Security of E2 against Truncated Differential Cryptanalysis

Shiho Moriai, Makoto Sugita, Kazumaro Aoki, and Masayuki Kanda

NTT Laboratories
1-1 Hikarinooka, Yokosuka, 239-0847, Japan
shiho@isl.ntt.co.jp,sugita@pcs.wslab.ntt.co.jp
maro@isl.ntt.co.jp,kanda@sucaba.isl.ntt.co.jp

Abstract. This paper studies the security offered by the block cipher E2 against truncated differential cryptanalysis. At FSE'99 Matsui and Tokita showed a possible attack on an 8-round variant of E2 without IT-Function (the initial transformation) and FT-Function (the final transformation) based on byte characteristics. To evaluate the security against attacks using truncated differentials, which mean bytewise differentials in this paper, we searched for all truncated differentials that lead to possible attacks for reduced-round variants of E2. As a result, we confirmed that there exist no such truncated differentials for E2 with more than 8 rounds. However, we found another 7-round truncated differential which lead to another possible attack on an 8-round variant of E2 without IT- or FT-Function *with less complexity*. We also found that the 7-round truncated differential is useful to distinguish a 7-round variant of E2 *with* IT- and FT-Functions from a random permutation. In spite of our severe examination, this type of cryptanalysis fails to break the full E2. We believe that this means that the full E2 offers strong security against this truncated differential cryptanalysis.

1 Introduction

The attacks using truncated differentials were introduced by Knudsen [K95]. It deals with truncated differentials, i.e. differentials where only a part of the difference can be predicted. Although the notion of truncated differentials he introduced is wide, with a byte-oriented cipher it is natural to study bytewise differentials as truncated differentials. The truncated differential can partly deal with the so called multiple-path for a Markov cipher [LMM91], which is a set of differential characteristics with the same input difference pattern and the same output difference pattern, hence the maximum probability of *truncated differential* can be higher than that of differential characteristics. Moreover, the truncated differentials can allow the attackers more freedom in choosing plaintexts or ciphertexts. Therefore, studying the security against truncated differential cryptanalysis can provide a more strict evaluation of the security against differential cryptanalysis.

A truncated differential cryptanalysis of reduced-round variants of E2 was presented by Matsui and Tokita at FSE'99 [MT99]. Their analysis was based on

Howard Heys and Carlisle Adams (Eds.): SAC'99, LNCS 1758, pp. 106–117, 2000.

the "byte characteristic," where the values to the difference in a byte are distinguished between non-zero and zero. They found a 7-round byte characteristic, which leads to a possible attack on an 8-round variant of E2 without IT-Function (the initial transformation) and FT-Function (the final transformation).

This paper studies the security of E2 against this type of cryptanalysis. We show an algorithm which searches for all effective truncated differentials that lead to possible attacks of Feistel ciphers, which Matsui et al. didn't go into details about in [MT99]. Here "effective" means that the probability of the truncated differential for the cipher is higher than the probability of the truncated differential for a random permutation. To run the algorithm above, we have to compute all non-zero probabilities of truncated differentials of the round function. Since the round function of E2 has the SPN (Substitution Permutation Network) structure, we made use of the method for computing the maximum average of differential probability of general SPN structures shown by Sugita et al. [SKI99].

As a result, we found another 7-round truncated differential, which leads to a possible attack on an 8-round variant of E2 without IT- *or* FT-Function *with less complexity* than that offered by Matsui et al. Moreover, this truncated differential was also useful in distinguishing a 7-round variant of E2 *with* IT- and FT-Functions from a random function. However, no flaw by the cryptanalysis above was discovered for the full 12-round E2, i.e. E2 in the specification submitted to NIST as an AES candidate [E2].

The contents of this paper are as follows. First, in Section 2, we describe an algorithm to compute the probabilities for all truncated differentials of the round function with the SPN structure. Second, we show a search algorithm for the truncated differentials of E2 in Section 3. This algorithm is applicable to other ciphers with the Feistel structure. Section 4 describes possible scenarios of attacks on reduced-round variants of E2 using the truncated differentials found in Section 3 and estimates the required complexity for attacking.

