Differential Cryptanalysis and Impossible Differential Characteristics of Extended Feistel Networks

Huihui Yap

DSO National Laboratories
20 Science Park Drive, Singapore 118230
yhuihui@dso.org.sg

Abstract. Impossible differential cryptanalysis (IDC) is a variant of differential cryptanalysis (DC) against block ciphers whereby impossible differential characteristics are used to retrive a subkey material for the first or the last several rounds of block ciphers. Thus the security of a block cipher against IDC can be evaluated by impossible differential characteristics [1]. In this paper, we will first examine the security of Extended Feistel Networks (EFN) against DC and then use the U-method introduced in [1] to find impossible differential characteristics of EFN.

Key words: Differential Cryptanalysis, Extended Feistel Networks, Impossible Differential Characteristics

1 Introduction

Differential and linear cryptanalysis are the most common cryptanalyzing tools against block ciphers. However, provable security of block ciphers against differential and linear attacks may be insufficient because of their possible vulnerability to other types of cryptanalysis such as impossible differential cryptanalysis (IDC). This paper is organized as follows. Section 2 introduces three types of Extended Feistel Network (EFN) and states some known results regarding differential probability and IDC. Section 3 discusses the security of the these EFNs against differential cryptanalysis (DC). In Section 4, the U-method [1] is applied to the EFNs to find the maximum number of rounds for IDC.

2 Preliminaries

2.1 Notations

In this paper, we consider a round bijective function $F : GF(2)^m \rightarrow GF(2)^m$. We assume that round keys and input data are independent and uniformly random. Let $X = (X_1, \cdots X_n)$ and $Y = (Y_1, \cdots Y_n)$ be the input and output data block comprising n sub-blocks respectively, where $n \geq 4$. In addition, we use ΔX to denote a difference block.

With an input difference α and an output difference β, a differential is denoted by $\alpha \xrightarrow{F} \beta$ or simply just $\alpha \rightarrow \beta$ when the context is clear. On the other hand, we denote a r-round impossible differential characteristic by $\alpha \nrightarrow_r \beta$.

Finally, the "+" symbol is always taken to mean the $\oplus$ operator.

2.2 Extended Feistel Network

As introduced by [2], EFN are examples of Unbalanced Feistel Networks [4] whereby their sub-blocks are mixed through repeated application of keyed, non-linear F-functions. As in [2], we focus on three types of EFN, namely, EFN Type-I, EFN Type-II and EFN Type-III. EFN Type-I uses only one F-function in a round and the transformation can be described by

$$(Y_1, Y_2, \cdots, Y_{n-1}, Y_n) = (X_n, X_1, \cdots, X_{n-2}, X_{n-1} + F(X_n)).$$

For EFN Type-II, one F-function is used for every two consecutive sub-blocks. For $1 \leq i \leq n$, the transformation is defined by

$$Y_i = \begin{cases} X_n, & \text{if } i = 1, \\ X_{i-1}, & \text{if } i \neq 1 \text{ is odd}, \\ X_{i-1} + F(X_i), & \text{if } i \text{ is even}. \end{cases}$$

In this paper, we only consider EFN Type-II where n is even. For EFN Type-III, one F-function is used for every sub-block and is defined as follows:

$$(Y_1, Y_2, \cdots, Y_n) = (X_n, X_1 + F(X_2), \cdots, X_{n-1} + F(X_n)).$$

2.3 Differential Cryptanalysis

Definition 1. [3] For any $\Delta X, \Delta Y \in GF(2)^m$, the differential probability (average probability for all the possible keys) of a round function F is defined by

$$DP^F(\Delta X \rightarrow \Delta Y) = \frac{\#\{X \in GF(2)^m | F(X) + F(X + \Delta X) = \Delta Y\}}{2^m}.$$

Definition 2. The maximal differential probability of F is defined by

$$DP^F_{max} = \max_{\Delta X \neq 0, \Delta Y} DP^F(\Delta X \rightarrow \Delta Y).$$

