Designs, Codes and Cryptography (2019) 87:2683–2700
https://doi.org/10.1007/s10623-019-00642-9

Provable security against impossible differential and zero correlation linear cryptanalysis of some feistel structures

Dong Yang[1,2] · Wen-Feng Qi[1] · Hua-Jin Chen[1]

Received: 6 November 2017 / Revised: 10 May 2019 / Accepted: 11 May 2019 / Published online: 27 May 2019

Abstract
Impossible differential and zero correlation linear cryptanalysis are two important cryptanalytic methods. In this paper, we study the security of some Feistel structures against these two cryptanalytic methods. Throughout this paper, we consider the impossible differential and zero correlation linear hull that are independent of the choices of the non-linear parts. Based on that, a method is introduced to estimate the number of rounds that the longest impossible differential could cover for one kind of Feistel-SP structure. Fortunately, our method also applies to some generalized Feistel structures, such as the Type-2 generalized Feistel structure. Then we project our results to zero correlation by the links between impossible differential and zero correlation linear hull. Lastly, as an application of our method, we prove that there do not exist 15-round impossible differential and zero correlation linear hull for LBlock and TWINE.

Keywords Impossible differential · Zero correlation linear hull · Feistel structure · LBlock · TWINE

Mathematics Subject Classification 11B50 · 94A55 · 94A60

Communicated by R. Steinfeld.

✉ Wen-Feng Qi
wenfeng.qi@263.net

Dong Yang
yangdong_sky@126.com

Hua-Jin Chen
huajin_chen@126.com

[1] The National Digital Switching System Engineering & Technological Research Center, P.O. Box 407, 62 Kexue Road, Zhengzhou 450001, China

[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China

1 Introduction

Feistel structure and its variants are widely used in the designs of block ciphers, such as the Camellia [1], LBlock [17] and TWINE [13]. Thus the security of Feistel structure against known cryptanalytic techniques attract many attention. Impossible differential cryptanalysis (IDC) [3,8] and zero correlation linear cryptanalysis (ZCLC) [4] are extensions of the differential cryptanalysis [2] and linear cryptanalysis [10], respectively. It had been shown that these two attacks are very efficient against many block ciphers [5,6,9,14,15]. However, the security of the Feistel cipher against IDC and ZCLC have not been well studied.

In IDC and ZCLC, the key point is constructing impossible differential (ID) or zero correlation linear hull (ZCLH) that cover as many rounds as possible. Thus to prove the security of Feistel structure against IDC and ZCLC, a common way is to estimate the number of rounds that the longest ID and ZCLH could cover. Based on that, Sun et al. studied the security of the Feistel structure with SP-type round functions (Feistel-SP structure in short) in [12]. They considered the ID and ZCLH that are independent of S-boxes. In the rest of this paper, all the ID and ZCLH represent the impossible differential and zero correlation linear hull that are independent of S-boxes. Furthermore, the authors defined a special class of ID and ZCLH, named **independent ID** and **independent ZCLH** (see definition **3** of [12]), respectively. Let b be the size of the S-box and m be the number of S-boxes for the Feistel-SP structure. In the case that $m \leq 2^{b-1} - 1$, Sun et al. gave upper bounds on the rounds that the longest independent ID and independent ZCLH could cover. Note that the independent ID and independent ZCLH can not cover all the ID and ZCLH for the Feistel-SP structure, and thus Sun's upper bounds are incomplete.

In this paper, we focus on the Feistel-SP structure whose P is a permutation matrix, and we denote this structure as Feistel*-SP structure. We aim to provide upper bounds on the rounds that the longest ID and ZCLH could cover for this structure. The main results of this paper are as follows.

1. Based on the characteristic matrix proposed by Kim et al. [7], a new way is introduced to predict the internal difference for Feistel*-SP block ciphers.
2. A necessary and sufficient condition is given to judge whether a differential is impossible or not for Feistel*-SP structure. Combined with our new difference-prediction way, we show that the length of ID for Feistel*-SP structure is upper bounded by the *diffusion order* of the characteristic matrixes. Moreover, based on the links between ID and ZCLH, we project our results to ZCLH.
3. For generalized Feistel structures, we show that if their characteristic matrices are **1-property** matrixes, then the above method is also valid. For example, the Type-2 generalized Feistel structure [18] has **1-property** characteristic matrices.
4. Based on our method, we prove that there do not exist 15-round ID and ZCLH for LBlock and TWINE.

The rest of this paper is organized as follows. Section 2 introduces some necessary preliminaries. Section 3 introduces our new way to predict the internal differences for Feistel*-SP block ciphers. Section 4 gives upper bounds on the rounds of ID and ZCLH for the Feistel*-SP structure. Section 5 makes an application of our method to LBlock and TWINE. Finally, conclusions are drawn in Sect. 6.

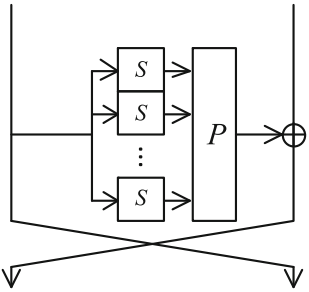


Fig. 1 Feistel structure with SP-type round function

2 Preliminaries

Let ε be a Feistel structure as shown in Fig. 1, where S is the S-box and P is the matrix of the permutation layer. **Throughout this paper, we only deal with the P which is a permutation matrix.** In [7], the characteristic matrices of ε are defined as follows.

Definition 1 ([7]) Let $(X_0, X_1, \ldots, X_{n-1})$ and $(Y_0, Y_1, \ldots, Y_{n-1})$ be the input and output of ε, respectively. The $n \times n$ encryption characteristic matrix En of ε is defined as: if Y_i is affected by X_j, then the (i, j) entry of En is set to $\mathbf{1}$; if Y_i is affected by $S(X_j)$, then the entry of En is set to $\mathbf{s}$; and the (i, j) entry is set to $\mathbf{0}$ if Y_i is not affected by X_j. Reversely, the decryption characteristic matrix of ε can be defined similarly.

According to Definition 1, we have

$$En = \begin{pmatrix} \mathbf{s} \cdot P, & I \\ I, & O \end{pmatrix} \text{ and } De = \begin{pmatrix} O, & I \\ I, & \mathbf{s} \cdot P \end{pmatrix},$$

where I and O are $\frac{n}{2} \times \frac{n}{2}$ identity and zero matrices, respectively.

Definition 2 ([7]) Let $\mathbf{\Delta} = (\Delta_0, \Delta_1, \ldots, \Delta_{n-1})$ be a difference vector. Then, the characteristic vector $\mathbf{V} = (v_0, v_1, \ldots, v_{n-1})$ corresponding to $\mathbf{\Delta}$ is defined as

$$v_i = \begin{cases} 0, & \text{if } \Delta_i = 0, \\ 1^*, & \text{if } \Delta_i \text{ is a nonzero fixed difference}, \\ 1, & \text{if } \Delta_i \text{ is a nonzero nonfixed difference}, \\ 2^*, & \text{if } \Delta_i \text{ is a difference of the form } 1 \oplus 1^*, \\ ?, & \text{if } \Delta_i \text{ is a nonfixed difference}. \end{cases}$$

In [7], the author defined the multiplication between characteristic matrices and characteristic vectors as

$$M \cdot \mathbf{V} = \left(\sum_{j=0}^{n-1} (M)_{0,j} \cdot v_j, \ldots, \sum_{j=0}^{n-1} (M)_{n-1,j} \cdot v_j \right),$$

where $(M)_{i,j}$ is the (i, j) entry of the characteristic matrix M for $0 \le i, j \le n-1$.

It can be seen that $(M)_{i,j} \cdot v_j$ represents the impact of the jth subblock input difference on the ith subblock output difference. The multiplication table of $(M)_{i,j} \cdot v_j$ is given in Table 1.

