SCIENCE CHINA
Information Sciences

• **Supplementary File** •

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, Chengdu* 610041*, China;*
[3]*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing,* 100878*, China*

Appendix A Applications of MILP-Aided Bit-Based Division Property for ARX Ciphers

Appendix A.1 Application to HIGHT

HIGHT [4] is a 64-bit block cipher with 128-bit key, and has been adopted as an International Standard by ISO/IEC. It consists of 32 rounds with four parallel Feistel functions in each round. The 64-bit internal value X_i can be considered as the concatenations of 8 bytes and denote by $X_i = X_{i,7}\|X_{i,6}\|\cdots\|X_{i,0}$ for $i = 0, 1, \ldots, 32$. An illustration of HIGHT's round function can be found in Fig. A1, where SK_{4i}, SK_{4i+1}, SK_{4i+2}, and SK_{4i+3} are subkey bytes. Since the concrete values of subkeys do not influence the MILP model, we omit the key schedule here. For more information, please refer to [4]. Note that the longest integral distinguishers for HIGHT in literatures are the 17-round ones proposed by Zhang *et al.* [8].

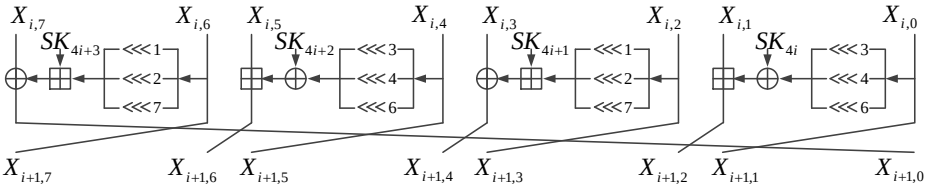

Figure A1 Round Function of HIGHT.

We construct the MILP model for HIGHT. By solving the corresponding MILP problems with Gurobi[1)], which is an openly available MILP optimizer, we detect two 18-round distinguishers, which achieve one more round than the previous best results. We also obtain some 11-, 12- and 17-round distinguishers, which are the same to those in [8]. This also indicates that our models are valid and they are useful to search integral distinguishers for ARX ciphers. The newly obtained 18-round integral distinguishers are listed as follows:

$$(\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^7\mathcal{C}^1) \xrightarrow{18\ \text{Rounds}} (\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^7\mathcal{B}^1,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8),$$
$$(\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^7\mathcal{C}^1,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8) \xrightarrow{18\ \text{Rounds}} (\mathcal{U}^7\mathcal{B}^1,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8),$$

where '$\mathcal{A}^i$' represents an i-bit vector with every bit active, '$\mathcal{B}^i$' denotes an i-bit vector with every bit satisfying zero-sum property, '$\mathcal{C}^i$' indicates an i-bit vector with every bit being constant, and '$\mathcal{U}^i$' means an i-bit vector and the properties of its internal bits are unknown. The comparison with some previous results can be found in Table A1, and some shorter-round integral distinguishers achieved by MILP method are provided in Table A2.

* Corresponding author (email: weiwangsdu@sdu.edu.cn)
1) http://www.gurobi.com/

Table A1 Summary and Comparison of Our Main Results.

Cipher	Block Size	Rounds	Data	#{Zero-Sum Bits}	Ref.
HIGHT	64	11	2^8	1	[8]
		12	2^{16}	1	
		17	2^{56}	1	
		18	2^{63}	1	Sect. Appendix A.1
LEA	128	6	2^{32}	1	[3]
		6	2^{32}	2	Sect. Appendix A.2
		7	2^{96}	1	
TEA/XTEA	64	15	2^{63}	1	[1]†
			2^{62}	1	Sect. Appendix A.2
			2^{63}	2	
KATAN/KTANTAN	32	90	2^{30}	1	Sect. Appendix A.2
		99	2^{31}	1	
		100‡	2^{31}	1	
	48	77	2^{46}	1	
		83.5	2^{47}	1	
	64	67.3	2^{62}	1	
		72.3	2^{63}	1	

#{**Zero-Sum Bits**}: The number of zero-sum bits.
†: Note that the 15-round zero-correlation linear approximations in [1] can be transformed into a 15-round integral distinguisher by applying Proposition 2 in [6].
‡: The distinguisher must start from the first round.

