (using fewer rounds) than ciphers with poorly designed key schedules. As a side result it was found that there exist ciphers for which the differential of the highest probability for one fixed key is also the differential of the highest probability for any other key. It is believed that this is the first such example provided in the literature.

1 Introduction

Most block ciphers today are so-called iterated ciphers. Here the ciphertext is computed as a function of the plaintext and the user-selected key, K, in a number of iterations. Typically, the user-selected key is input to a key scheduling algorithm, which returns a series of r keys, $K_1, \ldots, K_r$. Let $g(\cdot, \cdot)$ be a function which is a bijective mapping, when the second argument is fixed. Then the ciphertext is computed as c_r, where

$$c_i = g(c_{i-1}, K_i),$$

c_0 is the plaintext and the $K_i s$ are the so-called round keys. This is called an r-round iterated cipher. Since g is assumed to be injective for fixed K_i,

$$c_{i-1} = g^{-1}(c_i, K_i),$$

and the plaintext can be computed from the ciphertext and the round keys by inverting the encryption process.

P. Samarati et al. (Eds.): ESORICS 2004, LNCS 3193, pp. 322–334, 2004.

Differential cryptanalysis [2] and linear cryptanalysis [9] are the most effective short-cut attacks against iterated secret-key (block) ciphers today. The attacks have been applied to a wide range of ciphers and are applicable particularly to iterated block ciphers where a weak function is iterated a number of times.

The crucial step in differential and linear cryptanalysis is the search for so-called characteristics covering sufficiently many rounds of the cipher. An r-round characteristic is a tool to predict with a high probability some values of the ciphertext after each of the r rounds given some values of a plaintext blocks. In differential cryptanalysis one looks at differences between two plaintexts and their corresponding ciphertexts, in linear cryptanalysis one looks at linear relations between the bits in a plaintext, the key used and in the corresponding ciphertext. Characteristics over several rounds are constructed by combining characteristics over one round, which are usually easy to find by brute force. This combination of probabilities is only valid when the characteristics for single rounds are independent, which usually will be the case by assuming independent round keys, but which is almost never the case for practical ciphers.

An r-round differential [8] is a tool to predict with some probability some difference in a pair of ciphertexts after r rounds of encryption given some difference in two plaintexts. Thus, the probability of a differential will in general be higher than for a corresponding characteristic predicting the same ciphertext bits given the same plaintext bits. To prove resistance against differential attacks or to conclude to have found the best differential attack one must be able to bound or find the best differentials; a bound on the best characteristics is not sufficient. For all existing ciphers it is impossible to find the best differentials, e.g. for a 64 bit block cipher like the DES [16] there are $(2^{64})^2$ possible differentials.

The equivalent notion of a differential versus a characteristic for linear cryptanalysis is that of an r-round linear hull [13]. To prove resistance against linear attacks one must be able to bound or find the best linear hulls. This is also a hard problem for most practical ciphers.

[8] introduces the notion of a Markov cipher, for which a probability of an r-round differential characteristic can be found from the probabilities of the involved one-round characteristics, if it is assumed that the round keys are independent and uniformly random. Most iterated ciphers in use today are Markov ciphers. The theory of Markov ciphers for linear cryptanalysis was described in [14]. For both attacks it was shown that for almost all iterated ciphers, which are Markov ciphers, the distribution of the probabilities of differentials and of linear hulls converge to the uniform distribution after some number of rounds.

For many Markov ciphers it is possible to find the highest probabilities of characteristics for both differential and for linear cryptanalysis. [10] and [17] describe results of such a search algorithm for various ciphers, e.g., for the DES. However, it should be stressed that the search assumes that the round keys involved are independent. However, all practical ciphers take a relative small key and expand it to a series of dependent round keys. It remains an open problem to find an algorithm which efficiently computes the probabilities of characteristics over several rounds for iterated ciphers with such key schedules.

To explore this problem a series of tests were conducted on several small ciphers. The method is as follows. A cipher was chosen together with a number of different key schedules. Then for different numbers of rounds the probabilities of all differentials and all linear hulls were computed and various quantities recorded from the tests.

This paper is organised as follows. §2 describes our experiments in more detail and §3 discusses the results obtained. In §4 we discuss some possible future work and open problems and §5 gives some concluding remarks.

