Weaknesses in LOKI97

Lars R. Knudsen Vincent Rijmen*
University of Bergen, Dept. of Informatics
Hi-techcenter, N–5020 Bergen, Norway
larsr@ii.uib.no, vincent.rijmen@esat.kuleuven.ac.be

January 29, 1999

Abstract

We discuss the resistance of LOKI97 against linear and differential cryptanalysis, two theoretical attacks. It turns out there are weaknesses present in the round function of LOKI97, that allow to mount differential and linear attacks. We believe that these weaknesses are serious enough to conclude that LOKI97 is not a strong candidate for the AES.

1 Introduction

The block cipher LOKI97 [2] was designed by L. Brown and J. Pieprzyk. It has been submitted as a candidate for the Advanced Encryption Standard (AES). More information about the AES Development Effort can be found at the following URL: `http://www.nist.gov/aes/`. It is assumed that the reader is familiar with the description of LOKI97.

In this paper we discuss the resistance of the cipher against two theoretic attacks: differential cryptanalysis, which is a chosen plaintext attack, and linear cryptanalysis, which is a known plaintext attack. We also briefly discuss the applicability of partitioning cryptanalysis, an extension of linear cryptanalysis, which can be either chosen or known plaintext. Although these attacks are mostly theoretical, it is widely accepted that a modern block cipher should resist these attacks.

The results can be summarized as follows.

Differential cryptanlysis: One-bit input differences in the round function have a relatively large probability to result in one-bit output differences. LOKI97 has 31 two-round iterative characteristics with probability 2^{-10}, and one with probability 2^{-8}.

Linear and partitioning cryptanalysis: The f-function of LOKI97 is imbalanced. As a consequence, for certain values of the round keys, there are several iterative two-round linear relations. For 25% of the round keys, there is a two-round relation with a bias of 2^{-4}. The imbalance of the round function also opens the possibility for a partitioning attack. We describe how such an attack could be mounted.

In the next sections we explain the weaknesses in the round function and the forthcoming attacks in more detail.

*F.W.O. Postdoctoral Researcher, sponsored by the Fund for Scientific Research - Flanders (Belgium)

2 Differential Cryptanalysis

We consider words of 64 bits, numbered from 0 for the least significant bit, to 63 for the most significant bit. Let e_i be the 64-bit word that has a 1-bit in the ith position and 0-bits in all other positions, such that e_0 has the value 1 in the least significant bit. Loki97 operates on 128-bit words, which is denoted as tuples of two 64-bit words (X, Y).

2.1 Good Characteristics

Consider two inputs (L, R) and (L^*, R^*), where $L = L^*$ and R and R^* differ in one bit only $(R \oplus R^* = e_i)$. We study now the probability of a two-round iterative characteristic based on this difference.

2.1.1 The key addition

If $i < 63$, the difference e_i remains unchanged under the addition modulo 2^{64} of a round key with probability 0.5. If $i = 63$, the probability is 1. There are two key additions in every round.

2.1.2 The nonlinear function

In order to build a two-round iterative characteristic, it is required that two different inputs to the round function, can yield equal outputs. Or equivalently, we say that a nonzero input difference of the round function must be able to give zero output difference.

The probability that the output difference of the round function is zero depends on the number of 'active' S-boxes in the first layer, i.e. the number of S-boxes with a nonzero input difference. A straightforward implementation shows, that for $2^{13} - 2^8$ of the possible $2^{13} - 1$ nonzero input differences to S-box S1, the probability to get the output difference zero is 2^{-8}. For the remaining input differences, this probability is zero. Eleven of the thirteen one-bit input differences have this positive probability.

Similarly, for $2^{11} - 2^8$ of the possible $2^{11} - 1$ nonzero input differences to S-box S2, the probability to get the output difference zero is 2^{-8}. For the remaining input differences, the probability is zero. Eight of the eleven one-bit input differences have this positive probability.

