Improved Integral Cryptanalysis of Feistel Structures ⋆

Bing Sun[1,a], Xin Hai[1,b], Lei Cheng[1,c], Zhichao Yang[1], Wenyu Zhang[2,d]

[1] College of Science, National University of Defense Technology, Changsha, Hunan, P. R. China
[2] Shandong University of Finance and Economics, Jinan, Shandong, P. R. China
[a]happy_come@163.com, [b]artubo@126.com,
[c]chenglei_1111@163.com, [d]zhangwy@sdufe.edu.cn

Abstract. Feistel structure is among the most popular choices for designing ciphers. Recently, 3-round/5-round integral distinguishers for Feistel structures with non-bijective/bijective round functions are presented. At EUCRYPT 2015, Todo proposed the *Division Property* to effectively construct integral distinguishers for both Feistel and SPN structures. In this paper, firstly, it is proved that if $X \subseteq \mathbb{F}_2^n$ has the division property $\mathcal{D}_k^n$, the number of elements in X is at least 2^k, based on which we can conclude that if a multi-set X has the division property $\mathcal{D}_n^n$, it is in some sense equivalent to either $\mathbb{F}_2^n$ or $\emptyset$. Secondly, let d be the algebraic degree of the round function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ of a Feistel structure. If $d \leq n-1$, the corresponding integral distinguishers are improved as follows: there exists a 3-round integral distinguisher with at most 2^n chosen plaintexts and a 4-round integral distinguisher with at most 2^{2n-2} chosen plaintexts. These results can give new insights to both the division property and Feistel structures.

Keywords: Feistel structure, Integral cryptanalysis, Division property

1 Introduction

Integral cryptanalysis[1], which was first proposed by Knudsen and Wagner, is among the most important cryptanalytic techniques. With some special inputs, we check whether the sum of the corresponding ciphertexts is 0 or not. Usually, we do not need to investigate the details of the S-boxes and only view the S-boxes as bijective transformations over finite fields/vector spaces. In some other literatures, integral cryptanalysis is also known as square attack[2], saturation attack[3], multi-set attack[4], higher-order differential attack[5, 6] and so on. The following 4 integral properties of a multi-set X are the most used ones:

- ALL($\mathcal{A}$): Every value in $\mathbb{F}_2^n$ appears the same times in X.
- BALANCE($\mathcal{B}$): The Xor of all values in X is 0.

⋆ The work in this paper is supported by the Natural Science Foundation of China(No: 61402515).

- CONSTANT($\mathcal{C}$): The value is fixed to a constant for all texts in X.
- UNKNOWN($\mathcal{U}$): X is indistinguishable from random sets.

With these notations, we can determine that, after applying a bijective transformation, property $\mathcal{A}$ is reserved; the sum of two multi-sets with property $\mathcal{A}$ has property $\mathcal{B}$. However, assume a multi-set has property $\mathcal{B}$, it is hard to determine, after applying a nonlinear transformation, whether the output multi-set has property $\mathcal{B}$ or not. And if we could determine the property of the output multi-set, the integral distinguishers could be improved.

As the notations introduced above can only apply to word-oriented ciphers, in [7], Z'aba introduced the *bit-pattern* to evaluate the sum of some outputs. And this method is quite useful in constructing integral distinguishers for bit-oriented ciphers such as PRESENT and SERPENT. In [8–10], by using polynomials over finite fields, the authors proposed some algebraic techniques to construct integral distinguishers for block ciphers, such as $\mathcal{PURE}$ and ARIA.