2 Experiments

In this section we describe some experiments made on small Feistel ciphers with n-bit blocks and n-bit keys. A key schedule is introduced which take the n-bit key as input and which returns a series of round keys.

The test cipher is an eight-bit Feistel cipher, where eight text bits and four key bits are input to each round. Let X_L^i and X_R^i denote the left most respectively rightmost four bits of the eight bit text input to the ith round and K_i the ith round key, then the text output from the round function is calculated:

$$(X_L^{i+1}, X_R^{i+1}) = (X_R^i, F(X_R^i \oplus K_i) \oplus X_L^i)$$

where $F : \{0,1\}^4 \to \{0,1\}^4$ is a four to four bit nonlinear function and K_i is a four-bit round key.

Two versions of this cipher were chosen. One where F is a bijection and one where F is a randomly chosen mapping. The functions are

$$F_1 : \{10, 3, 11, 7, 5, 13, 2, 6, 8, 0, 4, 9, 12, 14, 1, 15\}$$

and

$$F_2 : \{5, 11, 9, 4, 7, 13, 8, 1, 1, 15, 7, 14, 2, 7, 9, 9\}$$

where the notation used means $F_1[0] = 10$, $F_1[1] = 3$, $F_1[2] = 11$ etc.

Five different key schedules were developed for our experiments. The first four key schedules all take an eight bit key K as input and produce r 4-bit round keys K_i for $i = 1, \ldots, r$. All four algorithms take the user-selected key and divide it into two 4-bit halves, K^L and K^R.

The first key schedule is defined as follows.

```
Key schedule 1:
Input: $K = K^L \mid K^R$

For $i = 1$ to $r/2$ do
  $K_{2i-1} = K^L$
  $K_{2i} = K^R$
For $i = 0$ to $r$ do $K_i = K_i$ XOR $i$
```

Here the round keys are constructed simply by repeating the user-selected key halves over the rounds. It is well-known that such key schedules leaves the cipher very vulnerable to so-called related-key attacks[6, 1] and the slide attacks [3]. To avoid these attacks, a round constant is added to the round keys. However, the key schedule is still weak, in that the even-numbered rounds in the cipher depend only on one key half and the odd-number rounds in the cipher depend only on the other key half. To avoid this symmetry the second key schedule uses the key halves in a different order over the rounds.

```
**Key schedule 2:**
Input: $K = K^L \mid K^R$

**For** $i = 1$ **to** $r/4$ **do**
  $K_{4i-3} = K^L$
  $K_{4i-2} = K^R$
  $K_{4i-1} = K^R$
  $K_{4i} \quad = K^L$
**For** $i = 0$ **to** $r$ **do** $K_i = K_i$ XOR $i$
```

As before, a round constant is added to the round keys. The two first schedules use the 4-bit halves of K directly, that is, the least significant bit of a round key depends only on the least significant bit of the two halves of the input key. To avoid such properties the third schedule uses rotations to spread the bits of K over all positions in the round keys.

```
**Key schedule 3:**
Input: $K = K^L \mid K^R$

$K_1 = K^L$
$K_2 = K^R$
$K_3 = \text{LeftShift}(K^L, 2) + \text{RightShift}(K^R, 2)$
$K_4 = \text{LeftShift}(K^R, 2) + \text{RightShift}(K^L, 2)$

**For** $i = 5$ **to** $r$ **do** $K_i = \text{Rotate}(K_{i-3}, 1)$
**For** $i = 1$ **to** $r$ **do** $K_i = K_i$ XOR $i$
```

Leftshift takes the two least significant bits of its input and shift these two positions to the left. *Rightshift* takes the two most significant bits of its input and shift these two positions to the right. As a consequence, the third round key K_3 depends on two bits from K^L and two bits from K^R, whereas the fourth round key K_4 depends on the remaining four bits from K^L and K^R. Then the remaining round keys are generated as rotated versions of previous round keys. To avoid trivial symmetries and weak keys, a round constant is exclusive-ored to all round keys.

