Yuechuan Wei, Ruilin Li, Ping Li, Chao Li. Impossible Differential Cryptanalysis on E2. JOURNAL OF COMPOUTER SCIENCE AND TECHNOLOGY : 1– Mon. Year

Impossible Differential Cryptanalysis on E2

Yuechuan Wei[1], Ruilin Li[2], Ping Li[2] and Chao Li[1,2,3]

[1]*School of Computer, National University of Defense Technology, Changsha, 410073, China*
[2]*Science College, National University of Defense Technology, Changsha, 410073, China*
[3]*State Key Laboratory of Information Security, Chinese Academy of Sciences, Beijing, 100190, China*

E-mail: wych004@163.com; {securitylrl, leave17}@gmail.com; lichao_nudt@sina.com

Received February 26, 2010

Abstract E2 is a 128-bit block cipher which employs a Feistel structure and 2-round SPN in round function. It is an AES candidate and was designed by NTT. In the former publications, E2 is supposed no more than 5-round impossible differential. In this paper, we describe some 6-round impossible differentials of E2. By using the 6-round impossible differential, we first present an attack on a 9-round reduced version of E2-256 without IT Function (the initial transformation) and FT-Function (the final transformation).

Keywords Block cipher, E2, Impossible differential attack, Data complexity, Time complexity

1 Introduction

Impossible differential cryptanalysis, proposed by Biham and Knudsen respectively, was first applied to the cipher DEAL[1] and later to Skipjack[2]. The main idea is to specify a differential of probability zero over some rounds of the cipher. Then one can derive the right keys by discarding the keys which lead to the impossible differential. Impossible differential cryptanalysis has been used to attack AES, Camellia, MISTY1 and so on, which got very good results[3, 4, 5, 6, 7, 8, 9].

The key step of impossible differential cryptanalysis is to retrieve the longest impossible differential. The main technique is miss-in-the-middle, namely to find two differential characteristics with probability 1 from encryption and decryption, and connect them together when there are some inconsistencies. In ref.[10], Kim *et al* introduced the $\mathcal{U}$-method to find impossible differential characteristics of various block ciphers. However, $\mathcal{U}$-method is so general that it is lack of pertinence for a given cipher, therefore, some information is often lost during calculating the impossible differential characteristics. Some longer impossible differential is can't be found by the $\mathcal{U}$-method.

E2[11] is a 128-bit block cipher designed and submitted to AES project by NTT. Its design criteria are conservative, adopting a Feistel network structure as a global structure and the 2-round SPN-structure in its round function. All operations used in the data randomization phase are byte table lookups and byte xor's except 32-bit multiplications in IT and FT, which successfully makes E2 a fast software cipher independent of target platforms.

A truncated differential cryptanalysis of

This work was supported by the Natural Science Foundation of China(No: 60803156) and the open research fund of State Key Laboratory of Information Security(No: 01-07).

reduced-round variants of E2 was presented by Matsui and Tokita in ref.[12]. They found a 7-round byte characteristic, which leads to a possible attack on an 8-round E2 without IT-Function and FT-Function. In ref.[13], Moriai et al. presented another 7-round truncated differential and improved the attack complexity of 8-round E2 without IT/FT functions. Ref.[14] studies the impossible differentials of E2. To search the impossible differentials, the authors applied the Shrinking technique, the miss-in-the-middle technique and so on. However, no impossible differential is found for E2 without IT/FT functions with more than 5 rounds. They declared that E2 is secure against cryptanalysis with impossible differential using currently known techniques.

In this paper, the security of E2 against impossible differential attacks are investigated. We first find some 6-round impossible differentials which lead to an attack of E2 reduced to 9 rounds without IT/FT functions. The attack is the first published attack on 9-round E2 without IT/FT functions. Like most cryptanalytic attacks on block ciphers, it is theoretical in the sense of the magnitude of the required data and time complexity and the attack does not have a serious impact on the full E2, since it has twelve rounds with IT and FT; however our results show that the security level of the E2 is much lower than the estimation of the designers.

The paper is organized as follows: Section 2 briefly introduces some notations and the E2 block cipher. In section 3, we describe some 6-round impossible differentials. Then the attack are discussed in section 4. Section 5 concludes the paper and summarizes our results.

2 Preliminaries

2.1 Notations

The following describes the notations which will be used in encryption and attack.

$L_i(R_i)$:	the left(right) half output of the i^{th} round;
$\Delta L_i(\Delta R_i)$:	the difference of the left(right) half output of the i^{th} round;
$K_{i,j}^{(1)}$:	the j^{th} byte of subkey in first layer of the i^{th} round function;
$K_{i,j}^{(2)}$:	the j^{th} byte of subkey in second layer of the i^{th} round function;
$\oplus$:	xor(exclusive or);
$\vert$:	bit string concatenation.