The addition $(M)_{i,j} \cdot v_j + (M)_{i,j'} \cdot v_{j'}$ represents the exclusive-or of corresponding differences, which is defined as

$$\begin{cases} 0 + v = v & \text{for } v \in \{0, 1^*, 1, 2^*, ?\}; \\ ? + v = ? & \text{for } v \in \{0, 1^*, 1, 2^*, ?\}; \\ 1^* + 1 = 2^* \text{ and } 1 + 2^* = ?. \end{cases}$$

Table 1 Multiplication table of $(M)_{i,j} \cdot v_j$ [7]

$(M)_{i,j} \cdot v_j$	Meaning
$\mathbf{0} \cdot v_j = 0$	The i-subblock output difference is not affected by the j-subblock input difference
$\mathbf{1} \cdot v_j = v_j$	The i-subblock output difference is affected by the j-subblock input difference
$\mathbf{s} \cdot v_j$	The i-subblock output difference is affected by the difference after the S-box for the j-subblock input difference
$\mathbf{s} \cdot 0 = 0$	For a zero difference, the output difference after a S-box is still zero
$\mathbf{s} \cdot 1^* = 1$ $\mathbf{s} \cdot 1 = 1$	For any nonzero difference, the output difference after a S-box will become nonzero nonfixed difference
$\mathbf{s} \cdot 2^* = ?$ $\mathbf{s} \cdot 1 = ?$	For a nonfixed difference, the output difference after a S-box is still nonfixed

Let ΔP be the input difference of ε. It is shown in [7] that the output difference of ΔP after r rounds has the following form

$$\overbrace{En \cdot (En \cdot (\cdots (En \cdot}^{r} \mathbf{V}_P))), \tag{1}$$

where $\mathbf{V}_P$ is the characteristic vector of ΔP. Thus the rth round output difference of ε can be predicted round by round based on En. The same also applies to De from the decryption direction. According to Eq. (1), the 1st round output difference can be predicted from entries of En directly. While for $r > 1$, we can not predict the rth round output difference from entries of En directly. To solve this problem, we propose an another way to predict the output difference.

3 A new way to predict the internal difference

Let M be the encryption or decryption characteristic matrix of ε throughout this section. Let $\mathbf{V} = (v_0, v_1, \ldots, v_{n-1})$ be the characteristic vector of an input difference. In this section, we will prove that

$$\overbrace{M \cdot (M \cdot (\cdots (M \cdot}^{r} \mathbf{V}))) = M^r \cdot \mathbf{V} \tag{2}$$

for $r \geq 1$. Hence, the rth round output difference can be predicted from entries of M^r directly.

In order to compute M^r, we need to define the multiplication and addition for entries of M. First, we introduce two new entries $\mathbf{1} + \mathbf{s}$ and $2\mathbf{s}$. For $v \in \{0, 1^*, 1, 2^*, ?\}$, set $(\mathbf{1} + \mathbf{s}) \cdot v = 0$ and $(2\mathbf{s}) \cdot v = 0$ if $v = 0$; set $(\mathbf{1} + \mathbf{s}) \cdot 1^* = 2^*$ and $(2\mathbf{s}) \cdot 1^* = ?$ if $v = 1^*$; otherwise, set $(\mathbf{1} + \mathbf{s}) \cdot v = ?$ and $(2\mathbf{s}) \cdot v = ?$. Then, the multiplication and addition for elements in $\{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1} + \mathbf{s}, 2\mathbf{s}\}$ are given as follows.

– **Multiplication**

  – Set $\mathbf{0} \cdot x = \mathbf{0}$ for $x \in \{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$, since $\mathbf{0} \cdot (x \cdot v) = \mathbf{0} \cdot v$, where v is an arbitray element of $\{0, 1^*, 1, 2^*, ?\}$.
  – Set $\mathbf{1} \cdot x = x$ for $x \in \{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$, since $\mathbf{1} \cdot (x \cdot v) = x \cdot v$.
  – Set $\mathbf{s} \cdot \mathbf{0} = \mathbf{0}$, since $\mathbf{s} \cdot (\mathbf{0} \cdot v) = \mathbf{0} \cdot v$; set $\mathbf{s} \cdot x = \mathbf{s}$ for $x = \mathbf{1}$ or $\mathbf{s}$, since $\mathbf{s} \cdot (x \cdot v) = \mathbf{s} \cdot v$ when $x = \mathbf{1}$ or $\mathbf{s}$; set $\mathbf{s} \cdot x = 2\mathbf{s}$ for $x = \mathbf{1}+\mathbf{s}$ or $2\mathbf{s}$, since $\mathbf{s} \cdot (x \cdot v) = (2\mathbf{s}) \cdot v$ when $x = \mathbf{1}+\mathbf{s}$ or $2\mathbf{s}$.

Note that cases "$(\mathbf{1}+\mathbf{s}) \cdot x$" and "$(2\mathbf{s}) \cdot x$" will not appear in $M \cdot M^i$, thus definitions of "$(\mathbf{1}+\mathbf{s}) \cdot x$" and "$(2\mathbf{s}) \cdot x$" are omitted.

– **Addition**

  – Set $\mathbf{0}+x = x+\mathbf{0} = x$ for $x \in \{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$, since $\mathbf{0} \cdot v + x \cdot v = x \cdot v + \mathbf{0} \cdot v = x \cdot v$.
  – Set $\mathbf{1}+\mathbf{1} = 0$, since $\mathbf{1} \cdot v + \mathbf{1} \cdot v = 0$; by the definition of $\mathbf{1}+\mathbf{s}$, we have $\mathbf{1}+\mathbf{s} = \mathbf{s}+\mathbf{1}$; set $\mathbf{1}+(\mathbf{1}+\mathbf{s}) = (\mathbf{s}+\mathbf{1})+\mathbf{1} = \mathbf{s}$, since $\mathbf{1} \cdot v + (\mathbf{1}+\mathbf{s}) \cdot v = (\mathbf{s}+\mathbf{1}) \cdot v + \mathbf{1} \cdot v = \mathbf{s} \cdot v$; set $\mathbf{1}+2\mathbf{s} = 2\mathbf{s}+\mathbf{1} = 2\mathbf{s}$, since $\mathbf{1} \cdot v + (2\mathbf{s}) \cdot v = (2\mathbf{s}) \cdot v + \mathbf{1} \cdot v = (2\mathbf{s}) \cdot v$.
  – Set $x+y = y+x = 2\mathbf{s}$ for $x, y \in \{\mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$, since $x \cdot v + y \cdot v = y \cdot v + x \cdot v = (2\mathbf{s}) \cdot v$ for $x, y \in \{\mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$.

It can be seen that the set $\{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$ is closed under the operations of multiplication and addition. Thus M^r is still a matrix over $\{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$. Based on these definitions, we give some properties that are needed to prove our conclusion.

Corollary 1 *If $x_0 \in \{\mathbf{0}, \mathbf{1}, \mathbf{s}\}$ and $x_1 \in \{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$, we have $x_0 \cdot (x_1 \cdot v) = (x_0 \cdot x_1) \cdot v$ for $v \in \{0, 1^*, 1, 2^*, ?\}$. If $x_0, x_1 \in \{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$, we have $x_0 \cdot v + x_1 \cdot v = (x_0 + x_1) \cdot v$ for $v \in \{0, 1^*, 1, 2^*, ?\}$.*

Lemma 1 *Let $x_0 \in \{\mathbf{0}, \mathbf{1}, \mathbf{s}\}$ and $x_1, x_2 \in \{\mathbf{0}, \mathbf{1}, \mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$. If $(x_1, x_2) \neq (\mathbf{1}, \mathbf{1})$, $(\mathbf{1}, \mathbf{1}+\mathbf{s})$ and $(\mathbf{1}+\mathbf{s}, \mathbf{1})$, then we have*

$$x_0 \cdot (x_1 \cdot v_1 + x_2 \cdot v_2) = (x_0 \cdot x_1) \cdot v_1 + (x_0 \cdot x_2) \cdot v_2$$

for $v_1, v_2 \in \{0, 1^*, 1, 2^*, ?\}$.

Proof When $x_0 \in \{\mathbf{0}, \mathbf{1}\}$, the conclusion is obvious. Thus, we only need to prove this lemma for $x_0 = \mathbf{s}$.

Case 1 x_1 or x_2 equals to $\mathbf{0}$. Without loss of generality, we set $t_1 = 0$. Then we have $x_0 \cdot (x_1 \cdot v_1 + x_2 \cdot v_2) = \mathbf{s} \cdot (x_2 \cdot v_2)$ and $(x_0 \cdot x_1) \cdot v_1 + (x_0 \cdot x_2) \cdot v_2 = (\mathbf{s} \cdot x_2) \cdot v_2$. According to Corollary 1, we have $\mathbf{s} \cdot (x_2 \cdot v_2) = (\mathbf{s} \cdot x_2) \cdot v_2$.