Theorem 1. *[3] Let F_1 and F_2 be consecutive and relatively independent round functions from $GF(2)^m$ to $GF(2)^m$. For any $\Delta X, \Delta Z \in GF(2)^m$,*

$$DP^{F_1, F_2}(\Delta X \rightarrow \Delta Z) = \sum_{\Delta Y} DP^{F_1}(\Delta X \rightarrow \Delta Y) \cdot DP^{F_2}(\Delta Y \rightarrow \Delta Z).$$

Theorem 2. *[3] For any bijective function F,*

$$\sum_{\Delta X} DP^F(\Delta X \rightarrow \Delta Y) = 1.$$

Throughout the rest of this paper, we will use $DP(\Delta X \rightarrow \Delta Y)$ instead of $DP^F(\Delta X \rightarrow \Delta Y)$.

2.4 Impossible Differential Characteristics

In this section, we will follow the notations and terminology of [1].

Definition 3. [1] The $n \times n$ Encryption Characteristic Matrix $\mathbf{E} = (E_{ij})_{n\times n}$ and $n\times n$ Decryption Characteristic Matrix $\mathbf{D} = (D_{ij})_{n\times n}$ are defined as follows.

$$E_{i,j} = \begin{cases} 0, & \text{if } Y_j \text{ is not affected by } X_i, \\ 1, & \text{if } Y_j \text{ is affected by } X_i, \\ 1_F, & \text{if } Y_j \text{ is affected by } F(X_i). \end{cases}$$

$$D_{i,j} = \begin{cases} 0, & \text{if } X_j \text{ is not affected by } Y_i, \\ 1, & \text{if } X_j \text{ is affected by } Y_i, \\ 1_F, & \text{if } X_j \text{ is affected by } F(Y_i) \text{ or } F^{-1}(Y_i). \end{cases}$$

Definition 4. [1] A matrix is a **1-property matrix** if the number of entries 1 ($\neq 1_F$) in each column of the matrix is zero or one.

Definition 5. [1] Given an input difference $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, the **input difference vector a** $= (a_1, a_2, \ldots, a_n)$ corresponding to α is defined as follows.

$$a_i = \begin{cases} 0, & \text{if } \alpha_i = 0, \\ 1^*, & \text{otherwise.} \end{cases}$$

Given an input difference, the possible output differences of each subblock after r rounds are summarized in Table 1. According to Table 1, we are only able to deduce the differences to which 0, 1, 1^* and 2^* each does not correspond. Let $U = \{0, 1, 1^*, 2^*\}$ and define an auxillary set $\bar{m}$ such that $\bar{m}$ is a subset of U, and, the elements of $\bar{m}$ correspond to the differences which cannot be represented by the entry m. Then $\bar{0} = \{1, 1^*\}$, $\bar{1} = \{1, 1^*\}$, $\bar{1^*} = \{0, 1^*, 2^*\}$ and $\bar{2^*} = \{1^*\}$.

It can be checked that if $a_i^r = m$ and $b_i^{r^{'}} \in \bar{m}$, or, $a_i^r \in \bar{m}$ and $b_i^{r^{'}} = m$, then there exists $\alpha \not\twoheadrightarrow_{r+r'} \beta$, J. Kim et al. [1] call this method that uses the elements of U to find impossible differential characteristics as ***U*-method**. An algorithm (Algorithm 1) was presented in [1] to compute the maximum number of rounds for the impossible differential differential characteristics which can be found in the U-method.

3 Provable Security for EFN against DC

In this section, results regarding the differential probability of each type of EFN are presented. Let p be the maximal average differential probability of a round function. Also, for all the proofs in this section, let the input difference and output difference be $\alpha = (\alpha_1, \cdots, \alpha_n) \neq 0$ and $\beta = (\beta_1, \cdots, \beta_n) \neq 0$ respectively.