A one-bit input difference will always make either one or two S-boxes active, depending on whether the bit causing the difference is replicated by the expansion E or not. The highest probabilities correspond to differences that make only one S-box active. Table 1 lists the positions of the input bits to E which are not expanded.

63	**62**	**61**	60	59	**31**	**30**	**29**		
55	**54**	**53**			**23**	**22**	**21**	20	19
47	**46**	**45**	44	43	**15**	**14**	**13**		
39	**38**	**37**	36	35	**7**	**6**	**5**		

Table 1: Positions of the input bits to E that are not expanded. The numbers in bold correspond to input bits i for which neither i nor $i + 32 \bmod 64$ is expanded.

Consider the inputs to the round function. A one-bit input difference e_i will go to a zero output difference with 'large' probability (2^{-8}) if it activates only one S-box and if the input

difference of the active S-box can result in a zero output difference.

The keyed permutation KP permutes the bits according to a key SKr as follows. If bit i of SKr is 1, input bit i is moved to position $i + 32 \bmod 64$ of the output. If bit i of SKr is 0, input bit i is moved to position i of the output. We distinguish between three types of positions of the input bits to the round function. Consider two inputs to the round function different in one bit only, in the ith position. If it holds that positions i and $i + 32 \bmod 64$ are not expanded by E, then a one-bit input difference (with a 1-bit in the ith position), stays a one-bit input difference after KP and E, and thus gives only one active S-box. (These bits are the bits in bold of Table 1.) If only one of the positions i and $i + 32 \bmod 64$ are expanded by E, the value of the keyed-permutation key determines whether the one-bit input difference yields one or two active S-boxes. There is one active S-box for one-bit input differences for which the difference bit is in one of the positions not in bold of Table 1 after the permutation KP. Finally if both the positions i and $i + 32 \bmod 64$ are expanded by E, then a one-bit input difference will result in two active S-boxes.

Summarizing, and taking into account that for both S-boxes there are some one-bit input differences that cannot result in an output difference 0, we have that a one-bit input difference at position i of the round function goes to an output difference 0 with probability 2^{-8} if and only if:

case a: $i \in \{7, 15, 23, 31, 39, 47, 55, 63\}$

case b: $i \in \{14, 19, 20, 30, 35, 36, 38, 43, 44, 54, 59, 60\}$ and the permutation key has a zero bit at position $i \bmod 32$.

case c: $i \in \{3, 4, 6, 11, 12, 22, 27, 28, 46, 51, 52, 62\}$ and the permutation key has a one bit at position $i \bmod 32$.

In fact, the probability is slightly larger than 2^{-8} because if the output difference of the first S-box layer is nonzero, the second layer of S-boxes can still produce a zero output difference. We ignore these effects in the following, but they only strengthen our results.

Combining the above results with the probabilities from the key addition, we get the following iterative two-round differential characteristics.

- One characteristic with probability 2^{-8} (difference in the most significant bit).
- 7 characteristics with probability 2^{-10} (differences from case a, except $i = 63$).
- 24 key-dependent characteristics with probability 2^{-10}, with a condition on one bit of the round key (differences from cases b and c).

These characteristics can be concatenated 7 times to make 15-round characteristics with probability 2^{-56} or 2^{-70}.

2.1.3 Resynchronization

The success rate of a differential attack is determined by the probability of a differential, rather than the probability of a differential characteristic: it is not important whether the pairs follow the whole characteristic, as long as they have the correct output differences (cf. [5]). In most cases, the probability of a good differential characteristic is a good approximation of the probability of the differential. It has been shown [4] that the mixed use of additions and exor

can cause *resynchronization*: pairs that deviate from the characteristic in a few rounds can 'come back' to the good difference values. For a detailed explanation of this effect, the reader is referred to [4].