The fourth schedule is yet more complex. Here a series of temporary round keys $TK_1, \ldots, TK_r$ are generated in manner similar to the previous one. Then these round keys are used in the cipher in question to generate the (real) round keys for the experiments. The cipher is used in counter mode and the resulting ciphertext halves are exclusive-ored to generate the (real) round keys $K_1, \ldots, K_r$.

```
Key schedule 4:
Input: $K = K^L \mid K^R$

$TK_1 = K^L$
$TK_2 = K^R$
$TK_3 = K^L$ XOR $K^R$

For $i = 4$ to $r$ do $TK_i = \text{Rotate}(TK_{i-3}, 1)$
For $i = 0$ to $r$ do $TK_i = TK_i$ XOR $i$
$TK := \{TK_1, \ldots, TK_r\}$
For $i = 1$ to $r$ do

  $C \ = (C^L \mid C^R) = \text{encrypt}(i, TK)$
  $K_i = C^L$ XOR $C^R$
```

The fifth key schedule simply uses independent round keys, that is, for the test cipher (an 8-bit Feistel cipher) the user-selected key is of a total of $4r$ bits.

For all the above key schedules an exhaustive search was implemented to find all differentials and linear hulls for all values of the user-selected key and for various number of rounds. For an r-round version of the cipher and for each key schedule the experiments were as follows:
For each value of the key all r-round differentials and all r-round linear hulls were computed. The hull and the differential with the highest probability taken over all inputs and all the keys were recorded. Also recorded was the deviation of the best differential/the best linear hull over all values of the keys and also the deviation of all differentials/all linear hulls over all values of the keys.

Clearly, for the fifth key schedule this experiment is very time-consuming for large numbers of rounds. However there is a more efficient implementation, here explained only for differential cryptanalysis. Compute a so-called transition matrix M for one round of the cipher, where an entry (i, j) contains the probability that a difference of i in the inputs to one round results in outputs of difference j. Thus M contains the probabilities of all one-round differentials. Then the probabilities all r-round differentials over the cipher can be found in M^r. A summary of the experiments are presented in the Tables 1, 2, 3 and 4.

3 Results

The tables containing the results for differential cryptanalysis are interpreted as follows: The column “Round” is the number of rounds used in the cipher and “KS” is the key schedule used. “Best diff” is the differential with the highest probability taken over all plaintexts and over all keys, and “probability” the corresponding probability p multiplied by 256 (number of inputs to the cipher).

Table 1. Best differentials on average for all keys and for one single key for 8-bit Feistel cipher with $F : \{10, 3, 11, 7, 5, 13, 2, 6, 8, 0, 4, 9, 12, 14, 1, 15\}$.

Round	KS	Best difference	Probability	Std. dev. best	Std. dev.
4	1	30→30	16.00	0.000	1.462
4	2	30→30	16.00	0.000	0.702
4	3	30→30	16.00	0.000	0.645
4	4	30→30	16.00	0.000	0.644
4	5	30→30	16.00	-	0.635
7	1	23→ac	10.00	0.000	1.411
7	2	50→50	3.62	2.853	0.366
7	3	30→30	3.12	3.432	0.149
7	4	30→30	2.41	2.615	0.120
7	5	30→30	2.20	-	0.051
10	1	58→cf	12.00	0.000	1.416
10	2	4b→f9	2.88	2.919	0.360
10	3	43→c3	1.56	1.603	0.140
10	4	24→14	1.44	1.707	0.108
10	5	30→30	1.07	-	0.006
16	1	0c→37	10.00	0.000	1.411
16	2	11→90	3.12	2.346	0.358
16	3	3e→5f	1.59	2.056	0.140
16	4	9f→10	1.45	1.649	0.109
16	5	30→30	1.00	-	0.004

Table 2. Best hulls on average for all keys and for one single key for 8-bit Feistel cipher with $F : \{10, 3, 11, 7, 5, 13, 2, 6, 8, 0, 4, 9, 12, 14, 1, 15\}$.

Round	KS	Best hull	Complexity	Std. dev. best	Std. dev.
4	1	ed→db	27.56	0.000	1.463
4	2	d4→ed	21.00	7.808	0.701
4	3	d4→ed	20.94	7.855	0.643
4	4	d7→ed	21.86	8.468	0.642
4	5	d4→ed	20.94	-	0.635
7	1	95→73	20.25	0.000	1.413
7	2	04→04	4.35	4.119	0.361
7	3	06→ed	2.15	2.429	0.135
7	4	0b→ed	2.20	2.264	0.103
7	5	06→ed	2.01	-	0.051
10	1	8b→90	18.06	0.000	1.417
10	2	7a→bd	3.53	5.108	0.355
10	3	93→ff	1.67	2.235	0.125
10	4	0d→1d	1.39	2.030	0.089
10	5	04→04	1.07	-	0.006
16	1	25→d2	18.06	0.000	1.413
16	2	8b→cb	3.31	6.525	0.353
16	3	51→5e	1.78	2.440	0.126
16	4	91→f0	1.40	1.896	0.089
16	5	08→ed	1.00	-	0.004

Table 3. Best differentials on average for all keys and for one single key for 8-bit Feistel cipher with $F : \{5, 11, 9, 4, 7, 13, 8, 1, 1, 15, 7, 14, 2, 7, 9, 9\}$.

