SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

September 2017, Vol. 60 098102:1–098102:3
doi: 10.1007/s11432-015-0376-x

New observation on division property

Bing SUN[1,2*], Xin HAI[1*], Wenyu ZHANG[3*], Lei CHENG[1] & Zhichao YANG[1]

[1]*College of Science, National University of Defense Technology, Changsha* 410073*, China;*
[2]*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing* 100878*, China;*
[3]*Shandong University of Finance and Economics, Jinan* 250012*, China*

Received June 7, 2016; accepted August 12, 2016; published online December 12, 2016

Citation Sun B, Hai X, Zhang W Y, et al. New observation on division property. Sci China Inf Sci, 2017, 60(9): 098102, doi: 10.1007/s11432-015-0376-x

Integral cryptanalysis [1–5] is among the most important cryptanalytic vectors. With some special inputs, we check whether the sum of the corresponding ciphertexts is 0 or not. In some other literatures, integral cryptanalysis is also known as square attack, saturation attack, multi-set attack, higher-order differential attack and so on.

Usually, it is difficult to determine the property of a multi-set which has the balaced property $\mathcal{B}$ after applying a nonlinear transformation. Thus if we could determine the property of the output multi-set, the integral distinguishers could be improved.

Todo [6] proposed in EUROCRYPT 2015 the division property to evaluate the sum of the outputs of a nonlinear function. 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 out 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, Sun et al. [7] 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.

In [6], Todo constructed a special subset with the division property $\mathcal{D}_k^n$. Since the number of elements in this subset is 2^k, we wonder whether we could construct some other subsets with the division property $\mathcal{D}_k^n$, however with less elements than 2^k, to reduce the data complexity of the integral distinguishers of Feistel structures.

Many block ciphers are designed based on the Feistel structure, such as DES [8] and Camellia [9]. A Feistel structure consists of r rounds, each of which is defined as follows. 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

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

* Corresponding author (email: happy_come@163.com, artubo@126.com, zhangwy@sdufe.edu.cn)
The authors declare that they have no conflict of interest.

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.

Definition 1 (Bit product function [6])**.** 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 (Division property [6])**.** 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 condition: $\sum_{x\in X} \pi_u(x) = 0$ if $w(u) < k$. Moreover, $\sum_{x\in X} \pi_u(x)$ becomes unknown if $w(u) \geqslant k$.

Definition 3 (Vectorial division property [6])**.** 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 $0 \leqslant k_i \leqslant n$. When the multi-set X has the division property $\mathcal{D}_k^{n,m}$, the multi-set fulfils the following condition: $\sum_{x\in X} \pi_U(x) = 0$ if $W(U) \not\succeq k$. Moreover, $\sum_{x\in X} \pi_U(x)$ becomes unknown if $W(U) \succeq k$.

Definition 4 (Collective division property [6])**.** 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 $\mathcal{D}^{n,m}_{k^{(0)},\ldots,k^{(t-1)}}$, the multi-set fulfils the following condition: $\sum_{x\in X} \pi_U(x) = 0$ 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, $0 \leqslant i_0 \leqslant t-1$ such that $W(U) \succeq k^{(i_0)}$.

To further characterize the division property, we need the following propositions. 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 $(\lceil x_0/d \rceil, \ldots, \lceil x_{m-1}/d \rceil)$.

Proposition 1. 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 $Y = \{(s_0(x_0), \ldots, s_{m-1}(x_{m-1}))|(x_0, \ldots, x_{m-1}) \in X\}$ [6]. If X has the collective division property $\mathcal{D}^{n,m}_{k^{(0)},\ldots,k^{(t-1)}}$, Y has the collective division property $\mathcal{D}^{n,m}_{\lceil k^{(0)}/d \rceil,\ldots,\lceil k^{(t-1)}/d \rceil}$.

Proposition 2 (Propagation for Feistel structure [6])**.** 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 $\mathcal{D}^{n,2}_{(k_2+\lceil 0/d \rceil,k_1),\ldots,(k_2+\lceil i/d \rceil,k_1-i),\ldots,(k_2+\lceil k_1/d \rceil,0)}$.

Now, we are going to give some bounds on the number of elements in a set which has special division property. The details of the proofs could be found through http://eprint.iacr.org/2015/459. 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 $\mathcal{D}_k^n$, $k \geqslant 1$. Then $\#X \equiv 0 \pmod 2$.

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

For the vectorial division property, we have:

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 $\#X \geqslant 2^{k_0+\cdots+k_{m-1}}$.

From these results, we could find that the data complexity of the integral constructed by Todo cannot be reduced. According to Theorem 1, we have:

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

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

Definition 5. 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 $X \sim \emptyset$.

Feistel structure is a popular choice to construct cryptographic schemes. With the condition $d \leqslant n-1$, 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 [6]. If $d_1 \leqslant d_2$, we have $r(n,d_1) \geqslant r(n,d_2)$.

This could be shown from the fact that for $k \in \mathbb{Z}^m$, if $d_1 \leqslant d_2$, 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 $d = \deg F \leqslant n-1$ 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-round integral distinguisher with 2^{2n-2} chosen plaintexts and the Xor sum of the right half of the ciphertexts is 0.

With the results of [6] and [7], we have:

Corollary 3. Let $d \leqslant n-1$. 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.

Conclusion. In this article, firstly, we showed some properties of a set $X \subseteq \mathbb{F}_2^n$ which has the division property $\mathcal{D}_k^n$. We proved that the number of different elements in X is at least 2^k. Therefore, from the aspect of the number of chosen plaintexts, the distinguishers constructed by the division property in EUROCRYPT 2015 cannot be improved. 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 $\mathcal{D}_n^n$.

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

Acknowledgements The authors thank Vincent Rijmen, Yosuke Todo and Xuan Shen for their helpful discussions. This work was supported by National Natural Science Foundation of China (Grant Nos. 61402515, 61672530), Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-14-003), Scientific Research Fund of Hunan Provincial Education Department (Grant No. YB2014B001), and Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20121501120004).

References

1 Knudsen L R, Wagner D. Integral cryptanalysis. Lect Notes Comput Sci, 2002, 2365: 112–127
2 Daemen J, Knudsen L R, Rijmen V. The block cipher square. Lect Notes Comput Sci, 1997, 1267: 149–165
3 Lucks S. The saturation attack — a bait for Twofish. Lect Notes Comput Sci, 2002, 2355: 1–15
4 Biryukov A, Shamir A. Structural cryptanalysis of SASAS. Lect Notes Comput Sci, 2001, 2045: 394–405
5 Lai X. Higher order derivatives and differential cryptanalysis. Springer Int Ser Eng Comput Sci, 1994, 276: 227–233
6 Todo Y. Structural evaluation by generalized integral property. Lect Notes Comput Sci, 2015, 9056: 287–314
7 Sun B, Liu Z, Rijmen V, et al. Links among impossible differential, integral and zero correlation linear cryptanalysis. Lect Notes Comput Sci, 2015, 9215: 95–115
8 Data encryption standard. FIPS 46–3. In National Institute of Standards and Technology. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
9 Aoki K, Ichikawa T, Kanda M, et al. Camellia: a 128-bit block cipher suitable for multiple platforms. In: Proceedings of the 7th Annual International Workshop, Selected Areas in Cryptography, Ontario, 2000. 39–56