In EUROCRYPT 2015, Todo proposed the *Division Property* to evaluate the sum of the outputs of a nonlinear function[11]. A multi-set X has the division property $\mathcal{D}_k^n$ if and only if for all Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $\deg f < k$, the sum of f on X is always 0. It has been pointed that the division property $\mathcal{D}_2^n$ is equivalent to the property $\mathcal{B}$. However, there is a gap between $\mathcal{D}_n^n$ and $\mathcal{A}$. Let X and Y be the input and output sets of an S-box, respectively, and d be the algebraic degree of the S-box. The newly proposed methods of constructing integrals for both Feistel and SPN structures are based on the following fact: If X has the division property $\mathcal{D}_k^n$, Y has the division property $\mathcal{D}_{\lceil k/d \rceil}^n$. The result shows that for a given Feistel structure, we can always construct a 3-round and a 5-round integral distinguisher in case the round function is non-bijective and bijective, respectively.

In CRYPTO 2015[12], Sun *et al.* proved that a zero correlation linear hull always implies the existence of an integral distinguisher. Therefore, we can construct integrals of a block cipher by finding zero correlation linear hulls. For example, based on the known zero correlation linear hulls of 3-round/5-round Feistel structures with non-bijective/bijective round functions, they theoretically proved that there always exist 3-round/5-round integral distinguishers for Feistel structures with non-bijective/bijective round functions.

Contributions. This paper mainly focuses on the study of characteristics of the division property and the improvement of the known integral distinguishers for Feistel structures. The main contributions of this paper are as follows:

(1) We prove that if $X \subseteq \mathbb{F}_2^n$ has the division property $\mathcal{D}_k^n$, $\#X \geq 2^k$;
(2) Although $\mathcal{D}_n^n$ and $\mathcal{A}$ are different, we prove that if a multi-set X has the division property $\mathcal{D}_n^n$, X is in some sense equivalent to either $\mathbb{F}_2^n$ or $\emptyset$ (we define this equivalence relation in Section 3);

Furthermore, when the algebraic degree of the round function d is no more than $n-1$, the 3-round integral distinguishers for Feistel structures could be improved in the following two directions:

(3) The data complexity of the known 3-round integral distinguishers is reduced from 2^{n+1} to 2^n;
(4) We prove that there always exists a 4-round integral distinguisher with 2^{2n-2} chosen plaintexts.

The rest of this paper is organized as follows: Sec. 2 gives the definitions of Feistel structure and the division property; Sec. 3 studies the properties of $\mathcal{D}_k^n$; Sec. 4 improves the known 3-round integral for Feistel structure and Sec. 5 concludes the paper.

2 Preliminary

We will briefly introduce the Feistel structure and the division property that will be used throughout this paper.

2.1 Feistel Structure

Many block ciphers are designed based on the Feistel structure, such as DES[13] and Camellia[14]. A Feistel structure consists of r rounds, each of which is defined as follows (See Fig.1). Denote by (L_{i-1}, R_{i-1}) the $2n$-bit input to the i-th round, and (L_i, R_i) the output of the i-th round. Then

$$\begin{cases} L_i = & F_i(L_{i-1}) \oplus R_{i-1}, \\ R_i = & L_{i-1}, \end{cases}$$

where F_i is the round function. In the following we use (n, d)-Feistel structure to denote a Feistel structure, where n is the number of input bits of the round function and d is the algebraic degree of the round function.

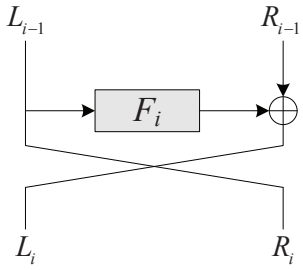

Fig. 1. Feistel Structure

2.2 Division Property

We will recall the definition of the division property, the vectorial division property and the collective division property introduced in [11], and then some examples will be given to make us better understand these conceptions.