Round	KS	Best difference	Probability	Std. dev. best	Std. dev.
4	1	e0→ce	16.00	0.000	1.457
4	2	c0→fc	9.50	2.403	0.627
4	3	c0→fc	9.50	2.403	0.562
4	4	fc→c0	9.81	2.309	0.559
4	5	c0→fc	9.50	-	0.550
7	1	d0→ec	12.00	0.000	1.414
7	2	50→50	3.50	3.782	0.369
7	3	10→10	2.59	3.142	0.150
7	4	c0→c0	2.87	3.623	0.122
7	5	c0→c0	2.79	-	0.055
10	1	ca→e2	12.00	0.000	1.429
10	2	0e→0c	2.62	2.209	0.359
10	3	44→81	1.55	1.647	0.140
10	4	0c→c0	1.45	1.630	0.109
10	5	c0→fc	1.15	-	0.008
16	1	19→9a	10.00	0.000	1.413
16	2	93→7c	2.88	1.870	0.358
16	3	7c→32	1.56	1.603	0.141
16	4	b6→dd	1.37	1.687	0.108
16	5	c0→f0	1.01	-	0.004

Table 4. Best hulls on average for all keys and for one single key for 8-bit Feistel cipher with $F : \{5, 11, 9, 4, 7, 13, 8, 1, 1, 15, 7, 14, 2, 7, 9, 9\}$.

Round	KS	Best hull	Complexity	Std. dev. best	Std. dev.
4	1	d6→cc	30.25	0.000	1.459
4	2	01→10	16.50	5.682	0.625
4	3	01→10	16.50	5.682	0.560
4	4	01→15	16.98	5.921	0.557
4	5	01→10	16.50	-	0.550
7	1	cc→a8	22.56	0.000	1.415
7	2	01→01	6.45	4.936	0.365
7	3	01→01	5.18	4.600	0.136
7	4	01→01	5.02	4.432	0.104
7	5	01→01	5.00	-	0.055
10	1	6d→6c	20.25	0.000	1.431
10	2	85→74	3.07	3.516	0.354
10	3	eb→fc	1.70	2.354	0.126
10	4	01→10	1.45	2.085	0.089
10	5	0c→0c	1.32	-	0.008
16	1	cb→4c	18.06	0.000	1.414
16	2	8a→a5	3.30	4.814	0.354
16	3	e2→bc	1.62	2.455	0.126
16	4	06→dc	1.41	2.060	0.089
16	5	0c→0c	1.01	-	0.004

The "Std. dev. best" is the standard deviation taken over all the keys for the best differential. The last column "Std. dev." is the standard deviation taken over all the keys and all the differentials. All the values are multiplied by 256 in order to get a mean equal to 1.0. Note that due to the way the experiments for key schedule five were implemented it is not possible to record the value of "Std. dev. best".

The results are calculated similarly in the linear case: "Best hull" is the linear hull with the highest bias ($|p - 1/2|$) taken over all plaintexts and all keys, and "complexity" the corresponding value $|p - 1/2|^2$. The deviations are calculated in the same way. All the values here are multiplied by $4 * 256$ in order to give a mean equal to 1.0. Also here it was not possible to record the value of "Std. dev. best" for key schedule five.

The computation for ciphers with independent round keys were carried out using transition matrices. Compute a matrix M with the probabilities of all one-round differentials. Then one can find the probabilities of all r-round differentials by calculation of the product M^r. Similar computations were done for linear hulls.

The results in Tables 1, 2, 3 and 4 suggest that a complex key schedule will add to the immunity against differential and linear attacks. By increasing the number of rounds it is seen that the probabilities of the best differential/linear hull converge the fastest to the uniform distribution with a complex key schedule. The standard deviation converges to zero as the probability distribution converges to the uniform distribution. It is also seen that the results for the most complex key schedule number four are closest to those using key schedule five, where independent keys are used.

