SCIENCE CHINA
Information Sciences

• LETTER •

April 2022, Vol. 65 149101:1–149101:3
https://doi.org/10.1007/s11432-019-2634-7

On the bit-based division property of S-boxes

Zejun XIANG, Xiangyong ZENG* & Shasha ZHANG

Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics,
Hubei University, Wuhan 430062*, China*

Received 4 May 2019/Revised 9 August 2019/Accepted 30 August 2019/Published online 24 May 2021

Citation Xiang Z J, Zeng X Y, Zhang S S. On the bit-based division property of S-boxes. Sci China Inf Sci, 2022, 65(4): 149101, https://doi.org/10.1007/s11432-019-2634-7

Dear editor,

The S-box, which is one of the most popular cipher components, has been extensively applied in modern symmetric-key primitives. Moreover, it is often the case that S-boxes are the only nonlinear components of the cipher. Thus, numerous previously conducted studies have been focused on the design criteria of S-boxes. The two mostly researched design criteria are resistances against differential and linear cryptanalysis. Recently, a new cryptanalysis technique called division property [1] was proposed at EUROCRYPT 2015. Although, various researches [2–4] have been conducted since it was proposed, the design criteria of S-boxes regarding division property are still not known to the public.

This study proposes two new notions called divisional optimal and divisional suboptimal S-boxes, which can serve as design criteria of S-boxes regarding the division property. We demonstrate that a divisional optimal S-box has the best resistance against divisional cryptanalysis. With an increase in the need for security in radio frequency identification (RFID) and sensor networks in the past decade, 4-bit S-boxes are more popular choices for lightweight cryptography owing to their compact implementations on both software and hardware. Thus, we focus on and analyze all the 4-bit S-boxes regarding the division property. We obtain 4150 divisional optimal permutation equivalence (PE) classes, but none of them are differential-linear optimal. However, we obtain 1536 PE classes of 4-bit S-boxes that are divisional suboptimal and differential-linear optimal at the same time. By applying these S-boxes to two lightweight block ciphers PRIDE [5] and PUFFIN [6], we show the power of divisional suboptimal S-box.

We first introduce the definition of (bit-based) division property and present bit-based division property propagations of S-boxes.

Definition 1 ([1])**.** Let $k=(k_{n-1},k_{n-2},\ldots,k_0)$, $k'=(k'_{n-1},k'_{n-2},\ldots,k'_0)$ be two n-dimensional vectors, and $k_i,k'_i\in\{0,1\},i=0,1,\ldots,n-1$. We denote $k\succeq k'$ if $k_i\geqslant k'_i$ for all i from 0 to $n-1$, otherwise $k\not\succeq k'$.

Definition 2 (Division property [1])**.** Let X be a multiset of $\mathbb{F}_2^n$, and $k^0,k^1,\ldots,k^{t-1}$ are n-dimensional vectors whose elements belong to $\{0,1\}$. The division property of X is $\mathcal{D}^{1,n}_{k^0,k^1,\ldots,k^{t-1}}$, if X satisfies the following conditions:

$$\bigoplus_{x\in X}\Pi_{i=0}^{n-1}x_i^{u_i}=0, \tag{1}$$

for all u belongs to the following set:

$$\{u\in\{0,1\}^n|u\not\succeq k^j,j=0,1,\ldots,t-1\}. \tag{2}$$

The Algorithm 1 in [4] illustrates the computations of division property propagations of any S-box for the given input division property, and we summarize the computations in the following lemma.

Lemma 1. Let S be an n-bit S-box. Assume that the input division property of S is $\mathcal{D}^{1,n}_{k}$, where k denotes an n-dimensional binary vector. Let u denote an n-dimensional binary vector. Then, the input division property k can propagate to u, if and only if there exists at least one monomial in $\Pi_{i=0}^{n-1}S_i^{u_i}$ such that it contains all the variables in $\{x_i|k_i=1,i=0,\ldots,n-1\}$.

Based on the division property propagations of S-boxes, the following definitions are important for characterizing the resistances of an S-box against divisional cryptanalysis.

Definition 3. Let f be a balanced n-variable Boolean function. The high-degree index of f is defined as the number of monomials in f with degree $n-1$. If the high-degree index of f equals n, then we call f a divisional optimal Boolean function.