Definition 1 (Bit Product Function). *[11] Let* $u = (u_0, \ldots, u_{n-1}) \in \mathbb{F}_2^n$ *and* $x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$. *The* Bit Product Function π_u *is defined as*

$$\pi_u(x) = \prod_{u_i=1} x_i.$$

Let $U = (u^{(0)}, \ldots, u^{(m-1)}) \in (\mathbb{F}_2^n)^m$ *and* $X = (x^{(0)}, \ldots, x^{(m-1)}) \in (\mathbb{F}_2^n)^m$. *The* Bit Product Function π_U *is defined as*

$$\pi_U(X) = \prod_{i=0}^{m-1} \pi_{u^{(i)}}\left(x^{(i)}\right).$$

In the definition above, for $x \in \mathbb{F}_2^n$, we always let $\pi_0(x) = 1$.

Definition 2 (Hamming Weight). *Let* $x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$. *The* Hamming Weight *of* x *is defined as*

$$w(x) = \#\{i | x_i \neq 0, i = 0, 1, \ldots, n-1\}.$$

Let $X = (x^{(0)}, \ldots, x^{(m-1)}) \in (\mathbb{F}_2^n)^m$. *The* Extended Hamming Weight *of* X *is defined as*

$$W(X) = \left(w(x^{(0)}), \ldots, w(x^{(m-1)})\right) \in \mathbb{Z}^m.$$

Let $x = (x_0, x_1, \ldots, x_{m-1}), y = (y_0, y_1, \ldots, y_{m-1}) \in \mathbb{Z}^m$. *We define* $x \succeq y$ *if for every* i, $0 \leq i \leq m-1$, $x_i \geq y_i$, *otherwise,* $x \not\succeq y$.

Definition 3 (Division Property). *[11] Let* X *be a multi-set whose elements take a value of* $\mathbb{F}_2^n$, *and* k *takes a value between* 0 *and* n. *When the multi-set* X *has the division property* $\mathcal{D}_k^n$, *it fulfils the following conditions:* $\sum_{x \in X} \pi_u(x) = 0$ *if* $w(u) < k$. *Moreover,* $\sum_{x \in X} \pi_u(x)$ *becomes unknown if* $w(u) \geq k$.

Definition 4 (Vectorial Division Property). *[11] Let* X *be the multi-set whose elements take a value of* $(\mathbb{F}_2^n)^m$, *and* $k = (k_0, \ldots, k_{m-1}) \in \mathbb{Z}^m$ *where* $0 \leq k_i \leq n$. *When the multi-set* X *has the division property* $\mathcal{D}_k^{n,m}$, *the multi-set fulfils the following conditions:* $\sum_{x \in X} \pi_U(x) = 0$ *if* $W(U) \not\succeq k$. *Moreover,* $\sum_{x \in X} \pi_U(x)$ *becomes unknown if* $W(U) \succeq k$.

Definition 5 (Collective Division Property). *[11] Let* X *be the multi-set whose elements take a value of* $(\mathbb{F}_2^n)^m$, *and* $k^{(0)}, \ldots, k^{(t-1)} \in \mathbb{Z}^m$. *When the multi-set* X *has the division property* $\mathcal{D}_{k^{(0)}, \ldots, k^{(t-1)}}^{n,m}$, *the multi-set fulfils the following conditions:* $\sum_{x \in X} \pi_U(x) = 0$ *if*

$$U \in \{V \in (\mathbb{F}_2^n)^m | W(V) \not\succeq k^{(0)}, \ldots, W(V) \not\succeq k^{(t-1)}\}.$$

Moreover, $\sum_{x \in X} \pi_U(x)$ *becomes unknown if there exists an* i_0, $0 \leq i_0 \leq t-1$ *such that* $W(U) \succeq k^{(i_0)}$.

Example 1. Let X be a k-dimension sub-space of $\mathbb{F}_2^n$, and $B_k = \{f : \mathbb{F}_2^n \to \mathbb{F}_2 | \deg f < k\}$ be the set of all the Boolean functions on $\mathbb{F}_2^n$ with algebraic degree no more than $k-1$. Then for any $f \in B_k$, we always have[5]

$$\sum_{x \in X} f(x) = 0.$$

Meanwhile, we can construct a function $g : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $\deg g = k$ and $\sum_{x \in X} g(x) = 1$. Therefore a k-dimension sub-space of $\mathbb{F}_2^n$ always has the division property $\mathcal{D}_k^n$.

