Impossible Boomerang Attack for Block Cipher Structures

Jiali Choy and Huihui Yap

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

Abstract. Impossible boomerang attack [5] (IBA) is a new variant of differential cryptanalysis against block ciphers. Evident from its name, it combines the ideas of both impossible differential cryptanalysis and boomerang attack. Though such an attack might not be the best attack available, its complexity is still less than that of the exhaustive search. In impossible boomerang attack, impossible boomerang distinguishers are used to retrieve some of the subkeys. Thus the security of a block cipher against IBA can be evaluated by impossible boomerang distinguishers. In this paper, we study the impossible boomerang distinguishers for block cipher structures whose round functions are bijective. Inspired by the $\mathcal{U}$-method in [3], we provide an algorithm to compute the maximum length of impossible boomerang distinguishers for general block cipher structures, and apply the algorithm to known block cipher structures such as Nyberg's generalized Feistel network, a generalized CAST256-like structure, a generalized MARS-like structure, a generalized RC6-like structure, etc.

Keywords: Block Ciphers, Impossible Boomerang Attack, Impossible Boomerang Distinguishers

1 Introduction

Differential and linear cryptanalysis are the most common cryptanalytic tools against block ciphers. Provable security against differential and linear cryptanalysis has been an important consideration in the design of block ciphers. However, this is not sufficient to guarantee the security of the block ciphers as they may be vulnerable to other types of cryptanalysis. Analysis of new cryptanalytic techniques is thus always desirable since it enhances the evaluation of the security of a block cipher and the design of more secure ciphers.

Impossible differential cryptanalysis and boomerang-type attacks (including the boomerang, amplified boomerang and rectangle attacks as well as their related-key variants) have been used in the cryptanalysis of many block ciphers. For instance, a 6-round impossible differential attack was mounted on MISTY1 in [2] recently while a full-round related-key rectangle attack was applied to the KASUMI cipher [1]. Hence the importance of these cryptanalytic techniques cannot be undermined.

In [5], a new extension of differential cryptanalysis, which J. Lu calls the impossible boomerang attack, was proposed. This attack combines the ideas of impossible differential cryptanalysis and boomerang attack, and makes use of an impossible boomerang distinguisher. Similar to a boomerang attack, a block cipher $\mathbf{E}$ is treated as two sub-ciphers $\mathbf{E}^0 \circ \mathbf{E}^1$. Two (or more) differentials with probability 1 for $\mathbf{E}^0$ and two (or more) differentials with probability 1 for $\mathbf{E}^1$ are used, where the XOR of the intermediate differences of these differentials is not equal to zero. In [5], the impossible boomerang attack was used to break 6-round AES-128, 7-round AES-192 and 7-round AES-256 in a single key attack scenario, and 8-round AES-192 and 9-round AES-256 in a related-key attack scenario involving two keys.

As mentioned in [5], the advantages of the IBA over the boomerang attacks are analogous to those of impossible differential cryptanalysis over differential cryptanalysis. A block cipher resistant to boomerang-type attack will not necessarily be resistant against an IBA. In boomerang-type distinguishers, one generally assumes that the output of one intermediate round of the cipher is uniformly distributed and is independent from that of the previous rounds. On the other hand, an impossible boomerang distinguisher does not require this assumption, which is often not the case. Therefore, an impossible boomerang distinguisher seems more reasonable than boomerang-type distinguishers [5].

Though we can always obtain an impossible differential from an impossible boomerang distinguisher for the same number of rounds, this is not true for their variants in a related-key attack scenario. As explained in [5], the flexibilities in choosing the key differences may enable more rounds of a block cipher to be broken using a related-key impossible boomerang attack. Since related-key IBA is a variant of the basic IBA, we will be concentrating on the study of impossible boomerang distinguishers which form the core of IBA.

Inspired by the $\mathcal{U}$-method in [3], we introduce the $\mathcal{UB}$-method and provide an algorithm to compute the maximum length of impossible boomerang distinguishers and implement it on some selected block ciphers. As we shall see later on, the maximum length for impossible boomerang distinguishers are equal to that for impossible differential distinguishers for certain ciphers, increasing the likelihood that IBA will be a feasible attack on them. Although the impossible boomerang attack may not be the best known attack for some of the block ciphers, we believe that the results are important and useful, since the attack can be applied to other block ciphers not mentioned here, and the technique introduced in this paper can be modified and used in other works as well.

The rest of the paper is organized as follows. In Section 2, we briefly describe the impossible boomerang attack proposed by J. Lu in [5]. Section 3 introduces some notions, including the $\mathcal{UB}$-method, for the impossible boomerang attack. In Section 4, we present some additional definitions related to the $\mathcal{UB}$-method and use them to determine an expression for the maximum length of impossible boomerang characteristics. An algorithm is proposed in Section 5 to compute the maximum length of impossible boomerang distinguishers for any general block cipher structure with bijective round functions. The algorithm is then applied to various block ciphers and the results are summarized in Section 6.

2 The Impossible Boomerang Attack

The attack, described in [5], combines the boomerang attack with impossible differential cryptanalysis, and is called the impossible boomerang attack (IBA).

2.1 Impossible Boomerang Distinguisher

Similar to a boomerang distinguisher, an impossible boomerang distinguisher, as depicted in Figure 1, treats a block cipher $\mathbf{E}$: $\{0,1\}^k \times \{0,1\}^B \rightarrow \{0,1\}^B$ as two sub-ciphers $\mathbf{E}^0 \circ \mathbf{E}^1$ and consists of

- a differential $w \rightarrow x$ with probability 1 for $\mathbf{E}^0$,
- a differential $w' \rightarrow x'$ with probability 1 for $\mathbf{E}^0$,
- a differential $y \rightarrow z$ with probability 1 for $(\mathbf{E}^1)^{-1}$,
- a differential $y' \rightarrow z'$ with probability 1 for $(\mathbf{E}^1)^{-1}$,

where w, w', x, x', y, y', z and z' are all B-bit blocks, and the condition $x \oplus x' \oplus z \oplus z' \neq 0$ holds.

We state the following theorem from [5], which provides the theoretical basis for our proposed algorithm to compute the maximum length of impossible boomerang distinguishers.

Theorem 1 *[5] Suppose that P and P' are B-bit blocks and K is a key for a B-bit block cipher $\boldsymbol{E}$, where $\boldsymbol{E} = \boldsymbol{E}^0 \circ \boldsymbol{E}^1$ for some $\boldsymbol{E}^0$ and $\boldsymbol{E}^1$. Let $w \rightarrow x$ and $w' \rightarrow x'$ be differentials with probability 1 for $\boldsymbol{E}^0_K$, and, $y \rightarrow z$ and $y' \rightarrow z'$ be differentials with probability 1 for $(\boldsymbol{E}^1_K)^{-1}$, where $x \oplus x' \oplus z \oplus z' \neq 0$. Then the following pairs of equations cannot hold at the same time:*

$$\boldsymbol{E}_K(P) \oplus \boldsymbol{E}_K(P') = y,$$

$$\boldsymbol{E}_K(P \oplus w) \oplus \boldsymbol{E}_K(P' \oplus w') = y'.$$

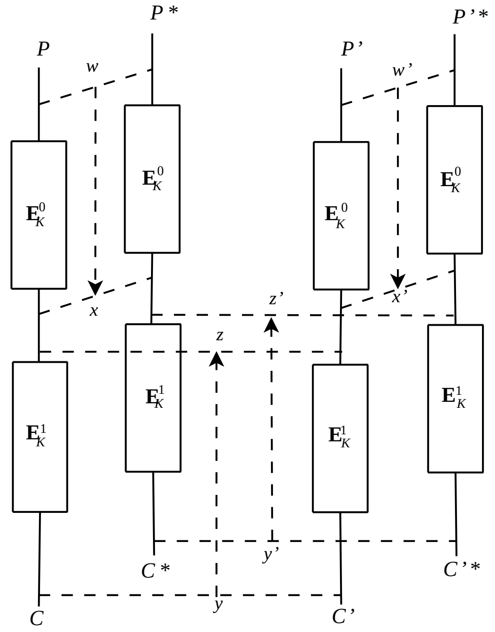

Fig. 1. An impossible boomerang distinguisher

The impossible boomerang distinguisher can be written as $(w, w') \not\twoheadrightarrow (y, y')$. Note that the two differentials for $\mathbf{E}^0$ or $\mathbf{E}^1$ may be identical as long as the condition $x \oplus x' \oplus z \oplus z' \neq 0$ holds.