Theorem 3. *If $r = 2n-1$ and the round function of the EFN Type-I is bijective, then the r-round differential probabilities are bounded by p^2.*

Proof. Let the output differences of the round function in the first $(n-1)$ rounds be $\epsilon_1, \cdots, \epsilon_{n-1}$ respectively. Then from Theorem 1, we have the following:

$$\begin{aligned} DP(\alpha \to \beta) = & \sum_{\epsilon_i, 1 \le i \le n+1} DP(\alpha_n \to \epsilon_1) \cdot DP(\alpha_{n-1} + \epsilon_1 \to \epsilon_2) \cdots \\ & \cdot DP(\alpha_2 + \epsilon_{n-2} \to \epsilon_{n-1}) \cdot DP(\alpha_1 + \epsilon_{n-1} \to \alpha_n + \beta_{n-1}) \\ & \cdot DP(\beta_{n-1} \to \alpha_{n-1} + \beta_{n-2} + \epsilon_1) \cdots \cdot DP(\beta_2 \to \alpha_2 + \beta_1 + \epsilon_{n-2}) \\ & \cdot DP(\beta_1 \to \alpha_1 + \beta_n + \epsilon_{n-1}) \end{aligned}$$

We shall show that at least two of the input differences in the above equation are non-zero. With Theorem 2, this will imply that $DP(\alpha \to \beta) \le p^2$. Suppose for a contradiction that at most one of the input differences is non-zero. If all input differences to the F-functions are zero, then $\alpha_n = 0$, $\epsilon_i = 0$, and $\alpha_{n-i} + \epsilon_i = 0$ for all $i = 1, \cdots, n-1$, which will in turn imply that $\alpha_1 = \cdots = \alpha_{n-1} = 0$. This contradicts that $\alpha \ne 0$. Hence exactly one of the input differences is non-zero and we have the following cases.

1. Suppose that only $\alpha_n \ne 0$. Hence $\alpha_n + \beta_{n-1} = 0$ and $\beta_{n-1} = 0$. It follows that $\alpha_n = 0$ which is a contradiction.
2. Suppose that only $\alpha_{n-i} + \epsilon_i \ne 0$ for exactly one value of i where $i = 1, \cdots,$ or $n-2$. Then $\alpha_{n-i} + \beta_{n-i-1} + \epsilon_i = 0$ and $\beta_{n-i-1} = 0$. It follows that $\alpha_{n-i} + \epsilon_i = 0$, a contradiction.
3. Suppose that only $\alpha_1 + \epsilon_{n-1} \ne 0$. Then $\alpha_n + \beta_{n-1} \ne 0$. Also $\alpha_n = 0$ and $\beta_{n-1} = 0$. It follows that $\alpha_n + \beta_{n-1} = 0$, a contradiction.
4. Suppose that only $\beta_{n-1} \ne 0$. Also $\alpha_n = 0$ and $\alpha_n + \beta_{n-1} = 0$. It follows that $\beta_{n-1} = 0$, a contradiction.
5. Suppose that only $\beta_i \ne 0$ for exactly one value of i where $i = 1, \cdots$ or $n-2$. Also $\alpha_{i+1} + \beta_i + \epsilon_{n-i-1} = 0$ and $\alpha_{i+1} + \epsilon_{n-i-1} = 0$. This implies that $\beta_i = 0$, again a contradiction.

Therefore at least two of the input differences are non-zero and $DP(\alpha \to \beta) \le p^2$.

Theorem 4. *If $n = 2k$ and the round function of the EFN Type-II is bijective, then the 3-round differential probabilities are bounded by p^2.*

Proof. Let the output differences of the first k F-functions be $\epsilon_1, \cdots, \epsilon_k$ respectively. Then from Theorem 1,

