Cryptanalysis of LOKI

Lars Ramkilde Knudsen
Aarhus Universitet Datalogisk Afdeling
Ny Munkegade
DK-8000 Aarhus C.

Abstract

In [BPS90] Brown, Pieprzyk and Seberry proposed a new encryption primitive, which encrypts and decrypts a 64-bit block of data using a 64-bit key. Furthermore they propose a way to build private versions of LOKI.
In this paper we show first that the keyspace of any LOKI-version is only 2^{60}, not 2^{64} as claimed. Therefore there are 15 equivalent keys for every key, that encrypts/decrypts texts the same way. An immediate consequence is, that the proposed Single Block Hash Mode is no good. It is very easy to find collisions.
Secondly we do differential cryptanalysis, introduced in [BS90] on LOKI and show that n-round LOKI, n $\leq$ 14 is vulnerable to this kind of attack, at least in principle. We show that we cannot find a characteristic with a probability high enough to break LOKI with 16 rounds.
Finally we consider differentials, introduced in [LMM91], versus characteristics, introduced in [BS90].

1 LOKI - a family of encryption primitives

In [BPS90] Brown, Pieprzyk and Seberry proposed a new encryption primitive, which encrypts and decrypts a 64-bit block of data using a 64-bit key. LOKI is interface compatible with the DES (ISO DEA-1) and its structure is very much like the structure of DES. Therefore it is obvious to try to do a differential attack proposed by Biham-Shamir in [BS90] on LOKI.
The main difference between DES and LOKI is the S-boxes. All 4 LOKI S-boxes are equal, take a 12 bit input and produce a 8 bit output. The output is evaluated through exponentations (with a fixed exponent) in 16 different fields generated by 16 irreducible polynomials.
Another difference between DES and LOKI is that in the latter, the key is added (modulo 2) just before and after 16 rounds of F-iterations.
Furthermore the P-permutation in LOKI allows us to find good fixpoints for the F-function, which we cannot do in DES.

2 The keyschedule algorithm

The keysize in LOKI is 64 bits. The key is divided into two halves of 32 bits, KL and KR, respectively. Initially KL and KR are added (modulo 2) to the left and right halves of the plaintext, see Figure 1.
The 32 bits of KL are used as the keys in the odd rounds, that is round no. 1,3,5,.....,15, in the following way:

$$K_{2i+1} = ROL_{12}(K_{2i-1}), \quad i \in \{1, ..., 7\}$$
$$\text{and } K_1 = KL$$

where ROL_{12} is 12 rotations of the key to the left.
Finally $ROL_{12}(K_{15}) = KL$ is added to the right half of the plaintext.
The 32 bits of KR are used as the keys in the even rounds, in the following way:

$$K_{2i+2} = ROL_{12}(K_{2i}), \quad i \in \{1, ..., 7\}$$
$$\text{and } K_2 = KR$$

Finally $ROL_{12}(K_{16}) = KR$ is added to the left half of the plaintext.
The initial and final addition of the key has an unfortunate impact on the keyspace of LOKI, as we will show in the following.
From Figure 1, we see that the final addition of KR and KL can be pushed 'upwards in the tree'. If we try to push KL upwards, then every time we pass the F-function on the right side, we have to add KL to the corresponding key. If we push KL to the top of the tree every even subkey K_i is added to KL and the initial addition of KL disappears.
Of course the same trick goes for the final addition of KR, and we obtain a rearranged model of LOKI, Figure 2.
Instead of 16 subkeys, 8 consisting of 32 bits from the set $\{k_0,....,k_{31}\}$ and 8 consisting of 32 bits from the set $\{k_{32},....,k_{63}\}$, we have 16 **actual subkeys**, AK_1, AK_2, ..., AK_{16}, each consisting of 32 **keybit-xors** from the set

$$\{a \oplus b \mid a \in \{k_0, ..., k_{31}\},\ b \in \{k_{32}, ..., k_{63}\}\}$$

We have the following theorem:

Theorem 1. *The keyspace of LOKI is* 2^{60}.

That is, for any key K, all keys of the form K $\oplus$ hhhhhhhh hhhhhhhh$_x$, where h is one of the hexadecimal symbols 0,1,....,e,f, are equivalent.
Proof:
An arbitrary bit-xor in an actual subkey has the form $k_i \oplus k_j$, where it holds that i-j = 0 mod 4, due to the fact that 12 = 32 mod 4, and where the indices i and j refer to the bit numbering in the original key. It is obvious