2.2 A Key Recovery Attack

IBA is a chosen plaintext attack. Let the block cipher $\mathbf{E}$: $\{0,1\}^k \times \{0,1\}^B \to \{0,1\}^B$ be a cascade of four sub-ciphers $\mathbf{E} = \mathbf{E}^\lambda \circ \mathbf{E}^0 \circ \mathbf{E}^1 \circ \mathbf{E}^\mu$. Suppose K_λ and K_μ are the guesses for the subkey used in $\mathbf{E}^\lambda$ and $\mathbf{E}^\mu$ respectively. The basic idea of IBA is as follows:

(1) Find an impossible boomerang distinguisher, $(w, w') \not\twoheadrightarrow (y, y')$ for $\mathbf{E}^0 \circ \mathbf{E}^1$.

(2) For a guess of K_λ and K_μ, compute and check whether a candidate quartet of plaintext/ciphertext pairs $((P, C), (P^*, C^*))$, $((P', C'), (P'^*, C'^*))$ satisfies the following four conditions:

$$\mathbf{E}^\lambda_{K_\lambda}(P) \oplus \mathbf{E}^\lambda_{K_\lambda}(P^*) = w,$$

$$\mathbf{E}^\lambda_{K_\lambda}(P') \oplus \mathbf{E}^\lambda_{K_\lambda}(P'^*) = w',$$

$$(\mathbf{E}^\mu_{K_\mu})^{-1}(C) \oplus (\mathbf{E}^\mu_{K_\mu})^{-1}(C') = y,$$

$$(\mathbf{E}^\mu_{K_\mu})^{-1}(C^*) \oplus (\mathbf{E}^\mu_{K_\mu})^{-1}(C'^*) = y'.$$

(3) If the quartet does satisfy the above conditions, then discard the subkey guess (K_λ, K_μ). Go to the previous step until the number of remaining subkeys is almost one.

As a concluding remark for this section, the basic impossible boomerang attack can be extended to a related-key impossible boomerang attack. Readers may refer to [5] for more details.

3 Basic Notions for IBA

In this section, we introduce and establish notions for IBA by modifying and extending those used in [3].

For a block cipher structure S, let the input and output of one round be $(X_1, X_2, \ldots, X_n)$ and $(Y_1, Y_2, \ldots, Y_n)$ respectively. Throughout this paper, we consider S whose round function F is bijective.

3.1 Basic Definitions and Operations

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

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

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

Definition 2 *[3] 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.*

Example. Consider the CLEFIA-like block cipher structure whereby one F-function is used for two consecutive subblocks. The transformation can be described by

$$(Y_1, Y_2, Y_3, Y_4) = (F(X_1) + X_2, X_3, F(X_3) + X_4, X_1).$$

Then the encryption and decryption characteristics matrices for CLEFIA-like block cipher structure are given by

$$\mathcal{E} = \begin{pmatrix} 1_F & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1_F & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \mathcal{D} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1_F \\ 0 & 0 & 0 & 1 \\ 1 & 1_F & 0 & 0 \end{pmatrix}.$$

Note that the matrices are 1-property matrices.

Definition 3 *[3] Given an input difference $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, the* input difference vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ *corresponding to α is defined as follows.*

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

The output difference after r rounds for α is denoted by α^r and the value of the i^{th} subblock of α^r is written as α_i^r. The corresponding difference vector after r rounds is denoted by $\mathbf{a}^r$, and its ith entry is denoted by a_i^r. For the decryption process, we use the notations $\beta, \beta^r, \beta_i^r, \mathbf{b}, \mathbf{b}^r$ and b_i^r instead.

Given an input difference, the possible output differences of each subblock after r rounds can be classified by five types of differences: zero difference, a nonzero nonfixed difference, a nonzero fixed difference, exclusive-or of a nonzero fixed difference and a nonzero nonfixed difference, and a nonfixed difference. This is summarized in Table 1.

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

a_i^r or b_i^r	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 ?

The set $\{0, 1, 1^*, 2^*\}$ is denoted by $\mathcal{U}$.

Computation of $\mathbf{a}^r$ (similar for $\mathbf{b}^r$) is as follows:

$$\begin{gathered}\mathbf{a}^1 = \mathbf{a} \cdot \mathcal{E}, \\ \mathbf{a}^2 = \mathbf{a}^1 \cdot \mathcal{E}, \\ \vdots \\ \mathbf{a}^r = \mathbf{a}^{r-1} \cdot \mathcal{E}.\end{gathered}$$

A multiplication of $\mathbf{a}$ and $\mathcal{E}$ (similar for $\mathbf{b}$ and $\mathcal{D}$) is defined by

$$\begin{aligned}\mathbf{a} \cdot \mathcal{E} &= (a_i)_{1\times n} \cdot (\mathcal{E}_{i,j})_{n\times n} \\ &= (\sum_i a_i \cdot \mathcal{E}_{i,j})_{1\times n}\end{aligned}$$

Table 2 lists all the possible cases of multiplication between an entry of the difference vector $\mathbf{a}$ and an entry of the matrix $\mathcal{E}$; and addition of $a_i \cdot \mathcal{E}_{i,j}$ and $a_{i'} \cdot \mathcal{E}_{i',j}$.

Table 2. Multiplication (left) and addition (right)($k \in \{0, 1, 1^*, 2^*, t\}, t, t' \geq 2$)

Multiplication ($a_i \cdot \mathcal{E}_{i,j}$)	Addition ($a_i \cdot \mathcal{E}_{i,j} + a_{i'} \cdot \mathcal{E}_{i',j}$)
$k \cdot 0 = 0$	$0 + k = k$
$k \cdot 1 = k$	$1 + 1 = 2$
$0 \cdot 1_F = 0$	$1 + 1^* = 2^*$
$1^* \cdot 1_F = 1$	$1 + 2^* = 3$
$1 \cdot 1_F = 1$	$1 + t = 1 + t$
$2^* \cdot 1_F = 2$	$1^* + t = 1 + t$
$t \cdot 1_F = t$	$2^* + t = 2 + t$
	$t + t' = t + t'$

In this paper, although we concentrate mainly on block ciphers with 1-property encryption and decryption characteristics matrices, the algorithm proposed in Section 5 can be modified for block ciphers with non 1-property matrices. We leave the modification of the algorithm to interested readers. Here, we will just list down the additional operations required for block ciphers with non 1-property matrices.

(1) Since $\gamma \oplus \gamma = 0$, we have two possible cases:

$$1^* + 1^* = \begin{cases} 0, & \text{if } \gamma = \gamma', \\ 1^*, & \text{if } \gamma \neq \gamma'. \end{cases}$$

(2) Since $\gamma' \oplus (\gamma \oplus \delta) = (\gamma' \oplus \gamma) \oplus \delta$, we have

$$1^* + 2^* = \begin{cases} 1, & \text{if } \gamma = \gamma', \\ 2^*, & \text{if } \gamma \neq \gamma'. \end{cases}$$

(3) $2^* + 2^* = 4$.