Appendix A.2 Application to Other ARX Ciphers

We also adopt the MILP method to search integral distinguishers for other ARX ciphers.

For LEA [3], we detect a 7-round integral distinguisher, which covers one more round than the one proposed by the designers. For TEA [7] and XTEA [5], we obtain two 15-round integral distinguishers, whose data requirements are respectively 2^{62} and 2^{63}.

Comparing to the 15-round one transformed from zero-correlation linear approximations [1], one of the newly detected distinguishers requires less data complexity and another results in more zero-sum bits. The newly obtained integral distinguishers for LEA, TEA, and XTEA are listed in Table A3.

Table A2 Integral Distinguishers for HIGHT.

11-round integral distinguishers with data complexity 2^8
$(\mathcal{A}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8) \xrightarrow{11\text{ Rounds}} (\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^7\mathcal{B}^1,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8)$
$(\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{A}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8) \xrightarrow{11\text{ Rounds}} (\mathcal{U}^7\mathcal{B}^1,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8)$
12-round integral distinguishers with data complexity $\mathbf{2^{16}}$
$(\mathcal{A}^8,\mathcal{A}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8) \xrightarrow{12\text{ Rounds}} (\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^7\mathcal{B}^1,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8)$
$(\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{C}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{C}^8,\mathcal{C}^8) \xrightarrow{12\text{ Rounds}} (\mathcal{U}^7\mathcal{B}^1,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8)$
17-round integral distinguishers with data complexity $\mathbf{2^{56}}$
$(\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{C}^8) \xrightarrow{17\text{ Rounds}} (\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^7\mathcal{B}^1,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8)$
$(\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{C}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8,\mathcal{A}^8) \xrightarrow{17\text{ Rounds}} (\mathcal{U}^7\mathcal{B}^1,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8,\mathcal{U}^8)$

Note that the whole structure of KATAN/KTANTAN [2] consists of two Linear Feedback Shift Registers (LFSR), which are transformed from two nonlinear Boolean functions f_a and f_b. In order to introduce irregular update into the round function, f_a involves constants IR's, which is illustrated in the following,

$$f_a(x_1,x_2,x_3,x_4,x_5) = x_1 \oplus x_2 \oplus (x_3 \wedge x_4) \oplus (x_5 \wedge IR) \oplus k_a,$$

where k_a denotes the subkey bit. Since IR's are different for different rounds, we will obtain integral distinguishers relying on the initial round if the concrete values of IR's are taken into consideration. But in order to obtain distinguisher independent of IR, we treat IR's as unknown constants, which results in distinguishers independent of the starting round. If the concrete values of IR's are not considered, we detect 99-round, 83.5-round, and 72.3-round distinguishers for KATAN/KTANTAN-32, 48, and 64, respectively. If the information of IR's is taken into account, the distinguishers for KATAN/KTANTAN-32 can be extended to 100-round. However, this improved distinguisher must start from the first round. Some distinguishers for KATAN/KTANTAN obtained by MILP method are presented in Table A4.

Table A3 Integral Distinguishers for LEA, TEA, and XTEA.

LEA	**6-round integral distinguishers with data complexity 2^{32}**
	$(\mathcal{A}^{32},\mathcal{C}^{32},\mathcal{C}^{32},\mathcal{C}^{32}) \xrightarrow{6\text{ Rounds}} (\mathcal{U}^{32},\mathcal{U}^{4}\mathcal{B}^{1}\mathcal{U}^{27},\mathcal{U}^{32},\mathcal{U}^{32})$
	$(\mathcal{C}^{32},\mathcal{C}^{32},\mathcal{C}^{32},\mathcal{A}^{32}) \xrightarrow{6\text{ Rounds}} (\mathcal{U}^{32},\mathcal{U}^{3}\mathcal{B}^{2}\mathcal{U}^{27},\mathcal{U}^{32},\mathcal{U}^{32})$
	7-round integral distinguisher with data complexity 2^{96}
	$(\mathcal{C}^{32},\mathcal{A}^{32},\mathcal{A}^{32},\mathcal{A}^{32}) \xrightarrow{7\text{ Rounds}} (\mathcal{U}^{32},\mathcal{U}^{4}\mathcal{B}^{1}\mathcal{U}^{27},\mathcal{U}^{32},\mathcal{U}^{32})$
TEA/XTEA	**15-round integral distinguisher with data complexity 2^{62}**
	$(\mathcal{A}^{32},\mathcal{A}^{30}\mathcal{C}^{2}) \xrightarrow{15\text{ Rounds}} (\mathcal{U}^{31}\mathcal{B}^{1},\mathcal{U}^{32})$
	15-round integral distinguisher with data complexity 2^{63}
	$(\mathcal{A}^{32},\mathcal{A}^{31}\mathcal{C}^{1}) \xrightarrow{15\text{ Rounds}} (\mathcal{U}^{30}\mathcal{B}^{2},\mathcal{U}^{32})$