2 Truncated Differentials of Round Function

First, we show examples of the transition rules between the input and output bytewise differences of the round function of E2 and define the truncated differential used in this paper. Throughout this paper we follow the notations used in the specification of E2 [E2] (see also Figure 1). The linear transformation in the round function (P-Function) is represented as follows.

$$^{\mathrm{t}}(z'_1, z'_2, \ldots, z'_8) = P\ ^{\mathrm{t}}(z_1, z_2, \ldots, z_8)$$

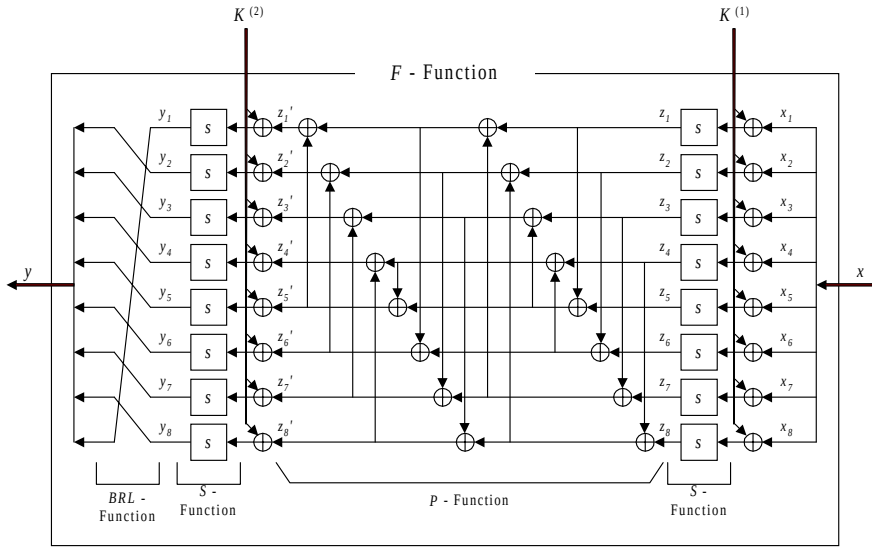

Fig. 1. The round function of E2

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{1}$$

Let $x = (x_1, x_2, \ldots, x_8)$, $y = (y_2, \ldots, y_8, y_1)$, and $z = (z_1, z_2, \ldots, z_8)$ be the input of the round function, the output of the round function, and the input of P-Function, respectively, and let $\Delta x \in (\mathrm{GF}(2)^8)^8$, $\Delta y \in (\mathrm{GF}(2)^8)^8$, and $\Delta z \in (\mathrm{GF}(2)^8)^8$ be the differences of x, y, and z, respectively.

$$\begin{array}{lll} \Delta x = (\Delta x_1, \Delta x_2, \ldots, \Delta x_8), & \Delta x_i \in \mathrm{GF}(2)^8 & \\ \Delta y = (\Delta y_2, \ldots, \Delta y_8, \Delta y_1), & \Delta y_i \in \mathrm{GF}(2)^8 & (i = 1, 2, \ldots, 8) \\ \Delta z = (\Delta z_1, \Delta z_2, \ldots, \Delta z_8), & \Delta z_i \in \mathrm{GF}(2)^8 & \end{array}$$

For example, when two bytes of the input x_1 and x_5 are changed, if $\Delta z_1 = \Delta z_5$, then three bytes of the output y_2, y_6, and y_1 are changed. Otherwise (i.e., if $\Delta z_1 \neq \Delta z_5$) all bytes except y_7 are changed. Assuming that the input values $x_1, x_2, \ldots, x_8$ and the input differences Δx_1 and Δx_5 are given randomly (while

the other Δx_i's are fixed to 0 ($i \neq 1, 5$)), the former event ($\Delta z_1 = \Delta z_5$) occurs with approximate probability 2^{-8} (though the exact value is $\frac{1}{255}$), and the latter event ($\Delta z_1 \neq \Delta z_5$) occurs with approximate probability $1 - 2^{-8}$. We describe the transition rules above between the input and output bytewise differences as follows.

$$(10001000) \rightarrow (10001001) \quad p \approx 2^{-8}$$
$$(10001000) \rightarrow (11111011) \quad p \approx 1 - 2^{-8}$$

The transition rules above are generalized to the transition rules between the input and output t-bitwise differences for a function with $m \times t$ bits input and output. We call these transition rules the truncated differentials of a function $f : (\mathrm{GF}(2)^t)^m \mapsto (\mathrm{GF}(2)^t)^m$. Formally, we define them as follows.