Note that the standard deviations for four rounds in Table 1 are zero for the first four key schedules and in each case for the best four-round differential $30 \rightarrow 30$. A closer analysis reveals that this differential has equal inputs in the first and fourth rounds and uses the combination through F of $3 \rightarrow 3$ (which has probability $1/4$) in both the second and third rounds. So presumably for all keys this differential has probability $(1/4)^2$. The reason is that for any fixed key the inputs to two consecutive rounds in a Feistel cipher uniquely determine both plaintext and ciphertext. Hence, these two inputs take together all 2^n values exactly once. Thus, the probabilities of a differential for a fixed key in a Feistel cipher over two consecutive rounds can be found by computing the product of the individual one-round probabilities.

Also note that the standard deviation over all the keys for the best differential/linear hull for the first key schedule is always zero. This key schedule is reminiscent of that of LOKI[4] and it is well-known that it gives rise to a number of related-key properties [7, 1], see Figure 1. More precisely, if $c = e_K(p)$ is the encrypted value of p using the key $K^L \mid K^R$, then it holds that $e_{K \oplus \alpha}(p \oplus \alpha) = c \oplus \alpha$, where $\alpha = (K^L \mid K^R)$. However, it was not known until now (as far as these authors are informed) that if there is a differential of probability p for some particular value of the secret key (where the probability is taken over all plaintexts), then the same differential has probability p for any other value of the

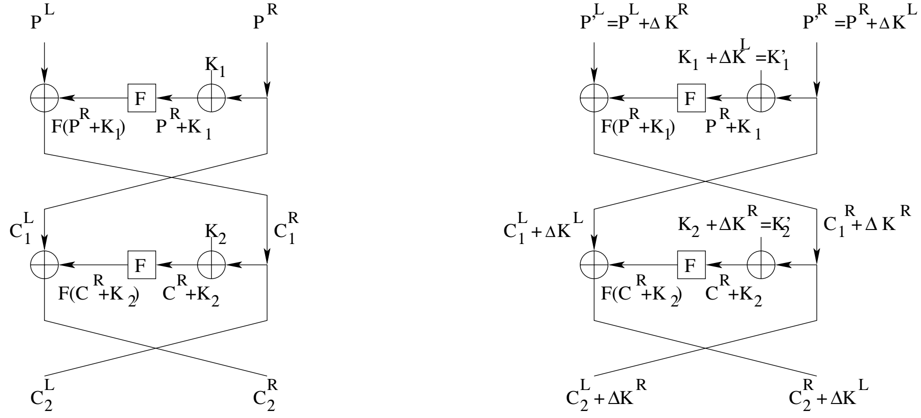

Fig. 1. Two rounds of a Feistel cipher where the keys in every second round are different by a constant. Two keys which differ by a value $\Delta K = (\Delta K^L, \Delta K^R)$ will have exactly the same dependency between the rounds for all keys during both differential and linear attacks. Notice that inputs and outputs of F are exactly the same in all rounds.

secret key. The reason is the following. Assume that there are s pairs of plaintexts $(p_{i,0}, p_{i,1})$ each of some difference β and which encrypted using the key value L yield $(c_{i,0}, c_{i,1})$ for $i = 1, \ldots s$, where the ciphertexts are of some difference γ. But then the s pairs of plaintexts $(p_{i,0} \oplus \alpha, p_{i,1} \oplus \alpha)$ which are of difference β encrypt to the pair $(c_{i,0} \oplus \alpha, c_{i,1} \oplus \alpha)$ of difference γ using the key value $L \oplus \alpha$. However this also means that for this cipher, the most likely differential for a fixed key is also the most likely differential for any other key. It is believed that this is the first reported example cipher in the literature with this property It is stressed however that this cipher is vulnerable to other attacks which are faster than exhaustive key search.

O'Connor [15] showed that for a randomly chosen n-bit permutation, the expected highest probability of a differential will be less than $2m/2^m$. In our tests, this bound is 16/256. Empirical results indicate that the expected probability of the best differential for a randomly chosen eight-bit permutation is about 10/256. This explains why for any number of rounds using the first key schedule the probability of the best differentials stay around 12/256 and does not decrease with the number of rounds. Also, is explains exactly why the standard deviation over all keys for these differentials is zero. A similar phenomenon can be explained for the linear cryptanalysis case.