Case 2 x_1 or x_2 equals to $\mathbf{1}$. Without loss of generality, we can set $x_1 = \mathbf{1}$. Since $(x_1, x_2) \neq (\mathbf{1}, \mathbf{1})$ and $(\mathbf{1}, \mathbf{1}+\mathbf{s})$, x_2 should be $\mathbf{s}$ or $2\mathbf{s}$. If $x_2 = \mathbf{s}$, then we have $x_0 \cdot (x_1 \cdot v_1 + x_2 \cdot v_2) = \mathbf{s} \cdot (v_1 + \mathbf{s} \cdot v_2)$ and $(x_0 \cdot x_1) \cdot v_1 + (x_0 \cdot x_2) \cdot v_2 = \mathbf{s} \cdot v_1 + \mathbf{s} \cdot v_2$. Since

$$\mathbf{s} \cdot (v_1 + \mathbf{s} \cdot v_2) = \begin{cases} \mathbf{s} \cdot v_2, & \text{if } v_1 = 0, \\ \mathbf{s} \cdot v_1, & \text{if } v_2 = 0, \\ ?, & \text{if } v_1 \neq 0 \text{ and } v_2 \neq 0. \end{cases}$$

and

$$\mathbf{s} \cdot v_1 + \mathbf{s} \cdot v_2 = \begin{cases} \mathbf{s} \cdot v_2, & \text{if } v_1 = 0, \\ \mathbf{s} \cdot v_1, & \text{if } v_2 = 0, \\ ?, & \text{if } v_1 \neq 0 \text{ and } v_2 \neq 0. \end{cases} \quad (3)$$

we have $\mathbf{s}\cdot(v_1+\mathbf{s}\cdot v_2)=\mathbf{s}\cdot v_1+\mathbf{s}\cdot v_2$. If $x_2=2\mathbf{s}$, then $\mathbf{s}\cdot(v_1+x_2\cdot v_2)=\mathbf{s}\cdot(v_1+2\mathbf{s}\cdot v_2)$ and $\mathbf{s}\cdot v_1+(\mathbf{s}\cdot 2\mathbf{s})\cdot v_2=\mathbf{s}\cdot v_1+2\mathbf{s}\cdot v_2$. Since

$$\mathbf{s}\cdot(v_1+2\mathbf{s}\cdot v_2)=\begin{cases}\mathbf{s}\cdot v_1, & \text{if } v_2=0,\\ ?, & \text{if } v_2\neq 0.\end{cases}$$

and

$$\mathbf{s}\cdot v_1+2\mathbf{s}\cdot v_2=\begin{cases}\mathbf{s}\cdot v_1, & \text{if } v_2=0,\\ ?, & \text{if } v_2\neq 0.\end{cases}$$

equation $\mathbf{s}\cdot(v_1+2\mathbf{s}\cdot v_2)=\mathbf{s}\cdot v_1+2\mathbf{s}\cdot v_2$ holds.

Case 3 $x_1=\mathbf{s}$ or $x_2=\mathbf{s}$. Without loss of generality, we can set $x_1=\mathbf{s}$. If $x_2=\mathbf{s}$, then we have $\mathbf{s}\cdot(x_1\cdot v_1+x_2\cdot v_2)=\mathbf{s}\cdot(\mathbf{s}\cdot v_1+\mathbf{s}\cdot v_2)$ and $(\mathbf{s}\cdot x_1)\cdot v_1+(\mathbf{s}\cdot x_2)\cdot v_2=\mathbf{s}\cdot x_1+\mathbf{s}\cdot x_2$. Note that

$$\mathbf{s}\cdot(\mathbf{s}\cdot v_1+\mathbf{s}\cdot v_2)=\begin{cases}\mathbf{s}\cdot v_2, & \text{if } v_1=0,\\ \mathbf{s}\cdot v_1, & \text{if } v_2=0,\\ ?, & \text{if } v_1\neq 0 \text{ and } v_2\neq 0,\end{cases}$$

combined with Eq. (3), we have $\mathbf{s}\cdot(\mathbf{s}\cdot v_1+\mathbf{s}\cdot v_2)=\mathbf{s}\cdot v_1+\mathbf{s}\cdot v_2$. If $x_2=\mathbf{1}+\mathbf{s}$ or $2\mathbf{s}$, then we have

$$\mathbf{s}\cdot(\mathbf{s}\cdot v_1+x_2\cdot v_2)=\begin{cases}\mathbf{s}\cdot v_1, & \text{if } v_2=0,\\ ?, & \text{if } v_2\neq 0.\end{cases}$$

For $\mathbf{s}\cdot v_1+(\mathbf{s}\cdot x_2)\cdot v_2$, we have the same conclusion, which implies $\mathbf{s}\cdot(\mathbf{s}\cdot v_1+x_2\cdot v_2)=\mathbf{s}\cdot v_1+(\mathbf{s}\cdot x_2)\cdot v_2$.

Case 4 When $x_1, x_2\in\{\mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$, we have

$$\mathbf{s}\cdot(x_1\cdot v_1+x_2\cdot v_2)=\begin{cases}0, & \text{if } v_1=v_2=0\\ ?, & \text{otherwise.}\end{cases}$$

It can be verified that $(\mathbf{s}\cdot x_1)\cdot v_1+(\mathbf{s}\cdot x_2)\cdot v_2$ has the same result. Thus, we have $\mathbf{s}\cdot(x_1\cdot v_1+x_2\cdot v_2)=(\mathbf{s}\cdot x_1)\cdot v_1+(\mathbf{s}\cdot x_2)\cdot v_2$ for $x_1, x_2\in\{\mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$. □

Remark 1 Since for the following conclusions, their proofs for $M=En$ are similar with that for $M=De$, we only give their proofs for $M=En$.

Lemma 2 *Let x_1 and x_2 be any two elements in the ith row of M^t for $1\le i\le n$ and $t\ge 1$. Then (x_1, x_2) can not equal to $(\mathbf{1},\mathbf{1})$, $(\mathbf{1},\mathbf{1}+\mathbf{s})$ or $(\mathbf{1}+\mathbf{s},\mathbf{1})$.*

Proof We prove this lemma by mathematical induction on t. If $t=1$, then $x_1\ x_2$ are two elements in the ith row of M, and thus this lemma can be gotten immediately. Assume this result is true for $t<r$. Next we prove this result for $t=r$. When $t=r$, we have $M^r=M\cdot M^{r-1}$. Let

$$M^{r-1}=\begin{pmatrix}M_0, & M_1\\ M_2, & M_3\end{pmatrix}.$$

Then

$$M^r=\begin{pmatrix}s\cdot P, & I\\ I, & O\end{pmatrix}\cdot\begin{pmatrix}M_0, & M_1\\ M_2, & M_3\end{pmatrix}=\begin{pmatrix}M_0^{'}+M_2, & M_1^{'}+M_3\\ M_0, & M_1\end{pmatrix}.$$

where $M_0^{'}=\mathbf{s}\cdot P\cdot M_0$ and $M_1^{'}=\mathbf{s}\cdot P\cdot M_1$. Since $\mathbf{s}\cdot x\in\{\mathbf{0},\mathbf{s},2\mathbf{s}\}$ for $x\in\{\mathbf{0},\mathbf{1},\mathbf{s},\mathbf{1}+\mathbf{s},2\mathbf{s}\}$, all entries of $M_0^{'}$ and $M_1^{'}$ belong to $\{\mathbf{0},\mathbf{s},2\mathbf{s}\}$. For any $0\le j_0\le\frac{n-1}{2}<j_1\le n-1$ and $0\le i\le n/2-1$, we have

$$\begin{cases}(M^r)_{i,j_0}=\left(M_0^{'}\right)_{i,j_0}+(M_2)_{i,j_0}\\ (M^r)_{i,j_1}=\left(M_1^{'}\right)_{i,j_1}+(M_3)_{i,j_1}\end{cases}.$$