$$\begin{aligned} DP(\alpha \to \beta) = & \sum_{\epsilon_i, 1 \le i \le k} DP(\alpha_2 \to \epsilon_1) \cdot DP(\alpha_4 \to \epsilon_2) \cdots \cdot DP(\alpha_{2k} \to \epsilon_k) \\ & \cdot DP(\alpha_1 + \epsilon_1 \to \alpha_{2k} + \beta_3) \cdot DP(\alpha_3 + \epsilon_2 \to \alpha_2 + \beta_5) \cdots \\ & \cdot DP(\alpha_{2k-3} + \epsilon_{k-1} \to \alpha_{2k-4} + \beta_{2k-1}) \\ & \cdot DP(\alpha_{2k-1} + \epsilon_k \to \alpha_{2k-2} + \beta_1) \\ & \cdot DP(\beta_3 \to \alpha_{2k-1} + \beta_2 + \epsilon_k) \\ & \cdot DP(\beta_5 \to \alpha_1 + \beta_4 + \epsilon_1) \cdot DP(\beta_7 \to \alpha_3 + \beta_6 + \epsilon_2) \cdots \\ & \cdot DP(\beta_{2k-1} \to \alpha_{2k-5} + \beta_{2k-2} + \epsilon_{k-2}) \\ & \cdot DP(\beta_1 \to \alpha_{2k-3} + \beta_{2k} + \epsilon_{k-1}) \end{aligned}$$

We shall show that at least two of the input differences in the above equation are non-zero. With Theorem 2, this will imply that $DP(\alpha \to \beta) \leq p^2$. Suppose for a contradiction that at most one of the input differences is non-zero. If all input differences are zero, then $\alpha_{2i} = 0$, $\epsilon_i = 0$ and $\alpha_{2i-1} + \epsilon_i = 0$ for all $1 \leq i \leq k$. This implies that $\alpha_{2i-1} = 0$ which contradicts that $\alpha \neq 0$. Hence exactly one of the input differences is non-zero and we have the following cases.

1. Suppose that only $\alpha_{2i} \neq 0$ for exactly one value of i where $i = 1, \cdots$, or $k-2$. Then $\alpha_{2i} + \beta_{2i+3} = 0$ and $\beta_{2i+3} = 0$. It follows that $\alpha_{2i} = 0$, a contradiction.
2. Suppose that only $\alpha_{2k-2} \neq 0$. Then $\alpha_{2k-2} + \beta_1 = 0$ and $\beta_1 = 0$. Hence $\alpha_{2k-2} = 0$, a contradiction.
3. Suppose that only $\alpha_{2k} \neq 0$. Also $\alpha_{2k} + \beta_3 = 0$ and $\beta_3 = 0$. It follows that $\alpha_{2k} = 0$ which is a contradiction.
4. Suppose that only $\alpha_1 + \epsilon_1 \neq 0$. Then $\alpha_{2k} + \beta_3 \neq 0$. But $\alpha_{2k} = 0$ and $\beta_3 = 0$ which imply that $\alpha_{2k} + \beta_3 = 0$, a contradiction.
5. Suppose that only $\alpha_{2i-1} + \epsilon_i \neq 0$ for exactly one value of i where $i = 2, \cdots$, or $k-1$. Then $\alpha_{2i-2} + \beta_{2i+1} \neq 0$. But $\alpha_{2i-2} = 0$ and $\beta_{2i+1} = 0$. It follows that $\alpha_{2i-2} + \beta_{2i+1} = 0$, a contradiction.
6. Suppose that only $\alpha_{2k-1} + \epsilon_k \neq 0$. Then $\alpha_{2k-2} + \beta_1 \neq 0$. But $\alpha_{2k-2} = 0$ and $\beta_1 = 0$ which imply that $\alpha_{2k-2} + \beta_1 = 0$, a contradiction.
7. Suppose that only $\beta_3 \neq 0$. Also $\alpha_{2k} = 0$ and $\alpha_{2k} + \beta_3 = 0$ which imply that $\beta_3 = 0$, a contradiction.
8. Suppose that only $\beta_{2i-1} \neq 0$ for exactly one value of i where $i = 3, \cdots$, or k. Also $\alpha_{2i-4} = 0$ and $\alpha_{2i-4} + \beta_{2i-1} = 0$ which follows that $\beta_{2i-1} = 0$, a contradiction.
9. Suppose that only $\beta_1 \neq 0$. Then $\alpha_{2k-2} = 0$ and $\alpha_{2k-2} + \beta_1 = 0$. This results in $\beta_1 = 0$ which is a contradiction.