The second key schedule will also have some of these properties, but here only in the cases where $\Delta K^R = \Delta K^L$, which is only the case for one of $2^{n/2}$ keys.

It is anticipated that the results of our experiments will translate also to ciphers with bigger block size. However, exhaustive searches for differentials and linear hulls in a cipher for much higher values of n is very difficult. The complexities of these searches are $\mathrm{O}(2^{3n})$ where n is the block size and the key size. Some further experiments in the reach of our computing capabilities were conducted.

- Feistel ciphers of size 10 and 12 bits were tested in the differential cryptanalysis case, where the nonlinear functions used were randomly chosen 5-bit respectively 6-bit bijective mappings, and where the key sizes are equal to the cipher size. The key schedules were chosen in a way similar to those reported in full detail above. The results of these tests are listed in Tables 5 and 6.
- Feistel ciphers of size eight, where the nonlinear function is a 5 to 4 bit S-box. Here the four-bit input to the S-box is expanded to five bits, where after a 5-bit round key was added. The key size of this cipher was 10 bits. This cipher models DES-like ciphers where the nonlinear function varies with the keys.
- An SP-network of 8 bits was tested, where one round consists of two 4 to 4 bit S-boxes together with a linear layer mixing the outputs of the boxes. The key size of this cipher is 8 bits.
- An SP-network of 9 bits was tested, where one round consists of three 3 to 3 bit S-boxes together with a linear layer mixing the outputs of the boxes. The key size of this cipher is 9 bits.

The results show that the uniform distribution is reached faster for the 10-bit and 12-bit block ciphers than for the 8-bit block ciphers reported on earlier. However, the overall picture is the same as before. A cipher with a well-designed key schedule reaches the uniform distribution of the probabilities of differentials and linear hulls faster than with a badly designed key schedule. A good (complex) key schedule therefore seems to help make a cipher more resistant to differential and linear attacks.

Finally we note that there are many block ciphers which have key schedules which are very simple and reminiscent of the weak key schedules from our experiments. A few examples are Skipjack[12], Noekeon[5], and MISTY[11].

4 Future Work

There is still open questions to try to explain from the experiments above. What exactly is the influence of the different key schedules on the complexity of linear and differential attacks. A few examples, why exactly is key schedule four better than key schedule three? Could there be some weaker dependencies between the round keys which also give high-probability differentials/hulls higher than the ones assuming independent round keys? Could there be an approximation in one round which when averaged over all inputs has a small probability but which due to a round key dependency between the several rounds actually has a much higher probability?

5 Concluding Remarks

There is a huge number of block ciphers proposed today, almost all of which has an ad-hoc designed key schedule for which very little is known. In this paper it

Table 5. Best differentials on average for all keys and for one single key for a 10-bit Feistel cipher.

Round	KS	Best difference	Probability	Std. dev.
4	1	1c0→200	32.00	1.436
4	2	1c0→200	32.00	0.443
4	3	1c0→200	32.00	0.385
4	4	1c0→200	32.00	0.382
4	5	1c0→200	32.00	1.518
7	1	008→163	12.00	1.415
7	2	020→001	3.31	0.254
7	3	200→200	2.32	0.071
7	4	200→200	2.50	0.056
7	5	200→200	2.31	0.051
10	1	2d1→255	14.00	1.411
10	2	07a→250	2.38	0.252
10	3	253→3d4	1.31	0.070
10	4	1de→193	1.22	0.054
10	5	1c0→200	1.05	0.004

Table 6. Best differentials on average for all keys and for one single key for a 12-bit Feistel cipher.

Round	KS	Best difference	Probability	Std. dev.
4	1	040→300	16.00	1.418
4	2	040→300	16.00	0.236
4	3	040→300	16.00	0.194
4	4	040→300	16.00	0.168
4	5	040→700	16.00	2.673
7	1	0fb→df	16.00	1.414
7	2	040→001	3.34	0.178
7	3	3c3→229	1.25	0.047
7	4	240→240	1.16	0.027
7	5	ec0→ec0	1.15	0.029
10	1	2cd→3b9	16.00	1.414
10	2	0f6→315	2.03	0.178
10	3	11c→1e5	1.24	0.047
10	4	0ac→247	1.12	0.027
10	5	e80→e80	1.00	0.004

has been demonstrated by experiments that the key schedule of iterated ciphers influence the distribution of the probabilities of differentials and linear hulls. The more complex the key schedules, the better resistance against differential and linear attacks.