Since $((M_2)_{i,j_0}, (M_3)_{i,j_1}) \neq (\mathbf{1}, \mathbf{1})$, $(\mathbf{1}, \mathbf{1}+\mathbf{s})$ or $(\mathbf{1}+\mathbf{s}, \mathbf{1})$ by assumption and $(M_0^{'})_{i,j_0}$, $(M_0^{'})_{i,j_0} \in \{\mathbf{0}, \mathbf{s}, 2\mathbf{s}\}$, we have $((M^r)_{i,j_0}, (M^r)_{i,j_1}) \neq (\mathbf{1}, \mathbf{1})$, $(\mathbf{1}, \mathbf{1}+\mathbf{s})$ or $(\mathbf{1}+\mathbf{s}, \mathbf{1})$. For $0 \leq j_0 < j_1 \leq \frac{n-1}{2}$ or $\frac{n+1}{2} \leq j_0 < j_1 \leq n-1$, we have similar conclusions. Thus pairs $(\mathbf{1}, \mathbf{1})$, $(\mathbf{1}, \mathbf{1}+\mathbf{s})$ and $(\mathbf{1}+\mathbf{s}, \mathbf{1})$ do not appear in the ith row of M^r for $0 \leq i \leq \frac{n-1}{2}$. □

Lemma 3 *The equation $M \cdot (M^t \cdot \mathbf{V}) = (M \cdot M^t) \cdot \mathbf{V}$ holds for $t \geq 1$.*

Proof Let $M = \left(a_{i,j}\right)_{n\times n}$ and $M^t = \left(b_{i,j}\right)_{n\times n}$. Since

$$M^t \cdot \mathbf{V} = \left(\sum_{j=0}^{n-1} b_{0,j} \cdot v_j, \ldots, \sum_{j=0}^{n-1} b_{n-1,j} \cdot v_j\right),$$

we have

$$M \cdot (M^t \cdot \mathbf{V}_P) = \left(\sum_{m=0}^{n-1} a_{0,m} \cdot u_m, \ldots, \sum_{m=0}^{n-1} a_{n-1,m} \cdot u_m\right), \tag{4}$$

where $u_m = \sum_{j=0}^{n-1} b_{m,j} \cdot v_j$ for $0 \leq m \leq n-1$. On one hand, by Corollary 1, Lemmas 1 and 2, we have

$$\begin{aligned}\sum_{m=0}^{n-1} a_{k,m} \cdot u_m &= \sum_{m=0}^{n-1} a_{k,m} \cdot \left(\sum_{j=0}^{n-1} b_{m,j} \cdot v_j\right) \\ &= \sum_{m=0}^{n-1}\sum_{j=0}^{n-1} (a_{k,m} \cdot b_{m,j}) \cdot v_j \\ &= \sum_{j=0}^{n-1} \left(\sum_{m=0}^{n-1} a_{k,m} \cdot b_{m,j}\right) \cdot v_j. \end{aligned} \tag{5}$$

On the other hand, we have

$$\begin{aligned}(M \cdot M^t) \cdot \mathbf{V} &= \left(\sum_{m=0}^{n-1} a_{k,m} \cdot b_{m,j}\right)_{n\times n} \cdot \mathbf{V} \\ &= \left(\sum_{j=0}^{n-1} \left(\sum_{m=0}^{n-1} a_{0,m} \cdot b_{m,j}\right) \cdot v_j, \ldots, \sum_{j=0}^{n-1} \left(\sum_{m=0}^{n-1} a_{n-1,m} \cdot b_{m,j}\right) \cdot v_j\right). \end{aligned} \tag{6}$$

By Eqs. (4), (5) and (6), this lemma is gotten. □

By Lemma 3, we know that Eq. (2) holds. Notice that when r is big enough, there will be no entries "$\mathbf{0}$" and "$\mathbf{1}$" in M^t. We denote the minimum integer t, such that there are no entries "$\mathbf{0}$" and "$\mathbf{1}$" in M^t, as the **diffusion order** of M, represented by $R(M)$. Then we present some properties that are relevant to the diffusion order.

Corollary 2 *If $r = R(M)$, then we have*

$$\left(M^r \cdot \mathbf{V}\right)_i = 1, 2^*\ or\ ?$$

for $0 \leq i \leq n-1$, where $(M^r \cdot \mathbf{V})_i$ represents the ith entry of vector $(M^r \cdot \mathbf{V})_i$. If $r = R(M)+1$, then we have

$$\begin{cases} (M^r \cdot \mathbf{V})_i = ?\ and\ (M^r \cdot \mathbf{V})_{i+n/2-1} = 1, 2^*\ or\ ?\ when\ M = En, \\ (M^r \cdot \mathbf{V})_{i+n/2-1} = ?\ and\ (M^r \cdot \mathbf{V})_i = 1, 2^*\ or\ ?\ when\ M = De \end{cases}$$

for $0 \le i \le n/2-1$. *If* $r > R(M)+1$, *then we have*

$$\left(M^r \cdot \mathbf{V}\right)_i = ?$$

for $0 \le i \le n-1$.

Proof Since $\mathbf{V}$ is nonzero, there must be a nonzero entry in $\mathbf{V}$. Without loss of generality, we assume v_j is nonzero, i.e. $v_j = 1$ or 1^*. When $r = R(M)$, we know that there are no entries "$\mathbf{0}$" and "$\mathbf{1}$" in M^r. Thus, we have $(M^r)_{i,j} = \mathbf{s}, \mathbf{1}+\mathbf{s}$ or $2\mathbf{s}$ for $0 \le i \le n-1$. Since $v_j = 1$ or 1^*, we have $(M^r)_{i,j} \cdot v_j = 1, 2^*$, or ?, which implies that $(M^r \cdot \mathbf{V})_i = 1, 2^*$ or ?.

When $r = R(M)+1$, we know that

$$\begin{cases} (M^r \cdot \mathbf{V})_i = \mathbf{s} \cdot (M^{r-1} \cdot \mathbf{V})_{P_t^{-1}(i)} + \left(M^{r-1} \cdot \mathbf{V}\right)_{i+n/2-1} \\ (M^r \cdot \mathbf{V})_{i+n/2-1} = \left(M^{r-1} \cdot \mathbf{V}\right)_i \end{cases}$$

for $0 \le i \le n/2-1$, where P_t is the permutation on $\{0, 1, \ldots, n/2-1\}$ induced by matrix P. Note that $\left(M^{r-1} \cdot \mathbf{V}\right)_j = 1, 2^*$ or ? for $0 \le j \le n-1$. Thus, we have $(M^r \cdot \mathbf{V})_i = ?$ and $(M^r \cdot \mathbf{V})_{i+n/2-1} = 1, 2^*$ or ? for $0 \le i \le n/2-1$.

The case for $r > R(M)+1$ can be proved similarly with the case that $r = R(M)+1$.

□

4 Upper bounds on the rounds of ID and ZCLH for ε

In this section, we first introduce Wu and Wang's method which aims to searching ID. Then we give upper bounds on the rounds of ID and ZCLH.

4.1 Wu and Wang's method

In [16], Wu and Wang introduced the *difference propagation system*, which describes the difference propagation behavior for a block cipher. For a Feistel cipher, let $\Delta X_{i-1} = (\Delta X_{i-1,j})_{0 \le j \le n/2-1}$ and $\Delta X_i = (\Delta X_{i,j})_{0 \le j \le n/2-1}$ respectively represent the left and the right branch input difference of the ith round. Then the difference propagation system can be built as:

$$\begin{cases} S(\Delta X_{i,j}) \oplus \Delta Y_{i,j} = 0 & \text{for } 1 \le i \le r \text{ and } 0 \le j \le n/2-1, \\ P \cdot \Delta Y_i^T \oplus \Delta X_{i-1} \oplus \Delta X_i = 0 & \text{for } 1 \le i \le r. \end{cases} \tag{7}$$

where $\Delta Y_i = (\Delta Y_{i,j})_{0 \le j \le n/2-1}$ is the output difference of ΔX_i after the S-boxes. This system can be further divided into two subsystems: $\mathcal{L}$ and $\mathcal{NL}$, where $\mathcal{L}$ includes all linear equations and $\mathcal{NL}$ includes all nonlinear equations.

Based on the difference proposition system, Wu and Wang introduced an algorithm to search ID for Feistel ciphers. Throughout this paper, we call this algorithm as WW-algorithm. The idea of this algorithm is simple: given the plaintext and ciphertext differences, the internal differences can be predicted based on system (7), and some new "known" variables can be gotten. Then based on these known variables, the algorithm can continue predict new information. This progress will terminate if a contradiction is detected or no new information is gotten.