Table A4 Integral Distinguishers for KATAN/KTANTAN Family of Block Ciphers.

KATAN/KTANTAN32	**90-round integral distinguisher with data complexity 2^{30}**
	$(\mathcal{C}^{2}\mathcal{A}^{30}) \xrightarrow{90\text{ Rounds}} (\mathcal{U}^{18}\mathcal{B}^{1}\mathcal{U}^{13})$
	99-round integral distinguisher with data complexity 2^{31}
	$(\mathcal{C}^{1}\mathcal{A}^{31}) \xrightarrow{99\text{ Rounds}} (\mathcal{U}^{18}\mathcal{B}^{1}\mathcal{U}^{13})$
	100-round integral distinguisher with data complexity 2^{31} starting from the first round
	$(\mathcal{C}^{1}\mathcal{A}^{31}) \xrightarrow{100\text{ Rounds}} (\mathcal{U}^{18}\mathcal{B}^{1}\mathcal{U}^{13})$
KATAN/KTANTAN48	**77-round integral distinguisher with data complexity 2^{46}**
	$(\mathcal{C}^{2}\mathcal{A}^{46}) \xrightarrow{77\text{ Rounds}} (\mathcal{U}^{28}\mathcal{B}^{1}\mathcal{U}^{19})$
	83.5-round integral distinguisher with data complexity 2^{47}
	$(\mathcal{C}^{1}\mathcal{A}^{47}) \xrightarrow{83.5\text{ Rounds}} (\mathcal{U}^{28}\mathcal{B}^{1}\mathcal{U}^{19})$
KATAN/KTANTAN64	**67.3-round integral distinguisher with data complexity 2^{62}**
	$(\mathcal{C}^{2}\mathcal{A}^{62}) \xrightarrow{67.3\text{ Rounds}} (\mathcal{U}^{38}\mathcal{B}^{1}\mathcal{U}^{25})$
	72.3-round integral distinguisher with data complexity 2^{63}
	$(\mathcal{C}^{1}\mathcal{A}^{63}) \xrightarrow{72.3\text{ Rounds}} (\mathcal{U}^{38}\mathcal{B}^{1}\mathcal{U}^{25})$

References

1 Bogdanov A, Wang M. Zero correlation linear cryptanalysis with reduced data complexity. In Canteaut A ed. Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, 2012, 29–48.

2 De Cannière C, Dunkelman O, Knezevic M. KATAN and KTANTAN - a family of small and efficient hardware-oriented block ciphers. In Clavier C, Gaj K eds. Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, 2009, 272–288.

3 Hong D, Lee J, Kim D, et al. LEA: a 128-bit block cipher for fast encryption on common processors. In Kim Y, Lee H, Perrig A eds. Information Security Applications - 14th International Workshop, WISA 2013, Jeju Island, Korea, 2013, 3–27.

4 Hong D, Sung J, Hong S, et al. HIGHT: a new block cipher suitable for low-resource device. In Goubin L, Matsui M eds. Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, 2006, 46–59.

5 Needham R, Wheeler D. TEA extensions. Report, Cambridge University, Cambridge, UK (October 1997), 1997.

6 Wen L, Wang M Q. Integral zero-correlation distinguisher for ARX block cipher, with application to SHACAL-2. In Susilo W, Mu Y eds. Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, 2014, 454–461.

7 Wheeler D, Needham R. TEA, a tiny encryption algorithm. In Preneel B ed. Fast Software Encryption: Second International Workshop. Leuven, Belgium, 1994, 363–366.

8 Zhang P, Sun B, Li C. Saturation attack on the block cipher HIGHT. In Garay J, Miyaji A, Otsuka A eds. Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa, Japan, 2009, 76–86.