Due to the available computing resources these experiments were conducted on small toy ciphers, however the authors have found no indication why the results should not apply also to ciphers with larger blocks. In fact, the constructed toy ciphers with independent round keys (or with a well-designed key-schedule) are most likely strong ciphers relative to their sizes. Just imagine a scaled-up version with 64-bit blocks, that is, with a randomly chosen (bijective) 32-bit mapping in the round function. Such a cipher is likely to be stronger than e.g., DES used with the same number of rounds.

References

1. E. Biham. New types of cryptanalytic attacks using related keys. In T. Helleseth, editor, *Advances in Cryptology: EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 398–409. Springer Verlag, 1993.
2. E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer Verlag, 1993.
3. A. Biryukov and D. Wagner. Slide attacks. In L. R. Knudsen, editor, *Fast Software Encryption, Sixth International Workshop, Rome, Italy, March 1999, Lecture Notes in Computer Science 1636*, pages 245–259. Springer Verlag, 1999.
4. L. Brown, J. Pieprzyk, and J. Seberry. LOKI - a cryptographic primitive for authentication and secrecy applications. In J. Seberry and J. Pieprzyk, editors, *Advances in Cryptology: AusCrypt'90, Lecture Notes in Computer Science 453*, pages 229–236. Springer Verlag, 1990.
5. J. Daemen, M. Peeters, G. Van Assche, and V. Rijmen. Nessie proposal: NOEKEON. Submitted as an NESSIE Candidate Algorithm. Available from `http://www.cryptonessie.org`.
6. L.R. Knudsen. Cryptanalysis of LOKI'91. In J. Seberry and Y. Zheng, editors, *Advances in Cryptology, AusCrypt 92, Lecture Notes in Computer Science 718*, pages 196–208. Springer Verlag, 1993.
7. L.R. Knudsen. Cryptanalysis of LOKI. In H. Imai, R.L. Rivest, and T. Matsumoto, editors, *Advances in Cryptology: AsiaCrypt'91, Lecture Notes in Computer Science 453*, pages 22–35. Springer Verlag, 1993.
8. X. Lai, J.L. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. In D.W. Davies, editor, *Advances in Cryptology - EUROCRYPT'91, Lecture Notes in Computer Science 547*, pages 17–38. Springer Verlag, 1992.
9. M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 386–397. Springer Verlag, 1993.
10. M. Matsui. On correlation between the order of S-boxes and the strength of DES. In A. De Santis, editor, *Advances in Cryptology - EUROCRYPT'94, Lecture Notes in Computer Science 950*. Springer Verlag, 1995.
11. M. Matsui. New block encryption algorithm MISTY. In E. Biham, editor, *Fast Software Encryption, Fourth International Workshop, Haifa, Israel, January 1997, Lecture Notes in Computer Science 1267*, pages 54–68. Springer Verlag, 1997.
12. NSA. Skipjack and KEA algorithm specifications. http://csrc.ncsl.nist.gov/encryption/skipjack-1.pdf, May 1998.
13. K. Nyberg. Linear approximations of block ciphers. In A. De Santis, editor, *Advances in Cryptology - EUROCRYPT'94, Lecture Notes in Computer Science 950*, pages 439–444. Springer Verlag, 1995.
14. O'Connor and Golic. A unified Markov approach to differential and linear cryptanalysis. In Josef Pieprzyk and Reihaneh Safavi-Naini, editors, *Advances in Cryptology – ASIACRYPT '94, Lecture Notes in Computer Science 917*, pages 387–397. Springer-Verlag, 1994.
15. L.J. O'Connor. On the distribution of characteristics in bijective mappings. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 360–370. Springer Verlag, 1994.

16. National Bureau of Standards. Data encryption standard. Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.
17. Toshio Tokita, Tohru Sorimachi, and Mitsuru Matsui. Linear cryptanalysis of LOKI and s2-DES. In Josef Pieprzyk and Reihanah Safavi-Naini, editors, *Advances in Cryptology – ASIACRYPT '94, Lecture Notes in Computer Science 917*, pages 293–303. Springer Verlag, 1994.