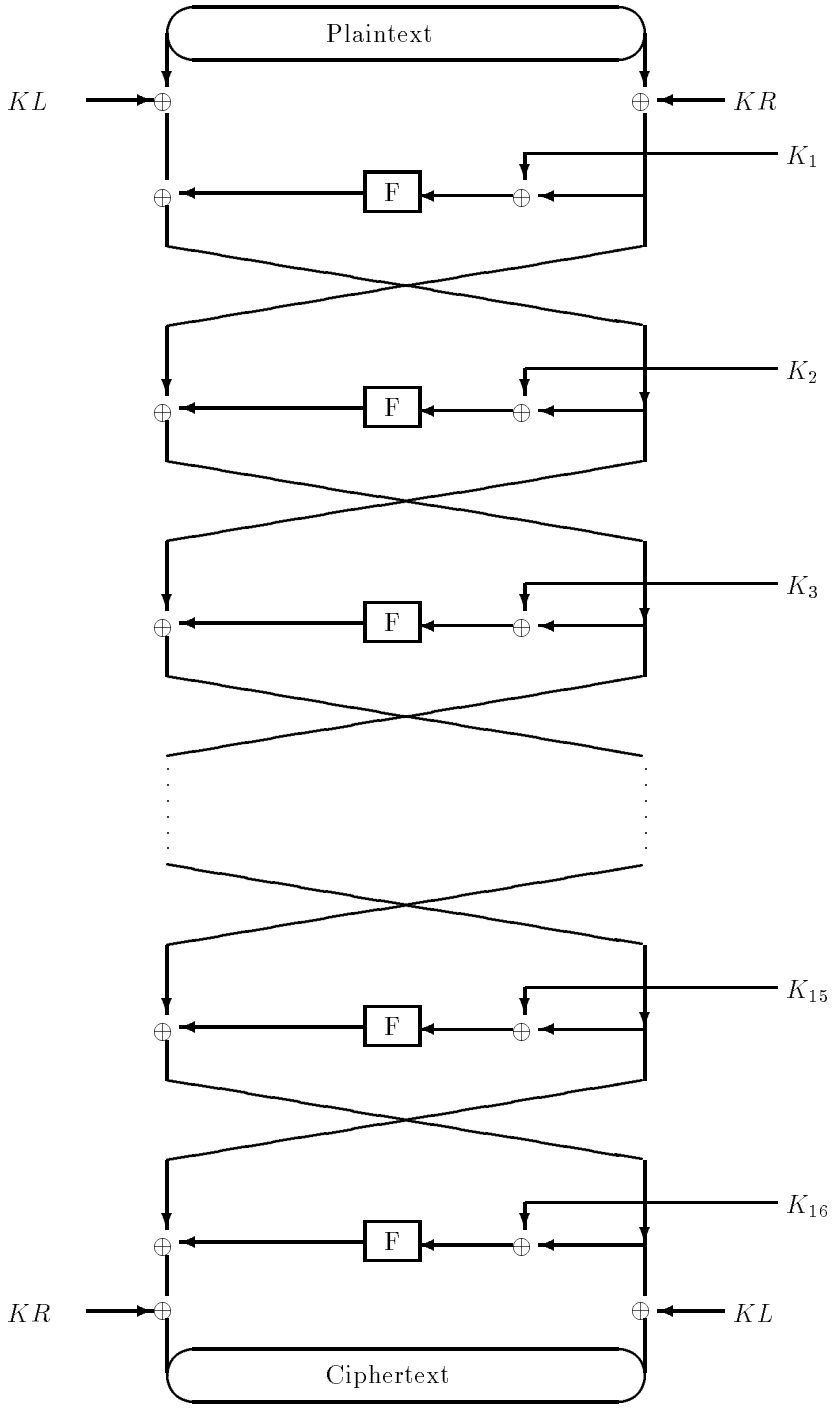


Figure 1. LOKI with 16 rounds

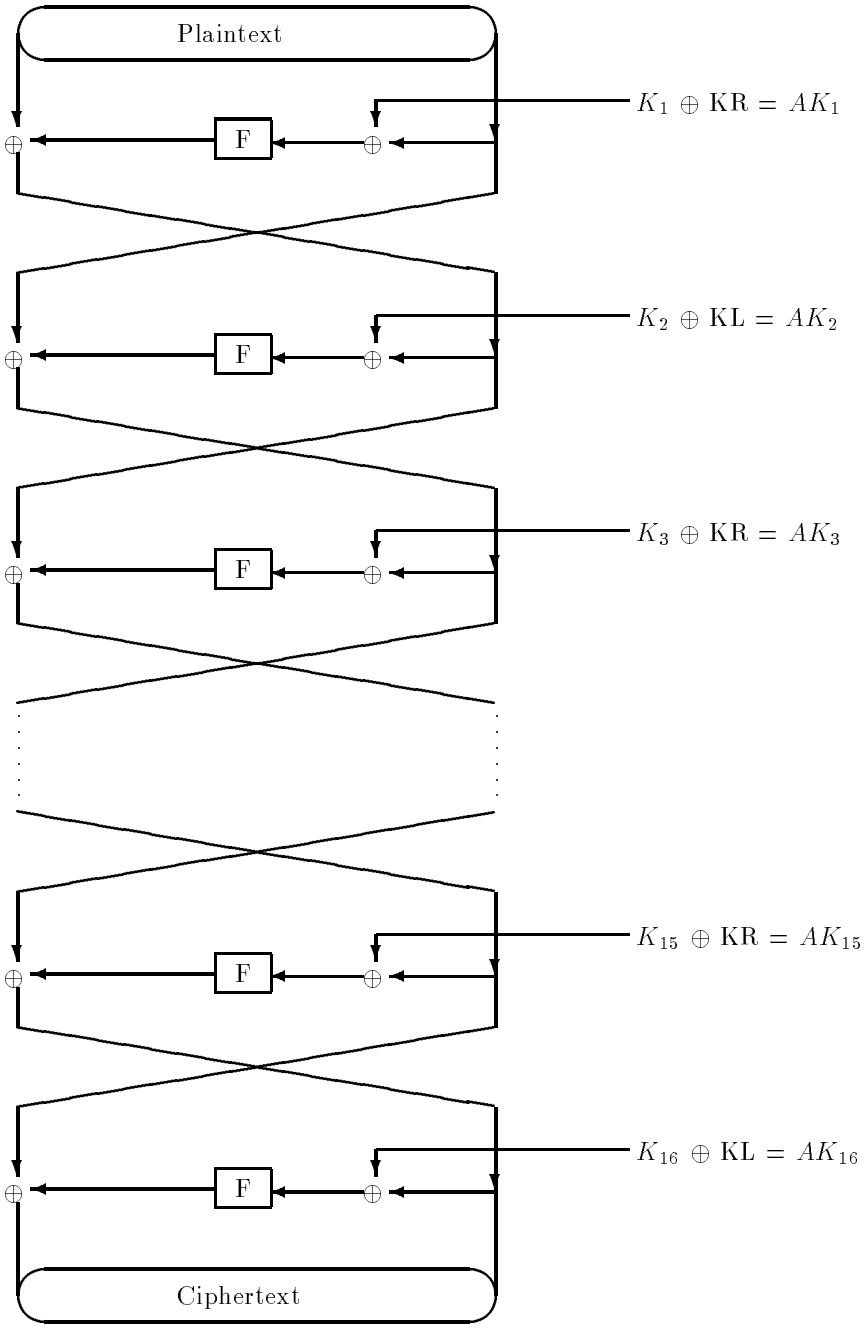


Figure 2. Rearranged LOKI with 16 rounds

that when modifying the key with the repeated hex digit h, k_i and k_j will be xor'ed with the same bit from h, whence all $k_i \oplus k_j$ and therefore all actual subkeys are unchanged. □

As an example suppose K = 13cd2452 d97e8b60$_x$ one gets the following 16 actual subkeys, regardless of the value of h:

AK_1	=	cab3af32$_x$	AK_2	=	cab3af32$_x$
AK_3	=	0b3baa5c$_x$	AK_4	=	fb7b29c5$_x$
AK_5	=	8b6d4644$_x$	AK_6	=	73145ad9$_x$
AK_7	=	e5acce41$_x$	AK_8	=	8425925f$_x$
AK_9	=	fd2c98ad$_x$	AK_{10}	=	98adfd2c$_x$
AK_{11}	=	f8425925$_x$	AK_{12}	=	1e5acce4$_x$
AK_{13}	=	145ad973$_x$	AK_{14}	=	6d46448b$_x$
AK_{15}	=	9c5fb7b2$_x$	AK_{16}	=	a5c0b3ba$_x$

2.1 Single Block Hash (SBH) Mode is no good

SBH described in [BPS90] is no good, because of Theorem 1. SBH is described as follows:

$$\begin{gathered} \mathrm{H}_0 = \mathrm{IV}, \quad \text{initial hash value} \\ \mathrm{H}_i = \mathrm{LOKI}(m_i \oplus H_{i-1},\ H_{i-1}) \oplus H_{i-1} \\ \mathrm{SBH} = H_n \end{gathered}$$

where LOKI(K,M) is the plaintext M encrypted using the key K. Assume we have a hashvalue H_n for $\mathrm{M} = m_1, m_2, \ldots\ldots, m_n$, where every m_i is of length 64 bits. The hashvalue for