With these new definitions, the addition operation is still always associative except for certain special cases. For example, for the sum $1+1^*+2^*$, $(1+1^*)+2^*$ gives 4 whereas $1+(1^*+2^*)$ gives 2 or 3. However, in these special cases, the sum evaluated both ways always results in a value ≥ 2 and $x^{(*)} + t = x + t$ (where $t \geq 2$) which always corresponds to a ?. Furthermore, one may check that the operation is also commutative save for a case where the resulting values derived both ways are always ≥ 2. Therefore, to sum three or more entries, always perform the addition from left to right. For example, $1 + 1^* + 1^* = 1$ or 2^* since $(1 + 1^*) + 1^* = 2^* + 1^*$.

3.2 Finding Impossible Boomerang Distinguishers

To find impossible boomerang distinguishers, from Theorem 1, we need four differentials with probability 1 and the XOR of the output difference of each differential must be non-zero. Also note that the two differentials for $\mathbf{E}^0$ or $\mathbf{E}^1$ may be identical.

As denoted in [3], $\mathcal{U} = \{0, 1, 1^*, 2^*\}$. Adopting a similar approach to [3], we may use the elements of $\mathcal{U}$ to find impossible boomerang characteristics. We call this method related to the impossible boomerang attack the $\mathcal{UB}$-method. In Table 3, we summarize all possible cases that satisfy the necessary conditions stated above. Here we use $(\gamma\delta)$ to denote 2^*, that is, $\gamma \oplus \delta$.

Therefore, any of the 26 cases above gives us an impossible boomerang characteristic for $r+r'$ rounds, $(\Delta\alpha, \Delta\alpha') \nrightarrow_{r+r'} (\Delta\beta, \Delta\beta')$.

Example. Consider the CLEFIA-like block cipher structure. Let $\alpha = (0,0,0,\gamma)$, $\alpha' = (0,0,0,\gamma')$, $\beta = (\gamma'',0,0,0)$ and $\beta' = (\gamma''',0,0,0)$, where $\gamma \oplus \gamma' \neq \gamma'' \oplus \gamma'''$. It can be checked that $\alpha_1^3 = \gamma$, $\alpha_1'^3 = \gamma'$, $\beta_1^4 = \gamma'$ and $\beta_1'^4 = \gamma''$. Hence, corresponding to Case $\gamma\gamma\gamma\gamma$ in Table 3,

$$((0,0,0,\gamma),(0,0,0,\gamma')) \nrightarrow_7 ((\gamma'',0,0,0),(\gamma''',0,0,0)),$$

is an impossible boomerang distinguisher with length 7 for CLEFIA.

4 Finding the Maximum Length of Impossible Boomerang Distinguishers

In this section, we introduce more definitions and concepts that will help us compute the maximum length of impossible boomerang characteristics that can be found by the $\mathcal{UB}$-method.

Definition 4 *[3] Let $m \in \mathcal{U}$. Given an input difference vector $\boldsymbol{a}$ and output difference vector $\boldsymbol{b}$, the maximum number of encryption and decryption rounds with respect to m, and, the ith entry of $\boldsymbol{a}$ and $\boldsymbol{b}$ respectively are defined by*

$$\mathcal{ME}_i(\mathbf{a}, m) = \max_r \{r | a_i^r = m\},$$

and

$$\mathcal{MD}_i(\mathbf{b}, m) = \max_r \{r | b_i^r = m\}.$$

The maximum number of encryption and decryption rounds with respect to m are defined as

$$\mathcal{ME}_i(m) = \max_{\mathbf{a} \neq 0} \{\mathcal{ME}_i(\mathbf{a}, m)\},$$

Table 3. Possible output differences $(\alpha_i^r, \alpha_i'^r)$ for encryption and $(\beta_i^{r'}, \beta_i'^{r'})$ for decryption

Case	Value of $(\alpha_i^r, \alpha_i'^r)$	Value of $(\beta_i^{r'}, \beta_i'^{r'})$	Condition
$\delta000$	$(\delta, 0)$	$(0, 0)$	-
$00\delta0$	$(0, 0)$	$(\delta, 0)$	-
$\gamma000$	$(\gamma, 0)$	$(0, 0)$	-
$00\gamma0$	$(0, 0)$	$(\gamma, 0)$	-
$\gamma\gamma00$	(γ, γ')	$(0, 0)$	$\gamma \neq \gamma'$
$00\gamma\gamma$	$(0, 0)$	(γ, γ')	$\gamma \neq \gamma'$
$\gamma0\gamma0$	$(\gamma, 0)$	$(\gamma', 0)$	$\gamma \neq \gamma'$
$\gamma\gamma\gamma0$	(γ, γ')	$(\gamma'', 0)$	$\gamma \oplus \gamma' \oplus \gamma'' \neq 0$
$0\gamma\gamma\gamma$	$(0, \gamma)$	(γ', γ'')	$\gamma \oplus \gamma' \oplus \gamma'' \neq 0$
$\gamma\gamma\gamma\gamma$	(γ, γ')	(γ'', γ''')	$\gamma \oplus \gamma' \neq \gamma'' \oplus \gamma'''$
$\gamma\gamma\delta0$	(γ, γ')	$(\delta, 0)$	$\gamma \oplus \gamma' = 0$
$\delta0\gamma\gamma$	$(\delta, 0)$	(γ, γ')	$\gamma \oplus \gamma' = 0$
$\gamma\delta\gamma0$	(γ, δ)	$(\gamma', 0)$	$\gamma \oplus \gamma' = 0$
$\gamma0\gamma\delta$	$(\gamma, 0)$	(γ', δ)	$\gamma \oplus \gamma' = 0$
$\gamma\gamma\gamma\delta$	(γ, γ')	(γ'', δ)	$\gamma \oplus \gamma' \oplus \gamma'' = 0$
$\gamma\delta\gamma\gamma$	(γ, δ)	(γ', γ'')	$\gamma \oplus \gamma' \oplus \gamma'' = 0$
$00\gamma(\gamma\delta)$	$(0, 0)$	$(\gamma, \gamma' \oplus \delta)$	$\gamma \oplus \gamma' = 0$
$\gamma(\gamma\delta)00$	$(\gamma, \gamma' \oplus \delta)$	$(0, 0)$	$\gamma \oplus \gamma' = 0$
$\gamma0(\gamma\delta)0$	$(\gamma, 0)$	$(\gamma' \oplus \delta, 0)$	$\gamma \oplus \gamma' = 0$
$(\gamma\delta)0\gamma0$	$(\gamma \oplus \delta, 0)$	$(\gamma', 0)$	$\gamma \oplus \gamma' = 0$
$\gamma\gamma(\gamma\delta)0$	(γ, γ')	$(\gamma'' \oplus \delta, 0)$	$\gamma \oplus \gamma' \oplus \gamma'' = 0$
$(\gamma\delta)0\gamma\gamma$	$(\gamma \oplus \delta, 0)$	(γ', γ'')	$\gamma \oplus \gamma' \oplus \gamma'' = 0$
$\gamma0(\gamma\delta)\gamma$	$(\gamma, 0)$	$(\gamma' \oplus \delta, \gamma'')$	$\gamma \oplus \gamma' \oplus \gamma'' = 0$
$(\gamma\delta)\gamma\gamma0$	$(\gamma \oplus \delta, \gamma')$	$(\gamma'', 0)$	$\gamma \oplus \gamma' \oplus \gamma'' = 0$
$\gamma\gamma\gamma(\gamma\delta)$	(γ, γ')	$(\gamma'', \gamma''' \oplus \delta)$	$\gamma \oplus \gamma' = \gamma'' \oplus \gamma'''$
$\gamma(\gamma\delta)\gamma\gamma$	$(\gamma, \gamma' \oplus \delta)$	(γ'', γ''')	$\gamma \oplus \gamma' = \gamma'' \oplus \gamma'''$

and

$$\mathcal{MD}_i(m) = \max_{\mathbf{b}\neq 0}\{\mathcal{MD}_i(\mathbf{b}, m)\}.$$

For the purpose of finding the maximum length of impossible boomerang distinguishers, we introduce the following definition.