Then we introduce that how does the algorithm predict information from the difference proposition system.

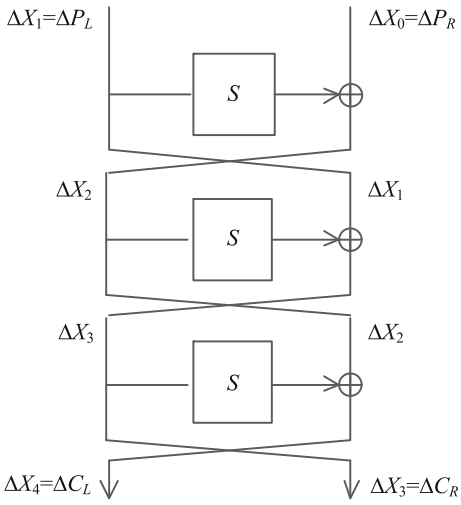


Fig. 2 3-round Feistel structure

Lemma 4 ([16]) *Suppose $\mathcal{L}$ has solutions and $\mathcal{L}'$ is the reduced augmented matrix of $\mathcal{L}$, then*

(1) *If an affine equation with only one variable, i.e., $\Delta X \oplus c = 0$ (c is a constant), is found in $\mathcal{L}'$, then $\Delta X \neq 0$ if and only if $c \neq 0$.*
(2) *If a linear equation with two variables, i.e., $\Delta X \oplus \Delta Y = 0$, is found in $\mathcal{L}'$, then $\Delta X \neq 0$ if and only if $\Delta Y \neq 0$.*

Lemma 5 ([16]) *Suppose S is a bijective S-box. For an equation $S(\Delta X) \oplus \Delta Y = 0$, ΔX is zero (resp. nonzero) if and only if ΔY is zero (resp. nonzero).*

Based on the above principles, the *WW*-algorithm can predict the internal differences when the plaintext and ciphertext differences are given. Throughout this paper, let ΔP and ΔC represent the plaintext and the ciphertext difference, respectively. Denote $\Delta P = \Delta P_L || \Delta P_R$ (resp. $\Delta C = \Delta C_L || \Delta C_R$), then the difference ΔX_2 in Fig. 2 can be computed by $\Delta X_2 = S(\Delta P_L) \oplus \Delta P_R$ (resp. $\Delta X_2 = S(\Delta C_R) \oplus \Delta C_L$). This means that the difference ΔX_2 can be gotten merely from ΔP (resp. ΔC). Besides, since $\Delta X_2 = S^{-1}(\Delta P_L \oplus \Delta C_R)$, then the difference ΔX_2 can also be gotten from ΔP combined with ΔC. Based on these observations, we divide the information gotten from *WW*-algorithm into three classes: the *first class information* represented by $\mathcal{A}$ is the information gotten from ΔP; the *second class information* represented by $\mathcal{B}$ is the information gotten from ΔC; while the *third class information* represented by $\mathcal{C}$ is the information gotten from ΔP combined with ΔC. From Lemmas 4 and 5, we can get that the elements in $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ have the difference forms 0, 1* or 1.

Then two conditions are given in [16] to judge whether there is a contradiction for the differential $\Delta P \rightarrow \Delta C$.

Proposition 1 ([16]) *For an r-round Feistel cipher, differential $\Delta P \rightarrow \Delta C$ is an impossible differential if one of the following two situations happens:*

(i) *System $\mathcal{L}$ has no solution, i.e., the rank of its coefficient matrix is not equal to the rank of its augment matrix.*
(ii) *There exists a variable of system (7) with both zero and nonzero values.*

In [11], Sun et. al. proved that the *WW*-algorithm can find all truncated impossible differentials for Feistel-*SP* blocks, and so we have

Corollary 3 *Differential $\Delta P \to \Delta C$ is an ID of a Feistel-SP structure if and only if one of the two conditions in Proposition 1 holds.*

Based on the above theories, we give uppers bound on the rounds of ID and ZCLH for ε.

4.2 Upper bounds on the rounds of ID and ZCLH

4.2.1 Upper bound for ID

Theorem 1 *If $r \geq R(En) + R(De) + 1$, then there does not exist r-round ID for ε.*

Before proving this theorem, we still need some other properties.

Lemma 6 *The following two conditions are equivalent.*

(1) *Differential $\Delta P \to \Delta C$ is an r-round ID of ε;*
(2) *There exists an variable $\Delta X_{i,j}$ in the difference proposition system such that $\Delta X_{i,j}$ has two unequal values.*

Proof "(1)→(2)". By Corollary 3, we know that $\Delta P \to \Delta C$ is an ID if and only if one of the two situations in Proposition 1 happens.

For situation (*ii*), there is an variable with both zero and nonzero values. If the variable is some $\Delta X_{i,j}$, then this lemma is obvious. If the variable is some $\Delta Y_{i,j}$, then $\Delta X_{i,j}$ is also an variable with both zero and nonzero values since $S(\Delta X_{i,j}) = \Delta Y_{i,j}$.

For situation (*i*), if we fix the order of all variables in system (7) as

$$x = \left[\Delta X_0, \Delta X_1, \Delta X_2, \Delta X_3, \ldots, \Delta X_r, \Delta X_{r+1}, \Delta Y_1, \ldots, \Delta Y_r\right],$$

then the linear system $\mathcal{L}$ can be represented as $A \cdot x^T = 0$, where

$$A = \begin{bmatrix} I & O & I & O & \cdots & O & O & O & P & O & \cdots & O \\ O & I & O & I & \cdots & O & O & O & O & P & \cdots & O \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ O & O & O & O & \cdots & I & O & I & O & O & \cdots & P \end{bmatrix}.$$

Since that P is a permutation matrix, any two equations in $\mathcal{L}$ have at most one common term, which is some $\Delta X_{i,j}$. Hence we know that if each linear equation of $\mathcal{L}$ has two unknown variables, then the equations in $\mathcal{L}$ are linearly independent, i.e., system $\mathcal{L}$ has solutions. Moving all known variables to the right of the equation. Thus if system $\mathcal{L}$ has no solution, then there exist two rows such that $\Delta X_{i,j} = u_0$ and $\Delta X_{i,j} = u_1$ with $u_0 \neq u_1$.

(2)→(1). Obviously. □

Lemma 7 *Let u_0 and u_1 be the two unequal values of $\Delta X_{i,j}$ in Lemma 6. Then the pair (u_0, u_1) can not confirm to the following forms*

$$\begin{cases} (?, x) \text{ or } (x, ?), & \text{where } x \in \{0, 1^*, 1, 2^*, ?\}, \\ (1, x) \text{ or } (x, 1), & \text{where } x \in \{1^*, 1, 2^*\}, \\ (2^*, x) \text{ or } (x, 2^*), & \text{where } x \in \{0, 2^*\}. \end{cases}$$

Proof Note that ? represents a non-fixed difference, thus if difference $\Delta X_{i,j}$ confirms to ?, then $\Delta X_{i,j}$ can assume any of the 2^b values, where b is the bit number of $\Delta X_{i,j}$. Thus, if u_0 or u_1 confirms to ?, then u_0 will equal to u_1 with a positive probability. Similarly, if one

of u_0 and u_1 confirms to 1 and the other one is not the zero difference, then u_0 will equal to u_1 with a positive probability. If u_0 or u_1 confirms to 2^*, without loss of generality assume u_0 confirms to 2^*. Then u_0 can be disposed as $u_0 = u_0' \oplus \Delta$, where u_0' is a nonzero fixed difference and Δ is a nonzero non-fixed difference. Thus, u_0 can equal to any value except u_0'. Thus, if u_1 confirms to 0 or 2^*, then u_0 will equal to u_1 with a positive probability. □

Next we present some properties about the internal differences based on the characteristic matrices.

