SCIENCE CHINA
Information Sciences

• **Supplementary File** •

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*

Appendix A Why we choose TABBDP?

The superior of TABBDP mainly reflects on the propagation table, and we will take RECTANGLE's S-box as an illustration. Note that the algebraic degree of RECTANGLE's S-box is equal to 3, and the propagation of conventional division property only have the following possibilities.

$$\begin{cases} \text{The output division property is } \mathcal{D}^4_{\{4\}}, & \text{if the input division property is } \mathcal{D}^4_{\{4\}}. \\ \text{The output division property is } \mathcal{D}^4_{\{1\}}, & \text{if the input division property is } \mathcal{D}^4_{\{3\}}, \mathcal{D}^4_{\{2\}}, \text{ or } \mathcal{D}^4_{\{1\}}. \\ \text{The output division property is } \mathcal{D}^4_{\{0\}}, & \text{if the input division property is } \mathcal{D}^4_{\{0\}}. \end{cases} \tag{A1}$$

On the other hand, the propagation table of RECTANGLE's S-box can be found in **Table A1**. We take $\boldsymbol{k} = [0, 0, 1, 1]$ as an example, and suppose that an input multi-set has bit-based division property $\mathcal{D}^{1^4}_{\{[0,0,1,1]\}}$. Being aware of that $\mathcal{D}^{1^4}_{\{[0,0,1,1]\}}$ belongs to the case of $\mathcal{D}^4_{\{2\}}$ in conventional division property, which implies that the output division property is $\mathcal{D}^4_{\{1\}}$. Note that $\mathcal{D}^4_{\{1\}}$ corresponds to $\mathcal{D}^{1^4}_{\mathbb{K}}$, where $\mathbb{K} = \{[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 1, 0], [0, 0, 0, 1]\}$, in bit-based division property. But **Table A1** shows that the output bit-based division property is actually $\mathcal{D}^{1^4}_{\mathbb{K}'}$, where $\mathbb{K}' = \{[0, 0, 0, 1], [0, 1, 0, 0], [1, 0, 1, 0]\}$. Since the construction of propagation table considers the ANF of the S-box, some useful information besides the algebraic degree is retained. These information allows us to deduce a more proper division property for the output multi-set. Thus, we have reasons to believe that TABBDP is more powerful than conventional division property.

Appendix B Application of TABBDP to RECTANGLE

Appendix B.1 RECTANGLE [3]

RECTANGLE [3] is a new lightweight block cipher and utilizes SP-network. The design philosophy is to allow lightweight and fast implementations using bit-slice technique. 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`. Since our analysis does not involve subkeys, the key schedule is not involved here. We omit the suffix and simply write RECTANGLE for simplicity.

We use a representation similar to the representation of Serpent in [1] to express the 64-bit internal state of RECTANGLE. The figure describes data block by rectangle of 4 rows and 16 columns. Let $\boldsymbol{a} = (a[0], a[1], \ldots, a[63])$ denote a cipher state, the cipher state is described in a two-dimensional way, as illustrated in the following.

$$\begin{bmatrix} a[48] & a[49] & \cdots & a[63] \\ a[32] & a[33] & \cdots & a[47] \\ a[16] & a[17] & \cdots & a[31] \\ a[0] & a[1] & \cdots & a[15] \end{bmatrix}$$

The non-linear operation `SubColumn` includes 16 parallel applications of S-boxes to the 4 bits in the same column. We illustrate the round function of RECTANGLE in **Figure B1**.

The designers gave a 7-round higher-order integral distinguisher in [3]. 2^{48} plaintexts were required in order to observe zero-sum bits after seven rounds of encryption.

* Corresponding author (email: mqwang@sdu.edu.cn)

