SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

December 2017, Vol. 60 128101:1–128101:3
doi: 10.1007/s11432-016-9170-y

Toward a further understanding of bit-based division property

Ling SUN[1,2] & Meiqin WANG[1,2,3*]

[1]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan* 250100*, China;*
[2]*Science and Technology on Communication Security Laboratory, Chengdu* 610041*, China;*
[3]*State Key Laboratory of Cryptology, P.O. Box* 5159*, Beijing* 100878*, China*

Received April 21, 2017; accepted June 21, 2017; published online November 8, 2017

Citation Sun L, Wang M Q. Toward a further understanding of bit-based division property. Sci China Inf Sci, 2017, 60(12): 128101, doi: 10.1007/s11432-016-9170-y

The division property of a multiset, which is a generalization of the integral property, was proposed by Todo [1] at EUROCRYPT 2015. Since division property can precisely depict the implicit properties between ALL and BALANCE properties, it allows us to efficiently construct integral distinguisher even if the round function of the block cipher is non-bijective, bit-oriented, and low-degree.

Definition 1 (Division property [1])**.** Let $\mathbb{X}$ be a multiset whose elements take values from $\mathbb{F}_2^{\ell_0} \times \mathbb{F}_2^{\ell_1} \times \cdots \times \mathbb{F}_2^{\ell_{m-1}}$. When multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{\ell_0,\ell_1,\ldots,\ell_{m-1}}$, where $\mathbb{K}$ denotes a set of m-dimensional vectors whose i-th element takes a value between 0 and ℓ_i, it fulfills the following conditions:

$$\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases} \text{unknown}, & \exists \boldsymbol{k} \in \mathbb{K} \text{ s.t. } Wt(\boldsymbol{u}) \succeq \boldsymbol{k}, \\ 0, & \text{otherwise}, \end{cases}$$

where $\pi_{\boldsymbol{u}}(\boldsymbol{x})$ denotes the bit product function, whose definition can be found in [1].

Remark 1. If there are $\boldsymbol{k} \in \mathbb{K}$ and $\boldsymbol{k}' \in \mathbb{K}$ satisfying $\boldsymbol{k} \succeq \boldsymbol{k}'$ in division property $\mathcal{D}_{\mathbb{K}}^{\ell_0,\ell_1,\ldots,\ell_{m-1}}$, $\boldsymbol{k}$ can be removed from $\mathbb{K}$, because it is redundant.

The division property reflects the properties of a multiset. When a multiset undergoes some operations, its division property changes accordingly. Todo [1] proved several propagation rules governing the division property, which can be summarized with the following five rules (also listed in [2]): Substitution, Copy, XOR, Split, and Concatenation. Because this article mainly considers propagation of the division property of the S-box, we list only the Substitution rule below.

Rule 1 (Substitution [2])**.** Let F be a function that consists of m S-boxes, where the bit length and algebraic degree of the i-th S-box are ℓ_i and d_i, respectively. The input and output take values from $\mathbb{F}_2^{\ell_0} \times \mathbb{F}_2^{\ell_1} \times \cdots \times \mathbb{F}_2^{\ell_{m-1}}$, and $\mathbb{X}$ and $\mathbb{Y}$ denote the input and output multisets, respectively. Assuming that $\mathbb{X}$ has division property $\mathcal{D}_{\mathbb{K}}^{\ell_0,\ell_1,\ldots,\ell_{m-1}}$, where $\mathbb{K}$ denotes a set of m-dimensional vectors whose i-th element takes a value between 0 and ℓ_i, the division property of $\mathbb{Y}$ is $\mathcal{D}_{\mathbb{K}'}^{\ell_0,\ell_1,\ldots,\ell_{m-1}}$, as

$$\mathbb{K}' \leftarrow \left(\left\lceil \frac{k_0}{d_0} \right\rceil, \left\lceil \frac{k_1}{d_1} \right\rceil, \ldots, \left\lceil \frac{k_{m-1}}{d_{m-1}} \right\rceil \right),$$
$$\forall \boldsymbol{k} = (k_0, k_1, \ldots, k_{m-1}) \in \mathbb{K},$$

where $\mathbb{K} \leftarrow \boldsymbol{k}$ represents $\mathbb{K} \triangleq \mathbb{K} \cup \{\boldsymbol{k}\}$.

A special case of division property, the bit-based division property [3] traces the division property at the bit-level. Since it takes more information about the primitives into consideration, it enables

* Corresponding author (email: mqwang@sdu.edu.cn)
The authors declare that they have no conflict of interest.

the detection of better distinguishers. Although bit-based division property was successfully applied to SIMON32 [4] in [3], its feasibility to some bit-oriented block ciphers with S-boxes was unknown.

In this article, we integrate the algebraic normal form (ANF) of the S-box with the propagation of the division property, and devise a new method for tracing the propagation of the bit-based division property of the S-box. Since we replace the original Substitution rule with a more subtle propagation table reflecting more details of the S-box, we call our new method table-aided bit-based division property (TABBDP). Thus, the bit-based division property can be applied to search integral distinguishers for bit-oriented block ciphers with S-boxes.