Definition 1 ($\boldsymbol{\chi}$-Function). *Let χ be the function $\mathrm{GF}(2)^t \rightarrow \mathrm{GF}(2)$ defined as follows.*

$$\chi(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}$$

Let $\boldsymbol{\chi}(x_1, x_2, \ldots, x_m) = (\chi(x_1), \chi(x_2), \ldots, \chi(x_m))$.

Definition 2 (Truncated Differential). *Let δx, $\delta y \in \mathrm{GF}(2)^m$ denote the input differential and output differential of the truncated differential of the function f, respectively.*

$$\delta x = (\delta x_1, \delta x_2, \ldots, \delta x_m), \quad \delta x_i \in \mathrm{GF}(2) \qquad (i = 1, 2, \ldots, m)$$
$$\delta y = (\delta y_1, \delta y_2, \ldots, \delta y_m), \quad \delta y_i \in \mathrm{GF}(2)$$

where $\delta x_i = \chi(\Delta x_i)$ and $\delta y_i = \chi(\Delta y_i)$.
Let $p_f(\delta x, \delta y)$ denote the probability of the truncated differential of the function f. $p_f(\delta x, \delta y)$ is defined by

$$p_f(\delta x, \delta y) = \max_{\substack{\Delta x \neq 0 \\ \boldsymbol{\chi}(\Delta x) = \delta x}} \Pr_{x \in (\mathrm{GF}(2)^t)^m} [\, \boldsymbol{\chi}(f(x) \oplus f(x \oplus \Delta x)) = \delta y \,] \qquad (2)$$

We define the pair of δx and δy as the truncated differential of the function f and represent it as follows:

$$\delta x \rightarrow \delta y \quad \text{with probability } p_f(\delta x, \delta y).$$

To search exhaustively for the effective truncated differentials of the whole cipher, we need to derive all possible truncated differentials of the round function with non-zero probability. Sugita [SKI99] showed a method for calculating the maximum average of differential probability of the SPN structure, assuming that the differential probability of the s-boxes is uniformly distributed for any nonzero

input difference and any nonzero output difference*. According to [SKI99, Section 5], we can calculate efficiently the probabilities of the truncated differentials of the round function of E2, $p_F(\delta x, \delta y)$, for every $\delta x, \delta y \in \mathrm{GF}(2)^8$. We begin by introducing the following semi-order $\preceq$ in $\mathrm{GF}(2)^m$.

Definition 3 (Semi-order). *For every $\delta x, \delta y \in \mathrm{GF}(2)^m$, we define the semi-order $\preceq$ in $\mathrm{GF}(2)^m$ as follows.*

$$\delta x \preceq \delta y \quad \stackrel{\mathrm{def}}{\Longleftrightarrow} \quad {}^{\forall} i \ (1 \le i \le m); \quad \delta y_i = 0 \ \Rightarrow \ \delta x_i = 0,$$

where $\delta x = (\delta x_1, \delta x_2, \ldots, \delta x_m)$ and $\delta y = (\delta y_1, \delta y_2, \ldots, \delta y_m)$.

Algorithm 1 (Calculation of the Probabilities of Truncated Differentials of the Round Function of E2).

1. For every $\delta z, \delta z' \in \mathrm{GF}(2)^8$, we define $\mathrm{M}(\delta z, \delta z')$ for P-Function as follows.

$$\begin{aligned}&\mathrm{M}(\delta z, \delta z')\\ &= \#\{(\Delta z, \Delta z') \in ((\mathrm{GF}(2)^8)^8 \setminus \{\mathbf{0}\})^2 \mid \Delta z' = P\Delta z, \boldsymbol{\chi}(\Delta z) \preceq \delta z, \boldsymbol{\chi}(\Delta z') \preceq \delta z'\},\end{aligned}$$

$$\begin{aligned}\text{where } \delta z = (\delta z_1, \delta z_2, \ldots, \delta z_8), \quad & \delta z_i = \chi(\Delta z_i)\\ \delta z' = (\delta z'_1, \delta z'_2, \ldots, \delta z'_8), \quad & \delta z'_i = \chi(\Delta z'_i)\end{aligned}$$