Therefore at least two of the input differences are non-zero and $DP(\alpha \to \beta) \leq p^2$.

Theorem 5. *If the round function of the EFN Type-III is bijective, then the* 3*-round differential probabilities are bounded by* p^2.

Proof. Let the output differences of the first $(2n-3)$ F-functions be $\epsilon_1, \cdots, \epsilon_{2n-3}$ respectively. Then from Theorem 1,

$$\begin{aligned} DP(\alpha \to \beta) = \sum_{\epsilon_i, 1 \leq i \leq 2n-3} & DP(\alpha_2 \to \epsilon_1) \cdot DP(\alpha_3 \to \epsilon_2) \cdots DP(\alpha_n \to \epsilon_{n-1}) \\ & \cdot DP(\alpha_1 + \epsilon_1 \to \epsilon_n) \cdots DP(\alpha_{n-2} + \epsilon_{n-2} \to \epsilon_{2n-3}) \\ & \cdot DP(\alpha_{n-1} + \epsilon_{n-1} \to \alpha_{n-2} + \beta_1 + \epsilon_{n-2}) \\ & \cdot DP(\alpha_n + \epsilon_n \to \alpha_{n-1} + \beta_2 + \epsilon_{n-1}) \\ & \cdot DP(\alpha_1 + \epsilon_1 + \epsilon_{n+1} \to \alpha_n + \beta_3 + \epsilon_n) \\ & \cdot DP(\alpha_2 + \epsilon_2 + \epsilon_{n+2} \to \alpha_1 + \beta_4 + \epsilon_1 + \epsilon_{n+1}) \cdots \\ & \cdot DP(\alpha_{n-3} + \epsilon_{n-3} + \epsilon_{2n-3} \to \alpha_{n-4} + \beta_{n-1} + \epsilon_{n-4} + \epsilon_{2n-4}) \\ & \cdot DP(\beta_1 \to \alpha_{n-3} + \beta_n + \epsilon_{n-3} + \epsilon_{2n-3}) \end{aligned}$$

Similar to the previous proof, suppose that at most one of the input differences is non-zero. If all input differences are zero, then $\alpha_2 = \cdots = \alpha_n = 0$, $\epsilon_1 = 0$ and $\alpha_1 + \epsilon_1 = 0$. So $\alpha_1 = 0$ which contradicts that $\alpha \neq 0$.

1. Suppose that only $\alpha_i \neq 0$ for exactly one value of i where $i = 2, \cdots$, or n. Then $\epsilon_i = 0$ and $\alpha_i + \epsilon_i = 0$. It follows that $\alpha_i = 0$, a contradiction.
2. Suppose that only $\alpha_1 + \epsilon_1 \neq 0$. Also $\epsilon_{n+1} = 0$ and $\alpha_1 + \epsilon_1 + \epsilon_{n+1} = 0$. It follows that $\alpha_1 + \epsilon_1 = 0$ which is a contradiction.
3. Suppose that only $\alpha_i + \epsilon_i \neq 0$ for exactly one value of i where $i = 2, \cdots$, or n. Then $\alpha_i = 0$ and $\epsilon_i = 0$. It follows that $\alpha_i + \epsilon_i = 0$, a contradiction.
4. Suppose that only $\alpha_i + \epsilon_i + \epsilon_{n+i} \neq 0$ for exactly one value of i where $i = 1, \cdots$, or $n - 3$. Also $\alpha_i + \epsilon_i = 0$ and $\epsilon_{n+i} = 0$ which follows that $\alpha_i + \epsilon_i + \epsilon_{n+i} = 0$, a contradiction.
5. Suppose that only $\beta_1 \neq 0$. Then $\alpha_{n-2} + \epsilon_{n-2} = 0$ and $\alpha_{n-2} + \beta_1 + \epsilon_{n-2} = 0$. This results in $\beta_1 = 0$ which is a contradiction.

Therefore at least two of the input differences are non-zero and $DP(\alpha \to \beta) \leq p^2$.