Example 2. Let X have the division property $D^{n,2}_{(1,5),(4,4),(5,2),(6,0),(6,5)}$. See Fig.2, if (u_0, u_1) is in the gray part, for example $(u_0, u_1) = (7, 1)$, we cannot determine $\sum_{x \in X} \pi_{(u_0,u_1)}(x)$. Otherwise, for example $(u_0, u_1) = (2, 4)$, we always have $\sum_{x \in X} \pi_{(u_0,u_1)}(x) = 0$. According to the definition of collective division property, $D^{n,2}_{(1,5),(4,4),(5,2),(6,0),(6,5)}$ is the same as $D^{n,2}_{(1,5),(4,4),(5,2),(6,0)}$ since from Fig. 2, we can see that these two division properties have the same (u_0, u_1) such that $\sum_{x \in X} \pi_{(u_0,u_1)}(x)$ is either 0 or undetermined.

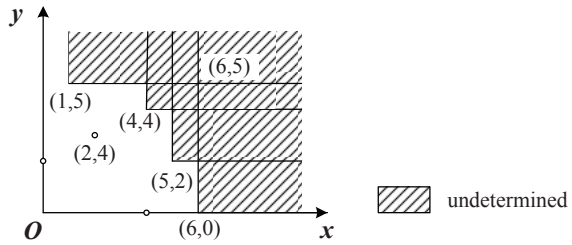

Fig. 2. Division Property $D^{n,2}_{(1,5),(4,4),(5,2),(6,0)}$

To further characterize the division property, we need the following proposition. Let $x = (x_0, \ldots, x_{m-1}) \in \mathbb{Z}^m$ and $0 \neq d \in \mathbb{Z}$. We simply use $\lceil x/d \rceil$ to denote the vector $(\lceil x_0/d \rceil, \ldots, \lceil x_{m-1}/d \rceil)$.

Property 1. [11] Let X be the multi-set whose elements take a value of $(\mathbb{F}_2^n)^m$, $s_0, \ldots, s_{m-1}$ be m $n \times n$ S-boxes and $\deg(s_0) = \cdots = \deg(s_{m-1}) = d$. The multi-set Y is computed as $Y = \{(s_0(x_0), \ldots, s_{m-1}(x_{m-1}))|(x_0, \ldots, x_{m-1}) \in X\}$. If X has the collective division property $\mathcal{D}^{n,m}_{k^{(0)},\ldots,k^{(t-1)}}$, Y has the collective division property $\mathcal{D}^{n,m}_{\lceil k^{(0)}/d \rceil,\ldots,\lceil k^{(t-1)}/d \rceil}$.

Property 2 (Propagation for Feistel Structure). [11] Let X be the input of a 1-round Feistel structure $\mathcal{F}$ which has division property $\mathcal{D}^{n,2}_{(k_1,k_2)}$. Assume the algebraic degree of the round function is d. Then the output of $\mathcal{F}$ has the division property $\mathcal{D}^{n,2}_{(k_2+\lceil 0/d \rceil,k_1),\ldots,(k_2+\lceil i/d \rceil,k_1-i),\ldots,(k_2+\lceil k_1/d \rceil,0)}$.

3 Properties of $\mathcal{D}_k^n$ and $\mathcal{D}_{(k_0,\ldots,k_{m-1})}^{n,m}$

In this section, we will give some bounds on the number of elements in a set which has special division property. Notice that when X is a multi-set, an element of $\mathbb{F}_2^n$ may appear several times in X, however, when X is a subset of $\mathbb{F}_2^n$, an element of $\mathbb{F}_2^n$ appears at most 1 time in X.

