From: maro@isl.ntt.co.jp
To: AESFirstRound@nist.gov
Subject: Search for Impossible Differential of E2
Date: Fri, 16 Apr 1999 00:48:26 JST
Sender: maro@sucaba.isl.ntt.co.jp

Dear Director/ITL,

I submit the report titled
  Search for Impossible Differential of E2
using PostScript. The file is generated with gzip and uuencode. If you cannot print the file, please ask me.

Best regards,

/ NTT Laboratories
/ AOKI, Kazumaro
/ E-mail: maro@isl.ntt.co.jp

Search for Impossible Differential of *E2*

Kazumaro Aoki and Masayuki Kanda
NTT Laboratories*

April 15, 1999

Abstract

This paper studies the search for the impossible differentials of ***E2***. We apply the Shrinking technique, the miss-in-the-middle technique, and a new search algorithm to ***E2***. As a result, no impossible differential is found for ***E2*** with more than 5 rounds. We conclude that ***E2*** is secure against cryptanalysis using impossible differentials derived by the currently known techniques.

Keywords. impossible differential, cryptanalysis with impossible differentials, ***E2***

1 Introduction

Cryptanalysis with impossible differentials was introduced by Biham et al. [BBS98] and is powerful. This attack uses differentials with probability 0, which are called *impossible differentials*. If attackers can find no impossible differentials for a cipher, the cipher cannot be attacked by cryptanalysis with impossible differentials.

Generally speaking, the search for impossible differentials is difficult because much complexity is required to guarantee completeness. Only two techniques are known: the *Shrinking technique* [BBS99a][1], and *miss-in-the-middle* technique [BBS99c]. The former is a search algorithm for impossible differentials that offers reduced complexity; the latter generates impossible differentials by connecting two (truncated) differentials with probability 1.

We apply the Shrinking technique, the miss-in-the-middle technique, and our new search algorithm that includes the miss-in-the-middle technique, to ***E2***. As a result, no impossible differential is found for ***E2*** with more than 5 rounds. We conclude that ***E2*** is secure against cryptanalysis with impossible differentials using currently known techniques.

2 Shrinking Technique

2.1 Technique

The Shrinking technique, which is used with the miss-in-the-middle technique, is a simple search algorithm for impossible differentials.

The basic strategy of the miss-in-the-middle technique is as follows.

*Email: {maro@,kanda@sucaba.}isl.ntt.co.jp

[1] We did not see the paper, but we discussed this with Biryukov at FSE'99, and we think the contents of the reference are the same as [BBS99b].

Step 1: Choose input difference X of the cipher.
Step 2: Obtain all possible differences at the r-th round Z_r from the input difference.
Step 3: Search the set of bit position(s) of the differences Z_r whose values are always zero (nonzero). If no such set can be found, go back to Step 1. If no such position can be found for all input differences, no impossible differential exists for the cipher.
Step 4: Choose output difference Y of the cipher.
Step 5: Obtain all possible differences Z'_r at the same r-th round from the output difference.
Step 6: Check whether the value(s) at the same bit position(s) as Step 3 of the differences Z'_r is always nonzero (zero). If the check is satisfied, it means that we have found an impossible differential with respect to the input difference X and output difference Y. Otherwise, go back to Step 4 until all output differences have been checked. If the check has not examined all input differences, go back to Step 1.

Because the above steps involve excessive computational complexity, however, it is too difficult to directly apply the miss-in-the-middle technique to cipher. Against this problem, [BBS99a] introduced the idea of using a shrunken model of the original cipher; they called this the Shrinking technique. Roughly speaking, the shrunken model is a variant of the original cipher, that has a similar global structure to the cipher. That is, if the block length of the cipher is ds bits long and the primitive operation is s bits long, the block length of the model is ds' bits long and the primitive operation is s' bits long where s' is smaller than s.

Since the shrunken model has a similar global structure to the cipher, i.e., both use the same d, finding impossible differentials in the shrunken model indicates that there are also similar impossible differentials in the original cipher. Hence, if ds' can be set to a suitable value, one can apply the miss-in-the-middle technique to the shrunken model and find impossible differentials.

2.2 Result

We applied the Shrinking technique and the miss-in-the-middle technique to ***E2***. ***E2*** without IT- and FT-Function is a byte-oriented cipher, where $s = 8$, $d = 16$. Because of the computational complexity, we considered the shrunken model with $s' = 1$, $d = 16$. We let $X = (x_1, x_2, \ldots, x_{16})$ denote an input difference, where x_i denotes "state" such as *zero* or *nonzero*. Similarly, we define Z_j as a difference at intermediate round j; Y is an output difference.

Fortunately, without the IT- and FT-Function ***E2*** has only a bijective s-box and bitwise XOR. Thus, obviously, the properties of the shrunken model are the same as those of ***E2***. That is,

- Zero difference is always derived from the zero difference created in the s-box. Also, nonzero difference is always derived from nonzero difference.
- Zero difference is derived from both zero differences through bitwise XOR.
- Nonzero difference is derived from zero difference and nonzero difference within the bitwise XOR.
- We cannot know whether zero or nonzero is derived from both nonzero differences within the bitwise XOR. We call this state *otherwise*, which gives us no useful information in locating impossible differentials.

Because of the above properties, it is sufficient to consider the following in applying the algorithm.

- The state of x_i and y_i is either *zero* or *nonzero*.