$$M^* \ = \ m_1 \oplus s_1, \ldots\ldots\ldots, m_n \oplus s_n,$$

where s_i = hhhhhhhh hhhhhhhh$_x$, h $\in$ {0,1,.....,e,f}, is

$$\begin{gathered} \mathrm{H}_0^* = \mathrm{IV} = \mathrm{H}_0, \\ \mathrm{H}_1^* = \mathrm{LOKI}(m_1 \oplus s_1 \oplus IV,\ IV) \oplus IV = \mathrm{LOKI}(m_1 \oplus IV,\ IV) \oplus IV = \mathrm{H}_1 \\ \mathrm{H}_2^* = \mathrm{LOKI}(m_2 \oplus s_2 \oplus H_1^*,\ H_1^*) \oplus H_1^* = \mathrm{LOKI}(m_2 \oplus H_1,\ H_1) \oplus H_1 = \mathrm{H}_2 \\ \ldots\ldots\ldots \\ \mathrm{H}_i^* = \mathrm{LOKI}(m_i \oplus s_i \oplus H_{i-1}^*,\ H_{i-1}^*) \oplus H_{i-1}^* = \\ \mathrm{LOKI}(m_i \oplus H_{i-1},\ H_{i-1}) \oplus H_{i-1} = \mathrm{H}_i \\ \ldots\ldots\ldots \\ \mathrm{H}_n^* = \mathrm{H}_n \end{gathered}$$

It means, we can easily find 16^n messages, that will be hashed to the same hash value.

3 Differential cryptanalysis on (Standard) LOKI

In this section we will do differential cryptanalysis on LOKI. Differential cryptanalysis was introduced by Biham and Shamir [BS90] and is a method, which analyses the effect of particular differences in plaintext pairs on the differences of the resultant ciphertext pairs. That is, by choosing a certain difference in a plaintext pair, we can put probabilities on the different possible resultant ciphertext pairs. In the following we will use the notion of Biham-Shamir from [BS90]. For further details please consult these papers.
A table, which shows these probabilities is called a *pairs XOR distribution table*. For one S-box in LOKI it is a table with $2^{12} * 2^8 = 2^{20} = 1{,}048{,}576$ entries. The average value of the entries is 16 and of the 1,048,576 entries 99,9% are non-zero. That is, only 951 entries are zero. We write X $\rightarrow$ Y, if an inputxor X can result in an inputxor Y.
The first step in a differential attack is to find good characteristics. In [BS90] Biham-Shamir state, that the best characteristics for a 16-round DES attack is obtained by concatenating a 2-round iterative characteristic with itself a certain number of times (see [BS90] page 27). The best 2-round iterative characteristic in DES has a probability of $\frac{1}{234}$ [BS90]. For LOKI we have:

Theorem 2. *To have two equal outputs of the F-function based on two different inputs, we have to have at least two neighbouring S-boxes with different inputs.*

Proof
Assume we have two equal outputs of the F-function based on two different inputs, which differ only in the input to one S-box. Due to the E-expansion the inputxor to that S-box must have the following form:

$$0000a_1a_2a_3a_40000 \quad (binary),$$

where $a_1a_2a_3a_4 \neq 0000$.
The two left-outermost and the two right-outermost bits determine the Sfn_r-function to be used in the evaluation. But these selectionbits are equal, which means the two inputs are evaluated through the same Sfn_r-function. If $00a_1a_2a_3a_400 = p \oplus q$ (i.e. $p \neq q$) then since the outputs are equal (x is an irreducible polynomial) we have:

$$p^{31} \ (mod\ x) \ = \ q^{31} \ (mod\ x) \ \Rightarrow \ p \ = \ q.$$

since gcd(31,255)=1. A contradiction. □

There exists many iterative characteristics where two neighbouring S-boxes

have different inputs. The best one has a probability of [BS91]

$$\frac{118}{2^{20}} \simeq 2^{-13,12}$$

No iterative characteristic where more than two S-boxes have different inputs is better than the abovementioned. However we can find 3-round iterative characteristics, which are better.

Definition 1. *A $\mathcal{F}$-fixpoint is an inputxor x, for which $\mathcal{F}(x) = x$, with some probability. $\mathcal{F}(x)$ is the random variable with distribution induced by putting $\mathcal{F}(x) = F(a) \oplus F(b)$, where a and b are uniformly chosen, such that $a \oplus b = x$.*