From the results, we see that EFN Type-I requires a much larger number of rounds to be secure against differential cryptanalysis as compared to EFN Type-II and EFN Type-III. The results for EFN Type-II and Type-III are comparable with the main results of [5] whereby the average differential probabilities over at least 2 rounds of Feistel-variant A structure and 1 round of Feistel-variant B structure are both upperbounded by p^2. On the other hand, the average differential probabilities over at least 5 rounds of CLEFIA, MISTY-FO-variant A, B, C and D structures are upperbounded by $p^4 + 2p^5$, p^4, p^4, $2p^4$ and $2p^4$ respectively.

4 Impossible Differential Characteristics of EFN

The Encryption and Decryption Characteristics Matrices of EFN Type-I, Type-II and Type-III are all 1-property matrices, hence we can use Algorithm 1 in [1] to obtain the following results. Here $\alpha_i \neq 0$ and $\beta_i \neq 0$.

Proposition 1. *The maximum number of rounds for impossible differential characteristics that can be found by the U-method for EFN Type-I is* $n^2 + n - 1$. *The generalized impossible differential characteristics is*

$$(\alpha_1, 0, \cdots, 0) \nrightarrow_{n^2+n-1} (0, \cdots, 0, \beta_n).$$

Proposition 2. *For n even, the maximum number of rounds for impossible differential characteristics that can be found by the U-method for EFN Type-II is* $2n + 1$. *The generalized impossible differential characteristics are*

$$(\alpha_1, 0, \cdots, 0) \nrightarrow_{2n+1} (0, \beta_2, 0, \cdots, 0),$$

$$(0, 0, \alpha_3, 0, \cdots, 0) \nrightarrow_{2n+1} (0, 0, 0, \beta_4, 0, \cdots, 0),$$

$$\vdots$$

$$(0, \cdots, 0, \alpha_{n-1}, 0) \nrightarrow_{2n+1} (0, \cdots, 0, \beta_n).$$

Proposition 3. *The maximum number of rounds for impossible differential characteristics that can be found by the U-method for EFN Type-III is $n+2$. An generalized impossible differential characteristics is*

$$(0, \cdots, 0, \alpha_n) \nrightarrow_{n+2} (0, \beta_2, 0, \cdots, 0).$$

In particular, we consider the case when $n = 4$. Readers may refer to the appendix for the tables which depict an impossible differential characteristics for each EFN. As in the case of differential cryptanalysis, the security against impossible differential cryptanalysis improve with more F-functions in each round.

Acknowlegements. The author would like to thank Dr Khoongming Khoo for his invaluable suggestions with this paper.

References

1. J. Kim, S.Hong, J. Sung, S. Lee, J. Lim and S. Sung, "Impossible Differential Cryptanalysis fir Block Cipher Structures", *INDOCRYPT 2003*, LNCS 2904, pp. 82-96, Springer-Verlag, 2003.
2. Subariah Ibrahim, Mohd Aizaini Maarof and Mohd Salihin Ngadiman, "Practical Security against Differential Cryptanalysis for Extended Feistel Network," Universiti Teknologi Malaysia.
3. J. Sung, A. Lee, J. Lim, S. Hong and S.Park, "Provable Security for the Skipjack-like Structure against Differential Cryptanalyis and Linear Cryptanalysis", *ASIACRYPT 2000*, LNCS 1976, pp. 274-288, Springer-Verlag 2000.
4. B. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block-Cipher Design", *Fast Software Encryption 1996*, LNCS 1039, pp. 121-144, Springer, 1996.
5. J. Kim, C. Lee, J. Sung, S. Hong, S. Lee and J. Lim, "Seven New Block Cipher Structures with Provable Security against Differential Cryptanalysis", IEICE Transactions fundamentals of Electronics, Communications and Computer Sciences, No.10, pp 3047-3058, 2008.

A Tables

Table 1. Entries of difference vectors and corresponding type of differences

Entry	Corresponding type of difference
0	zero difference, denoted by 0
1	nonzero nonfixed difference, denoted by δ
1^*	nonzero fixed difference, denoted by γ
2^*	nonzero fixed difference $\oplus$ nonzero nonfixed difference, denoted by $\gamma \oplus \delta$
$t(\geq 2)$	nonfixed difference, denoted by ?

