Zero-sum Distinguishers for Round-reduced GIMLI Permutation

Jiahao Cai[1,2,3], Zihao Wei[1,2,3], Yingjie Zhang[1,2,3], Siwei Sun[1,2,3] and Lei Hu[1,2,3]
[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China*
[2]*Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, China*
[3]*School of Cyber Security, University of Chinese Academy of Sciences, China*

Keywords: GIMLI, Integral, Division Property, Zero-sum, Degree evaluation, MILP.

Abstract: GIMLI is a 384-bit permutation proposed by Bernstein *et al.* at CHES 2017. It is designed with the goal of achieving both high security and high performance across a wide range of hardware and software platforms. Since GIMLI can be used as a building block for many cryptographic schemes, it is important to understand its concrete security. To the best of our knowledge, third party cryptanalysis of GIMLI is limited. In this paper, we identify some zero-sum distinguishers for 14-round GIMLI with the inside-out technique, which are one-round longer than the integral distinguishers presented by the designers. Although we obtain improved cryptanalysis results, these zero-sum distinguishers are far from threatening the full version of GIMLI.

1 INTRODUCTION

Permutations with large state sizes and desired cryptographic properties facilitate the construction of many cryptographic schemes, including high-security (tweakable) block ciphers, stream ciphers, message authentication codes, hash functions, *etc*. For example, the winner of the SHA-3 competition, Keccak hash function, uses a permutation operating on a 1600-bit state known as the Keccak-f permutation (Bertoni et al., 2013). Also, we have message authentication code (Chaskey (Mouha et al., 2014)), and stream cipher (Salsa20 (Bernstein, 2008)) built on ARX permutations. However, existing designs suffer from the problem of showing significant performance variation when implemented in different platforms, severely limiting their range of applications. Therefore, a single primitive that performs well (not necessarily the best) on all common platforms will benefit the designers and implementors a lot.

With this goal in mind, Bernstein *et al.* presented the GIMLI design at CHES 2017 (Bernstein et al., 2017). What distinguishes GIMLI from previous designs is that its performance strikes the balance across a wide spectrum of platforms by skillfully avoiding those platform-specific hazards leading to poor performance for many primitives simultaneously. Therefore, cryptographic schemes designed based on GIMLI are expected to be efficient when implemented on 64-bit Intel/AMD server CPUs, 32-bit ARM smartphone CPUs, 32-bit ARM microcontrollers, 8-bit AVR microcontrollers, FPGAs, and ASICs with or without side-channel protections. We refer the reader to http://gimli.cr.yp.to for sample implementations and detailed benchmarks.

Given these merits of GIMLI, it has the potential to be employed in many future designs. Therefore, it is essential to have a thorough understanding of its security. Besides the initial cryptanalysis provided by the designers (Bernstein et al., 2017), we are aware of only one third party cryptanalysis (Hamburg, 2017). However, the claimed results of (Hamburg, 2017) is largely irrelevant to the original design, since the "attack" is against an artificial and ad-hoc mode (see http://gimli.cr.yp.to/statement.html for the statement from the GIMLI team). In this paper, we provide another third party cryptanalysis concerning Zero-Sum Distinguishers by using MILP, which has been used to automate many cryptanalytic techniques (Mouha et al., 2012; Sun et al., 2014; Xiang et al., 2016; Sasaki and Todo, 2017; Cui et al., 2016; Shi et al., 2018; Fu et al., 2016). We identify a set of zero-sum distinguishers for 14-round GIMLI. To the best of our knowledge, these are the best distinguishers for GIMLI so far.

Organization. In Section 2, we give a brief description of the GIMLI permutation. We show how

Cai, J., Wei, Z., Zhang, Y., Sun, S. and Hu, L.
Zero-sum Distinguishers for Round-reduced GIMLI Permutation.
DOI: 10.5220/0007249000380043
In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, pages 38-43
ISBN: 978-989-758-359-9

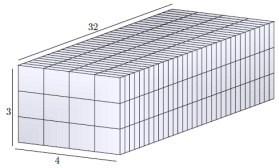

Fig 1: The state of GIMLI.

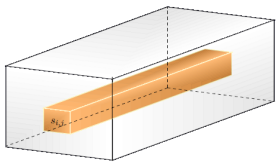

Fig 2: The 32-bit word $s_{i,j}$ in row i and column j.

to evaluate the algebraic degree of a boolean function with division property in Section 3, which is the main cryptanalytic tool employed in this work. The inside-out technique for finding zero-sums is introduced in Section 4. In Section 5, we identify many zero-sum distinguishers of 14-round GIMLI with the methods presented in Section 3 and Section 4. We conclude in Section 6 and give some discussion of future work.

2 DESCRIPTION OF THE GIMLI PERMUTATION

GIMLI is a 384-bit permutation. There are 24 rounds in GIMLI, numbered 24,23, ..., 1. The input 384-bit data is arranged into a 3×4 matrix of 32-bit words as shown in Fig. 1. Let $s_{i,j} \in \mathcal{W}$ denote the 32-bit word in row i and column j for $0 \le i < 3$ and $0 \le j < 4$, where $\mathcal{W}$ is the set of all 32-bit words (see Fig. 2). The 384-bit state is then manipulated according to Algorithm 2 to produce the output. The inverse of the GIMLI permutation can be derived from Algorithm 1 and we put it into Appendix 6.