Definition 4 (High-degree index of S-boxes)**.** Let S be a balanced n-bit S-box, and $S(x)=(s_{n-1}(x),s_{n-2}(x),\ldots,s_0(x))$, where $s_i(x)$ denotes the ith coordinate Boolean function of S. The high-degree index of S is defined as the sum of the high-degree indices of all $s_i(x)$'s.

Definition 5 (Divisional optimal S-box)**.** Let S denote a balanced n-bit S-box. We call S a divisional optimal S-box if the high-degree index of S equals n^2, i.e., all the coordinate Boolean functions of S are divisional optimal Boolean functions.

Theorem 1. Let S be a divisional optimal S-box. The division property propagations of S are as follows.

* Corresponding author (email: xzeng@hubu.edu.cn)

Table 1 Divisional suboptimal S-boxes

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S^0(x)$	6	c	8	3	4	d	0	7	2	a	9	f	1	5	e	b
$S^1(x)$	5	8	c	3	4	0	e	7	1	a	9	f	2	d	6	b
$S^2(x)$	3	8	2	0	a	5	e	7	1	c	4	b	9	f	6	d
$S^3(x)$	3	4	2	0	1	c	8	7	6	9	e	b	5	f	a	d

- If the input division property of S is $(1, 1, \ldots, 1)$, then the output division property of S is $(1, 1, \ldots, 1)$;
- If the input division property of S is k with $1 \leqslant \mathrm{wt}(k) \leqslant n-1$, then the output division property of S is $(1, 0, \ldots, 0)$, $(0, 1, \ldots, 0)$, …, $(0, 0, \ldots, 1)$. In other words, the output division property can take all the n unit vectors and none of the output bits are balanced.
- If the input division property of S is $(0, 0, \ldots, 0)$, then the output division property of S is $(0, 0, \ldots, 0)$.

For any 4-bit S-box S, we call it DL-optimal if the differential uniformity and linearity of S are equal to 4 and 8, respectively. Moreover, we call S a D-optimal S-box if its differential uniformity is equal to 4, and we call it an L-optimal S-box if its linearity is equal to 8. Thereafter, the distributions of all 4-bit S-boxes regarding D-optimal, L-optimal, and divisional optimal are analyzed. We utilized PE class to reduce the space of the analyzed S-boxes.

Definition 6 (PE [7]). Let P_i and P_o denote two bit permutation matrices and c_i and c_o denote two vectors. Then, the S-box S' defined by

$$S'(x) = P_o S(P_i(x \oplus c_i)) \oplus c_o$$

belongs to the PE class of S, that is, $S' \in \mathrm{PE}(S)$.

Theorem 2. Suppose that S and S' denote two n-bit S-boxes belonging to the same PE class, then S is divisional optimal if and only if S' is divisional optimal.

We exhaustively studied all the 4-bit S-boxes based on PE class and the results obtained are as follows.

- There are no S-boxes that are both divisional optimal and DL-optimal.
- There are no S-boxes that are both divisional optimal and D-optimal.
- There are 784 equivalence classes that are both divisional optimal and L-optimal, in which the best differential uniformity is equal to 8.
- Considering all the 4150 divisional optimal equivalence classes, the best differential uniformity is equal to 6 and 448 equivalence classes achieve this bound, in which the best linearity is euqal to 12.

Clearly, no 4-bit S-box exists that is both divisional optimal and DL-optimal. Thus, we make a trade-off between these cryptographic properties. In most cases, we note that differential and linear attacks are more serious threats than division property based integral attacks for many ciphers. Consequently, we would sacrifice division property for optimal differential and linear properties.

Definition 7 (Divisional suboptimal S-box). Let S be a balanced n-bit S-box. If the high-degree indices of $n-1$ coordinate Boolean functions equal n and the high-degree index of the remaining one coordinate Boolean function equals $n-1$, we call S a divisional suboptimal S-box.