2.2 The E2 Block Cipher

E2 is a 12-round Feistel cipher with 2-round SPN structure in its round function and the linear layer used is proved to be optimal[15, 16]. The strategy of 2-round SPN structure is proposed in ref.[17]. It based on using mn-bit round functions consisting of four-layers: 1st non-linear transformation layer with n parallel m-bit s-boxes, 1st linear transformation layer, 2nd non-linear transformation layer with n parallel m-bit s-boxes, and 2nd linear transformation layer(sometimes the fourth layer is omitted). Ref.[17] shows that the round function with the 2-round SPN structure requires one-forth as many rounds as the 1-round SPN structure to achieve the same differential and linear probabilities.

Besides, E2 has a preprocess, IT-Function, as well as a postprocess, FT-Function. The decryption process is the same as the encryption process except for the order of the subkeys. Fig.1 shows the outline of the E2 encryption process.

Let P and C be the plaintext and cipertext respectively, L_{r-1} and R_{r-1} be the left and the right halves input of the r^{th} round, and K_r be the subkey of the r^{th} round. Then the encryption process of E2 can be written as:

$$\begin{aligned} L_0|R_0 &= IT(P), \\ L_r &= R_{r-1} \oplus F(L_{r-1}, K_r)(r = 1, 2 \ldots, 12), \\ R_r &= L_{r-1}, \\ C &= FT(R_{12}|L_{12}). \end{aligned}$$

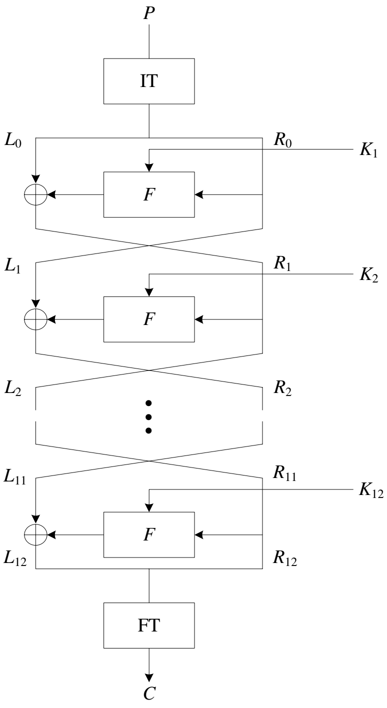

Fig. 1. Encryption Process of E2

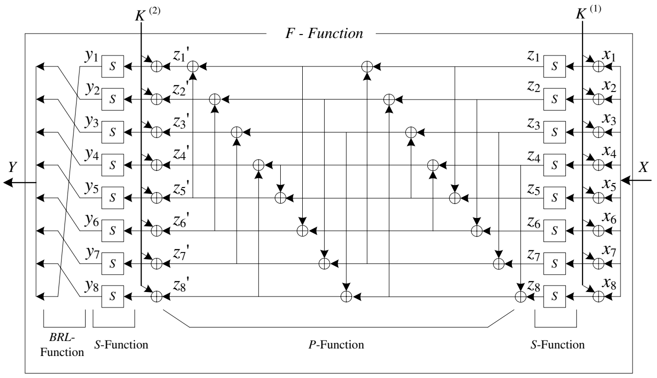
$K^{(2)}$
$K^{(1)}$
F - Function
Y
X
y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8
S
z_1' z_2' z_3' z_4' z_5' z_6' z_7' z_8'
z_1 z_2 z_3 z_4 z_5 z_6 z_7 z_8
x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8
BRL-Function
S-Function
P-Function
S-Function

Fig. 2. Round Function of E2

In this paper, we will consider E2 without IT/FT functions. Fig.2 outlines the round function. Round function consists of S-Function, P-Function, and BRL-Function. Refer to [11] for details of the specification and notations. For readers' convenience, we give algebraic description of the variable $z_i^{'}$ in the round function in terms of the intermediate values z_i as follows:

$$P : (\mathbb{F}_2^8)^8 \to (\mathbb{F}_2^8)^8:$$
$$z_1|z_2|z_3|z_4|z_5|z_6|z_7|z_8 \to z_1^{'}|z_2^{'}|z_3^{'}|z_4^{'}|z_5^{'}|z_6^{'}|z_7^{'}|z_8^{'}$$

$$\begin{aligned} z_1^{'} &= z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7 \\ z_2^{'} &= z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8 \\ z_3^{'} &= z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8 \\ z_4^{'} &= z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8 \\ z_5^{'} &= z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_6 \\ z_6^{'} &= z_1 \oplus z_2 \oplus z_3 \oplus z_6 \oplus z_7 \\ z_7^{'} &= z_2 \oplus z_3 \oplus z_4 \oplus z_7 \oplus z_8 \\ z_8^{'} &= z_1 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_8 \end{aligned}$$