Lemma 8 *Let $\mathbf{V}_p$ and $\mathbf{V}_c$ be the characteristic vectors of ΔP and ΔC, respectively. If the value of $\Delta X_{i,j} (0 \le i \le r, 0 \le j \le n/2-1)$ is gotten from ΔP (resp. ΔC), then the value of $\Delta X_{i,j}$ confirms to $(En^i \cdot \mathbf{V}_p)_{j+n/2-1}$(resp. $(De^{r-i} \cdot \mathbf{V}_c)_{j+n/2-1}$).*

Proof If the value of $\Delta X_{i,j}$ is gotten from ΔP (resp. ΔC), then $\Delta X_{i,j}$ can be seen as the output difference of ΔP (resp. ΔC) after i (resp. $r-i$) rounds encryption (resp. decryption). Thus by the analysis of Sect. 3, we know that the value of $\Delta X_{i,j}$ confirms to $(En^i \cdot \mathbf{V}_p)_j$ (resp. $(De^{r-i} \cdot \mathbf{V}_c)_j$). □

Lemma 9 *The third class information $\mathcal{C}$ is empty if $r \ge R(En) + R(De) + 1$.*

Proof We prove this lemma by negative approach. Assuming that $\mathcal{C}$ is nonempty, then we will show that there always exists a contradiction. Since $\mathcal{C}$ is nonempty, there exist an element v in the $\mathcal{C}$, which is gotten before all the other elements in $\mathcal{C}$. Without loss of generality, we set that v indicates the difference value of $\Delta X_{i,j}$.

Replacing $\Delta Y_{i,j}$ by $S(\Delta X_{i,j})$ in system (7), then there are only three equations containing $\Delta X_{i,j}$, which are

$$\begin{aligned}
&\text{(i) } S(\Delta X_{i-1,P_t^{-1}(j)}) \oplus \Delta X_{i-2,j} \oplus \Delta X_{i,j} = 0,\\
&\text{(ii) } S(\Delta X_{i,j}) \oplus \Delta X_{i-1,P_t(j)} \oplus \Delta X_{i+1,P_t(j)} = 0,\\
&\text{(iii) } S(\Delta X_{i+1,P_t^{-1}(j)}) \oplus \Delta X_{i,j} \oplus \Delta X_{i+2,j} = 0.
\end{aligned}$$

We can see the information of $\Delta X_{i,j}$ must be predicted through one of the three equations.

If the information is predicted through equation (i), then variables $\Delta X_{i-1,P_t^{-1}(j)}$ and $\Delta X_{i-2,j}$ must be known before $\Delta X_{i,j}$. Let $v_{i-1,P_t^{-1}(j)}$ and $v_{i-2,j}$ respectively be difference values of $\Delta X_{i-1,P_t^{-1}(j)}$ and $\Delta X_{i-2,j}$ gotten by the *WW*-algorithm. Note that v is gotten before all the other element in $\mathcal{C}$, thus we have

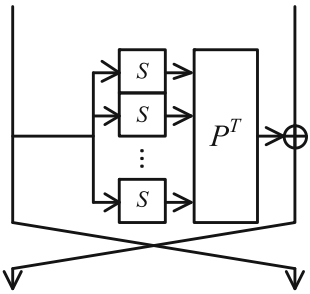
$$\begin{aligned}
&v_{i-1,P_t^{-1}(j)} \in \mathcal{A}, v_{i-2,j} \in \mathcal{B}, \text{ or}\\
&v_{i-1,P_t^{-1}(j)} \in \mathcal{B}, v_{i-2,j} \in \mathcal{A}.
\end{aligned}$$

If $v_{i-1,P_t^{-1}(j)} \in \mathcal{A}, v_{i-2,j} \in \mathcal{B}$, then $v_{i-1,P_t^{-1}(j)}$ and $v_{i-1,j}$ confirms to $\left(En^{i-1} \cdot \mathbf{V}_p\right)_{P_t^{-1}(j)+n/2-1}$ and $\left(De^{r-i+2} \cdot \mathbf{V}_c\right)_{j+n/2-1}$, respectively, by Lemma 8. As $r \ge R(En)+R(De)+1$, if $i-1 \le R(En)+1$ then $r-i+2 \ge R(De)+1$. By Corollary 2, we know that $v_{i-2,j}$ confirms to ?, which contradicts with that $v_{i-2,j} \in \mathcal{B}$. If $i-1 \ge R(En)+2$, then we have $v_{i-1,P_t^{-1}(j)}$ confirms to ? by Corollary 2, which contradicts with that $v_{i-1,P_t^{-1}(j)} \in \mathcal{A}$.

If $v_{i-1,P_t^{-1}(j)} \in \mathcal{B}, v_{i-2,j} \in \mathcal{A}$, then $v_{i-1,P_t^{-1}(j)}$ and $v_{i-2,j}$ confirm to $\left(De^{r-i+1} \cdot \mathbf{V}_c\right)_{P_t^{-1}(j)+n/2+1}$ and $\left(En^{i-2} \cdot \mathbf{V}_p\right)_{j+n/2-1}$, respectively. If $i-2 \le R(En)-1$, then $r-i+1 \ge R(De)+1$ and $v_{i-1,P_t^{-1}(j)}$ confirms to ? by Corollary 2. It contradicts with that $v_{i-1,P_t^{-1}(j)} \in \mathcal{B}$. If $i-2 = R(En)$, then $r-i+1 \ge R(De)$. By Corollary 2, we know that $v_{i-1,P_t^{-1}(j)}$ and $v_{i-2,j}$ confirm to 1, 2^* or ?. Since

$$\Delta X_{i,j} = S(\Delta X_{i-1,P_t^{-1}(j)}) \oplus \Delta X_{i-2,j}, \tag{8}$$

Fig. 3 Dual structure of ε



we have v confirms to ?, which contradicts with that $v \in \mathcal{C}$. If $i-2 = R(En)+1$, then $r-i+1 \geq R(De)-1$. On one hand, we have $\left(En^{i-2} \cdot \mathbf{V}_p\right)_{j+n/2-1} = 1, 2^*$ or ?. On the other hand, note that $\left(De^{r-i+1} \cdot \mathbf{V}_c\right)_{P_t^{-1}(j)+n/2+1} = \left(De^{r-i+2} \cdot \mathbf{V}_c\right)_{P_t^{-1}(j)}$ and $r-i+2 \geq R(De)$, we have $\left(De^{r-i+1} \cdot \mathbf{V}_c\right)_{P_t^{-1}(j)+n/2+1} = 1, 2^*$ or ?. By Eq. (8), we have v confirms to ?, which contradicts with that $v \in \mathcal{C}$. If $i-2 \geq R(En)+2$, then $v_{i-2,j}$ confirms to ?, which contradicts with that $v_{i-1,P_t^{-1}(j)} \in \mathcal{A}$.

When the information of $\Delta X_{i,j}$ is gotten from equation (i) or (ii), we have the similar proofs. Thus the assumption that $\mathcal{C}$ is nonempty is invalid. □

By the proof of Lemma 9, we can see that the internal differences gotten from ΔP together with ΔC confirm to the form ? when $r \geq R(En)+R(De)+1$. Then we give the proof of Theorem 1.

Proof (Proof of Theorem 1) We prove this theorem by negative approach. Assuming that $\Delta P \rightarrow \Delta C$ be an r-round ID of ε^r. By Lemma 6, we know that there exists an variable $\Delta X_{i,j}$ with two unequal values. By Lemmas 7 and 9, these two values must come from ΔP and ΔC, respectively. On one hand, we have that the two values can not confirm to the forms given in Lemma 7.

On the other hand, we have that the two values of $\Delta X_{i,j}$ should confirm to $(En^i \cdot \mathbf{V}_P)_{n/2+j}$ and $(De^{r-i} \cdot \mathbf{V}_C)_{n/2+j}$, respectively. If $i > m+1$, we have $(En^i \cdot \mathbf{V}_P)_{n/2+j} =$? by Corollary 1. If $i = m+1$, then $r-i \geq m$, which implies that $(En^i \cdot \mathbf{V}_P)_{n/2+j} = 1, 2^*$ or ? and $(De^{r-i} \cdot \mathbf{V}_C)_{n/2+j} = 1, 2^*$ or ? by Corollary 1. If $i \leq m$, then we have $r-i \geq m+1$ and $(De^{r-i} \cdot \mathbf{V}_C)_{n/2+j} =$?. It can be seen that the two unequal values of $\Delta X_{i,j}$ confirm to forms given in Lemma 7, which implies a contradiction. Thus, there is no r-round ID for ε if $r \geq R(En)+R(De)+1$. □

4.2.2 Upper bound for ZCLH

In [11], Sun *et al.* gave the definition of dual structure for the Feistel structure.

