SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

November 2018, Vol. 61 118102:1–118102:3
https://doi.org/10.1007/s11432-017-9321-7

MILP-aided bit-based division property for ARX ciphers

Ling SUN[1,2], Wei WANG[1*], Ru LIU[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, No.* 30 *Research Institute of China Electronics Technology Group Corporation, Chengdu* 610041*, China;*
[3]*State Key Laboratory of Cryptology, P.O. Box* 5159*, Beijing* 100878*, China*

Received 11 September 2017/Accepted 30 November 2017/Published online 21 May 2018

Citation Sun L, Wang W, Liu R, et al. MILP-aided bit-based division property for ARX ciphers. Sci China Inf Sci, 2018, 61(11): 118102, https://doi.org/10.1007/s11432-017-9321-7

Division property, which was proposed by Todo [1] at EUROCRYPT 2015, is a new technique to detect integral property. It could explicitly depict the hidden properties between the traditional ALL and BALANCE properties in integral cryptanalysis [2], which made it an effective method to search integral distinguishers. The definition is given as follows.

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].

As a special case of division property, bit-based division property [3] propagates division property at the bit-level, and enables us to detect longer distinguishers because more information, besides the algebraic degree, is taken into consideration. At ASIACRYPT 2016, Xiang et al. [4] introduced mixed integer linear programming (MILP) method to search integral distinguishers based on bit-based division property automatically. The searching problem is converted into an MILP problem, which can be solved by some openly available MILP optimizers. But their algorithms were restricted to ciphers with bitwise permutations. Soon after, the feasibility of MILP method to search integral distinguishers for primitives with non-bit-permutation linear layers was settled by Sun et al. [5]. Recently, Todo et al. [6] exploited the MILP method to analyze algebraic normal form (ANF) of the Boolean function, and proposed the cube attacks on non-blackbox polynomials, which was used to analyze some stream ciphers.

Since the appearance of division property, there has been little progress in the automatic search of division property for ARX ciphers, which constitute a broad class of symmetric ciphers and are composed of bitwise operations, such as modular addition, bit rotation, bit shift and XOR. In this article, we aim to solve this problem.

The division property focuses on the parity $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x})$ is 0 or unknown, which naturally divides the m-dimensional vector space $\mathbb{Z}_{\ell_0+1} \times \mathbb{Z}_{\ell_1+1} \times \cdots \times \mathbb{Z}_{\ell_{m-1}+1}$ into two sets, where $\mathbb{Z}_\ell \triangleq \{0, 1, \ldots, \ell-1\}$. These two sets, whose sizes reflect the power of the division property, are used to trace propagations for some operations in the

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

following.

Definition 2 (Known-region and unknown-region)**.** Let $\mathbb{X}$ be a multi-set, whose elements belong to $\mathbb{F}_2^{\ell_0} \times \mathbb{F}_2^{\ell_1} \times \cdots \times \mathbb{F}_2^{\ell_{m-1}}$, with division property $\mathcal{D}_{\mathbb{K}}^{\ell_0,\ell_1,\ldots,\ell_{m-1}}$. For any $\boldsymbol{k}$ in $\mathbb{K}$, let

$$\mathbb{S}_{\boldsymbol{k}}^n = \{\boldsymbol{a} \in \mathbb{Z}_{\ell_0,\ell_1,\ldots,\ell_{m-1}} | W(\boldsymbol{a}) \succeq W(\boldsymbol{k})\},$$

where $\mathbb{Z}_{\ell_0,\ell_1,\ldots,\ell_{m-1}} \triangleq \mathbb{Z}_{\ell_0+1} \times \mathbb{Z}_{\ell_1+1} \times \cdots \times \mathbb{Z}_{\ell_{m-1}+1}$. And let $\mathbb{S}_{\mathbb{K}}^n$ be

$$\mathbb{S}_{\mathbb{K}}^n = \bigcup_{\boldsymbol{k}\in\mathbb{K}} \mathbb{S}_{\boldsymbol{k}}^n = \left\{ \boldsymbol{u} \middle| \bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \text{unknown} \right\}.$$

We call $\mathbb{S}_{\mathbb{K}}^n$ the unknown-region deduced by the division property, and its complementary set is called the known-region.

In order to realize the automatic search of bit-based division property for ARX ciphers, the key point is to transform the division property propagation of r-round encryption into a system of linear inequalities. Because the expressions of the initial division property and the stopping rule, and the MILP models for some basic operations, except for the modular addition operation, have been settled in the former studies [4–6], we only focus on the construction of MILP model for the modular addition operation.

First of all, we give an iterated Boolean expression of the modular addition operation.