3 Some 6-Round Impossible Differentials

In ref.[14], the authors drew the conclusion that there was no impossible differentials for E2 without IT/FT functions with more than 5-round. In this section, we show one impossible differential of 6-round E2 in Fig.3.

We assert that the 6-round differential

$$(0|0|0|0|a|0|0|0, 0|0|0|0|0|00|0) \xrightarrow{6-round}$$
$$(0|0|0|0|0|0|0|0, 0|0|0|0|0|h|0|0)$$

is impossible, where a and h denote any non-zero value.

Consider an input difference $(\Delta L_0, \Delta R_0) = (0|0|0|0|a|0|0|0, 0|0|0|0|0|0|0|0)$, after passing through the first and the second round, it becomes as follows(where c_i also denote non-zero value):

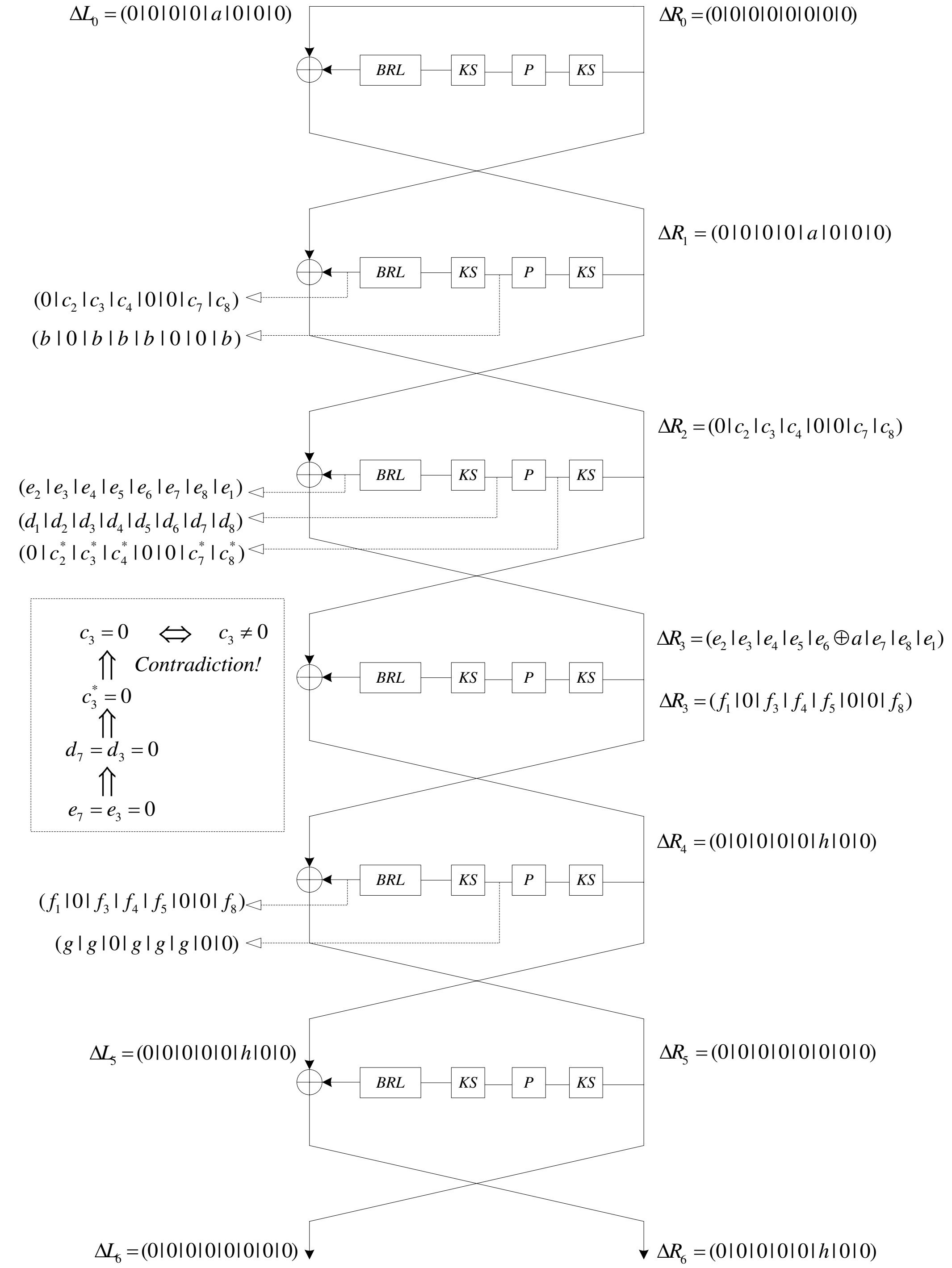
$\Delta L_0 = (0|0|0|0|a|0|0|0)$
$\Delta R_0 = (0|0|0|0|0|0|0|0)$
BRL
KS
P
KS
$\Delta R_1 = (0|0|0|0|a|0|0|0)$
$(0|c_2|c_3|c_4|0|0|c_7|c_8)$
$(b|0|b|b|b|0|0|b)$
$\Delta R_2 = (0|c_2|c_3|c_4|0|0|c_7|c_8)$
$(e_2|e_3|e_4|e_5|e_6|e_7|e_8|e_1)$
$(d_1|d_2|d_3|d_4|d_5|d_6|d_7|d_8)$
$(0|c_2^*|c_3^*|c_4^*|0|0|c_7^*|c_8^*)$
$c_3 = 0 \Leftrightarrow c_3 \neq 0$
$\Uparrow$ Contradiction!
$c_3^* = 0$
$\Uparrow$
$d_7 = d_3 = 0$
$\Uparrow$
$e_7 = e_3 = 0$
$\Delta R_3 = (e_2|e_3|e_4|e_5|e_6 \oplus a|e_7|e_8|e_1)$
$\Delta R_3 = (f_1|0|f_3|f_4|f_5|0|0|f_8)$
$\Delta R_4 = (0|0|0|0|0|h|0|0)$
$(f_1|0|f_3|f_4|f_5|0|0|f_8)$
$(g|g|0|g|g|g|0|0)$
$\Delta L_5 = (0|0|0|0|0|h|0|0)$
$\Delta R_5 = (0|0|0|0|0|0|0|0)$
$\Delta L_6 = (0|0|0|0|0|0|0|0)$
$\Delta R_6 = (0|0|0|0|0|h|0|0)$