Theorem 3. Let $S(x) = (s_{n-1}(x), s_{n-2}(x), \ldots, s_0(x))$ be an n-bit divisional suboptimal S-box. Then, there exist i $(0 \leqslant i \leqslant n-1)$ and $u \in \mathbb{F}_2^n$ with $\mathrm{wt}(u) = n-1$, such that x^u is not in the ANF of $s_i(x)$. Moreover, the division property propagations are as follows:

- If the input division property of S is $(1, 1, \ldots, 1)$, then the output division property of S is $(1, 1, \ldots, 1)$.
- If the input division property of S is u, then the output division property of S is

$$(1, 0, \ldots, 0, \underset{\underset{i\text{-th}}{\uparrow}}{0}, 0, \ldots, 0, 0), \ldots, (0, 0, \ldots, 1, \underset{\underset{i\text{-th}}{\uparrow}}{0}, 0,$$

$$\ldots, 0, 0), (0, 0, \ldots, 0, \underset{\underset{i\text{-th}}{\uparrow}}{0}, 1, \ldots, 0, 0), \ldots, (0, 0, \ldots,$$

$$0, \underset{\underset{i\text{-th}}{\uparrow}}{0}, 0, \ldots, 0, 1).$$

- If the input division property of S is denoted by k with $1 \leqslant \mathrm{wt}(k) \leqslant n-2$, or $\mathrm{wt}(k) = n-1$ and $k \neq u$, then the output division property of S is $(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)$. Therefore, the output division property can take all the n unit vectors.
- If the input division property of S is $(0, 0, \ldots, 0)$, then the output division property of S is $(0, 0, \ldots, 0)$.

Theorem 4. Suppose that S and S' are two n-bit S-boxes belonging to the same PE class, then S is divisional suboptimal if and only if S' is divisional suboptimal.

After an exhaustive analysis of all 4-bit S-boxes, the results obtained are as follows:

- There are 1536 equivalence classes that are both divisional suboptimal and DL-optimal.
- There are 1536 equivalence classes that are both divisional suboptimal and D-optimal.
- There are 7296 equivalence classes that are both divisional suboptimal and L-optimal.

Thus, only the suboptimal divisional 4-bit S-boxes can be obtained without forfeiting the differential and linear properties. To illustrate the advantages of using suboptimal divisional S-boxes, four alternative S-boxes are presented (see Table 1) for two lightweight block ciphers PRIDE and PUFFIN. These alternative S-boxes agree with the design criteria of the original S-boxes, and they have the same differential and linear properties. Moreover, these alternative S-boxes enjoy extra advantages of having better resistances against divisional cryptanalysis. When these four alternative S-boxes are used in PRIDE, we can only find 6-round integral distinguishers, while the original PRIDE has an 8-round distinguisher. When these four alternative S-boxes are used in PUFFIN, three of them have 8-round distinguishers and one of them has a 9-round distinguisher. However, the original PUFFIN has a 9-round distinguisher.

Conclusion. This study investigated the design criteria of S-box against divisional cryptanalysis. A new notion called high-degree index was proposed. Based on this new notion, we defined S-boxes called divisional optimal S-boxes with the best resistance against divisional cryptanalysis. Moreover, the new design criteria were applied to 4-bit S-boxes, and experimental results showed that 4-bit S-boxes cannot achieve both the best differential-linear and divisional properties. In addition, we proposed another kind of S-boxes with suboptimal resistance against divisional cryptanalysis called divisional suboptimal S-boxes. We obtained 1536 divisional suboptimal S-box classes which achieved the best differential and linear properties at the same time. Without loss of the cipher's security against differential and linear cryptanalysis, we applied our divisional suboptimal S-boxes to two lightweight ciphers PRIDE and PUFFIN. The experimental results illustrated that the divisional suboptimal S-boxes indeed improved the ciphers' security against divisional cryptanalysis.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61802119).

References

1 Todo Y. Structural evaluation by generalized integral property. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 287–314

2 Sun B, Hai X, Zhang W Y, et al. New observation on division property. Sci China Inf Sci, 2017, 60: 098102

3 Sun L, Wang M Q. Toward a further understanding of bit-based division property. Sci China Inf Sci, 2017, 60: 128101

4 Xiang Z J, Zhang W T, Bao Z Z, et al. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, 2016. 648–678

5 Albrecht M R, Driessen B, Kavun E B, et al. Block ciphers - focus on the linear layer (feat. PRIDE). In: Proceedings of Annual Cryptology Conference, Santa Barbara, 2014. 57–76

6 Cheng H J, Heys H M, Wang C. PUFFIN: a novel compact block cipher targeted to embedded digital systems. In: Proceedings of Euromicro Conference on Digital System Design: Architectures, Methods and Tools, Parma, 2008. 383–390

7 Saarinen M J O. Cryptographic analysis of all 4 × 4-bit s-boxes. In: Proceedings of International Workshop on Selected Areas in Cryptography, Toronto, 2011. 118–133