Table 2. A 19-round impossible differential characteristics of EFN Type-I

Round (r)	Difference vector	α_r	Round (r)	Difference vector	α_r
$\downarrow 0$	$(1^*,0,0,0)$	$(\gamma,0,0,0)$	10	$(1,2,1^*,0)$	$(\delta,?,\gamma,0)$
1	$(0,1^*,0,0)$	$(0,\gamma,0,0)$	11	$(0,1,2,1^*)$	$(0,\delta,?,\gamma)$
2	$(0,0,1^*,0)$	$(0,0,\gamma,0)$	12	$(1^*,0,1,1)$	$(\gamma,0,\delta,\delta)$
3	$(0,0,0,1^*)$	$(0,0,0,\gamma)$	13	$(1,1^*,0,0)$	$(\delta,\gamma,0,0)$
4	$(1^*,0,0,1)$	$(\gamma,0,0,\delta)$	14	$(0,1,1^*,0)$	$(0,\delta,\gamma,0)$
5	$(1,1^*,0,1)$	$(\delta,\gamma,0,\delta)$	15	$(0,0,1,1^*)$	$(0,0,\delta,\gamma)$
6	$(1,1,1^*,1)$	$(\delta,\delta,\gamma,\delta)$	16	$(1^*,0,0,0)$	$(\gamma,0,0,0)$
7	$(1,1,1,2^*)$	$(\delta,\delta,\delta,\gamma\oplus\delta)$	17	$(0,1^*,0,0)$	$(0,\gamma,0,0)$
8	$(2^*,1,1,3)$	$(\gamma\oplus\delta,\delta,\delta,?)$	18	$(0,0,1^*,0)$	$(0,0,\gamma,0)$
9	$(3,2^*,1,4)$ $(2,1^*,1,1)$	$(?,\gamma\oplus\delta,\delta,?)$ $(?,\gamma,\delta,\delta)$	$\uparrow 19$	$(0,0,0,1^*)$	$(0,0,0,\gamma)$

Table 3. A 9-round impossible differential characteristics of EFN Type-II

Round (r)	Difference vector	α_r
$\downarrow 0$	$(1^*,0,0,0)$	$(\gamma,0,0,0)$
1	$(0,1^*,0,0)$	$(0,\gamma,0,0)$
2	$(0,1,1^*,0)$	$(0,\delta,\gamma,0)$
3	$(0,1,1,1^*)$	$(0,\delta,\delta,\gamma)$
4	$(1^*,1,1,2)$	$(\gamma,\delta,\delta,?)$
5	$(2,2^*,1,3)$	$(?,\gamma\oplus\delta,\delta,?)$
6	$(3,4,2^*,4)$ $(1,1,1^*,0)$	$(?,?,\gamma\oplus\delta,?)$ $(\delta,\delta,\gamma,0)$
7	$(0,0,1,1^*)$	$(0,0,\delta,\gamma)$
8	$(1^*,0,0,0)$	$(\gamma,0,0,0)$
$\uparrow 9$	$(0,1^*,0,0)$	$(0,\gamma,0,0)$

Table 4. A 6-round impossible differential characteristics of EFN Type-III

Round (r)	Difference vector	α_r
$\downarrow 0$	$(0,0,0,1^*)$	$(0,0,0,\gamma)$
1	$(1^*,0,0,1)$	$(\gamma,0,0,\delta)$
2	$(1,1^*,0,1)$	$(\delta,\gamma,0,\delta)$
3	$(1,2,1^*,1)$	$(\delta,?,\gamma,\delta)$
4	$(1,3,3,2^*)$	$(\delta,?,?,\gamma\oplus\delta)$
5	$(2^*,4,6,5)$ $(1^*,0,0,0)$	$(\gamma\oplus\delta,?,?,?)$ $(\gamma,0,0,0)$
$\uparrow 6$	$(0,1^*,0,0)$	$(0,\gamma,0,0)$