Fig. 3. 6-Round Impossible Differential of E2

$$\begin{aligned}(\Delta L_1, \Delta R_1) &= (0|0|0|0|0|0|0|0, 0|0|0|0|a|0|0|0),\\ (\Delta L_2, \Delta R_2) &= (0|0|0|0|a|0|0|0, 0|c_2|c_3|c_4|0|0|c_7|c_8).\end{aligned}$$

In the third round, after the first subkey addition and the S layer, ΔR_2 becomes $(0|c_2^*|c_3^*|c_4^*|0|0|c_7^*|c_8^*)$, where c_i^* is non-zero value. After the linear layer P it becomes $(d_1|d_2|d_3|d_4|d_5|d_6|d_7|d_8)$, thus the output difference of the second subkey addition and the

S layer in the third round has the form of $(e_1|e_2|e_3|e_4|e_5|e_6|e_7|e_8)$. Whether the values of d_is and e_is ($i = 1 \ldots 8$) are zero or not is uncertain. The BRL-function makes the output difference be $(e_2|e_3|e_4|e_5|e_6|e_7|e_8|e_1)$. Therefore the 3-round differential ends with

$$\begin{gathered}(\Delta L_3, \Delta R_3) = \\ (0|c_2|c_3|c_4|0|0|c_7|c_8, e_2|e_3|e_4|e_5|e_6 \oplus a|e_7|e_8|e_1).\end{gathered}$$

Consider the other direction now, when rolling back the 6^{th} round output difference $(0|0|0|0|0|0|0|0, 0|0|0|0|0|h|0|0)$ though 3-round transformation, we get the following differences(f_i is non-zero value):

$$\begin{aligned}(\Delta L_5, \Delta R_5) &= (0|0|0|0|0|h|0|0, 0|0|0|0|0|0|0|0), \\ (\Delta L_4, \Delta R_4) &= (f_1|0|f_3|f_4|f_5|0|0|f_8, 0|0|0|0|0|h|0|0).\end{aligned}$$