   $\mathrm{M}(\delta z, \delta z')$ can be easily calculated by a simple rank calculation as follows.

$$\mathrm{M}(\delta z, \delta z') = 2^{8(16-\mathrm{rank}\begin{pmatrix} P & E \\ \mathcal{F}(\overline{\delta z}, \overline{\delta z}') & \end{pmatrix})} - 1,$$

   where $\overline{\delta z}$ and $\overline{\delta z}'$ are the complements of δz and $\delta z'$, respectively. P denotes the matrix represented by Equation (1), E denotes the 8×8 identity matrix, and $\mathcal{F}(\overline{\delta z}, \overline{\delta z}')$ denotes the 16×16 diagonal matrix whose (i, i) component equals $\overline{\delta z}_i$ for $i = 1, \cdots, 8$, and $\overline{\delta z}'_{i-8}$ for $i = 9, \cdots, 16$.

2. For every $\delta z, \delta z' \in \mathrm{GF}(2)^8$, we define $\mathrm{N}(\delta z, \delta z')$ for P-Function as follows.

$$\begin{aligned}&\mathrm{N}(\delta z, \delta z')\\ &= \#\{(\Delta z, \Delta z') \in ((\mathrm{GF}(2)^8)^8 \setminus \{\mathbf{0}\})^2 \mid \Delta z' = P\Delta z, \boldsymbol{\chi}(\Delta z) = \delta z, \boldsymbol{\chi}(\Delta z') = \delta z'\}\end{aligned}$$

   $\mathrm{N}(\delta z, \delta z')$ can be calculated recursively, using the following relation [SKI99].

$$\mathrm{N}(\delta z, \delta z') = \mathrm{M}(\delta z, \delta z') - \sum_{(\widetilde{\delta z}, \widetilde{\delta z}') \prec (\delta z, \delta z')} \mathrm{N}(\widetilde{\delta z}, \widetilde{\delta z}') \qquad (3)$$

* Strictly speaking, let $n_s(\Delta x, \Delta y) = \#\{x | s(x) \oplus s(x \oplus \Delta x) = \Delta y\}$ and the following is assumed:

$$n_s = \begin{cases} \frac{1}{2^t - 1} & \text{if } \Delta x \Delta y \neq 0 \\ 1 & \text{if } \Delta x = \Delta y = 0 \\ 0 & \text{otherwise.} \end{cases}$$

3. For every $\delta x, \delta y \in \mathrm{GF}(2)^8$, calculate the probability of truncated differential of the round function $p_F(\delta x, \delta y)$ according to the following relations [SKI99].

$$p_F(\delta x, \delta y) = \sum_{\delta z} \mathrm{N}(\delta z, \delta z') q^{w_{\mathrm{H}}(\delta y)} p_S(\delta x, \delta z) \tag{4}$$

$$p_S(\delta x, \delta z) = \max_{\substack{\Delta x \neq 0 \\ \boldsymbol{\chi}(\Delta x) = \delta x}} \Pr_{x \in (\mathrm{GF}(2)^8)^8} [\, \boldsymbol{\chi}(S(x) \oplus S(x \oplus \Delta x)) = \delta z \,] \tag{5}$$

where $w_{\mathrm{H}}(\delta y)$ denotes the Hamming weight of δy and q is the maximum average of the differential probability of s-box. We have $q = 1/(2^8 - 1)$ under the assumption that differential probability of the s-boxes is uniformly distributed for any nonzero input difference and any nonzero output difference.

3 The Search for Truncated Differentials of E2

In this section we search for all truncated differentials that lead to possible attacks on (reduced-round variants of) E2. Below we show a search algorithm for all "effective" truncated differentials of a Feistel cipher with R rounds and blocksize $2mt$ bits. In this paper, "effective" means that the truncated differential could lead to possible attacks, in other words, the probability of the truncated differential is equal or higher than the probability with which the truncated differential holds for a random permutation[**].

This search algorithm consists of recursive procedures. Note that the search algorithm is the depth first search rather than the breadth first search considering the required memory. The "depth" corresponds to the number of rounds of the Feistel cipher.