Table A1 Propagation table of RECTANGLE's S-box

Input $\mathcal{D}^{1^4}_{\{\boldsymbol{k}\}}$	Output $\mathcal{D}^{1^4}_{\mathbb{K}'}$
$\boldsymbol{k}=[0,0,0,0]$	$\mathbb{K}'=\{[0,0,0,0]\}$
$\boldsymbol{k}=[0,0,0,1]$	$\mathbb{K}'=\{[0,0,0,1],[0,0,1,0],[0,1,0,0],[1,0,0,0]\}$
$\boldsymbol{k}=[0,0,1,0]$	$\mathbb{K}'=\{[0,0,0,1],[0,0,1,0],[0,1,0,0],[1,0,0,0]\}$
$\boldsymbol{k}=[0,0,1,1]$	$\mathbb{K}'=\{[0,0,0,1],[0,1,0,0],[1,0,1,0]\}$
$\boldsymbol{k}=[0,1,0,0]$	$\mathbb{K}'=\{[0,0,0,1],[0,0,1,0],[0,1,0,0],[1,0,0,0]\}$
$\boldsymbol{k}=[0,1,0,1]$	$\mathbb{K}'=\{[0,0,1,1],[0,1,0,0],[1,0,0,0]\}$
$\boldsymbol{k}=[0,1,1,0]$	$\mathbb{K}'=\{[0,0,1,1],[0,1,0,0],[1,0,0,0]\}$
$\boldsymbol{k}=[0,1,1,1]$	$\mathbb{K}'=\{[0,0,1,1],[0,1,0,0],[1,0,0,1]\}$
$\boldsymbol{k}=[1,0,0,0]$	$\mathbb{K}'=\{[0,0,0,1],[0,0,1,0],[0,1,0,0],[1,0,0,0]\}$
$\boldsymbol{k}=[1,0,0,1]$	$\mathbb{K}'=\{[0,0,1,1],[0,1,0,1],[0,1,1,0],[1,0,0,0]\}$
$\boldsymbol{k}=[1,0,1,0]$	$\mathbb{K}'=\{[0,0,1,0],[0,1,0,1],[1,0,0,0]\}$
$\boldsymbol{k}=[1,0,1,1]$	$\mathbb{K}'=\{[0,1,1,0],[1,0,1,1],[1,1,0,1]\}$
$\boldsymbol{k}=[1,1,0,0]$	$\mathbb{K}'=\{[0,0,1,1],[0,1,0,0],[1,0,0,0]\}$
$\boldsymbol{k}=[1,1,0,1]$	$\mathbb{K}'=\{[0,1,1,0],[1,0,1,0],[1,1,0,1]\}$
$\boldsymbol{k}=[1,1,1,0]$	$\mathbb{K}'=\{[0,0,1,1],[0,1,0,1],[1,0,0,0]\}$
$\boldsymbol{k}=[1,1,1,1]$	$\mathbb{K}'=\{[1,1,1,1]\}$

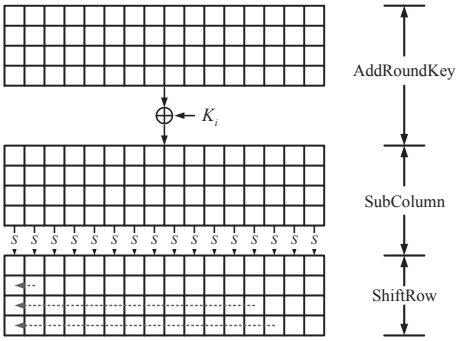

Figure B1 Round function of RECTANGLE.

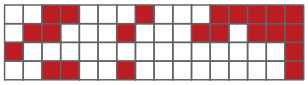

Figure B2 Zero-sum bits after five rounds of encryption.

Appendix B.2 7-round higher-order integral distinguisher

We combine TABBDP with higher-order differential attack. Firstly, we find a 5-round integral distinguisher by using TABBDP whose input multi-set satisfies $\mathcal{D}^{1^{64}}_{\{\texttt{[00010001,00010001]}\}}$. After analysing, we know that there still are 22 bits satisfy zero-sum property after five rounds of encryption, which are illustrated in **Figure B2**. The squares dyed in red in **Figure B2** correspond to the bits with zero-sum property. We randomly generate 2^{10} master keys and verify the zero-sum bits. The experimental results show that the bits corresponding to those red squares in **Figure B2** indeed satisfy zero-sum property after five rounds of encryption.

In order to get the 7-round higher-order integral distinguisher, we extend two rounds before the 5-round integral distinguisher. This procedure is illustrated in **Figure B3**. Note that the resulting higher-order integral distinguisher requires 2^{36} plaintexts to observe zero-sum bits after seven rounds of encryption, which is 2^{12} less than the original one.

Appendix B.3 8-round higher-order integral distinguisher

Firstly, we find a 6-round integral distinguisher by applying early reduce technique to TABBDP whose input multi-set satisfies $\mathcal{D}^{1^{64}}_{\{\texttt{[00030003,00030003]}\}}$, *i.e.*, we traverse eight bits located at the given positions. If we do not use early reduce technique, we observe rapid inflation in memory complexity, which prevents us from getting this integral distinguisher. We give a comparison for the number of vectors in $\mathbb{K}$ before and after using this technique in **Table B1**.