Definition 5 *Let $m, m' \in \mathcal{U}$. The maximum number of encryption rounds with respect to m and m', denoted by $\mathcal{ME}_i(m, m')$, is defined as the maximum number of rounds, r, such that there exist input difference vectors a and a' with $a_i^r = m$ and $a_i'^r = m'$. Similarly, the maximum number of decryption rounds with respect to m and m', denoted by $\mathcal{MD}_i(m, m')$, is defined as the maximum number of rounds, r', such that there exist input difference vectors b and b' with $b_i^{r'} = m$ and $b_i'^{r'} = m'$.*

Based on these definitions and the previous section, we may establish the following theorem.

Theorem 2 *Consider the round function of a block cipher structure as a bijective black box. If we use the notation*

$$\mathcal{M}_1 = \max_{1\leq i\leq n}\{\mathcal{ME}_i(1, 0) + \mathcal{MD}_i(0)\},$$

$$\mathcal{M}_2 = \max_{1\leq i\leq n}\{\mathcal{ME}_i(0) + \mathcal{MD}_i(1, 0)\},$$

$$\mathcal{M}_3 = \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(0)\},$$

$$\mathcal{M}_4 = \max_{1 \le i \le n} \{\mathcal{ME}_i(0) + \mathcal{MD}_i(1^*)\},$$

$$\mathcal{M}_5 = \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(1^*)\},$$

then the maximum length of impossible boomerang distinguishers, $\mathcal{M}$, is given by

$$\mathcal{M} = \max_{1 \le i \le 5} \{\mathcal{M}_i\},$$

Proof. Referring to Table 3, we know that $\mathcal{M}$ is the maximum length considering all 26 cases.
Case $\delta 000$: $\mathcal{M}_{\delta 000} = \mathcal{M}_1$.
Case $00\delta 0$: $\mathcal{M}_{00\delta 0} = \mathcal{M}_2$.
Case $\gamma 000$: $\mathcal{M}_{\gamma 000} = \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*, 0) + \mathcal{MD}_i(0)\}$. Since $\mathcal{ME}_i(1^*, 0) \le \min\{\mathcal{ME}_i(1^*), \mathcal{ME}_i(0)\}$,

$$\mathcal{M}_{\gamma 000} \le \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(0)\} = \mathcal{M}_3.$$

Case $00\gamma 0$: $\mathcal{M}_{00\gamma 0} = \max_{1 \le i \le n} \{\mathcal{ME}_i(0) + \mathcal{MD}_i(1^*, 0)\}$. Since $\mathcal{MD}_i(1^*, 0) \le \min\{\mathcal{MD}_i(1^*), \mathcal{MD}_i(0)\}$,

$$\mathcal{M}_{00\gamma 0} \le \max_{1 \le i \le n} \{\mathcal{ME}_i(0) + \mathcal{MD}_i(1^*)\} = \mathcal{M}_4.$$

Case $\gamma\gamma 00$: $\mathcal{M}_{\gamma\gamma 00} = \mathcal{M}_3$.
Case $00\gamma\gamma$: $\mathcal{M}_{00\gamma\gamma} = \mathcal{M}_4$.
Case $\gamma 0 \gamma 0$: $\mathcal{M}_{\gamma 0 \gamma 0} = \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*, 0) + \mathcal{MD}_i(1^*, 0)\}$. Since $\mathcal{ME}_i(1^*, 0) \le \min\{\mathcal{ME}_i(1^*), \mathcal{ME}_i(0)\}$ and $\mathcal{MD}_i(1^*, 0) \le \min\{\mathcal{MD}_i(1^*), \mathcal{MD}_i(0)\}$,

$$\mathcal{M}_{\gamma 0 \gamma 0} \le \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(1^*)\} = \mathcal{M}_5.$$

Case $\gamma\gamma\gamma 0$: $\mathcal{M}_{\gamma\gamma\gamma 0} = \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(1^*, 0)\}$. Since $\mathcal{MD}_i(1^*, 0) \le \min\{\mathcal{MD}_i(1^*), \mathcal{MD}_i(0)\}$,

$$\mathcal{M}_{\gamma\gamma\gamma 0} \le \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(1^*)\} = \mathcal{M}_5.$$

Case $0\gamma\gamma\gamma$: $\mathcal{M}_{0\gamma\gamma\gamma} = \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*, 0) + \mathcal{MD}_i(1^*)\}$. Since $\mathcal{ME}_i(1^*, 0) \le \min\{\mathcal{ME}_i(1^*), \mathcal{ME}_i(0)\}$,

$$\mathcal{M}_{0\gamma\gamma\gamma} \le \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(1^*)\} = \mathcal{M}_5.$$

Case $\gamma\gamma\gamma\gamma$: $\mathcal{M}_{\gamma\gamma\gamma\gamma} = \mathcal{M}_5$.

Case $\gamma\gamma\delta 0$: $\mathcal{M}_{\gamma\gamma\delta 0} = \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(1, 0)\}$. Since $\mathcal{MD}_i(1, 0) \le \min\{\mathcal{MD}_i(1), \mathcal{MD}_i(0)\}$,

$$\mathcal{M}_{\gamma\gamma\delta 0} \le \max_{1 \le i \le n} \{\mathcal{ME}_i(1^*) + \mathcal{MD}_i(0)\} = \mathcal{M}_3.$$

Case $\delta 0\gamma\gamma$: $\mathcal{M}_{\delta 0\gamma\gamma} = \max_{1 \le i \le n} \{\mathcal{ME}_i(1, 0) + \mathcal{MD}_i(1^*)\}$. Since $\mathcal{ME}_i(1, 0) \le \min\{\mathcal{ME}_i(1), \mathcal{ME}_i(0)\}$,

$$\mathcal{M}_{\delta 0\gamma\gamma} \le \max_{1 \le i \le n} \{\mathcal{ME}_i(0) + \mathcal{MD}_i(1^*)\} = \mathcal{M}_4.$$

Case $\gamma\delta\gamma 0$: $\mathcal{M}_{\gamma\delta\gamma 0} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*,1)+\mathcal{M}\mathcal{D}_i(1^*,0)\}$. Since $\mathcal{M}\mathcal{E}_i(1^*,1) \leq \min\{\mathcal{M}\mathcal{E}_i(1^*),\mathcal{M}\mathcal{E}_i(1)\}$ and $\mathcal{M}\mathcal{D}_i(1^*,0) \leq \min\{\mathcal{M}\mathcal{D}_i(1^*),\mathcal{M}\mathcal{D}_i(0)\}$,

$$\mathcal{M}_{\gamma\delta\gamma 0} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(1^*)\} = \mathcal{M}_5.$$