TABBDP. For some bit-oriented block ciphers, the unique difficulty in handling their bit-based division property lies in the lack of bit-based division property propagation of the S-box. To overcome this problem, we analyze the ANF of the S-box.

Suppose that $\boldsymbol{x} = (x_0, x_1, \ldots, x_{\ell-1})$ and $\boldsymbol{y} = (y_0, y_1, \ldots, y_{\ell-1})$ are the input and output of an ℓ-bit S-box. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input and output multisets, respectively. Suppose that $\mathbb{X}$ follows the division property $\mathcal{D}^{1^\ell}_{\{\boldsymbol{k}\}}$, which implies that $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{j}}(\boldsymbol{x})$ is unknown for any $\boldsymbol{j} \in \mathbb{F}_2^\ell$ with $\boldsymbol{j} \succeq \boldsymbol{k}$.

According to the definition of the division property, determining the division property $\mathcal{D}^{1^\ell}_{\mathbb{K}}$ of $\mathbb{Y}$ corresponding to $\boldsymbol{k}$ is equivalent to identifying which vectors $\boldsymbol{k}'$ will make the parity $\bigoplus_{\boldsymbol{y}\in\mathbb{Y}} \pi_{\boldsymbol{k}'}(\boldsymbol{y})$ of $\pi_{\boldsymbol{k}'}(\boldsymbol{y})$ an unknown value. For any ℓ-bit string $\boldsymbol{k}'$, to judge whether the parity of $\pi_{\boldsymbol{k}'}(\boldsymbol{y})$ is always even, we check the ANF of $\pi_{\boldsymbol{k}'}(\boldsymbol{y})$. Suppose that

$$\pi_{\boldsymbol{k}'}(\boldsymbol{y}) = \prod_{i=0}^{\ell-1} \pi_{k_i'}(y_i) = \bigoplus_{\boldsymbol{u}\in\mathbb{F}_2^\ell} a_{\boldsymbol{u}} \pi_{\boldsymbol{u}}(\boldsymbol{x}),$$

where $a_{\boldsymbol{u}} \in \mathbb{F}_2$ are constants depending on $\pi_{\boldsymbol{k}'}(\boldsymbol{y})$ and $\boldsymbol{u}$. If there exists $\boldsymbol{j} \in \mathbb{F}_2^\ell$ satisfying $\boldsymbol{j} \succeq \boldsymbol{k}$ such that $a_{\boldsymbol{j}} = 1$, then the parity of $\pi_{\boldsymbol{k}'}(\boldsymbol{y})$ is unknown, since the value of $\bigoplus_{x\in\mathbb{X}} \pi_{\boldsymbol{j}}(\boldsymbol{x})$ is unknown. Otherwise, the parity of $\pi_{\boldsymbol{k}'}(\boldsymbol{y})$ is always even. After deducing all vectors $\boldsymbol{k}' \in \mathbb{F}_2^\ell$ making $\bigoplus_{\boldsymbol{y}\in\mathbb{Y}} \pi_{\boldsymbol{k}'}(\boldsymbol{y})$ unknown, we obtain the division property of the output multiset by reducing those redundant vectors.

This derivation utilizes only the definition of the division property, guaranteeing the validity of the resulting bit-based division property propagation. Repeating the former deduction process for each $\boldsymbol{k} \in \mathbb{F}_2^\ell$, we obtain the propagation rule for an S-box at the bit-level. This propagation rule can be organized into a two-column table called a propagation table. The 1st column stores the vectors $\boldsymbol{k}$ representing the input division properties, and the 2nd column lists the values of the corresponding output division properties. With this propagation table, the propagation of the bit-based division property through S-boxes becomes a simple table look-up, and its feasibility for some bit-oriented block ciphers with S-boxes is settled.

Improved TABBDP. When attempting to apply TABBDP, we found that its huge time and memory complexities became major obstacles. Not only does TABBDP break the intermediate states into bits, requiring more space in which to store the vectors, the exponential growth in the number of vectors included in $\mathbb{K}$ also produces rapid inflation in memory complexity. As a result, the time needed to deal with these vectors also increases.

A similar problem is also encountered when applying the traditional division property to some complicated primitives. Zhang and Wu [5] evaluated the security of the generalized Feistel structure (GFS) against integral attacks using the traditional division property, and found that it was difficult to directly trace propagation when branch number m of the GFS was larger than 14, owing to the rapid expansion of the vectors in the division property. They devised a technique called the early reduce technique to simplify the propagation procedure, which worked by detecting and discarding "useless" vectors. The feasibility of the early reduce technique relies on the following observation.