Lemma 1. *Let X be a non-empty subset of $\mathbb{F}_2^n$ with the division property $\mathcal{D}_k^n$, $k \geq 1$. Then $\#X \equiv 0 \pmod 2$.*

Proof. According to the definition of the division property, for $k = 1$, we always have

$$\sum_{x \in X} \pi_0(x) = \sum_{x \in X} 1 = \#X \equiv 0 \pmod 2.$$

Theorem 1. *Let X be a non-empty subset of $\mathbb{F}_2^n$ with the division property $\mathcal{D}_k^n$. Then $\#X \geq 2^k$.*

Proof. Firstly, according to Lemma 1, we can check that if $k = 1$, $\#X \geq 2$. Assume for $k = k_0 < n$, $A \neq \emptyset$ is a subset of $\mathbb{F}_2^n$ and has the division property $\mathcal{D}_{k_0}^n$, we have $\#A \geq 2^{k_0}$.

Now, assume $B \subseteq \mathbb{F}_2^n$ has the division property $\mathcal{D}_{k_0+1}^n$ and $B \neq \emptyset$. Since B has at least 2 different elements, there exists at least one position t such that the t-th elements of B are not equal to a constant. Without loss of generality, let $t = 0$ and

$$B_0 = \{(x_0, x_1, \ldots, x_{n-1}) \in B | x_0 = 0\} \neq \emptyset,$$
$$B_1 = \{(x_0, x_1, \ldots, x_{n-1}) \in B | x_0 = 1\} \neq \emptyset.$$

Therefore, $B_0 \cap B_1 = \emptyset$ and $B_0 \cup B_1 = B$.

Since B has the division property $\mathcal{D}_{k_0+1}^n$,

$$\sum_{x \in B} x_0 \pi_u(x) = 0, \quad w(u) < k_0$$

thus

$$\sum_{x \in B} x_0 \pi_u(x) = \sum_{x \in B, x_0 = 1} \pi_u(x) = \sum_{x \in B_1} \pi_u(x) = 0,$$

where $w(u) < k_0$, which implies B_1 has the division property $\mathcal{D}_{k_0}^n$.

On the other hand, for $w(u) < k_0$,

$$\sum_{x \in B} \pi_u(x) = \sum_{x \in B_0} \pi_u(x) + \sum_{x \in B_1} \pi_u(x) = 0.$$

Since

$$\sum_{x \in B_0} \pi_u(x) = \sum_{x \in B} \pi_u(x) - \sum_{x \in B_1} \pi_u(x) = 0, \quad w(u) < k_0,$$

we can conclude that B_0 has the division property $\mathcal{D}^n_{k_0}$. Therefore,

$$\#B = \#B_0 + \#B_1 \geq 2^{k_0} + 2^{k_0} = 2^{k_0+1}.$$

By using the same technique, we can prove the following Theorem for the vectorial division property:

Theorem 2. *Let $X \neq \emptyset$ be a subset of $(\mathbb{F}_2^n)^m$ with the vectorial division property $\mathcal{D}^{n,m}_{(k_0,\ldots,k_{m-1})}$. Then $\#X \geq 2^{k_0+\cdots+k_{m-1}}$.*

Corollary 1. *Let $X \neq \emptyset$ be a subset of $\mathbb{F}_2^n$ with the division property $\mathcal{D}^n_n$. Then $X = \mathbb{F}_2^n$.*

This could be deduced directly from Theorem 1. However, we could give an independent proof as follows:

Proof. Assume $A \neq \mathbb{F}_2^n$, therefore $B = \mathbb{F}_2^n - A$ is non-empty.

Since both $\mathbb{F}_2^n$ and A have the division property $\mathcal{D}^n_n$, B also has the division property $\mathcal{D}^n_n$.