Let $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$, $\boldsymbol{y} = (y_0, y_1, \ldots, y_{n-1})$, and $\boldsymbol{z} = (z_0, z_1, \ldots, z_{n-1})$ be n-bit vectors with $\boldsymbol{z} = \boldsymbol{x} \boxplus \boldsymbol{y}$. Then the Boolean functions of z_i's can be iteratively calculated by

$$\begin{cases} z_{n-1} = x_{n-1} \oplus y_{n-1} \oplus c_{n-1},\ c_{n-1} = 0, \\ z_i = x_i \oplus y_i \oplus c_i, \\ c_i = x_{i+1} \wedge y_{i+1} \oplus (x_{i+1} \oplus y_{i+1}) \wedge c_{i+1}, \\ i = n-2, n-3, \ldots, 0. \end{cases} \tag{1}$$

MILP model for $\boldsymbol{z} = \boldsymbol{x} \boxplus \boldsymbol{y}$. Inspired by the iterated Boolean expression of modular addition, we notice that the computation of every z_i can be decomposed into a series of bitwise basic operations, including Copy, AND, and XOR. Since we already have the MILP models for these basic operations, we are able to construct MILP model for the modular addition operation, iteratively.

Model 1 (Modular addition $\boldsymbol{z} = \boldsymbol{x} \boxplus \boldsymbol{y}$)**.** Assuming

$$(x_0^d, x_1^d, \ldots, x_{n-1}^d, y_0^d, y_1^d, \ldots, y_{n-1}^d) \xrightarrow{\boxplus} (z_0^d, z_1^d, \ldots, z_{n-1}^d),$$

a division trail of the modular addition operation $\boldsymbol{x} \boxplus \boldsymbol{y}$, the following linear inequality system covers all possible division trails.

$$\begin{cases} x_{n-1}^d - t_0 - t_1 = 0, \\ y_{n-1}^d - t_2 - t_3 = 0, \\ t_0 + t_2 - z_{n-1}^d = 0, \\ v_0 - t_1 \geqslant 0, \\ v_0 - t_3 \geqslant 0, \\ v_0 - t_1 - t_3 \leqslant 0, \\ v_0 - g_0 - r_0 = 0, \\ \boldsymbol{x_{n-i-2}^d - u_{3i} - u_{3i+1} - u_{3i+2} = 0}, \\ \boldsymbol{y_{n-i-2}^d - u_{3n+3i-6} - u_{3n+3i-5}} \\ \quad \boldsymbol{- u_{3n+3i-4} = 0}, \\ \boldsymbol{u_{3i} + u_{3n+3i-6} + g_i - z_{n+i-2}^d = 0}, \\ \boldsymbol{v_{i+1} - u_{3i+1} \geqslant 0}, \\ \boldsymbol{v_{i+1} - u_{3n+3i-5} \geqslant 0}, \\ \boldsymbol{v_{i+1} - u_{3i+1} - u_{3n+3i-5} \leqslant 0}, \\ \boldsymbol{u_{3i+2} + u_{3n+3i-4} - m_i = 0}, \\ \boldsymbol{q_i - m_i \geqslant 0}, \\ \boldsymbol{q_i - r_i \geqslant 0}, \\ \boldsymbol{q_i - m_i - r_i \leqslant 0}, \\ \boldsymbol{v_{i+1} + q_i - w_i = 0}, \\ \boldsymbol{w_i - g_{i+1} - r_{i+1} = 0}, \\ x_1^d - u_{3n-9} - u_{3n-8} - u_{3n-7} = 0, \\ y_1^d - u_{6n-15} - u_{6n-14} - u_{6n-13} = 0, \\ u_{3n-9} + u_{6n-15} + g_{n-3} - z_1^d = 0, \\ v_{n-2} - u_{3n-8} \geqslant 0, \\ v_{n-2} - u_{6n-14} \geqslant 0, \\ v_{n-2} - u_{3n-8} - u_{6n-14} \leqslant 0, \\ u_{3n-7} + u_{6n-13} - m_{n-3} = 0, \\ q_{n-3} - m_{n-3} \geqslant 0, \\ q_{n-3} - r_{n-3} \geqslant 0, \\ q_{n-3} - m_{n-3} - r_{n-3} \leqslant 0, \\ v_{n-2} + q_{n-3} - w_{n-3} = 0, \\ x_0^d + y_0^d + w_{n-3} - z_0^d = 0, \end{cases}$$

where t_*, u_*, v_*, m_*, g_*, r_*, q_*, and w_* are intermediate variables allowing us to propagate the basic operations, and the inequalities in bold should be iterated for $i = 0, 1, \ldots, n-4$.