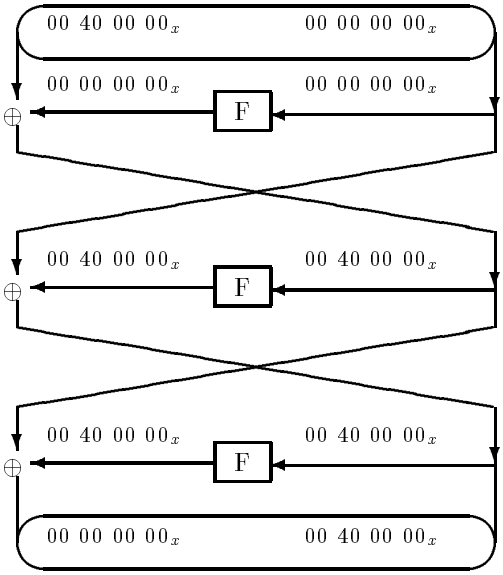
We obtain the best probabilities for a non-trivial input/outputxor combination, when the inputs differ only in the inputs to one S-box. We therefore first try to find $\mathcal{F}$-fixpoints, which differ only in the inputs to S-box 4.
Remark: In LOKI we have that xor-addition of pairs is linear in the E-ekspansion and the P-permutation. That is E(X$\oplus$X*) = E(X)$\oplus$E(X*) and P(X$\oplus$X*) = P(X)$\oplus$P(X*).
Let B = $b_{31}b_{30}.....b_1b_0$ be an inputxor to the F-function (before E). The 12 inputbitxors to S-box 4 are $b_3b_2b_1b_0b_{31}....b_{24}$. We have that $b_i = 0$ for i = 0,1,...,27 and that $b_{31}b_{30}b_{29}b_{28} \neq 0000$, because the inputs differ only in the input to S-box 4. Let $c_{31}c_{30}.....c_0$ be an outputxor from the F-function (before the P-permutation). $c_{31}c_{30}.....c_{24}$ are outputbitxors from S-box 4. Therefore $c_j = 0$ for j = 0,1,.....,23, because the inputs to the S-boxes 3,2 and 1 are equal. After the P-permutation we have outputxor C = $c_{31}c_{23}c_{15}c_7.....c_8c_0$. If B is a $\mathcal{F}$-fixpoint we must have C = B. It means that $b_{31} = c_{31} = 1$ and that $b_j = c_j = 0$ for j = 0,1,.....,30. Therefore we have a $\mathcal{F}$-fixpoint 80000000_x, if the combination $080_x \rightarrow 80_x$ is possible in LOKI. It is furthermore the only $\mathcal{F}$-fixpoint, where the inputs differ only to S-box 4.
By similar calculations we find that we have $\mathcal{F}$-fixpoints where the inputs differ to only S-box 3, 2 and 1, as follows:
00400000_x, if the combination $040_x \rightarrow 20_x$ is possible.
00002000_x, if the combination $020_x \rightarrow 08_x$ is possible.
00000010_x, if the combination $010_x \rightarrow 02_x$ is possible.
From *pairs XOR distribution table* we find that we have 3 fixpoints for LOKI where the inputs differ only to one S-box.

80000000_x with the probability $\frac{14}{4096}$

00400000_x with the probability $\frac{28}{4096}$

00000010_x with the probability $\frac{14}{4096}$

We have other $\mathcal{F}$-fixpoints for LOKI, where the inputs differ to more than one S-box. However none of these have a probability higher than the 3 abovementioned. Using these fixpoints we can build iterative characteristics. The following, which we will call **the fixpoint characteristic** is the best:



The total probability becomes $\frac{28^2}{4096^2} \simeq 2^{-14.4}$. That is if we have a plaintext pair, whose sum is 00400000 00000000$_x$, then after 3 rounds of encryption the sum will be 00000000 00400000$_x$ with probability $2^{-14.4}$.

We have checked, that for DES we have no fixpoints, where the inputs differ in less than 3 S-boxes. Although we may find fixpoints, where the inputs differ in 3 or more S-boxes, it cannot be used to build a better (iterative) characteristic, than the 2-round iterative characteristic given by Biham-Shamir [BS90].

3.1 Attacks on LOKI

For every attack we use the rearranged model of LOKI, that is, in every n-round LOKI we push the final addition of the key-halves 'upwards in the tree'. That gives n actual subkeys plus an initial addition of some keybit-xors, these being zero for n=16.
To find a complete 64-bit key (or 256 keybit-xors that determines 16 equivalent keys) we need to know 3 actual subkeys. In other words finding

AK_n, AK_{n-1} and AK_{n-2} enables us to find all the keybit-xors we need. In [BS90] Biham-Shamir use an estimate, they call S/N-ratio, to find out how many pairs are needed for the attacks (on DES).

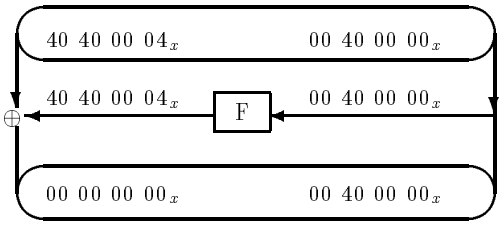
$$\text{S/N} = \frac{2^k * p}{\alpha * \beta},$$

where k = number of keybits we are looking for
p = probability of the characteristic
α = average count (of keys) per counted pair
β = ratio of counted to all pairs.