From the property of Feistel structure, we have $\Delta L_4 = \Delta R_3$, hence, $(f_1|0|f_3|f_4|f_5|0|0|f_8)$ is the same as $(e_2|e_3|e_4|e_5|e_6 \oplus a|e_7|e_8|e_1)$, So we can get $e_3 = e_7 = e_8 = 0$, thus $d_3 = d_7 = d_8 = 0$ since subkey addition and S-boxes transformations are bijective. d_i can be expressed as the linear combination of c_i^* according to the linear layer P, which implies the following equations hold(just $d_3 = d_7 = 0$ is used):

$$\begin{aligned}c_2^* \oplus c_4^* \oplus c_7^* \oplus c_8^* &= 0, \\ c_2^* \oplus c_3^* \oplus c_4^* \oplus c_7^* \oplus c_8^* &= 0.\end{aligned}$$

From the above equations we know that c_3^* is zero, which contradicts with $c_3 \neq 0$ since subkey addition doesn't change the difference and S-boxes transformations are bijective.

Similarly, we can get other 6-round impossible differentials of $E2$. We define w_i as 8-byte vector, in which only the i^{th} byte is non-zero, for example, w_1 denotes $(a|0|0|0|0|0|0|0)$. If $(w_i, 0) \rightarrow (0, w_j)$ is an impossible differential, then $(w_j, 0) \rightarrow (0, w_i)$ is also an impossible differential since the encryption and the decryption are the same for Feistel cipher. The 6-round impossible differentials of E2 found by the way of Section.3 can be written as follows(for $i \leq j$).

$$\begin{array}{ll}
(w_1, 0) \xrightarrow{6-round} (0, w_1), & (w_1, 0) \xrightarrow{6-round} (0, w_3), \\
(w_1, 0) \xrightarrow{6-round} (0, w_5), & (w_1, 0) \xrightarrow{6-round} (0, w_6), \\
(w_1, 0) \xrightarrow{6-round} (0, w_8), & (w_2, 0) \xrightarrow{6-round} (0, w_5), \\
(w_2, 0) \xrightarrow{6-round} (0, w_6), & (w_2, 0) \xrightarrow{6-round} (0, w_8), \\
(w_3, 0) \xrightarrow{6-round} (0, w_5), & (w_3, 0) \xrightarrow{6-round} (0, w_6), \\
(w_3, 0) \xrightarrow{6-round} (0, w_8), & (w_4, 0) \xrightarrow{6-round} (0, w_6), \\
(w_4, 0) \xrightarrow{6-round} (0, w_8), & (w_5, 0) \xrightarrow{6-round} (0, w_5), \\
(w_5, 0) \xrightarrow{6-round} (0, w_6), & (w_5, 0) \xrightarrow{6-round} (0, w_8), \\
(w_6, 0) \xrightarrow{6-round} (0, w_6), & (w_6, 0) \xrightarrow{6-round} (0, w_7), \\
(w_7, 0) \xrightarrow{6-round} (0, w_8). &
\end{array}$$

4 Impossible Differential Attack on E2 Reduced to 9 Rounds

With the 6-round impossible differential, a 9-round impossible differential attack on E2 without IT/FT function can be obtained. The attack is based on the above 6-round impossible differentials with additional two rounds at the beginning and one round at the end as shown in Fig.4.

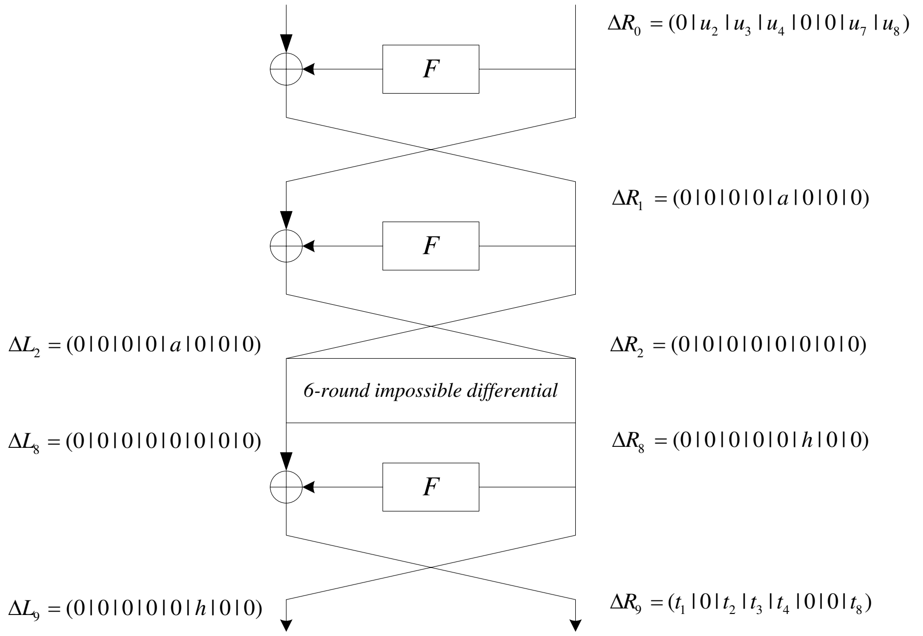
$\Delta R_0 = (0|u_2|u_3|u_4|0|0|u_7|u_8)$
F
$\Delta R_1 = (0|0|0|0|a|0|0|0)$
F
$\Delta L_2 = (0|0|0|0|a|0|0|0)$
$\Delta R_2 = (0|0|0|0|0|0|0|0)$
6-round impossible differential
$\Delta L_8 = (0|0|0|0|0|0|0|0)$
$\Delta R_8 = (0|0|0|0|0|h|0|0)$
F
$\Delta L_9 = (0|0|0|0|0|h|0|0)$
$\Delta R_9 = (t_1|0|t_2|t_3|t_4|0|0|t_8)$