Observation 1 ([5]). Let $\boldsymbol{k}$ and $\boldsymbol{k}'$ be two vectors that propagate to $\{\boldsymbol{k}^{(0)}, \boldsymbol{k}^{(1)}, \ldots, \boldsymbol{k}^{(q-1)}\}$ and $\{\boldsymbol{k}'^{(0)}, \boldsymbol{k}'^{(1)}, \ldots, \boldsymbol{k}'^{(q'-1)}\}$, respectively, through the round function. If there exists a vector $\boldsymbol{k}'^{(j)} \in \{\boldsymbol{k}'^{(0)}, \boldsymbol{k}'^{(1)}, \ldots, \boldsymbol{k}'^{(q'-1)}\}$, such that $\boldsymbol{k}^{(i)} \succeq \boldsymbol{k}'^{(j)}$ for each $\boldsymbol{k}^{(i)} \in \{\boldsymbol{k}^{(0)}, \boldsymbol{k}^{(1)}, \ldots, \boldsymbol{k}^{(q-1)}\}$, $\Omega \cup \{\boldsymbol{k}, \boldsymbol{k}'\}$ and $\Omega \cup \{\boldsymbol{k}'\}$ propagate to the same division property for any vector set Ω.

Thus, if $\boldsymbol{k} \in \mathbb{K}$ and $\boldsymbol{k}' \in \mathbb{K}$ are vectors satisfying the property in Observation 1, we need only propagate $\mathbb{K}\backslash\{\boldsymbol{k}\}$ instead of $\mathbb{K}$ to get the output division property. We find that the early reduce technique also can be applied to TABBDP. If there are many vector pairs in $\mathbb{K}$ that follow the property in Observation 1, the number of vectors in $\mathbb{K}$ drops dramatically. Thus, the time to propagate the vectors in $\mathbb{K}$ is reduced and the number of vectors in the resulting output division property may be controlled.

With this in mind, we adopt the early reduce technique into TABBDP using an addition table called an early reduce table. This table includes

two columns: the 1st column represents vector $\boldsymbol{k}'$ and the corresponding values in the 2nd column are the vectors $\boldsymbol{k}$ that can be reduced by $\boldsymbol{k}'$. When we want to apply the early reduce technique to TABBDP, an additional early reduce procedure should be performed following the original reduce procedure. In this step, we check the early reduce table and delete all $\boldsymbol{k}$ with a corresponding $\boldsymbol{k}'$ included in $\mathbb{K}$. We apply this technique to the analysis of many objectives, and observe that the number of vectors in $\mathbb{K}$ decreases tremendously.

Improved higher-order integral distinguishers for RECTANGLE. RECTANGLE [6] is a new lightweight block cipher that utilizes SP-network. The block size is 64 bits, and the key length is 80 or 128 bits. Each of the 25 rounds consists of three steps: AddRoundKey, SubColumn, and ShiftRow. After the last round, there is a final AddRoundKey. Please refer to [6] for more details. The designers of RECTANGLE gave a 7-round higher-order integral distinguisher with data complexity 2^{48}.

In this article, we detect two new higher-order integral distinguishers for RECTANGLE by utilizing TABBDP. One covers 7 rounds with data complexity 2^{36}, which is 2^{12} less than the previous distinguisher, and another achieves 8 rounds, whose data requirement is 2^{48} chosen plaintexts. Note that the newly obtained 8-round distinguisher attains one more round than that proposed by the designers while maintaining the data complexity. (We do not list the details of the construction of the distinguishers due to space limitations. Please refer to the supplementary files for more information.)

Generalized bit-based division property: potential usage scenarios for word-oriented block ciphers. TABBDP can also be applied to searching for integral distinguishers for some word-oriented block ciphers. We successfully used it to find integral distinguishers for LBlock [7] and TWINE [8]. Although we did not obtain any new integral distinguishers for these ciphers, we believe that considering the S-box at the bit level is of significant importance, even for a word-oriented block cipher. A more adequate invocation of the details of an encryption algorithm usually guarantees a better analysis result.

Acknowledgements The work was supported by National Basic Research Program of China (973 Program) (Grant No. 2013CB834205), National Natural Science Foundation of China (Grant No. 61572293), and Science and Technology on Communication Security Laboratory of China (Grant No. 9140c110207150c11050).

Supporting information The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Todo Y. Structural evaluation by generalized integral property. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015. 287–314
2 Todo Y. Integral cryptanalysis on full MISTY1. In: Proceedings of Annual Cryptology Conference on Advances in Cryptology — CRYPTO 2015. Berlin: Springer, 2015. 413–432
3 Todo Y, Morii M. Bit-based division property and application to SIMON family. In: Proceedings of International Conference on Fast Software Encryption. Berlin: Springer, 2016. 357–377
4 Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK lightweight block ciphers. In: Proceedings of the 52nd Annual Design Automation Conference, San Francisco, 2015
5 Zhang H L, Wu W L. Structural evaluation for generalized feistel structures and applications to LBlock and TWINE. In: Proceedings of International Cryptology Conference on Progress in Cryptology — INDOCRYPT 2015. Berlin: Springer, 2015. 218–237
6 Zhang W T, Bao Z Z, Lin D D, et al. RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Sci China Inf Sci, 2015, 58: 122103
7 Wu W L, Zhang L. LBlock: a lightweight block cipher. In: Proceedings of the 9th International Conference on Applied Cryptography and Network Security, Nerja, 2011. 327–344
8 Suzaki T, Minematsu K, Morioka S, et al. TWINE: a lightweight block cipher for multiple platforms. In: Proceedings of the 19th International Conference on Selected Areas in Cryptography, Windsor, 2012. 339–354