The main difference of the S/N-ratio in DES and in LOKI is the calculation of α. Looking for keybits entering n S-boxes in DES yields an α of 4^n. In LOKI four of the keybit-xors entering S4 enter S3 as well. Other keybit-xors enter S1 and so forth. Looking for keybit-xors entering one S-box in LOKI gives an α of 16. Looking for keybit-xors entering two neighbouring S-boxes still gives an α of 16. The following tabel shows α for different search criteria. There are several types of attacks depending

	α
One S-box	16
Two neighbouring S-boxes	16
Two not neighbouring S-boxes	16^2
Three S-boxes	16
Four S-boxes	1

on the number of rounds that are not covered by the characteristics used in the attacks. That is, a xR-attack on a n-round cryptosystem is an attack where we use a (n-x)-round characteristic.
LOKI with 4 rounds can be broken in a way quite similar to the one given in [BS90] for breaking DES with 4 rounds using independent subkeys. We do 3R attacks using 4 characteristics, each one with a probability of 1 and find every keybit-xor using only 16 ciphertexts. We made 200 different tests, all of them showing that the right keybit-xors were the most suggested keyvalues.
LOKI with 6 rounds can be broken using 2 3-round characteristics with probabilities of 2^{-12} and 2^{-13}, respectively, to find AK_6. We made 20 tests looking for AK_6. In every test the right values of the keybitxors were the most suggested values using a total of 2^{15} pairs. For LOKI with 8 rounds the best attack we have found is a 3R attack, using the following one-round characteristic, the **start-characteristic**:



with prob. $\frac{36}{4096}$

We concatenate it with the fixpoint characteristic plus one round with the trivial fixpoint 00 00 00 00$_x$. The total probability is $2^{-14.4} \times \frac{36}{4096} \simeq 2^{-21.2}$. We need 2^{24} pairs for a successful attack. For n ≤ 9, 3R-attacks (see [BS90]) are possible, but for n > 9 the probabilities of the characteristics get too small. But for $9 <$ n < 14 we can choose a 2R-attack, using the fixpoint characteristic and in some attacks the start-characteristic. Whether to use the start-characteristic or not is determined as follows:
If we need a r-round characteristic, we concatenate the fixpoint characteristic with itself $\frac{r}{3}$ times. If the last round of the obtained characteristic is a round with the fixpoint 00 40 00 00$_x$, we remove this last round and use the start-characteristic as the **first** round, thus obtaining a r-round characteristic with a probability improved by a factor $\frac{36}{28}$. For n = 14 the best attack is a 1R attack using a 13-round characteristic built alone from the fixpoint characteristic.
We will show in more details how LOKI with 13 rounds can be broken using 2^{53} pairs in a 2R-attack. We concatenate the start-characteristic with 3 fixpoint characterstics plus one round with the trivial fixpoint 00 00 00 00$_x$. The total probability of the characteristic becomes $(\frac{28}{4096})^6 \times \frac{36}{4096} \simeq 2^{-50}$, see Figure 3.

We know that 24 bits of the ciphertext pairs in the output of the 12. round should be equal. Furthermore we know the inputsum to the 11. round, which means we can check 24 bits of the right halves of the ciphertext pairs. If the bits are not as expected, we filter out the ciphertext pair. From the ciphertexts we know the inputs to the 13. round and we know the expected outputsums of all the pairs in the 13. round. Using 2^{32} counters we get

$$S/N \simeq \frac{2^{32} * 2^{-50}}{1 * 2^{-24}} = 2^6$$

Using 2^{53} pairs, we get 2^{29} $(2^{53} * 2^{-24})$ pairs each suggesting one arbitrary 32 bit keyvalue. The right keyvalue is suggested about 8 times and with a high probability it is the one most suggested keyvalue. Now we can decrypt all pairs one round and do a 2R- or 1R-attack on the remaining 12-round cryptosystem using characteristics with higher probability than 2^{-50} and find AK_{12} and AK_{11} in a similar way.
Tabel 1 below contains estimates of how many pairs are needed for different