Algorithm 2 (Search for all Effective Truncated Differentials of Feistel Cipher with R Rounds and Blocksize $2mt$ Bits)

Let $X^{(r)}, Y^{(r)} \in \mathrm{GF}(2)^m$ be the input and output differences of the truncated differential of the r-th round function. Thus $(X^{(0)}, X^{(1)})$ is the truncated differential of the plaintext. Let $\mathcal{P}_r$ be the variable which holds the probability of the r-round truncated differential. $\mathcal{P}_0$ should be initialized to be 1, *i.e.*, $\mathcal{P}_0 := 1$.

1. Calculate all the probabilities of the truncated differentials of the round function $p_F(\delta x, \delta y)$. They should be sorted in order of the probability of truncated differentials for each input difference.
2. For all truncated differential of the plaintext, (*i.e.*, $^{\forall} X^{(0)} \in \mathrm{GF}(2)^m$ and $^{\forall} X^{(1)} \in \mathrm{GF}(2)^m$) call the procedure [The 1st round], i.e., the procedure [The r-th round] for $r = 1$. After finishing the procedure [The 1st round] for all $X^{(0)}$ and $X^{(1)}$, exit the program.

[**] Although there is a claimed attack on the first 16 rounds of Skipjack using the truncated differential with smaller probability than a random permutation [KRW99], we are not concerned here with this case.

3. [The r-th round] For each $X^{(r)}$, set the output truncated differential of the round function $Y^{(r)} \in \mathrm{GF}(2)^m$ in order of the probability of the truncated differential.
   - Let $p_r := p_F(X^{(r)}, Y^{(r)})$.
   - If $\mathcal{P}_{r-1} \times p_r < 2^{-2mt}$, then try another $X^{(r)}$.
   - Call the procedure [The r-th Xor].

   If $r \neq 1$, return to the procedure [The $(r-1)$-st Xor], otherwise (*i.e.*, $r = 1$), return to Step 2.

4. [The r-th Xor] At the XOR operation of the r-th round in the Feistel cipher, $X^{(r+1)}$ is derived from $X^{(r-1)}$ and $Y^{(r)}$. Here the difference may be canceled out: $1 \oplus 1 = 0$ with probability $\frac{1}{255} (\approx 2^{-t})$, while $1 \oplus 1 = 1$ with probability $\frac{254}{255}$, assuming that the difference is independent and uniformly distributed. When the cancelation occurs c times, the probability is approximately $(2^{-t})^c$. The number of all possible values of $X^{(r+1)}$ is $2^{w_{\mathrm{H}}(X^{(r-1)} \wedge Y^{(r)})}$. For each $X^{(r+1)}$, call the following procedure.
   - Let $\mathcal{P}_r := \mathcal{P}_{r-1} \times p_r \times (2^{-t})^c$, where $c = w_{\mathrm{H}}(X^{(r-1)} \vee Y^{(r)}) - w_{\mathrm{H}}(X^{(r+1)})$.
   - If $\mathcal{P}_r < 2^{-2mt}$, then try another $X^{(r+1)}$.
   - If $\mathcal{P}_r$ is lower than the probability for a random function, i.e., if $\mathcal{P}_r < 2^{t \times (w_{\mathrm{H}}(X^{(r)}) + w_{\mathrm{H}}(X^{(r+1)})) - 2mt}$, then try another $X^{(r+1)}$.
   - If $r < R$, call the procedure [The $(r+1)$-st round], else print the truncated differential:

     $$(X^{(0)}, X^{(1)}) \to (X^{(R+1)}, X^{(R)}) \quad \text{with probability } \mathcal{P}_R.$$

   Return to the procedure [The $(r-1)$-st round].

At the procedure [The r-th Xor] of each round in the algorithm above, if the probability of the r-round truncated differential is lower than the probability with which the truncated differential holds for a random permutation, we don't have to continue the search for the truncated differential for longer rounds. This makes the search efficient by pruning off unnecessary candidates. This is because the following theorem holds for Feistel ciphers.