In some ARX ciphers, the subkeys are involved via the modular addition operation. Thus, we need to consider the propagation of $\boldsymbol{z} = \boldsymbol{x} \boxplus \boldsymbol{k}$, where $\boldsymbol{k}$ is an unknown constant. The following proposition deals with the propagation through the operation AND with a subkey, which plays an important role in building MILP model for $\boldsymbol{z} = \boldsymbol{x} \boxplus \boldsymbol{k}$.

Proposition 1. Suppose that $\boldsymbol{x}$, $\boldsymbol{y}$ and $\boldsymbol{k}$ are n-bit vectors with $\boldsymbol{y} = \boldsymbol{x} \wedge \boldsymbol{k}$, where $\boldsymbol{k}$ is a subkey,

i.e., an unknown constant. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input and output multi-sets, respectively. Assuming that $\mathbb{X}$ has division property $\mathcal{D}^{1^n}_{\mathbb{K}_\mathbb{X}}$, the division property of $\mathbb{Y}$ is $\mathcal{D}^{1^n}_{\mathbb{K}_\mathbb{Y}}$. Then the known-region deduced by $\mathbb{K}_\mathbb{Y}$ contains the known-region deduced by $\mathbb{K}_\mathbb{X}$.

By Proposition 1, we can directly ignore the operation AND with a subkey when we propagate the bit-based division property, and the resulting distinguishers in this way are valid for all keys. Thus, the propagation of bit-based division property for $\boldsymbol{z} = \boldsymbol{x} \boxplus \boldsymbol{k}$ is reduced to propagate bit-based division property from $\boldsymbol{x}$ to $\boldsymbol{z}$ for

$$\begin{cases} z_{n-1} = x_{n-1} \oplus c_{n-1},\ c_{n-1} = 0, \\ z_i = x_i \oplus c_i,\ c_i = x_{i+1} \oplus x_{i+1} \wedge c_{i+1}, \\ i = n-2, n-3, \ldots, 0. \end{cases}$$

The MILP model for $\boldsymbol{z} = \boldsymbol{x} \boxplus \boldsymbol{k}$ is similar to Model 1, so we omit it for space limitation. Some variants of the modular addition operation, such as $\boldsymbol{z} = (\boldsymbol{x} \| \boldsymbol{0}) \boxplus \boldsymbol{k}$ and $\boldsymbol{z} = (\boldsymbol{0} \| \boldsymbol{x}) \boxplus \boldsymbol{k}$, can be observed when the modular addition operation is combined with a shift operation. The corresponding MILP models can be obtained by firstly reducing (1) according to some known information first and then propagating basic operations step by step.

With these new models, we are able to establish MILP models for the search of bit-based division property for ARX ciphers. To ensure the validity of the model, we also do some experiments on some small variants as well as on some specific ARX ciphers, and the experimental results indicate that all zero-sum bits obtained under this model indeed satisfy integral property, which guarantees the correctness of the former discussion.

Applications. As an illustration, we apply MILP method to search integral distinguishers for some ARX ciphers.

We construct the MILP model for HIGHT [7]. By solving the corresponding MILP problems with Gurobi[1)], we detect two 18-round distinguishers, which achieve one more round than the previous best results.

For LEA [8], we detect a 7-round integral distinguisher, which covers one more round than the one proposed by the designers.

We also evaluate the bit-based division properties for other ARX ciphers. For more details, please refer to Appendix A.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61572293), National Basic Research Program of China (973 Program) (Grant No. 2013CB834205), Science and Technology on Communication Security Laboratory of China (Grant No. 9140c110207150c11050), Key Science Technology Project of Shandong Province (Grant No. 2015GGX101046), and Chinese Major Program of National Cryptography Development Foundation (Grant No. MMJJ20170102).

Supporting information Appendix A. 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, Sofia, 2015. 287–314
2 Knudsen R, Wagner D. Integral cryptanalysis. In: Proceedings of International Workshop on Fast Software Encryption, Leuven, 2002. 112–127
3 Todo Y, Morii M. Bit-based division property and application to SIMON family. In: Proceedings of International Conference on Fast Software Encryption, Bochum, 2016. 357–377
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 Sun L, Wang W, Wang M Q. MILP-aided bit-based division property for primitives with non-bit-permutation linear layers. 2016. https://eprint.iacr.org/2016/811.pdf
6 Todo Y, Isobe T, Hao Y L, et al. Cube attacks on non-blackbox polynomials based on division property. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2017. 250–279
7 Hong D, Sung J, Hong S, et al. HIGHT: a new block cipher suitable for low-resource device. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems, Yokohama, 2006. 46–59
8 Hong D, Lee J, Kim D, et al. LEA: a 128-bit block cipher for fast encryption on common processors. In: Proceedings of International Workshop on Information Security Applications, Jeju Island, 2013. 3–27

1) http://www.gurobi.com/.