Definition 3 ([11]) Let $\mathcal{F}_{SP}$ be a Feistel structure with SP-type round function. Let σ be the operation that exchanges the left and right halves of a state. Then the dual structure $\mathcal{F}_{SP}^{\perp}$ of $\mathcal{F}_{SP}$ is defined as $\sigma \circ \mathcal{F}_{P^T S} \circ \sigma$.

It can be verified that if P is a permutation matrix, then $\mathcal{F}_{P^T S}$ is equivalent to $\mathcal{F}_{SP^T}$. Thus the dual structure of ε can be represented by the structure $\varepsilon^{\perp}$ in Fig. 3. Based on the dual structure, Sun *et al.* proved the following theorem.

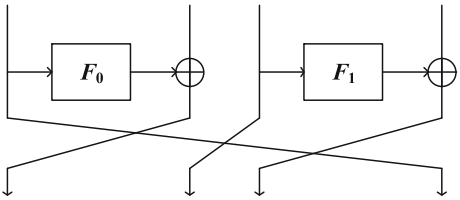


Fig. 4 Type-2 generalized Feistel structure

Theorem 2 ([11]) *$a \to b$ is an r-round ID of $\mathcal{F}_{SP}$ if and only if it is an r-round ZCLH of $\mathcal{F}_{SP}^{\perp}$.*

So we know that searching ZCLH of ε is equivalent to searching ID of $\varepsilon^{\perp}$. Then based on the theories of Sect. 4.2.1, the upper bound on the rounds of ZCLH for ε can be gotten.

4.2.3 Extension of our method

Except for the Feistel*-*SP* structure, our method also applies to some other Feistel structures to prove their security against IDC and ZCLC. Note that if the nonlinear part of a Feistel structure is bijective, we can treat it as an S-box. Thus saccording to Definition 1, we can define the characteristic matrices for any Feistel structures with bijective nonlinear parts. Then we define a special kind of characteristic matrix.

Definition 4 Let M be a characteristic matrix of a Feistel structure. If the number of entry "**s**" and the number of entry "**1**" in each column and row are all at most 1, then M is called **1-property** matrix.

By the analysis in Sects. 3 and 4.2.1, we know that if the characteristic matrices of a Feistel structure are **1-property** matrix, then our method can apply to this kind Feistel structure. For example, the Type-2 generalized Feistel structure [18] in Fig. 4. If we treat its round function as an S-box, then its characteristic matrices are **1-property** matrix. Then by our method, we get that the longest ID and ZCLH of this structure will not exceed 10 rounds.

5 Applications to LBlock and TWINE

In this section, we apply our method to block ciphers LBlock and TWINE, respectively. Based on some properties of LBlock and TWINE, tight bounds on the rounds of ID and ZCLH of these two ciphers are given.

5.1 Bounds for LBlock

LBlock is a lightweight block cipher proposed by Wu and Zhang in ACNS'11. The round function of LBlock is given in Fig. 5. According to Definition 1, the encryption and decryption matrices of LBlock are

$$En = \begin{pmatrix} P_1 \cdot (s \cdot P_0), & P_1 \\ I, & O \end{pmatrix} \text{ and } De = \begin{pmatrix} O, & I \\ P_1^{-1}, & s \cdot P_0 \end{pmatrix},$$

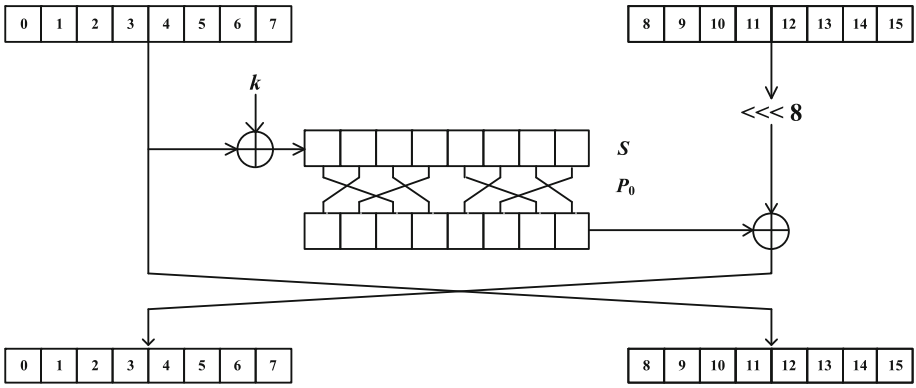


Fig. 5 Round function of LBlock

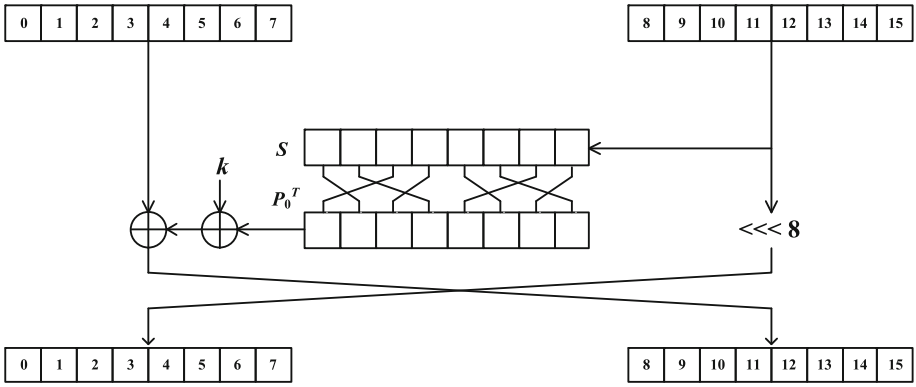


Fig. 6 Dual structure of round function of LBlock

respectively, where

$$P_0 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, P_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

It can be seen that P_1 is the matrix representation of the operation "$\ggg 8$".

The dual structure of the round function of LBlock is given in Fig. 6. The encryption and decryption matrices of the dual structure are

$$En^{\perp} = \begin{pmatrix} O, & P_1 \\ I, & s \cdot P_0^{-1} \end{pmatrix} \text{ and } De^{\perp} = \begin{pmatrix} (s \cdot P_0^{-1}) \cdot P_1^{-1}, & I \\ P_1^{-1}, & O \end{pmatrix},$$

respectively. It can be seen that En, De, $R(En^{\perp})$ and $R(De^{\perp})$ are **1-property** matrix. By computation, we have $R(En) = R(De) = R(En^{\perp}) = R(De^{\perp}) = 8$. Thus according to Theorem 1, we know that the rounds of ID and ZCLH of LBlock is upper bounded by 17.

Next, we present some properties of character matrices of LBlock. Based on these properties, tight bounds for ID and ZCLH of LBlock are given.

Let N_M^j be the number of entries "**0**" and "**1**" in the jth row of matrix M. By computation, we have

$$\begin{cases} N_{En^7}^j = 0, N_{En^7}^{j+8} = 1, \\ N_{De^7}^j = 1, N_{De^7}^{j+8} = 0, \\ N_{(En^\perp)^7}^j = 1, N_{(En^\perp)^7}^{j+8} = 0, \\ N_{(De^\perp)^7}^j = 0, N_{(De^\perp)^7}^{j+8} = 1, \end{cases} \text{for } 0 \le j \le 7. \tag{9}$$

By the above observations on characteristic matrices of LBlock, we have the following lemma.

Lemma 10 *Let* $\mathbf{V}$ *be a characteristic vector of LBlock. Let* $W_H(\mathbf{V})$ *be the number of nonzero entries in* $\mathbf{V}$. *If* $W_H(\mathbf{V}) \ge 3$, *then we have* $(M^i \cdot \mathbf{V})_j =?$ *for* $i \ge 7$ *and* $0 \le j \le 15$, *where* M *is a characteristic matrix of LBlock.*

Proof According to (9), we know that the number of "**0**" and "**1**" in each row of M^i is at most 1 for $i \ge 7$. Thus if $W_H(\mathbf{V}) \ge 3$, then there exist two positions j_0 and j_1 in the jth row of M^i for $i \ge 7$ such that $(\mathbf{V})_{j_0} \ne 0$, $(\mathbf{V})_{j_1} \ne 0$ and $(M^i)_{j,j_0}, (M^i)_{j,j_1} \in \{\mathbf{s}, \mathbf{1}+\mathbf{s}, 2\mathbf{s}\}$. Since

$$(M^i \cdot \mathbf{V})_j = (M^i)_{j,j_0} \cdot (\mathbf{V})_{j_0} + (M^i)_{j,j_1} \cdot (\mathbf{V})_{j,j_1},$$

we have $(M^i \cdot \mathbf{V})_j =?$. □

Based on Lemma 10, we have:

Corollary 4 *Let* $\mathbf{V}_P$ *and* $\mathbf{V}_C$ *be the characteristic vectors of* ΔP *and* ΔC, *respectively. If* $W_H(\mathbf{V}_P) \ge 3$ *or* $W_H(\mathbf{V}_C) \ge 3$, *then the third class information is empty when* $r \ge 15$.