Let $x_0 \in A$ such that for any $x \in A$, $w(x_0) \geq w(x)$, and let $y_0 \in B$ such that for any $y \in B$, $w(y_0) \geq w(y)$. Then we have

$$\pi_{x_0}(x) = \begin{cases} 1 & x = x_0, \\ 0 & x \neq x_0. \end{cases} \qquad \pi_{y_0}(y) = \begin{cases} 1 & y = y_0, \\ 0 & y \neq y_0. \end{cases}$$

Therefore,

$$\sum_{x \in A} \pi_{x_0}(x) = 1, \qquad \sum_{y \in B} \pi_{y_0}(y) = 1.$$

Since both A and B have the division property $\mathcal{D}^n_n$, we have $w(x_0) \geq n$ and $w(y_0) \geq n$. Thus $x_0 = y_0 = 2^n - 1$ which is contradicted with $A \cap B = \emptyset$.

Based on these results, we could give the following Corollary:

Corollary 2. *Let $\mathbb{F}_2^n = \{a_0, \ldots, a_{2^n-1}\}$, X be a multi-set whose elements take a value of $\mathbb{F}_2^n$, and $t_{x,X}$ be the times that x appears in X. If X has the division property D^n_n, we have*

$$t_{a_0,X} \equiv \cdots \equiv t_{a_{2^n-1},X} \pmod 2.$$

Assume a multi-set X has the division property $\mathcal{D}^n_k$, and let the multi-set $Y = X \cup \{a, a\}$. Then Y also has the division property $\mathcal{D}^n_k$. This fact leads to the following definition:

Definition 6. *Let X and Y be multi-sets whose elements take a value of $\mathbb{F}_2^n$. Then X is equivalent with Y, denoted by $X \sim Y$, if and only if for any $a \in \mathbb{F}_2^n$, $t_{a,X} \equiv t_{a,Y} \pmod 2$.*

Therefore, if $X \sim Y$, X and Y always have the same division property.

Theorem 3. *Let X be a multi-set whose elements take a value of $\mathbb{F}_2^n$. If X has the division property D^n_n, we have either $X \sim \mathbb{F}_2^n$ or $X \sim \emptyset$.*

4 Improved Integral Distinguishers for Feistel Structures

With the condition $d \leq n-1$, we will improve the known 3-round integral distinguishers for Feistel structures in two directions: The first one is to reduce the data complexity from 2^{n+1} to 2^n; the second one is to increase the rounds of integral distinguisher from 3 to 4.

Lemma 2. *Let $r(n,d)$ be the rounds of the integral distinguisher of (n,d)-Feistel structure which could be found by Algorithm 1 in [11]. If $d_1 \leq d_2$, we have $r(n,d_1) \geq r(n,d_2)$.*

This could be shown from the fact that for $k \in \mathbb{Z}^m$, if $d_1 \leq d_2$, we always have $\lceil k/d_1 \rceil \succeq \lceil k/d_2 \rceil$.

Theorem 4. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the round function of a Feistel structure and $d = \deg F \leq n-1$ be the algebraic degree of F. For such a Feistel structure:*

(1) There always exists a 3-round integral distinguisher with 2^n chosen plaintexts and the Xor sum of the right half of the ciphertexts is 0.
(2) There always exists a 4-integral distinguisher with 2^{2n-2} chosen plaintexts and the Xor sum of the right half of the ciphertexts is 0.

Proof. Since the technique are the same, we only give a detailed proof for the 4-round distinguisher.

According to Lemma 2, it is sufficient to give the proof for $d = n-1$.