In each round of LOKI97 the right half of the texts is added modulo 2^{64} to two round keys. A one-bit (XOR) difference in the texts will remain unchanged after the addition of a round key with probability 1/2. In general, a modular addition of a constant (a round key) will transform a one-bit difference to an n-bit difference with probability 2^{-n}. Note, that the value of n is restricted, depending on the position of the one-bit difference, e.g., if the difference is in the most significant bit, a one-bit difference always stays a one-bit difference (no effect of carry-bits).

In LOKI97, two types of resynchronization are possible:

- A one-bit input difference at the first round key addition of a round can go to an n-bit output difference for $n \geq 1$. After the second round key addition, the difference can go back to a one-bit difference with a total probability of 2^{-1}. To see this, note that one can consider the two round-key additions as one, from which the result follows. The probability that the output difference of the round function is zero however, depends on the position of the difference bit and the value of the permutation key: as long as the number of active S-boxes doesn't increase, the probability remains essentially the same, otherwise it drops with a factor 2^{-8} for each extra active S-box.

- A one-bit input difference at the second round key addition of the first round can go to an n-bit output difference for $n > 1$, go unchanged through the exor in the second round, and then become a one-bit difference again after the first round key addition of the third round, with some probability. The advantage here is that the round function input difference stays the same.

The improvement on the total characteristic's probability is cumbersome to determine analytically and depends on the exact bit positions of the difference bit through the rounds in a characteristic. Since it is our opinion that the probabilities of the characteristics reported in this paper are high even without incorporation of these "resynchronization properties" we did not perform these calculations.

2.2 Mounting an attack

There are two immediate ways to exploit the characteristics in an attack.

1. Use the first-round trick [1] and use 15-round characteristics from the second round to the sixteenth round. Use both halves of ciphertexts to filter out wrong pairs. This filtering will discard all wrong pairs. Search for the key in the first round.

2. Use 15-round characteristics, from the plaintexts to the 15th round, starting and ending with a zero-round. Search for the key in the last round. Filtering of wrong pairs is done by inspection of right halves of ciphertexts.

We estimate that at most 2^{56} chosen plaintexts are needed for this attack.

3 Linear and Partitioning Cryptanalysis

The round function of LOKI97 uses two S-box layers. In the second S-box layer, part of the S-boxes' inputs are determined by the round key alone, in other words, for a given key they are fixed. If, for a given key, all possible text inputs are applied to the second S-box layer, not all possible outputs are reached and the output bits are not balanced. This observation allows us to mount a linear attack [6] and (probably) a partitioning attack [3] (cf. Section 3.2).

3.1 Linear Cryptanalysis

In order to mount a linear attack, a linear approximation of the block cipher (or part thereof) has to be found. We distinguish between two types of linear approximations.

type I: A type I approximation exploits correlations between a sum of input bits of the round function and a sum of its output bits. This type of approximation is used in the attack on DES [6]. However, the double S-box layer in LOKI97 as well as the design of the S-boxes themselves ensure that there are no high correlations between sums of input bits and sums of output bits.

type II: A type II approximation exploits imbalance in the output of the round function. Only every second round needs to be taken into account.

For the linear attack on LOKI97, we not only have to consider the output balance of the round function, but also the modular round key addition. It is well known that a modular addition has maximal correlation between the least significant bit of the input and the least significant bit of the output. For other bits, the correlation may be smaller, depending on the value of the round key. Table 2 gives numerical values for some of the correlations. The least significant bits of the output of the round function are output bits of an instance of S-box S1.

addition				round function			
	relation	bias	key fraction		relation	bias	key fraction
(a)	$i_0 \oplus o_0$	0.5	1	(f)	$i_0 \oplus o_0$	2^{-4}	0.25
(b)	$i_1 \oplus o_1$	0.5	0.5	(g)	$i_1 \oplus o_1$	2^{-4}	0.25
(c)	$i_0 \oplus i_1 \oplus o_0 \oplus o_1$	0.5	0.5	(h)	$i_0 \oplus i_1 \oplus o_0 \oplus o_1$	2^{-5}	1
(d)	$i_1 \oplus o_0 \oplus o_1$	0.5	0.5				
(e)	$i_0 \oplus i_1 \oplus o_1$	0.5	0.5				

Table 2: Biases of linear relations over the modular addition and the round function, involving only the two least significant bits of the input (denoted with i_t) and output (denoted with o_t). It is also indicated for what fraction of the keys the relations hold with the given bias.