Fig. 4. 9-Round Impossible Differential Attack to E2

The attack procedure is as follows:

Step 1 Precalculation: for S-box, define $T(\alpha,\beta) = \{x \in \mathbb{F}_2^8 | S(x \oplus \alpha) \oplus S(x) = \beta\}$, then take all possible values of (α,β), and store $T(\alpha,\beta)$ in a table.

Step 2 Choose structure of plaintexts as follows:

$$\begin{aligned} L_0 &= (y_1|y_2|y_3|y_4|y_5|y_6|y_7|y_8) \\ R_0 &= (\alpha_1|x_2|x_3|x_4|\alpha_5|\alpha_6|x_7|x_8) \end{aligned}$$

where $x_i (i = 2,3,4,7,8)$, $y_i(1 \le i \le 8)$ take all possible values in $\mathbb{F}_2^8$, $\alpha_i(i = 1,5,6)$ and $\beta_i(2 \le i \le 8)$ are constants in $\mathbb{F}_2^8$. For each possible value of $(y_1,y_2,y_3,y_4,y_5,y_6,y_7,y_8,x_2,x_3,x_4,x_7,x_8)$, we can get a unique 128-bit string. Hence, a structure includes 2^{104} plaintexts and there are $2^{104\times 2}/2 = 2^{207}$ plaintext pairs in a structure. So the 2^{17} structures yield a total of 2^{224} plaintext pairs.

Step 3 Keep only the pairs whose ciphertexts differential $(\Delta L_9, \Delta R_9)$ satisfy the following:

$$\begin{aligned} \Delta L_9 &= (0|0|0|0|0|h|0|0) \\ \Delta R_9 &= (t_1|0|t_2|t_3|t_4|0|0|t_8) \end{aligned}$$

where $t_i(i = 1,2,3,4,8)$ are unknown non-zero values. The expected number of remaining pairs is about $2^{224} \times 2^{-80} = 2^{144}$.

Step 4 Guess the 64-bit subkey $K_9^{(1)}$ and 5 subkey bytes $K_{9,1}^{(2)}$, $K_{9,2}^{(2)}$, $K_{9,4}^{(2)}$, $K_{9,5}^{(2)}$, $K_{9,6}^{(2)}$.

Step 4.1 For every remaining pair (L_0,R_0) and (L_0^*,R_0^*), guess the 64-bit subkey $K_9^{(1)}$ and compute

$$\begin{aligned} Z_9 &= PS(L_9 \oplus K_9^{(1)}), \\ Z_9^* &= PS(L_9^* \oplus K_9^{(1)}). \end{aligned}$$

Step 4.2 Guess the 5 bytes of $K_9^{(2)}$ and compute

$$\begin{aligned} q_1 &= s(Z_{9,1} \oplus K_{9,1}^{(2)}) \oplus s(Z_{9,1}^* \oplus K_{9,1}^{(2)}) \oplus R_{9,8} \oplus R_{9,8}^*, \\ q_2 &= s(Z_{9,2} \oplus K_{9,2}^{(2)}) \oplus s(Z_{9,2}^* \oplus K_{9,2}^{(2)}) \oplus R_{9,1} \oplus R_{9,1}^*, \\ q_3 &= s(Z_{9,4} \oplus K_{9,4}^{(2)}) \oplus s(Z_{9,4}^* \oplus K_{9,4}^{(2)}) \oplus R_{9,2} \oplus R_{9,2}^*, \\ q_4 &= s(Z_{9,5} \oplus K_{9,5}^{(2)}) \oplus s(Z_{9,5}^* \oplus K_{9,5}^{(2)}) \oplus R_{9,3} \oplus R_{9,3}^*, \\ q_5 &= s(Z_{9,6} \oplus K_{9,6}^{(2)}) \oplus s(Z_{9,6}^* \oplus K_{9,6}^{(2)}) \oplus R_{9,4} \oplus R_{9,4}^*. \end{aligned}$$

Then check whether $q_i = 0 (1 \le i \le 5)$ and keep only the qualified pairs. Since the probability is about 2^{-40}, the expected number of the remaining pairs is $2^{144} \times 2^{-40} = 2^{104}$.