- X is nonzero, i.e., $\exists i[x_i = \mathit{nonzero}]$. So is Y.
- The state of z_{j_i} is *zero*, *nonzero*, or *otherwise*.
- Once the state of z_{j_i} becomes *otherwise*, the states of subsequent z_{*_i} never become *zero* or *nonzero*.
- Z_r, all of whose states are *otherwise*, i.e., $\forall i[z_{r_i} = \mathit{otherwise}]$, is of no further use.

We executed the above algorithm for all input differences of the shrunken model. As a result, we found that all states of Z_r are *otherwise* for $r \geq 4$, and that 5-round ***E2*** without IT- and FT-Function has the longest impossible differentials.

3 New Search Algorithm

3.1 Algorithm

In general, locating an impossible differential is very difficult because the theory of impossible differentials remains under construction. However, we can use the following algorithm if the cipher is byte-oriented. The strategy of the algorithm is as follows.

Step 1: Choose input differences of the cipher heuristically. According to our experience, the input difference of differentials with high probability generates a long impossible differential.
Step 2: Search all possible differentials whose input difference is chosen by Step 1.
Step 3: Check all output differences of the possible differentials derived in Step 2. If there exists an output difference that is not contained in the set of all possible values of differences, it means that we have found an impossible differential.

Let the block length of the cipher be ds bits long, where the primitive operation of the cipher is s bits long and let $S = \mathrm{GF}(2)^s$. We define the difference operation as addition in $\mathrm{GF}(2)^{ds}$. To realize Step 2, we define the difference set and the operations for the difference sets.

Definition 1 (**Difference Set**) We call a set of differences a *difference set*. A difference set is a subset of S^d.

Definition 2 (**Operations on Difference Sets**) Let

$$x_j = f(x_{i_1}, x_{i_2}, \ldots, x_{i_t}) \quad (x_j, x_{i_1}, x_{i_2}, \ldots, x_{i_t} \in S)$$

be an s bit operation of the cipher. We define the operation f on the difference sets D_{i_1}, D_{i_2}, ..., and D_{i_t} as

$$\begin{aligned} & f(D_{i_1}, D_{i_2}, \ldots, D_{i_t}) \\ = \; & \{f(x_{i_1}, x_{i_2}, \ldots, x_{i_t}) \oplus f(x_{i_1} \oplus d_{i_1}, x_{i_2} \oplus d_{i_2}, \ldots, x_{i_t} \oplus d_{i_t}) \\ & |x_{i_1} \in S,\ x_{i_2} \in S,\ \ldots,\ x_{i_t} \in S,\ d_{i_1} \in D_{i_1},\ d_{i_2} \in D_{i_2},\ \ldots,\ d_{i_t} \in D_{i_t}\}. \end{aligned}$$

Algorithm 1
Step 1: Initialize the difference sets $D_i \subseteq S$ $(i = 1, 2, \ldots, d)$ using proper values.
Step 2: Following the specification of the cipher, calculate

$$D_j = f(D_{i_1}, D_{i_2}, \ldots, D_{i_t})$$

step by step, where f is one of the primitive operations of the cipher.
Step 3: Confirm whether $D_j \neq S$ holds or not for $j = 1, 2, \ldots, r$, when finishing all set operations corresponding to the cipher operations. We have found an impossible differential if $\exists j[D_j \neq S]$.

3.2 Results

Since ***E2*** without IT- and FT-Function has 8 bit primitive operations let $S = \mathrm{GF}(2)^8$. We follow the transitions of D_1, D_2, ..., and D_{16}. However, even if we use Algorithm 1, we cannot computationally search all cases. We only consider the initial values of D_1, D_2, ..., and D_{16} that satisfy $D_i = \{x\},\ D_j = \{0\}\ (\forall j \neq i)$ for all $1 \leq i \leq 16,\ x \in S$.

As a result, the longest impossible differentials we found using the miss-in-the-middle technique are 5 rounds. We note that 5-round impossible differentials exist for a DES-like cipher with bijective F-Functions [K98]. The impossible differentials discussed in this paper are a subset of theirs.

4 Conclusion

We applied the Shrinking technique, the miss-in-the-middle technique, and a new search algorithm to identify the impossible differentials of ***E2***. We confirmed that ***E2*** has at most 5-round impossible differentials. Thus, it seems that ***E2*** is secure against cryptanalysis with impossible differentials using the current all search algorithms for identifying impossible differentials.

Acknowledgment

We wish to thank Alex Biryukov for answering our questions about the Shrinking technique at FSE'99 break time.

References

[BBS98] E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials. Technical Report CS0947, Technion — Computer Science Department, 1998. (`http://www.cs.technion.ac.il/~biham/Reports/SkipJack/`).

[BBS99a] 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*, Volume 1592 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Heidelberg, New York, 1999. to appear.

[BBS99b] E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials. Technical Report CS0947.revised, Technion — Computer Science Department, 1999. (`http://www.cs.technion.ac.il/~biham/Reports/SkipJack/`).

[BBS99c] E. Biham, A. Biryukov, and A. Shamir. Miss in the Middle Attacks on IDEA, Khufu and Khafre. In L. Knudsen, editor, *preproceedings of Fast Software Encryption — 6th International Workshop, FSE'99*, pp. 121–137, 1999. (A preliminary version was presented at CRYPTO'98 rump session).

[K98] L. R. Knudsen. DEAL - A 128-bit Block Cipher. Technical Report no. 151, Department of Informatics,University of Bergen, Norway, 1998. (`http://www.ii.uib.no/~larsr/newblock.html`).