Corollary 5 *If* $W_H(\mathbf{V}_P) \ge 3$ *or* $W_H(\mathbf{V}_C) \ge 3$, *and if* $r \ge 15$, *then* $\Delta P \to \Delta C$ *is an* r *-round possible differential of LBlock.*

The proofs of Corollaries 4 and 5 are similar with that of Lemma 9 and Theorem 1, respectively. Then, we give the upper bounds on the rounds of ID and ZCLH for LBlock.

Theorem 3 *If* $r \ge 15$, *then there do not exist* r*-round ID and ZCLH of LBlock.*

Proof By Corollary 5, we only need to check if there exist 15 -round ID $\Delta P \to \Delta C$ with $W_H(\mathbf{V}_P) < 3$ and $W_H(\mathbf{V}_C) < 3$. By checking out all these 15-round differentials by the *WW*-algorithm, there is no 15-round ID. Thus there does not exist r-round ID of LBlock when $r \ge 15$.

Notice that $En^\perp$ and $De^\perp$ have similar properties with matrices En and De, thus we have the same conclusion for ZCLH. □

5.2 Bounds for TWINE

TWINE is a lightweight block cipher proposed by Suzaki et al. [13]. The round functions of TWINE adopt an variant of the Type-2 generalized Feistel structure (see Fig. 7). According to Definition 1, the encryption and decryption matrices of round function of TWINE are

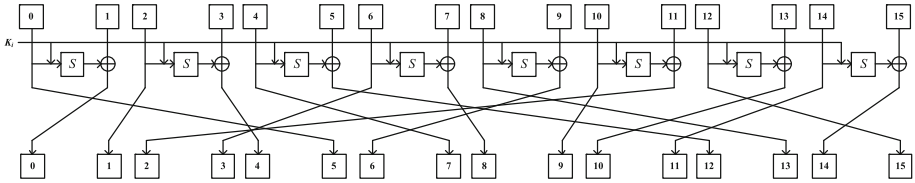


Fig. 7 Round function of TWINE

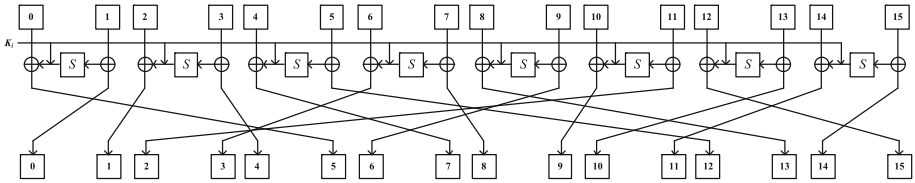


Fig. 8 Dual structure of round function of TWINE

$$En = \begin{pmatrix} \mathbf{s} \cdot P_0, & P_0 \\ P_1, & O \end{pmatrix}, De = \begin{pmatrix} O, & P_1^{-1} \\ P_0^{-1}, & \mathbf{s} \cdot P_1^{-1} \end{pmatrix},$$

respectively, where

$$P_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, P_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

The dual structure of TWINE is given in Fig. 8, and the encryption and decryption matrices of the dual structure are

$$En^{\perp} = \begin{pmatrix} O, & P_0 \\ P_1, & \mathbf{s} \cdot P_0 \end{pmatrix}, De^{\perp} = \begin{pmatrix} s \cdot P_1^{-1}, & P_1^{-1} \\ P_0^{-1}, & O \end{pmatrix},$$

respectively. By computation, we have

$$\begin{cases} R(En) = R(De) = R(En^{\perp}) = R(De^{\perp}) = 8, \\ N_{En^7}^{2j} = 0, N_{En^7}^{2j+1} = 1, \\ N_{De^7}^{2j} = 1, N_{De^7}^{2j+1} = 0, \\ N_{(En^{\perp})^7}^{2j} = 1, N_{(En^{\perp})^7}^{2j+1} = 0, \\ N_{(De^{\perp})^7}^{2j} = 0, N_{(De^{\perp})^7}^{2j+1} = 1, \end{cases} \quad \text{for } 0 \le j \le 7.$$

Similar with the analysis in Sect. 5.1, we have:

Theorem 4 *There do not exist r-round ID or ZCLH of TWINE if* $r \ge 15$.

6 Conclusion

In this paper, we studied the security of the Feistel*-SP structure. Upper bounds on the rounds of ID and ZCLH of this structure are given. Moreover, we showed that our method also apply to some generalized Feistel structures, such as the Type-2 generalized Feistel structure. As applications of our method, we proved that there do not exist 15-round ID and ZCLH for LBlock and TWINE. In our future work, we will focus on the security for more generic Feistel-SP structures.

Acknowledgements This work is supported by the National Natural Science Foundations of China under Grant Nos. 61521003, 61602510, 61672533 and National Cryptography Development Fund of China under Grant Nos. MMJJ20170103 and MMJJ20180204.

References

1. Aoki K., Ichikawa T., Kanda M., et al.: Camellia: a 128-bit block cipher suitable for multiple platforms—design and analysis. In: Stinson D.R., Tavares S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001).
2. Biham E., Shamir A.: Differential Cryptanalysis of the Data Encryption Standard. Springer, New York (1993).
3. Biham E., Biryukov A., Shamir A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Stern J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999).
4. Bogdanov A., Rijmen V.: Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Des. Codes Crypt. **70**(3), 369–383 (2014).
5. Bogdanov A., Geng H., Wang M., et al.: Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO Standards Camellia and CLEFIA. In: Lange T., Lauter K., Lisoněk P. (eds.) SAC 2013. LNCS, vol. 8282, pp. 306–323. Springer, Heidelberg (2014).
6. Boura C., Naya-Plasencia M., Suder V.: Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon. In: Sarkar P., Iwata T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 179–199. Springer, Heidelberg (2014).
7. Kim J., Hong S., Lim J.: Impossible differential cryptanalysis using matrix method. Discret. Math. **310**(5), 988–1002 (2010).
8. Knudsen L.R.: DEAL—a 128-bit block cipher Technical report. Department of Informatics, University of Bergen, Bergen (1998).
9. Lv J., Dunkelman O., Keller N., Kim J.-S.: New impossible differential attacks on AES. In: Chowdhury D.R., Rijmen V., Das A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 279–293. Springer, Heidelberg (2008).
10. Matsui M.: Linear cryptanalysis method for DES cipher. In: Helleseth T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994).
11. Sun B., Liu Z., Rijmen V., et al.: Links among impossible differential, integral and zero correlation linear cryptanalysis. In: Gennaro R., Robshaw M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 95–115. Springer, Berlin (2015).
12. Sun B., Liu M., Guo J., Rijmen V., Li R.: Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In: Fischlin M., Coron J.-S. (eds.) EUROCRYPT 2016. Part I, LNCS, vol. 9665, pp. 196–213. Springer, Heidelberg (2016).
13. Suzaki T., Minematsu K., Morioka S., Kobayashi E.: TWINE: a lightweight block cipher for multiple platforms. In: Wu H., Knudsen L.R. (eds.) SAC 2012. LNCS, vol. 7707, pp. 339–354. Springer, Heidelberg (2013).
14. Wang Y., Wu W.: Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE. In: Susilo W., Mu Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 1–16. Springer, Heidelberg (2014).
15. Wen L., Wang M., Bogdanov A.: Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: improved cryptanalysis of an ISO standard. Inf. Process. Lett. **114**(6), 322–330 (2014).

16. Wu S., Wang M.: Automatic search of truncated impossible differentials for word-oriented block ciphers. In: Galbraith S., Nandi M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 283–302. Springer, Heidelberg (2012).
17. Wu W., Zhang L.: LBlock: a lightweight block cipher. In: Lopez J., Tsudik G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344. Springer, Heidelberg (2011).
18. Zheng Y., Matsumoto T., Imai H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 461–480. Springer, Heidelberg (1990).