Step 5 Guess the 64-bit subkeys $K_1^{(1)}$ and $K_1^{(2)}$, for every remaining plaintext pair (L_0, R_0) and (L_0^*, R_0^*),

$$\begin{aligned} L_0 &= (y_1|y_2|y_3|y_4|y_5|y_6|y_7|y_8) \\ R_0 &= (\alpha_1|x_2|x_3|x_4|\alpha_5|\alpha_6|x_7|x_8) \\ L_0^* &= (y_1^*|y_2^*|y_3^*|y_4^*|y_5^*|y_6^*|y_7^*|y_8^*) \\ R_0^* &= (\alpha_1|x_2^*|x_3^*|x_4^*|\alpha_5|\alpha_6|x_7^*|x_8^*) \end{aligned}$$

Compute (L_1, R_1) and (L_1^*, R_1^*), choose pairs whose difference satisfy $R_1 \oplus R_1^* = (0|0|0|0|0|h|0|0)$ where h is not zero. Since the probability is about 2^{-56}, the expected number of the remaining pairs is $2^{104} \times 2^{-56} = 2^{48}$.

Step 6 Guess the 64-bit subkey $K_2^{(1)}$ and 5 subkey bytes $K_{2,1}^{(2)}$, $K_{10,2}^{(2)}$, $K_{10,3}^{(2)}$, $K_{10,4}^{(2)}$, $K_{10,8}^{(2)}$, perform the following:

Step 6.1 For every remaining pair (L_0, R_0) and (L_0^*, R_0^*), and the corresponding output of the first round (L_1, R_1) and (L_1^*, R_1^*), guess $K_2^{(1)}$ and compute:

$$\begin{aligned} Z_2 &= PS(R_1 \oplus K_2^{(1)}), \\ Z_2^* &= PS(R_1^* \oplus K_2^{(1)}). \end{aligned}$$

Step 6.2 Guess the 5 bytes of $K_2^{(2)}$ and compute

$$\begin{aligned} q_1 &= s(Z_{2,1} \oplus K_{2,1}^{(2)}) \oplus s(Z_{2,1}^* \oplus K_{2,1}^{(2)}) \oplus R_{1,8} \oplus R_{1,8}^*, \\ q_2 &= s(Z_{2,2} \oplus K_{2,2}^{(2)}) \oplus s(Z_{2,2}^* \oplus K_{2,2}^{(2)}) \oplus R_{1,1} \oplus R_{1,1}^*, \\ q_3 &= s(Z_{2,4} \oplus K_{2,4}^{(2)}) \oplus s(Z_{2,4}^* \oplus K_{2,4}^{(2)}) \oplus R_{1,2} \oplus R_{1,2}^*, \\ q_4 &= s(Z_{2,5} \oplus K_{2,5}^{(2)}) \oplus s(Z_{2,5}^* \oplus K_{2,5}^{(2)}) \oplus R_{1,3} \oplus R_{1,3}^*, \\ q_5 &= s(Z_{2,6} \oplus K_{2,6}^{(2)}) \oplus s(Z_{2,6}^* \oplus K_{2,6}^{(2)}) \oplus R_{1,4} \oplus R_{1,4}^*. \end{aligned}$$

Then check whether $q_i = 0 (5 \leq i \leq 1)$. If yes, discard the candidate value of $(K_1^{(1)}, K_1^{(2)}, K_2^{(1)}, K_{2,i}^{(2)}, K_9^{(1)}, K_{9,i}^{(2)})(i = 1, 2, 4, 5, 6)$.

Since such a difference is impossible, every key that proposes such a difference is a wrong key. After analyzing 2^{48} ciphertexts pairs, there remain only about $2^{336}(1 - 2^{-40})^{2^{48}}$ wrong candidate value of $(K_1^{(1)}, K_1^{(2)}, K_2^{(1)}, K_{2,i}^{(2)}, K_9^{(1)}, K_{9,i}^{(2)})(i = 1, 2, 4, 5, 6)$, which is much less than 1.