Theorem 1.

$$\mathcal{P}_r < 2^{t(w_{\mathrm{H}}(X^{(r)}) + w_{\mathrm{H}}(X^{(r+1)})) - 2mt} \tag{6}$$

$$\Longrightarrow \ \mathcal{P}_{r+1} < 2^{t(w_{\mathrm{H}}(X^{(r+1)}) + w_{\mathrm{H}}(X^{(r+2)})) - 2mt} \tag{7}$$

Proof) We have

$$\mathcal{P}_{r+1} = \mathcal{P}_r \times p_{r+1} \times (2^{-t})^c.$$

From Equation (6) and since $c = w_{\mathrm{H}}(X^{(r)} \vee Y^{(r+1)}) - w_{\mathrm{H}}(X^{(r+2)})$ *holds, where* c *is the number of times when the cancelation happens in the procedure* [THE $r+1$-TH XOR]*, we have*

$$\begin{aligned}\mathcal{P}_{r+1} &< 2^{t(w_{\mathrm{H}}(X^{(r)})+w_{\mathrm{H}}(X^{(r+1)}))-2mt} \times p_{r+1} \times 2^{-t(w_{\mathrm{H}}(X^{(r)} \vee Y^{(r+1)})-w_{\mathrm{H}}(X^{(r+2)}))} \\ &= 2^{t(w_{\mathrm{H}}(X^{(r+1)})+w_{\mathrm{H}}(X^{(r+2)}))-2mt} \times p_{r+1} \times 2^{t(w_{\mathrm{H}}(X^{(r)})-(w_{\mathrm{H}}(X^{(r)} \vee Y^{(r+1)})))}\end{aligned}$$

We have $p_{r+1} \leq 1$ *and* $2^{t(w_{\mathrm{H}}(X^{(r)})-(w_{\mathrm{H}}(X^{(r)} \vee Y^{(r+1)})))} \leq 1$*, since*

$$w_{\mathrm{H}}(X^{(r)}) - (w_{\mathrm{H}}(X^{(r)} \vee Y^{(r+1)})) \leq 0$$

holds. Therefore,

$$\mathcal{P}_{r+1} < 2^{t(w_{\mathrm{H}}(X^{(r)})+w_{\mathrm{H}}(X^{(r+1)}))-2mt}$$

holds. The proof is complete.

4 Attacks on Reduced-Round Variants of E2

Using Algorithm 2 we searched for all truncated differentials that lead to possible attacks for reduced-round variants of E2. As a result, we confirmed that there exist no such truncated differentials for E2 with more than 7 rounds. The best*** 7-round truncated differential that leads to possible attacks on reduced-round variants of E2 is shown in Figure 2. This 7-round truncated differential holds with probability of about 2^{-104}†; for a random round function the probability of the truncated differential is expected to be $(2^{-8})^{14} = 2^{-112}$, which is significantly smaller. Therefore, this truncated differential is useful to derive subkey information of the last round and to distinguish from a random permutation.

Moreover, this 7-round truncated differential is connected with the truncated differentials of IT- and FT-Functions with probability about 1. In IT- and FT-Functions, 32-bit multiplications with subkeys are used. Since this multiplication is modulo 2^{32} (roughly speaking, the upper 32-bit of the resultant 64-bit is discarded), this multiplication has the following trivial truncated differential as shown in [MT99].

$$(1000) \rightarrow (1000) \qquad p \approx 1$$

*** Here the "best" means that the ratio of the probability of the truncated differential to the probability for a random permutation is the highest.

† The more strict probability we computed was $248q^{14}+18q^{15}+39q^{16}+157q^{17}+22q^{18}+62q^{19}+225q^{20}+158q^{21}+172q^{22}+191q^{23}+205q^{24}+202q^{25}+189q^{26}+194q^{27}+246q^{28}+137q^{29}+10q^{30}+93q^{31}+37q^{32}+173q^{33}+9q^{34}+162q^{35}+74q^{36}+95q^{37}+156q^{38}+28q^{39}+\cdots$, while the probability of the best known truncated differential [MT99] was computed as $q^{14}+231q^{15}+168q^{16}+135q^{17}+115q^{18}+157q^{19}+163q^{20}+217q^{21}+90q^{22}+208q^{23}+59q^{24}+91q^{25}+80q^{26}+158q^{27}+41q^{28}+130q^{29}+250q^{30}+227q^{31}+102q^{32}+118q^{33}+40q^{34}+246q^{35}+13q^{36}+146q^{37}+98q^{38}+153q^{39}+8q^{40}+\cdots$, where q is the maximum average of the differential probability of s-box. Under our assumption $q = 1/(2^8-1)$ for any nonzero input difference and any nonzero output difference of s-box.