Among the 63 vectors after six rounds of encryption, the Hamming weights of 62 vectors are equal to one and the hamming weight of the remaining one is equal to 2. The unique vector with hamming weight equal to 2 is `[00000000,00000003]`, which implies that the 62-nd and 63-rd bit of the state after six rounds of encryption satisfy zero-sum property. We randomly generate 2^{10} master keys and verify the zero-sum property. The experimental results show that these two bits indeed satisfy

Table B1 Comparison of number of vectors for RECTANGLE with input division property $\mathcal{D}^{1^{64}}_{\{\texttt{[00030003,00030003]}\}}$

Round	**1**	**2**	**3**	**4**	**5**	**6**
$\#\mid\mathbb{K}\mid^{u}$	1	2304	260281	-†	-†	-†
$\#\mid\mathbb{K}\mid^{eu}$	1	1668	4207	455	34	63‡

1: $\#\mid\mathbb{K}\mid^{u}$: The number of vectors in the TABBDP.
2: $\#\mid\mathbb{K}\mid^{eu}$: The number of vectors after using early reduce technique.
†: For the rapid inflation of memory complexity, we can not trace the propagation after 4 rounds of encryption.
‡: Even through early reduce technique does not change the division property achieved through one round function, it may prematurely reduce the division property to a terminate condition just as what has been pointed out in [2]. So we do not use early reduce technique in the last round.

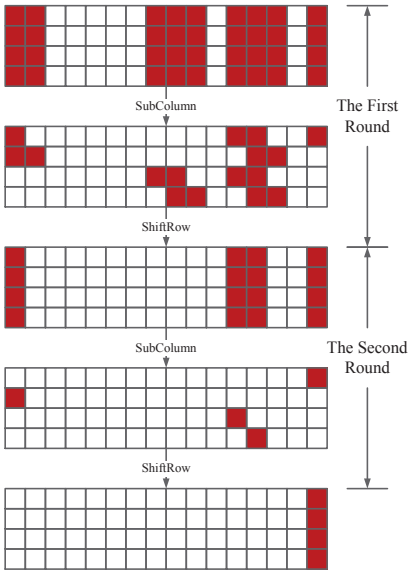

Figure B3 Extending the 5-round integral distinguisher to a 7-round higher-order integral distinguisher.

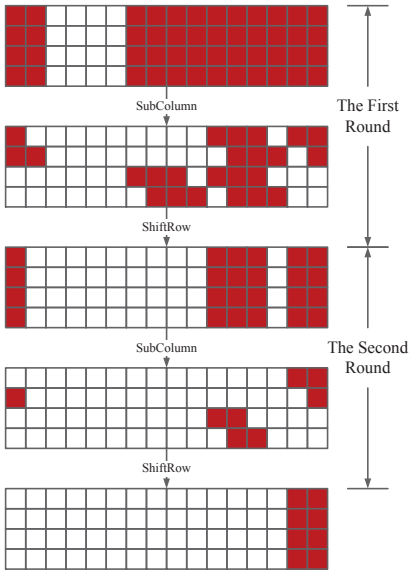

Figure B4 Extending the 6-round integral distinguisher to an 8-round higher-order integral distinguisher.

zero-sum property after six rounds of encryption.

With this 6-round integral distinguisher, we construct an 8-round higher-order integral distinguisher. Similarly to the procedure of constructing the 7-round higher-order integral distinguisher, we extend two rounds before the 6-round integral distinguisher found above, which is illustrated in **Figure B4**. Note that this new higher-order integral distinguisher attains one more round than the one provided by the designers.

References

1 Biham E, Dunkelman O, Keller N. The rectangle attackrectangling the serpent. In: Advances in CryptologyEUROCRYPT 2001. Berlin: Springer, 2001, 340-357
2 Zhang H L, Wu W L. Structural evaluation for generalized feistel structures and applications to LBlock and TWINE. In: Progress in Cryptology–INDOCRYPT 2015. Switzerland: Springer, 2015, 218-237
3 Zhang W T, Bao Z Z, Lin D D, et al. RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Science China Information Sciences, 2015, 58(12): 1-15