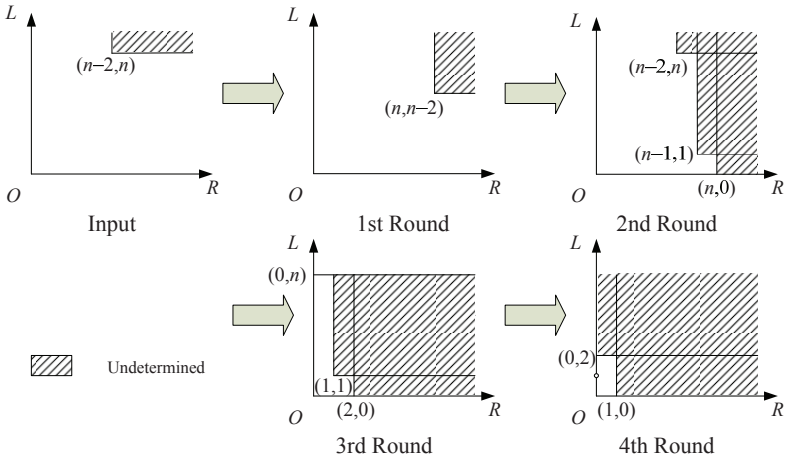

Fig. 3. Propagation of 4-round $(n, n-1)$-Feistel structure

Let the inputs be $(c_0c_1x_0 \cdots x_{n-3}, x_{n-2} \ldots x_{2n-3}) \in (\mathbb{F}_2^n)^2$, where $(c_0c_1) \in \mathbb{F}_2^2$ is a constant and $x_0x_1 \ldots x_{2n-3}$ can take all values in $\mathbb{F}_2^{2n-2}$.

Since the input set has the division property $D^{n,2}_{(n-2,n)}$. According to the propagation of the Feistel structure, the output set of the first round has the division property $D^{n,2}_{(n+\lceil 0/d\rceil,n-2),\ldots,((n+\lceil (n-2)/d\rceil,0))} = D^{n,2}_{(n,n-2)}$.

Then, the output set of the second round has the division property

$$D^{n,2}_{(n-2+\lceil 0/d\rceil,n),\cdots,(n-2+\lceil i/d\rceil,n-i),\cdots,(n-2+\lceil n/d\rceil,0)}.$$

which is equal to $\mathcal{D}^{n,2}_{(n-2,n),(n-1,1),(n,0)}$.

Similarly, we can get that the output of the third round has the division property $\mathcal{D}^{n,2}_{(0,n)(1,1),(2,0)}$ and the output of the forth round has the division property $\mathcal{D}^{n,2}_{(0,2),(1,0)}$, which means for any u, $w(u) = 1$, let C_L and C_R be the left and right halves of the output of the forth round, respectively. We always have

$$\sum_{x_0,\ldots,x_n} \pi_0(C_L)\pi_u(C_R) = 0,$$

which indicates $\sum_{x_0,\ldots,x_n} C_R = 0$.

Moreover, we can only determine that the output of the fifth round has the division property $\mathcal{D}^{n,2}_{(0,1),(1,0)}$, which means we cannot determine whether the output is balanced or not.

With the results of [11] and [12], we have

Corollary 3. *Let $d \leq n-1$. There always exists a 4-round integral distinguisher for Feistel structures. Furthermore, if the round function is bijective, there always exists a 5-round integral distinguisher for Feistel structures.*

5 Conclusion

In this paper, firstly, we showed some property of a set $X \subseteq \mathbb{F}_2^n$ which has the division property $\mathcal{D}^n_k$. We proved that the number of different elements in X is at least 2^k. If a non-empty subset X of $\mathbb{F}_2^n$ has the division property D^n_n, X is equal to $\mathbb{F}_2^n$, from which we can conclude that if a multi-set X is not equivalent to the empty set, there is no essential difference between $\mathbb{F}_2^n$ and a multi-set X which has the division property $\mathcal{D}^n_n$.

Table 1. Integral Distinguishers for (n, d)-Feistel Structures

d	Rounds	Input	Data	Round Function
n	3	$\mathcal{D}^{n,2}_{(1,n)}$	2^{n+1}	non-bijective
$\leq n-1$	3	$\mathcal{D}^{n,2}_{(0,n)}$	2^n	
$\leq n-1$	4	$\mathcal{D}^{n,2}_{(n-2,n)}$	2^{2n-2}	
$\leq n-1$	5	$\mathcal{D}^{n,2}_{(n-1,n)}$	2^{2n-1}	bijective

*For all these distinguishers, the right halves of the outputs are balanced.