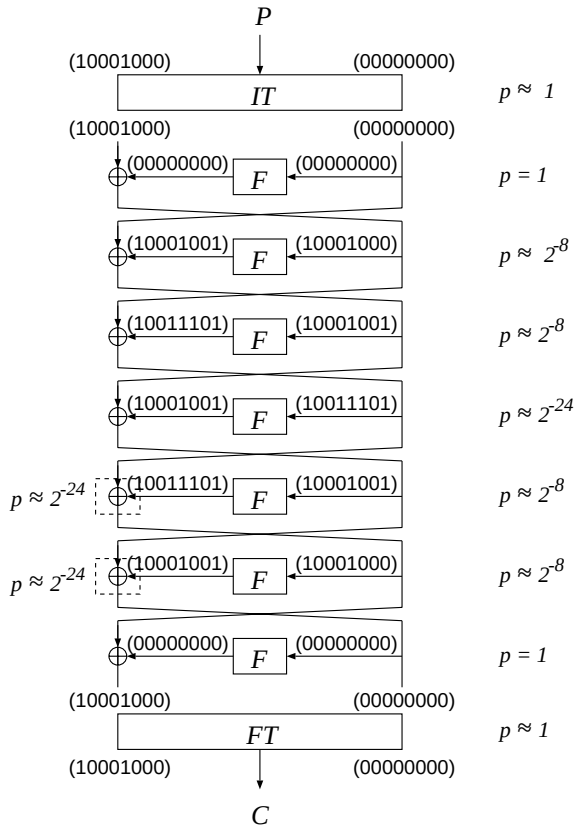

Fig. 2. The best 7-round truncated differential of E2

Hence the 7-round truncated differential shown in Figure 2 can skip IT- and FT-Functions with probability about 1. Additionally, the positions of the bytes which have a non-zero difference are not changed by BP-Function (or BP^{-1}-Function) in IT-Function (or FT-Function). It follows that we have the following truncated differential connecting the plaintext and ciphertext for a 7-round variant of E2.

$$(10001000\ 00000000) \rightarrow (10001000\ 00000000) \qquad p \approx 2^{-104}$$

4.1 E2 Reduced to 8 Rounds without *IT*- or *FT*-Function

We show a possible scenario of an attack of E2 reduced to 8 rounds without IT- or FT-Function. Below we show an attack to derive the last round key (the round key the 8-th round) without FT-Function.

Prepare the chosen plaintexts with the difference pattern (10001000 00000000) and guess the last round keys and get the output of the 7-th round using the ci-

phertexts. According to [MT99, Section 5, Lemma 1], when we have 2^{109} chosen plaintext pairs, if the number of pairs whose output differences follow the difference pattern (10001000 00000000) is more than 20, we can judge the guessed key is right and otherwise we can judge the guessed key is wrong. For a correct key the probability that the number of pairs whose output differences follow the difference pattern (10001000 00000000) is more than 20 is 99%, while the probability is 2^{-121} for a wrong key.

The required 2^{109} chosen plaintext pairs can be generated from 2^{94} chosen plaintext blocks ($94 = 109 - 16 + 1$). The attack on an 8-round variant of E2 without IT- and FT-Functions shown in [MT99] required 2^{100} chosen plaintext blocks. Moreover, we do not have to choose special plaintexts [MT99, Section 5.2] since the probability that correct pairs are detected is much larger than the probability that wrong pairs appear.

Note that the complexity of the procedure above for deriving the last round keys (128 bits) exceeds the complexity of exhaustive search $O(2^{128})$. We've not confirmed whether an improved attack with complexity less than $O(2^{128})$ is possible.

4.2 E2 Reduced to 7 Rounds with *IT*- and *FT*-Function

The 7-round truncated differential shown in Figure 2 is also useful to distinguish the 7-round variant of E2 with IT- and FT-Functions from a random permutation.