Table 2 learns us that by combining the relations (a) and (f), we can build a two-round approximation involving only the least significant bits. It holds for 25% of the round keys, with a bias of 2^{-4}. Thus, we have a 16-round linear relation with bias $2^7(2^{-4})^8 = 2^{-25}$, that holds for $(1/4)^8 = 2^{-16}$ of the keys. We estimate that for these 'weak keys' a linear attack can be mounted, requiring at most 2^{56} known plaintexts. Other approximations have a lower bias. They can be used to increase the fraction of keys that can be attacked. E.g., using

(c) and (h) we can build an approximation with bias 2^{-33}, holding for 2^{-8} of the keys. We are convinced that for every key an approximation can be found, but the required number of known plaintexts will increase.

3.2 Partitioning Cryptanalysis

Partitioning cryptanalysis was developed by Harpes and Massey as a generalization of linear cryptanalysis [3]. A partitioning attack can be a chosen plaintext or a known plaintext attack. The plaintexts and ciphertexts are classified into a number of mutually disjoint sets (a partition). A partitioning attack can be mounted, if the plaintext-ciphertext pairs distribution is not uniform. The advantage of a partitioning attack over a linear attack is that it will work for all keys, but it requires a much more complex analysis of the observed plaintext-ciphertext pairs.

For the case of LOKI97, the partitioning of plaintexts and ciphertexts should probably occur according to the value of the least significant byte, either of the left half or the right half of the texts. Thus we would have a partition with 256 sets S_i.

$$X \in S_i \Leftrightarrow X \& \mathtt{FF_x} = i$$

In every two rounds, this byte is changed in the following ways:

- Key is added: this changes the byte in an unknown, but deterministic way: all texts of a set S_i are mapped to texts in the set $S_{i+K_1+K_2 \bmod 256}$.
- Round function output is exored. The least significant byte of the round function output equals the output of an instance of S1, with part of the input of S1 fixed by the unknown round key. This output is not uniformly distributed.

The result is that the probability that a plaintext from the set S_i is mapped to a ciphertext in the set S_j, depends on the value of i and j. It is left as an open question how efficient an attack based on these observation is.

4 Conclusion

The round function of LOKI97 exhibits several high-probability differential characteristics. Furthermore, the partially fixed input (for a given key) in the second S-box layer results in some cases in a biased output, opening the way for a linear attack. It is our opinion that the results presented in this paper makes LOKI97 a weak candidate for AES. A contemporary block cipher with a 128-bit block ought to resist differential and linear attack much better than LOKI97.

References

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

[2] L. Brown and J. Pieprzyk. Introducing the new LOKI97 block cipher. 1998.

[3] C. Harpes and J.L. Massey. The interpolation attack on block ciphers. In E. Biham, editor, *Fast Software Encryption '97, LNCS 1267*, pages 13–27. Springer-Verlag, 1997.

[4] L.R. Knudsen, V. Rijmen, R.L. Rivest and M.J.B. Robshaw. On the design and security of RC2. In S. Vaudenay, editor, *Fast Software Encryption '98, LNCS 1372,* pages 206–221. Springer-Verlag, 1998.

[5] X. Lai, J.L. Massey and S. Murphy, Markov ciphers and differential cryptanalysis. In D.W. Davies, editor, *Advances in Cryptology, Proceedings Eurocrypt'91, LNCS 547*, pages 17–38. Springer-Verlag, 1991.

[6] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93, LNCS 765*, pages 386–397. Springer Verlag, 1993.