Case $\gamma 0\gamma\delta$: $\mathcal{M}_{\gamma 0\gamma\delta} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*,0)+\mathcal{M}\mathcal{D}_i(1^*,1)\}$. Since $\mathcal{M}\mathcal{E}_i(1^*,0) \leq \min\{\mathcal{M}\mathcal{E}_i(1^*),\mathcal{M}\mathcal{E}_i(0)\}$ and $\mathcal{M}\mathcal{D}_i(1^*,1) \leq \min\{\mathcal{M}\mathcal{D}_i(1^*),\mathcal{M}\mathcal{D}_i(1)\}$,

$$\mathcal{M}_{\gamma 0\gamma\delta} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(1^*)\} = \mathcal{M}_5.$$

Case $\gamma\gamma\gamma\delta$: $\mathcal{M}_{\gamma\gamma\gamma\delta} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(1^*,1)\}$. Since $\mathcal{M}\mathcal{D}_i(1^*,1) \leq \min\{\mathcal{M}\mathcal{D}_i(1^*),\mathcal{M}\mathcal{D}_i(1)\}$,

$$\mathcal{M}_{\gamma\gamma\gamma\delta} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(1^*)\} = \mathcal{M}_5.$$

Case $\gamma\delta\gamma\gamma$: $\mathcal{M}_{\gamma\delta\gamma\gamma} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*,1)+\mathcal{M}\mathcal{D}_i(1^*)\}$. Since $\mathcal{M}\mathcal{E}_i(1^*,1) \leq \min\{\mathcal{M}\mathcal{E}_i(1^*),\mathcal{M}\mathcal{E}_i(1)\}$,

$$\mathcal{M}_{\gamma\gamma\gamma\delta} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(1^*)\} = \mathcal{M}_5.$$

Case $00\gamma(\gamma\delta)$: $\mathcal{M}_{00\gamma(\gamma\delta)} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(0)+\mathcal{M}\mathcal{D}_i(1^*,2^*)\}$. Since $\mathcal{M}\mathcal{D}_i(1^*,2^*) \leq \min\{\mathcal{M}\mathcal{D}_i(1^*),\mathcal{M}\mathcal{D}_i(2^*)\}$,

$$\mathcal{M}_{00\gamma(\gamma\delta)} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(0)+\mathcal{M}\mathcal{D}_i(1^*)\} = \mathcal{M}_4.$$

Case $\gamma(\gamma\delta)00$: $\mathcal{M}_{\gamma(\gamma\delta)00} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*,2^*)+\mathcal{M}\mathcal{D}_i(0)\}$. Since $\mathcal{M}\mathcal{E}_i(1^*,2^*) \leq \min\{\mathcal{M}\mathcal{E}_i(1^*),\mathcal{M}\mathcal{E}_i(2^*)\}$,

$$\mathcal{M}_{\gamma(\gamma\delta)00} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(0)\} = \mathcal{M}_3.$$

Case $\gamma 0(\gamma\delta)0$: $\mathcal{M}_{\gamma 0(\gamma\delta)0} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*,0)+\mathcal{M}\mathcal{D}_i(2^*,0)\}$. Since $\mathcal{M}\mathcal{E}_i(1^*,0) \leq \min\{\mathcal{M}\mathcal{E}_i(1^*),\mathcal{M}\mathcal{E}_i(0)\}$ and $\mathcal{M}\mathcal{D}_i(2^*,0) \leq \min\{\mathcal{M}\mathcal{D}_i(2^*),\mathcal{M}\mathcal{D}_i(0)\}$,

$$\mathcal{M}_{\gamma 0(\gamma\delta)0} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(0)\} = \mathcal{M}_3.$$

Case $(\gamma\delta)0\gamma 0$: $\mathcal{M}_{(\gamma\delta)0\gamma 0} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(2^*,0)+\mathcal{M}\mathcal{D}_i(1^*,0)\}$. Since $\mathcal{M}\mathcal{E}_i(2^*,0) \leq \min\{\mathcal{M}\mathcal{E}_i(2^*),\mathcal{M}\mathcal{E}_i(0)\}$ and $\mathcal{M}\mathcal{D}_i(1^*,0) \leq \min\{\mathcal{M}\mathcal{D}_i(1^*),\mathcal{M}\mathcal{D}_i(0)\}$,

$$\mathcal{M}_{(\gamma\delta)0\gamma 0} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(0)+\mathcal{M}\mathcal{D}_i(1^*)\} = \mathcal{M}_4.$$

Case $\gamma\gamma(\gamma\delta)0$: $\mathcal{M}_{\gamma\gamma(\gamma\delta)0} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(2^*,0)\}$. Since $\mathcal{M}\mathcal{D}_i(2^*,0) \leq \min\{\mathcal{M}\mathcal{D}_i(2^*),\mathcal{M}\mathcal{D}_i(0)\}$,

$$\mathcal{M}_{\gamma\gamma(\gamma\delta)0} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(1^*)+\mathcal{M}\mathcal{D}_i(0)\} = \mathcal{M}_3.$$

Case $(\gamma\delta)0\gamma\gamma$: $\mathcal{M}_{(\gamma\delta)0\gamma\gamma} = \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(2^*,0)+\mathcal{M}\mathcal{D}_i(1^*)\}$. Since $\mathcal{M}\mathcal{E}_i(2^*,0) \leq \min\{\mathcal{M}\mathcal{E}_i(2^*),\mathcal{M}\mathcal{E}_i(0)\}$,

$$\mathcal{M}_{(\gamma\delta)0\gamma\gamma} \leq \max_{1\leq i\leq n}\{\mathcal{M}\mathcal{E}_i(0)+\mathcal{M}\mathcal{D}_i(1^*)\} = \mathcal{M}_4.$$

Case $\gamma 0(\gamma\delta)\gamma$: $\mathcal{M}_{\gamma 0(\gamma\delta)\gamma} = \max_{1\leq i\leq n}\{\mathcal{ME}_i(1^*,0)+\mathcal{MD}_i(2^*,1^*)\}$. Since $\mathcal{ME}_i(1^*,0) \leq \min\{\mathcal{ME}_i(1^*),\mathcal{ME}_i(0)\}$ and $\mathcal{MD}_i(2^*,1^*) \leq \min\{\mathcal{MD}_i(2^*),\mathcal{MD}_i(1^*)\}$,

$$\mathcal{M}_{\gamma 0(\gamma\delta)\gamma} \leq \max_{1\leq i\leq n}\{\mathcal{ME}_i(1^*)+\mathcal{MD}_i(1^*)\} = \mathcal{M}_5.$$

Case $(\gamma\delta)\gamma\gamma 0$: $\mathcal{M}_{(\gamma\delta)\gamma\gamma 0} = \max_{1\leq i\leq n}\{\mathcal{ME}_i(2^*,1^*)+\mathcal{MD}_i(1^*,0)\}$. Since $\mathcal{ME}_i(2^*,1^*) \leq \min\{\mathcal{ME}_i(2^*),\mathcal{ME}_i(1^*)\}$ and $\mathcal{MD}_i(1^*,0) \leq \min\{\mathcal{MD}_i(1^*),\mathcal{MD}_i(0)\}$,

$$\mathcal{M}_{(\gamma\delta)\gamma\gamma 0} \leq \max_{1\leq i\leq n}\{\mathcal{ME}_i(1^*)+\mathcal{MD}_i(1^*)\} = \mathcal{M}_5.$$

Case $\gamma\gamma\gamma(\gamma\delta)$: $\mathcal{M}_{\gamma\gamma\gamma(\gamma\delta)} = \max_{1\leq i\leq n}\{\mathcal{ME}_i(1^*)+\mathcal{MD}_i(1^*,2^*)\}$. Since $\mathcal{MD}_i(1^*,2^*) \leq \min\{\mathcal{MD}_i(1^*),\mathcal{MD}_i(2^*)\}$,

$$\mathcal{M}_{\gamma\gamma\gamma(\gamma\delta)} \leq \max_{1\leq i\leq n}\{\mathcal{ME}_i(1^*)+\mathcal{MD}_i(1^*)\} = \mathcal{M}_5.$$

