Weaknesses in LOKI97

Vincent Rijmen   Lars R. Knudsen

June 15, 1998

Abstract

We explain two weaknesses that are present in the round function of LOKI97. 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://csrc.nist.gov/encryption/aes/aes_home.htm`.

The two weaknesses that we found in LOKI97, are the following.

1. LOKI97 has a two-round iterative characteristic with probability 2^{-8}.
2. The f-function of LOKI97 is imbalanced. As a consequence, for certain values of the round keys, there are iterative two-round linear relations with a bias of 2^{-4}.

In the next sections we explain the weaknesses in more detail.

2 Differential Cryptanalysis

Consider two inputs (L, R) and (L^*, R^*), where $L = L^*$ and R and R^* differ in the most significant bit only ($R \oplus R^* = \mathtt{8000000000000000}_{\mathtt{x}}$). We denote this difference $(0, \alpha)$.

Since this difference remains unchanged under the addition modulo 2^{64} of a round key, we know that the left half of the output difference of the first round will be α. In order to determine the right half of the output difference, we have to consider the nonlinear f-function.

The input difference of the f-function equals α. Depending on the value of one round key bit, the keyed permutation will preserve the difference, or move the 'difference bit' to another position (position 31). In both cases, we have that after the expansion, the input difference of seven S-boxes is zero. Depending on the position of the difference bit after the permutation, the input difference of the first S-box (an instance of S1) or the input difference of the fifth S-box (an instance of S2) equals $\mathtt{80}_{\mathtt{x}}$. In both cases the output difference equals zero with probability 2^{-8}. Since the second layer of S-boxes has now an input difference zero, the output difference of the f-function will be zero. Thus, we have that the output difference of the round equals $(\alpha, 0)$ with the same probability.

In fact, the probability of our characteristic 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.

In the second round, the input difference of the f-function equals zero, and with probability one, we get the required output difference of $(0, \alpha)$ back.

This characteristic can be concatenated to a 14- or 16-round characteristic with probability 2^{-56}, respectively 2^{-64}.

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

1. Use the first-round trick [1] and use a 15-round characteristic 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 a 15-round charateristic, 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 Cryptanalysis

In the second S-box layer, part of the S-box inputs are determined by the round key alone, i.e., for a given key they are fixed. The consequence is that the output becomes inbalanced. We can use this to mount a linear attack [3].

Consider the least significant bit of the last S-box of the second layer (an instance of S1). For 25% of the round keys it is biased, with a bias of 2^{-4}. Since modular addition equals exclusive-or in the least significant bits, the addition of a round key will not affect the bias. This means that for some keys we can construct a so-called type II linear relation where one needs an approximation in only every second round. The relation can be iterated any number of rounds. E.g., we get that for $(1/4)^8 = 2^{-16}$ of the keys, we will have a 16-round linear relation with bias $2^7(2^{-4})^8 = 2^{-25}$.

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

4 Conclusion

LOKI97 is broken.

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] 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.