Prepare the chosen plaintexts with the difference pattern (10001000 00000000) and observe the differences of the ciphertexts. According to Matsui et al.'s theory, when we have 2^{106} chosen plaintext pairs, if at least one pair follows the difference pattern (10001000 00000000), we can regard it as the 7-round variant of E2 with IT- and FT-Functions, otherwise we regard it as a random permutation. The probability that the number of pairs whose output differences follow the difference pattern (10001000 00000000) is more than 1 is 98%, while the probability is 2% for a random permutation. The required 2^{106} chosen plaintext pairs can be generated from 2^{91} plaintext blocks ($91 = 106 - 16 + 1$).

5 Conclusion

This paper introduced search algorithms for finding effective truncated differentials useful in truncated differential cryptanalysis. Applying to E2, we found an attack on an 8-round variant of E2 without IT- or FT-Function requiring 2^{94} chosen plaintexts, which is fewer than that required by the best known attack. We also found that it is possible to distinguish a 7-round variant of E2 *with* IT- and FT-Functions from a random function using 2^{91} chosen plaintexts.

In spite of our severe examination, this type of cryptanalysis fails to break the full E2. We believe that this means that the full E2 offers strong security against truncated differential cryptanalysis.

Table 1. Attacks on reduced-round variants of E2

Attack 1: Extract the last round key information

Matsui et al.'s result	8-round E2 without IT and FT 2^{100} chosen plaintexts
Our result	8-round E2 without IT or FT 2^{94} chosen plaintexts

Note) The attack complexities may be above $O(2^{128})$.

Attack 2: Distinguish from a random permutation

Matsui et al.'s result	7-round E2 without IT and FT 2^{97} chosen plaintexts
Our result	7-round E2 with IT and FT 2^{91} chosen plaintexts

Appendix: Truncated Differentials of Rijndael

We also searched for truncated differentials of Rijndael [DR98] under the similar condition that the differential probability of the S-boxes is uniformly distributed for any nonzero input difference and any nonzero output difference. In [DR98] the designers stated that, for 6 rounds or more, no attacks faster than exhaustive key search have been found. For differential characteristics of Rijndael, they stated that it can be proven that there are no 4-round differential trails with a predicted prop ratio (probability) above 2^{-150}.

As the result of our search, there existed no truncated differentials for Rijndael with more than 4 rounds that has higher probability than a randomly chosen permutation. There existed 218,700,000 4-round truncated differentials that has the same probability as a randomly chosen permutation. For differentials of Rijndael, we found a 5-round differential with probability 1.06×2^{-128}, and there existed no differentials for Rijndael with more than 5 rounds that have higher probability than $\frac{1}{2^{128}-1}$.

References

DR98. J.Daemen and V.Rijmen, "The Rijndael Block Cipher," 1998, available at `http://www.esat.kuleuven.ac.be/~rijmen/rijndael/`.

K95. L.R.Knudsen, "Truncated and Higher Order Differentials," Fast Software Encryption — Second International Workshop, Lecture Notes in Computer Science 1008, pp.196–211, Springer-Verlag, 1995.

KRW99. L.R.Knudsen, M.J.B.Robshaw, and D.Wagner, "Truncated Differentials and Skipjack," Advances in Cryptology — CRYPTO'99, Lecture Notes in Computer Science 1666, pp.165–180, Springer-Verlag, 1999.

LMM91. X.Lai, J.L.Massey, and S.Murphy, "Markov Ciphers and Differential Cryptanalysis," Advances in Cryptology — EUROCRYPT'91, Lecture Notes in Computer Science 547, pp.17–38, Springer-Verlag, 1991.

MT99. M.Matsui and T.Tokita, "Cryptanalysis of a Reduced Version of the Block Cipher E2," in pre-proceedings of Fast Software Encryption'99, pp.70–79, 1999.

E2. Nippon Telegraph and Telephone Corporation, "Specification of E2 — a 128-bit Block Cipher," 1999, available at `http://info.isl.ntt.co.jp/e2/`.

SKI99. M.Sugita, K.Kobara, and H.Imai, "Pseudorandomness and Maximum Average of Differential Probability of Block Ciphers with SPN-Structures like E2," in proceedings of the second Advanced Encryption Standard candidate conference, pp.200–214, 1999.

V99. S.Vaudenay, "On the Security of CS-Cipher," in pre-proceedings of Fast Software Encryption'99, pp.259–274, 1999.