Case $\gamma(\gamma\delta)\gamma\gamma$: $\mathcal{M}_{\gamma(\gamma\delta)\gamma\gamma} = \max_{1\leq i\leq n}\{\mathcal{ME}_i(1^*,2^*)+\mathcal{MD}_i(1^*)\}$. Since $\mathcal{ME}_i(1^*,2^*) \leq \min\{\mathcal{ME}_i(1^*),\mathcal{ME}_i(2^*)\}$,

$$\mathcal{M}_{\gamma(\gamma\delta)\gamma\gamma} \leq \max_{1\leq i\leq n}\{\mathcal{ME}_i(1^*)+\mathcal{MD}_i(1^*)\} = \mathcal{M}_5.$$

The result now follows immediately. □

Example. For CLEFIA, we computed $\mathcal{ME}_1((0,0,0,1^*),1^*) = 3$ and $\mathcal{MD}_1((1^*,0,0,0),1^*) = 4$. By running through all possible difference vectors **a** and **b**, it can be verified that $\mathcal{ME}_1(1^*) = 3$ and $\mathcal{MD}_1(1^*) = 4$. Checking through all values of i where $1 \leq i \leq 4$, we have

$$\begin{aligned}\mathcal{M}_5 &= \max_{1\leq i\leq 4}\{\mathcal{ME}_i(1^*)+\mathcal{MD}_i(1^*)\}\\ &= \mathcal{ME}_1(1^*)+\mathcal{MD}_1(1^*)\\ &= 7.\end{aligned}$$

By computing the values of $\mathcal{M}_1$ to $\mathcal{M}_4$, we obtain $\mathcal{M}_1 = \mathcal{M}_2 = 5$ and $\mathcal{M}_3 = \mathcal{M}_4 = 6$. These imply that $\mathcal{M} = \mathcal{M}_5 = 7$. Hence, for CLEFIA, the maximum length of impossible boomerang distinguishers that can be found in the $\mathcal{UB}$ method is 7, and a corresponding 7-round impossible boomerang characteristic is $((0,0,0,\gamma),(0,0,0,\gamma)) \nrightarrow_7 ((\gamma',0,0,0),(\gamma'',0,0,0))$, where $\gamma' \neq \gamma''$.

5 An Algorithm to Compute the Length of Impossible Boomerang Distinguishers

In this section, we present an algorithm to compute the maximum number of rounds, $\mathcal{M}$, for the impossible boomerang characteristics which can be found by the $\mathcal{UB}$-method. By modifying this algorithm, we may also identify the specific forms of impossible boomerang distinguishers.

At the outset, we shall assume that the block cipher structure that the algorithm is applied to has round functions which are bijective. Furthermore, the encryption and decryption characteristic matrices, $\mathcal{E}$ and $\mathcal{D}$ are assumed to be 1-property matrices. We employ the same variables as in Tables 6 and 7 of [3]. They are summarized in Tables 4 and 5 below.

Table 4. The meaning of variables used in Algorithm 1. ($y \geq 0$)

Variables	Meanings
$e_{i,j} = 0$	$\mathcal{E}_{i,j} = 0$
$e_{i,j} = 1$	$\mathcal{E}_{i,j} = 1$ or 1_F
$\tilde{e}_{i,j} = 0$	$\mathcal{E}_{i,j} = 1$ ($x^* \cdot \mathcal{E}_{i,j} = x^*$ preserves $*$.)
$\tilde{e}_{i,j} = 1$	$\mathcal{E}_{i,j} = 0$ ($x^* \cdot \mathcal{E}_{i,j} = 0$) or $\mathcal{E}_{i,j} = 1_F$ ($x^* \cdot \mathcal{E}_{i,j} = x$)
$a_i^r = y$ (resp. x)	The i^{th} entry of difference vector $\mathbf{a}^r$ is y (resp. x^*)
$\hat{a}_i^r = 0$	The i^{th} entry of difference vector $\mathbf{a}^r$ has no $*$
$\hat{a}_i^r = -1$	The i^{th} entry of difference vector $\mathbf{a}^r$ has $*$

Table 5. Multiplication between an entry of difference vector and an entry of matrix in Algorithm 1

An entry c, ($\hat{a}_i^r$) of difference vectors	An entry d, ($\tilde{e}_{i,j}$) of $\mathcal{E}$	$c \cdot d$	$\hat{a}_i^r + \tilde{e}_{i,j} = s_i$ if ($s_i = 1$) $s_i \leftarrow 0$
x^*, (-1)	0, (1)	0	0
x^*, (-1)	1_F, (1)	x	0
x^*, (-1)	1, (0)	x^*	-1
x, (0)	0, (1)	0	0
x, (0)	1_F, (1)	x	0
x, (0)	1, (1)	x	0

```
Step 1 : Input the encryption characteristic matrix $\mathcal{E} = (\mathcal{E}_{ij})_{n \times n}$

for $i = 0$ to $n - 1$
    for $j = 0$ to $n - 1$
        if $\mathcal{E}_{i,j} = 0$, then $e_{i,j} \leftarrow 0$ and $\tilde{e}_{i,j} \leftarrow 1$
        if $\mathcal{E}_{i,j} = 1$, then $e_{i,j} \leftarrow 1$ and $\tilde{e}_{i,j} \leftarrow 0$
        if $\mathcal{E}_{i,j} = 1_F$, then $e_{i,j} \leftarrow 1$ and $\tilde{e}_{i,j} \leftarrow 1$

Step 2 : Compute the values of $\mathcal{ME}_i(m)$ where $0 \leq i \leq n - 1$ and $m \in \{0, 1^*\}$.

$\mathcal{ME}_i(0) \leftarrow 0$, $\mathcal{ME}_i(2) \leftarrow 0$, for $0 \leq i \leq n - 1$

/* The $m$'s values $0, 1$, and $2$ indicate the entries $0, 1$, and $1^*$ respectively. */

For each input difference vector $\mathbf{x}$          /* $\mathbf{x}$ represents $\mathbf{x}^0$. */
    for $i = 0$ to $n - 1$
        if ($x_i^0 = 0$) $\hat{x}_i \leftarrow 0$
        else if ($x_i^0 = 1$) $\hat{x}_i \leftarrow -1$
        $\mathcal{ME}_i(\mathbf{x}, 0) \leftarrow 0$, $\mathcal{ME}_i(\mathbf{x}, 2) \leftarrow 0$
    $r \leftarrow 0$
    while (there exists some index $l$ such that $x_l^r \leq 2$)
        for $j = 0$ to $n - 1$
            $t_j \leftarrow 0$, $\hat{t}_j \leftarrow 0$
        /* $t_j$ and $\hat{t}_j$ are the temporary parameters to compute $\mathbf{x}^{r+1}$ and $\hat{\mathbf{x}}^{r+1}$. */
            for $i = 0$ to $n - 1$
                $t_j \leftarrow t_j + x_i^r \cdot e_{i,j}$
                $s_i \leftarrow \hat{x}_i^r + \tilde{e}_{i,j}$
                if ($s_i = 1$) $s_i \leftarrow 0$
                $\hat{t}_j \leftarrow \hat{t}_j + s_i$
        $r \leftarrow r + 1$
        $x_i^r \leftarrow t_i$, $\hat{x}_i^r \leftarrow \hat{t}_i$, for $0 \leq i \leq n - 1$

        for $i = 0$ to $n - 1$
            if ($x_i^r = 0$) $\mathcal{ME}_i(\mathbf{x}, 0) \leftarrow r$
            if ($x_i^r = 1$ and $\hat{x}_i^r = -1$) $\mathcal{ME}_i(\mathbf{x}, 2) \leftarrow r$

    for $i = 0$ to $n - 1$
        if ($\mathcal{ME}_i(0) \leq \mathcal{ME}_i(\mathbf{x}, 0)$) $\mathcal{ME}_i(0) \leftarrow \mathcal{ME}_i(\mathbf{x}, 0)$
        if ($\mathcal{ME}_i(2) \leq \mathcal{ME}_i(\mathbf{x}, 2)$) $\mathcal{ME}_i(2) \leftarrow \mathcal{ME}_i(\mathbf{x}, 2)$
```

Step 3 : Compute the values of $\mathcal{MD}_i(m)$ where $0 \leq i \leq n-1$ and $m \in \{0, 1^*\}$.