The time complexity of Step 4.1 requires about $2^{144} \times 2^{64} \times 2 = 2^{209}$ one round operations. The precalculation can decrease the complexity of Step 4.2, one can look up the table $T(Z_{9,k} \oplus Z_{9,k}^*, R_{9,i} \oplus R_{9,j})$ to judge whether the $q_i s$ are zero or not. This Step needs about $2^{144} \times 2^{64} \times 5 \approx 2^{210}$ table lookups. Step 5 has a time complexity of about $2^{104} \times 2^{128} \times 2 = 2^{233}$ one round operations. Step 6 needs $2^{48} \times 2^{64} \times 2 = 2^{113}$ one round operations and $2^{48} \times 2^{64} \times 5 \approx 2^{114}$ table lookups respectively.

Consequently, this attack requires about 2^{121} chosen plaintexts and less than 2^{230} encryptions of 9-round E2 and 2^{210} table lookups.

5 Conclusion

The block cipher E2 was proposed as an AES candidate. It employs a Feistel structure and a 2-layer SPN structure in round function. In this paper we describe some 6-round impossible differentials of E2, and present a 9-round attack on E2 without IT/FT when used with 256 key bits. Cryptanalysis given in this paper is the first security evaluation of E2 against impossible differential cryptanalysis.

References

[1] L. Knudsen. DEAL — A 128-bit Block Cipher. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, Feb. 1998.

[2] E. Biham, A. Biryukov, A. Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. EuroCrypt'1999, LNCS 1592, pp. 12–23. Springer–Verlag, 1999.

[3] W. Wu, W. Zhang, D. Feng. Impossible Differential Cryptanalysis of Reduced-

Round ARIA and Camellia. Journal of Computer Science and Technology 22(3), 449–456(2007).

[4] W. Wu, L. Zhang and W. Zhang. Improved Impossible Differential Cryptanalysis of Reduced–Round Camellia. SAC 2008, LNCS, pp., Springer–Verlag, 2009.

[5] J. Lu, J. Kim, N. Keller, and O. Dunkelman. Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. CT-RSA 2008, LNCS 4964, pp. 370-386. Springer–verlag, 2008.

[6] J. Lu, O. Dunkelman N. Keller and J. Kim. New Impossible Differential Attacks on AES. IndoCrypt 2008, LNCS 5365, pp. 279–293, Springer–Verlag, 2008.

[7] O. Dunkelman, N. Keller. An Improved Impossible Differential Attack on MISTY1. ASIACRYPT 2008, LNCS 5350, pp. 441–454, Springer–Verlag, 2008.

[8] H. Mala, M. Shakiba, M. Dakhilalian, G. Bagherikaram. New Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia-128. SAC 2009, LNCS 5867, pp. 281–294. Springer–Verlag, 2009.

[9] W. Zhang, J. Han Impossible Differential Analysis of Reduced Round CLEFIA. Inscrypt 2008, LNCS 5487, pp. 181–191, Springer–Verlag, 2009.

[10] J. Kim, S. Hong, J. Sung, S. Lee and J. Kim. Impossible differential cryptanalysis for block cipher structures, INDOCRYPT 2003, LNCS 2904, pp. 82–96. Springer–Verlag, 2003.

[11] NTT-Nippon Telegraph and Telephone Corporation: E2 : Efficient Encryption Algorithm. http://info.isl.ntt.co.jp/e2.

[12] M. Matsui, T. Tokita. Cryptanalysis of a Reduced Version of the Block Cipher E2. FSE 1999, LNCS 1636, pp. 71–80. Springer–Verlag, 1999.

[13] S. Moriai, M. Sugita, K. Aoki, M. Kanda. Security of E2 against Truncated Differential Cryptanalysis. SAC 1999, LNCS 1758, pp. 106–117. Springer–Verlag, 2000.

[14] K. Aoki, M. Kanda. Search for Impossible Differential of E2. http://csrc. nist. gov/encryption/aes/round1/comment.

[15] M. Sugita, K. Kobara, H. Imai, Pseudorandomness and Maximum Average of Differential Probability of Block Ciphers with SPN-Structures like E2. Proceedings of the second Advanced Encryption Standard candidate conference, pp. 200–214, 1999.

[16] M. Sugita. Security of Block Ciphers with SPN-Structures. Technical Report of IEICE. ISEC98-30.

[17] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Ohta. A Strategy for Constructing Fast Round Functions with Practical Security Against Differential and Linear Cryptanalysis. SAC 1998, LNCS 1556, pp. 264–279. Springer–Verlag, 1999.