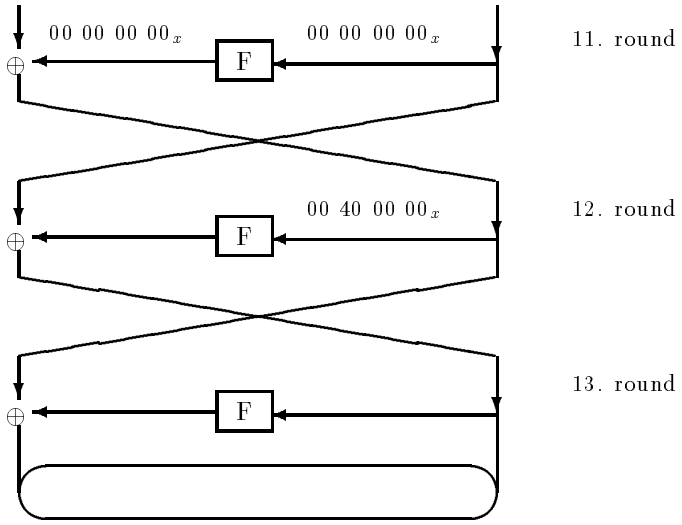
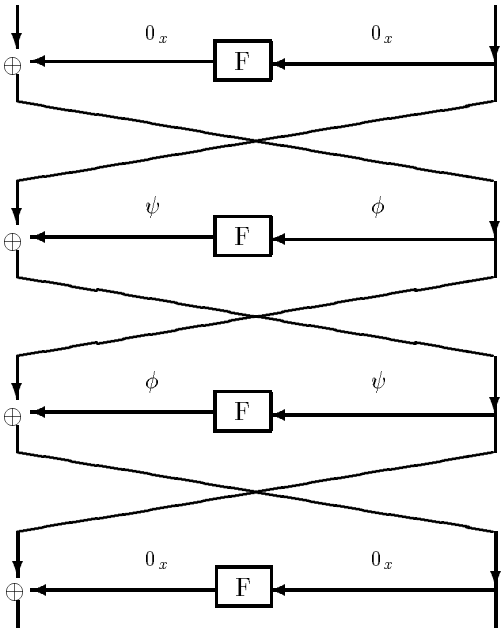


Figure 3.

kinds of attacks on LOKI. As indicated in the table we cannot break LOKI with 16 rounds doing a differential attack. The best attack we have found is to use a 15-round characteristic in a 1R attack. We concatenate the start-characteristic, 4 fixpoint characteristics, one round with the fixpoint 00 00 00 00_x and one round with the combination 00 40 00 $00_x \rightarrow$ 40 40 00 04_x. The total probability for the 15-round characteristic is $2^{-71.2}$ and the attack is not possible. A necessary condition for a successful 1R attack using a 15-round characteristic is that the probability of the characteristic is greater than 2^{-64}. We show that we cannot find such a characteristic. We need a few definitions:

Definition 2. *A round with the combination 00 00 00 $00_x \rightarrow$ 00 00 00 00_x we call a* **zero-round**.
If the rounds **(i−1)** *and* **(i+1)** *are zero-rounds, round* **i** *is of* **type A**.
If the rounds **(i−1)** *and* **(i+2)** *are zero-rounds, round* **i** *and round* **(i+1)** *are of* **type B**.

A round of type A must have the form $\phi_i \rightarrow$ 00 00 00 00_x. The best probability of such a round is $2^{-13.12}$ [BS91]. The two rounds of type B must have the following form:



By consulting the *pairs XOR distribution table* we find that we obtain the best probability for the two rounds if $\phi = \psi = 00\ 40\ 00\ 00_x$, that is exactly the situation we obtain using the fixpoint characteristic. The best probability for two rounds of type B is therefore $2^{-14.4}$. Now we can prove the following theorem:

Theorem 3. *For LOKI we cannot find a 15-round characteristic with a probability greater than* 2^{-64}.

Proof
The best non-trivial input/outputxor combination in LOKI has a probability of 2^{-6}. It means that some of the 15 rounds have to be zero-rounds with probability 1. At least 5 rounds must be zero-rounds, because 5 is the lowest value of x, such that:

$$(2^{-6})^{15-x} > 2^{-64}$$

If two neighbouring rounds are zero-rounds then all rounds are zero-rounds and we get equal plaintexts resulting in equal ciphertexts, a trivial fact. It means that we can have at most 8 zero-rounds and must have at least 5 zero-rounds in the 15-round characteristic (15R).

8 zero-rounds: First round and then every other round are zero-rounds. The remaining 7 rounds are all of type A. We get:

$$P(15R) \leq (2^{-13,12})^7 = 2^{-91,84}$$

7 zero-rounds: We have at least 4 rounds of type A. The remaining 4 (nonzero) rounds have a probability of at most 2^{-6}. We get:

$$P(15R) \leq (2^{-13,12})^4 \times (2^{-6})^4 = 2^{-76,48}$$

6 zero-rounds: We have at least 1 round of type A and two situations to examine:

1. Only one round of type A, thereby 4×2 rounds of type B.

$$P(15R) \leq 2^{-13,12} \times (2^{-14,4})^4 = 2^{-70,72}$$

2. Two or more rounds of type A.

$$P(15R) \leq (2^{-13,12})^2 \times (2^{-6})^7 = 2^{-68,24}$$

5 zero-rounds: We have two situations to examine:

1. One round of type A.

$$P(15R) \leq 2^{-13,12} \times (2^{-6})^9 = 2^{-67,12}$$

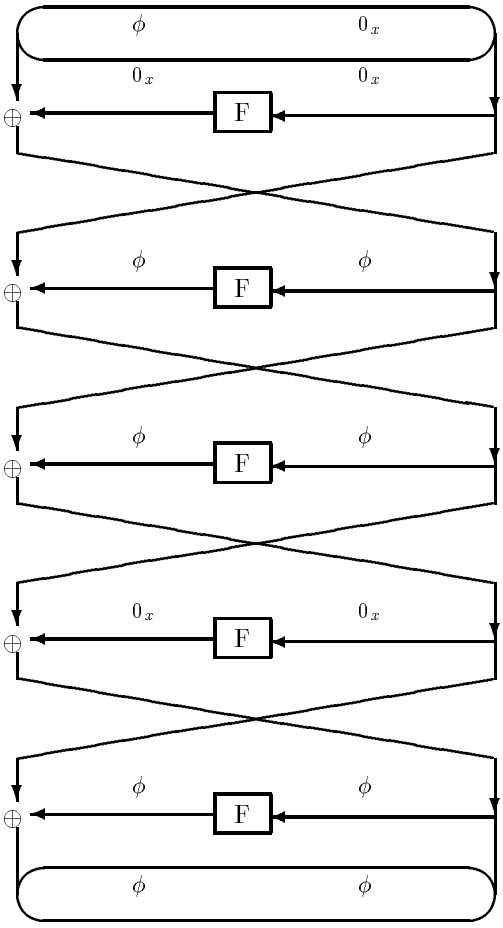
2. No rounds of type A and thereby 2×2 rounds of type B.

$$P(15R) \leq (2^{-14,4})^2 \times (2^{-6})^6 = 2^{-64,8}$$

□

4 Characteristics versus differentials

In [LMM91] Lai, Massey and Murphy described the underlying theory of differential cryptanalysis. They suggest the use of differentials instead of characteristics in a differential attack. The difference between a characteristic and a differential is that the former shows one specific *route* of getting from a certain inputsum to a certain outputsum whereas the latter considers all possible *routes*. It means that in general the probability for a differential is higher than for the corresponding characteristic. For LOKI we have considered the below 5-round characteristic, where ϕ =00 40 00 00_x, i.e. a situation evolved from using the fixpointcharacteristic. The



total probability is $(\frac{28}{4096})^3 \simeq 2^{-21,6}$. For the corresponding differential we have 1866 *routes* of getting from inputsum (ϕ,0) to outputsum (ϕ, ϕ). The estimated probability for the differential is $2^{-21,6} + 2^{-45}$, that is, not significantly higher than for the 5-round characteristic. Similar tests for differentials with more than 5 rounds have a much higher complexity and we didn't go further in our examinations. It seems unlikely that we can find a differential that enables us to get much further in the differential attacks.

Table 1. Estimates of needed pairs for differential attacks on LOKI

Rounds	Char.Prob.	S/N	Attack	Number of keybit-xors	Pairs Needed
4	1	2^8	3R	All	8
6	2^{-12}, 2^{-13}	2^4, 2^3	3R	All	2^{15}
8	2^{-21}	7	3R	28	2^{24}
9	2^{-29}	8	3R	32	2^{32}
9	2^{-29}	2^{27}	2R	32	2^{31}
10	2^{-36}	2^{20}	2R	32	2^{38}
11	2^{-43}	2^{13}	2R	32	2^{45}
12	2^{-43}	2^{13}	2R	32	2^{45}
13	2^{-50}	2^6	2R	32	2^{53}
14	2^{-58}	2^{-2}	2R	32	Not possible
14	2^{-58}	2^6	1R	12	2^{60}
15	2^{-65}	2^{-1}	1R	12	Not possible

Acknowledgements

Thanks to Ivan Bjerre Damgård for the help in shortening the proof of Theorem 1 and for moral support. Thanks to D.Å.T. for believing in me.

Bibliography

[LMM91] Xueija Lai, James L. Massey, Sean Murphy. *Markov Ciphers and Differential Cryptanalysis* Advances in Cryptology - EUROCRYPT'91. Springer Verlag, Lecture Notes 547.

[BPS90] Lawrence Brown, Josef Pieprzyk, Jennifer Seberry. *LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications.* Advances in Cryptology - AUSCRYPT '90. Springer Verlag, Lecture Notes 453, pp. 229-236, 1990.

[BS90] Eli Biham, Adi Shamir. *Differential Cryptanalysis of DES-like Cryptosystems.* Journal of Cryptology 1991.

[BS91] Eli Biham, Adi Shamir. *Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer.* Presented at CRYPTO '91.