Insert the matrix $\mathcal{D}$ into steps 1 and 2.

Step 4 : Compute the values of $\mathcal{ME}_i(1,0)$ where $0 \leq i \leq n-1$

$\mathcal{ME}_i(1,0) \leftarrow 0$, for $0 \leq i \leq n-1$

```
For each input difference vector $\mathbf{x}$ and each input difference vector $\mathbf{y}$
    for $i = 0$ to $n-1$
        if $(x_i^0 = 0)$ $\hat{x}_i \leftarrow 0$
        else if $(x_i^0 = 1)$ $\hat{x}_i \leftarrow -1$
        if $(y_i^0 = 0)$ $\hat{y}_i \leftarrow 0$
        else if $(y_i^0 = 1)$ $\hat{y}_i \leftarrow -1$
        $\mathcal{ME}_i(\mathbf{x}, \mathbf{y}, 1, 0) \leftarrow 0$

    $r \leftarrow 0$
    while (there exists some index $l$ such that $x_l^r \leq 2$ or $y_l^r \leq 2$ )
        for $j = 0$ to $n-1$
            $tx_j \leftarrow 0$, $\hat{tx}_j \leftarrow 0$
            $ty_j \leftarrow 0$, $\hat{ty}_j \leftarrow 0$
            for $i = 0$ to $n-1$
                $tx_j \leftarrow tx_j + x_i^r \cdot e_{i,j}$
                $sx_i \leftarrow \hat{x}_i^r + \tilde{e}_{i,j}$
                if $(sx_i = 1)$ $sx_i \leftarrow 0$
                $\hat{tx}_j \leftarrow \hat{tx}_j + sx_i$

                $ty_j \leftarrow ty_j + y_i^r \cdot e_{i,j}$
                $sy_i \leftarrow \hat{y}_i^r + \tilde{e}_{i,j}$
                if $(sy_i = 1)$ $sy_i \leftarrow 0$
                $\hat{ty}_j \leftarrow \hat{ty}_j + sy_i$

        $r \leftarrow r + 1$
        $x_i^r \leftarrow tx_i$, $\tilde{x}_i^r \leftarrow \hat{tx}_i$, for $0 \leq i \leq n-1$
        $y_i^r \leftarrow ty_i$, $\tilde{y}_i^r \leftarrow \hat{ty}_i$, for $0 \leq i \leq n-1$

    for $i = 0$ to $n-1$
        for $j = 0$ to $r$
            if $(x_i^j = 1$ and $\tilde{x}_i^j = 0$ and $y_i^j = 0$ and $\tilde{y}_i^j = 0)$ $\mathcal{ME}_i(\mathbf{x}, \mathbf{y}, 1, 0) \leftarrow j$

    if $(\mathcal{ME}_i(\mathbf{x}, \mathbf{y}, 1, 0) \leq \mathcal{ME}_i(1,0))$ $\mathcal{ME}_i(1,0) \leftarrow \mathcal{ME}_i(\mathbf{x}, \mathbf{y}, 1, 0)$
```

Step 5 : Compute the values of $\mathcal{MD}_i(1,0)$ where $0 \leq i \leq n-1$.

Insert the matrix $\mathcal{D}$ into step 4.

Step 6 : Compute the length $\mathcal{M}_1$.

Output $\max_{0 \leq i \leq n-1}\{\mathcal{ME}_i(1,0) + \mathcal{MD}_i(0)\}$.

Step 7 : Compute the length $\mathcal{M}_2$.

Output $\max_{0 \leq i \leq n-1}\{\mathcal{ME}_i(0) + \mathcal{MD}_i(1,0)\}$.

Step 8 : Compute the length $\mathcal{M}_3$.

Output $\max_{0 \leq i \leq n-1}\{\mathcal{ME}_i(2) + \mathcal{MD}_i(0)\}$.

Step 9 : Compute the length $\mathcal{M}_4$.

Output $\max_{0 \leq i \leq n-1}\{\mathcal{ME}_i(0) + \mathcal{MD}_i(2)\}$.

Step 10 : Compute the length $\mathcal{M}_5$.

Output $\max_{0 \leq i \leq n-1}\{\mathcal{ME}_i(2) + \mathcal{MD}_i(2)\}$.

Step 11 : Output the length $\mathcal{M}$.

Output $\max_{1 \leq i \leq 5}(\mathcal{M}_i)$.

Algorithm 1 to compute the length $\mathcal{M}$

6 Results for Some Block Cipher Structures

We applied Algorithm 1 to several block cipher structures such as a generalized Feistel network, a generalized CAST256-like structure, a generalized MARS-like structure, a generalized RC6-like structure, CLEFIA, a generalized Feistel scheme with an substitution-permutation round function, SMS4, as well as a Skipjack-like structure. All of them have 1-property matrices $\mathcal{E}$ and $\mathcal{D}$. The reader may refer to [7, 9, 10, 4, 8] for the details of these cipher structures. We also found the specific forms of impossible boomerang characteristics which give the maximum lengths for each structure. Even though the computer simulation was only tested on a finite number of subblocks, we are able to generalize the results due to the regular structural feature.

Table 6 gives the specific forms of various impossible boomerang characteristics for each structure. Table 7 summarizes our cryptanalytic results. In both tables, n denotes the number of subblocks and in the case of n always even, we let $n = 2m$. In Table 7, we also compare the maximum lengths for the impossible differential cryptanalysis (IDC) with that for the impossible boomerang attack (IBA). As can be observed, these two maximum lengths are equal for the generalized MARS structure.

Table 6. Impossible boomerang characteristics for some generalized Feistel networks (All α's, β's non-zero, i odd, $\alpha \neq \alpha'$, $\beta \neq \beta'$)