Secondly, we presented some new features of Feistel structures with respect to the integral attack. If $d \leq n-1$, the known integral distinguishers for 3-round Feistel structure could be improved. These results are shown in Table.1.

It has been a common view that the linear layer has less influence in constructing integral distinguishers. However, the method proposed by Todo uses little information of the linear layer. Therefore, we propose whether there exists an algorithm which could use both details of linear layer and nonlinear layer to improve the known integral distinguishers as an open problem.

Furthermore, when constructing an integral distinguisher, we do not need to evaluate $\sum_{x \in X} \pi_u(x)$ for all u such that $w(u) = 1$. For example, in the integral distinguisher for SIMON32 and SIMON48 constructed in [15], only part of the outputs are balanced. Therefore, we propose whether more information of the round function could be used to construct longer integral distinguisher as another open problem.

Acknowledgement

The authors wish to thank Vincent Rijmen, Yosuke Todo and Xuan Shen for their helpful discussions.

References

1. L.R. Knudsen, D. Wagner. Integral Cryptanalysis. Fast Software Encryption 2002, LNCS 2365, pp. 112–127, Springer–Verlag, 2002.
2. J. Daemen, L. R. Knudsen, V. Rijmen. The Block Cipher Square. Fast Software Encryption 1997, LNCS 1267, pp. 149–165, Springer–Verlag, 1997.
3. S. Lucks. The Saturation Attack — A Bait for Twofish. Fast Software Encryption 2001, LNCS 2355, pp. 1–15, Springer–Verlag, 2002.
4. A. Biryukov, A. Shamir. Structural Cryptanalysis of SASAS. EUROCRYPT 2001, LNCS 2045, pp. 394–405, Springer–Verlag, 2001.
5. X. Lai. Higher Order Derivatives and Differential Cryptanalysis. Communications and Cryptography: Two Sides of One Tapestry, 227 (1994)
6. L.R. Knudsen. Truncated and Higher Order Differentials. Fast Software Encryption 1994, LNCS 1008, pp. 196–211. Springer, Heidelberg (1995)
7. M. Z'aba, H. Raddum, M. Henricksen, E. Dawson. Bit-Pattern Based Integral Attack. FSE 2008, LNCS 5086, pp. 363–381, Springer-Verlag, 2008.
8. B. Sun, C. Li, L. Qu. Improved cryptanalysis of Block Ciphers with Low Algebraic Degree. FSE 2009. LNCS 5665, pp. 180–192, 2009, Springer-Verlag.
9. B. Sun, R. Li, L. Qu, C. Li. SQUARE Attack on Block Ciphers with Low Algebraic Degree. Science China Information Sciences 53(10), pp. 1988–1995, 2010.
10. P. Li, B. Sun, C. Li. Integral Cryptanalysis of ARIA. Inscrypt 2009, LNCS 6151, pp. 1–14, Springer-Verlag, 2010.
11. Y. Todo. Structural Evaluation by Generalized Integral Property. To appear in EUROCRYPT 2015.
http://eprint.iacr.org/2015/090

12. B. Sun, Z. Liu, V. Rijmen, R. Li, L. Cheng, Q. Wang, H. Alkhzaimi, C. Li. Links among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis. To appear in CRYPTO 2015.
http://eprint.iacr.org/2015/181
13. FIPS 46–3. Data Encryption Standard. In National Institute of Standards and technology, 1977.
14. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms. Availale at http://info.isl.ntt.co.jp/crypt/camellia/dl/support.pdf.
15. Q. Wang, Z. Liu, K. Varici, Y. Sasaki, V. Rijmen, Y. Todo. Cryptanalysis of reduced-round SIMON32 and SIMON48. In INDOCRYPT 2014, LNCS 8885, pp. 143–160. Springer, 2014.