Structure	Case	Impossible Boomerang Characteristics
GFN_m	$\gamma\gamma\gamma\gamma$	$((0,\ldots,0,\alpha_n),(0,\ldots,0,\alpha_n)) \not\twoheadrightarrow_{3m} ((\beta_1,0,\ldots,0),(\beta'_1,0,\ldots,0))$
	$\delta 000$	Many E.g. For GFN_3, $((0,0,0,\alpha_4,0,0),(0,\ldots,0,\alpha_6)) \not\twoheadrightarrow_{9} ((0,0,\beta_3,0,0,0),(0,0,\beta'_3,0,0,0))$
	000δ	Many E.g. For GFN_3, $((0,\ldots,0,\alpha_6),(0,\ldots,0,\alpha'_6)) \not\twoheadrightarrow_{9} ((0,\beta_2,0,\ldots,0),(\beta_1,0,\ldots,0))$
Generalized CAST256	$\gamma\gamma\gamma\gamma$	$((0,\ldots,0,\alpha_n),(0,\ldots,0,\alpha_n)) \not\twoheadrightarrow_{n^2-1} ((\beta_1,0,\ldots,0),(\beta'_1,0,\ldots,0))$
Generalized MARS	$\gamma\gamma\gamma\gamma$	$((0,\ldots,0,\alpha_n),(0,\ldots,0,\alpha_n)) \not\twoheadrightarrow_{2n-1} ((\beta_1,0,\ldots,0),(\beta'_1,0,\ldots,0))$
Generalized RC6	$\gamma\gamma\gamma\gamma$	$((0,\ldots,0,\alpha_i,0,\ldots,0),(0,\ldots,0,\alpha_i,0,\ldots,0)) \not\twoheadrightarrow_{4m-1}$ $((0,\ldots,0,\beta_{i+1},0,\ldots,0),(0,\ldots,0,\beta'_{i+1},0,\ldots,0))$
CLEFIA	$\gamma\gamma\gamma\gamma$	$((0,0,0,\alpha_4),(0,0,0,\alpha_4)) \not\twoheadrightarrow_{7} ((\beta_1,0,0,0),(\beta'_1,0,0,0))$
$GFSP_4$	$\gamma\gamma\gamma\gamma$	$((\alpha_1,0,0,0),(\alpha_1,0,0,0)) \not\twoheadrightarrow_{15} ((0,0,0,\beta_4),(0,0,0,\beta'_4))$
$SMS4$	$\gamma\gamma\gamma\gamma$	$((\alpha_1,0,0,0),(\alpha_1,0,0,0)) \not\twoheadrightarrow_{5} ((0,0,0,\beta_4),(0,0,0,\beta'_4))$
Skipjack-like	$00\gamma\gamma$	Many E.g. $((0,0,0,\alpha_4),(0,0,0,\alpha_4)) \not\twoheadrightarrow_{12} ((0,\beta_2,0,0),(0,\beta'_2,0,0))$

6.1 Additional Comments

Generalized CAST256 : In [3] and [8], the authors conjectured that the maximum length of the impossible differential distinguisher for generalized CAST256 is $n^2 - 1$. This value was derived based on Figure 3 in [8]. In contrast, we looked at the structure shown in Figure 1 of [7]. Based on this diagram, we found the maximum length of the impossible differential distinguisher to be n^2+n-1 instead.

$\mathbf{GFSP_4}$: In [10], the authors only gave the upper bounds of the maximum differential/linear probabilities of 16-round $GFSP_4$. However, in the light of our results, both for IDC and IBA, we recommend the use of at least 25 rounds for this scheme.

Table 7. Summary of our results. (A: The maximum number (r) of rounds for impossible differential characteristics. B: The maximum number (r) of rounds for impossible boomerang characteristics.)

Block Cipher Structure	IDC		IBA	
	A	Comment	B	Comment
GFN_m	$r = 3m + 2$ $(m \geq 3)$	[3]	$r = 3m$ $(m \geq 2)$	This paper
Generalized CAST256	$r = n^2 + n - 1$ $(n \geq 3)$	This paper	$r = n^2 - 1$ $(n \geq 3)$	This paper
Generalized MARS	$r = 2n - 1$ $(n \geq 3)$	[3]	$r = 2n - 1$ $(n \geq 3)$	This paper
Generalized RC6	$r = 4m + 1$ $(m \geq 2)$	[3]	$r = 4m - 1$ $(m \geq 2)$	This paper
CLEFIA	9	[9]	7	This paper
$GFSP_4$	19	This paper	15	This paper
SMS4	6	This paper	5	This paper
Skipjack-like	15	[8]	12	This paper

SMS4 : While the maximum lengths of the distinguishers found for IDC and IBA are quite small, note that this analysis only considers the general structure of the ciphers without taking into account the specific properties of the round functions. For example, for SMS4, a 12-round impossible differential characteristic was published in [6], formed by combining two 6-round differentials. Our results, however, give a definite lower bound for the number of rounds that can be attacked with an impossible differential or impossible boomerang distinguisher.

Skipjack-like structure : Our approach also works for the truncated case. With reference to Figure 1 of [8], a 15-round impossible truncated differential was found in [8], which agrees with the result which we found by the $\mathcal{U}$-method. By applying our Algorithm 1, we unveiled a 12-round impossible truncated boomerang distinguisher.

7 Conclusion

In this paper, we introduced a widely applicable method, called the $\mathcal{UB}$-method, to find various impossible boomerang characteristics for general block cipher structures. We presented Algorithm 1 which is used to determine the maximum length of impossible boomerang distinguishers that can be found by the $\mathcal{UB}$-method. Algorithm 1 was then applied to find the maximum length of impossible boomerang distinguishers for several known block cipher structures. By modifying Algorithm 1, we found the specific forms of impossible boomerang characteristics for each structure.

While our research presented in this paper only considers the general structure of the ciphers, it provides a definite lower bound for the maximum length of an impossible boomerang distinguisher. It is likely that longer ones may be found when the specific properties of the round functions are taken into account. Furthermore, we saw that the lower bound for the maximum length of an impossible boomerang distinguisher is comparable to that of an impossible differential characteristic for some block ciphers. Since impossible boomerang attack may be a feasible attack on certain ciphers, our results will be useful in the study of the latter, which will in turn shed more light on variants of the attack such as the related-key version.

Acknowledgements

The authors would like to thank Khoongming Khoo for his helpful comments and suggestions, and also the anonymous reviewers for their valuable comments.

References

1. E. Biham, O. Dunkelman, and N. Keller, "A Related-Key Rectangle Attack on the Full KASUMI", ASIACRYPT 2005, LNCS 3788, pp. 443-461, Springer-Verlag, 2005.
2. O. Dunkelman and N. Keller, "An Improved Impossible Differential Attack on MISTY1", ASIACRYPT 2008, LNCS 5350, pp. 441-454, Springer-Verlag, 2008.
3. J. Kim, S.Hong, J. Sung, S. Lee, J. Lim, and S. Sung, "Impossible Differential Cryptanalysis for Block Cipher Structures", INDOCRYPT 2003, LNCS 2904, pp. 82-96, Springer-Verlag, 2003.
4. F. Liu, W. Ji, L. Hu, J. Ding, S. Lv, A. Pyshkin, and R. Weinmann, "Analysis of the SMS4 Block Cipher", ACISP 2007, LNCS 4586, pp. 158-170, Springer-Verlag, 2007.
5. J. Lu, "Cryptanalysis of Block Ciphers", Technical Report RHUL-MA-2008-19, `http://www.rhul.ac.uk/mathematics/techreports`, 30 July 2008.
6. J. Lu, "Attacking Reduced-Round Versions of the SMS4 Block Cipher in the Chinese WAPI Standard", ICICS 2007, LNCS 4861, pp. 306-318, 2007.
7. S. Moriai and S. Vaudenay, "On the Pseudorandomness of Top-Level Schemes of Block Ciphers", ASIACRYPT 2000, LNCS 1976, pp. 289-302, Springer-Verlag, 2000.
8. J. Sung, S. Lee, J. Lim, S. Hong, and S. Park, "Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis", ASIACRYPT 2000, LNCS 1976, pp. 274-288, Springer-Verlag, 2000.
9. Y. Tsunoo, E. Tsujihara, M. Shigeri, T. Saito, T. Suzaki, and H. Kubo, "Impossible Differential Cryptanalysis of CLEFIA", FSE 2008, LNCS 5086, pp. 398-411, Springer-Verlag, 2008.
10. W. Wu, W. Zhang, and D. Lin, "On the Security of Generalized Feistel Scheme with SP Round Function", International Journal of Network Security, Vol. 3, No. 3, pp. 215-224, Nov 2006.