Algorithm 1: The GIMLI permutation.

Input: $\mathbf{s} = (s_{i,j}) \in \mathcal{W}^{3\times 4}$
Output: $\mathsf{GIMLI}(\mathbf{s}) = (s_{i,j}) \in \mathcal{W}^{3\times 4}$

for r from 24 downto 1 inclusive **do**
  for $j \in \{0,\cdots,3\}$ **do**
    $x \leftarrow s_{0,j} \lll 24$
    $y \leftarrow s_{1,j} \lll 9$
    $z \leftarrow s_{2,j}$
    $s_{2,j} \leftarrow x \oplus (z \ll 1) \oplus ((y \wedge z) \ll 2)$
    $s_{1,j} \leftarrow y \oplus x \oplus ((x \vee z) \ll 1)$
    $s_{0,j} \leftarrow z \oplus y \oplus ((x \wedge y) \ll 3)$
  end
  if $r \mod 4 = 0$ **then**
    $s_{0,0}, s_{0,1}, s_{0,2}, s_{0,3} \leftarrow s_{0,1}, s_{0,0}, s_{0,3}, s_{0,2}$
  else if $r \mod 4 = 2$ **then**
    $s_{0,0}, s_{0,1}, s_{0,2}, s_{0,3} \leftarrow s_{0,2}, s_{0,3}, s_{0,0}, s_{0,1}$
  end
  if $r \mod 4 = 0$ **then**
    $s_{0,0} = s_{0,0} \oplus \mathsf{0x9e377900} \oplus r$
  end
end
return $(s_{i,j})$

3 ALGEBRAIC DEGREE EVALUATION WITH DIVISION PROPERTY

The Division property, introduced by Todo at EUROCRYPT 2015 (Todo, 2015), is a generalization of the integral property, and its bit-based version was applied in the cryptanalysis of SIMON at FSE 2016 (Todo and Morii, 2016).

Let $\mathbb{F}_2$ denote the finite field of two elements, and $\mathbb{Z}$ represent the set of integers. The Hamming weight $wt(\mathbf{v})$ of a vector $\mathbf{v} \in \mathbb{F}_2^n$ is defined as the number of nonzero entries in $\mathbf{v}$. For vectors $\mathbf{k} = (k_0, k_1, \cdots, k_{n-1})$ and $\mathbf{u} = (u_0, u_1, \cdots, u_{n-1})$ in $\{0,1\}^n \subseteq \mathbb{Z}$, we say $\mathbf{u} \succcurlyeq \mathbf{k}$ if $u_i \ge k_i$ for any $i \in \{0,\cdots,n-1\}$.

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an n-variable boolean function whose *Algebraic Normal Form* (ANF) is

$$f(\mathbf{x}) = \bigoplus_{\mathbf{v}\in\mathbb{F}_2^n} a_{\mathbf{v}}^f \cdot \mathbf{x}^{\mathbf{v}}$$

where $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$, $\mathbf{x}^{\mathbf{v}} = \prod_{i=0}^{n-1} x_i^{v_i}$, and we call $a_{\mathbf{v}}^f \in \mathbb{F}_2$ the ANF coefficient of f. The algebraic degree of f is defined as $deg(f) = \max\{wt(\mathbf{v}) : a_{\mathbf{v}}^f \neq 0\}$. A vectorial boolean function $\mathbf{G} = (g_0, \cdots, g_{m-1}) : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a sequence of m boolean functions $g_i : \mathbb{F}_2^n \to \mathbb{F}_2$ with $0 \le i < m$, and the algebraic degree $deg(\mathbf{G})$ of $\mathbf{G}$ is defined as $\max\{deg(g_i) : 0 \le i < m\}$.

Definition 1 (Bit-based Division Property (Todo and Morii, 2016))**.** *Let $\mathbb{X}$ be a multiset whose elements belong to $\mathbb{F}_2^n$. When the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{1^n}$, where $\mathbb{K}$ denotes a subset of $\{0,1\}^n \subseteq \mathbb{Z}^n$, it satisfies the following condition*

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x}) = \begin{cases} \text{unknown} & \text{if there are } \mathbf{k} \in \mathbb{K},\ s.t.\ \mathbf{u} \succcurlyeq \mathbf{k} \\ 0 & \text{otherwise} \end{cases}$$

where $\mathbf{u} = (u_0, u_1, \cdots, u_{n-1}) \in \{0,1\}^n \subseteq \mathbb{Z}^n$, $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^n$, *and* $\pi_{\mathbf{u}}(\mathbf{x}) = \prod_{i=0}^{n-1} x_i^{u_i}$.

If a multiset $\mathbb{X}$ has division property $\mathcal{D}_{\mathbb{K}}^{1^n}$, after the application of a vectorial boolean function $\mathbf{F} : \mathbb{F}_2^n \to$

$\mathbb{F}_2^m$, the division property of the output multiset $\mathbb{Y}$ becomes $\mathcal{D}^{1^m}_{\mathbb{K}'}$. We say $\mathcal{D}^{1^n}_{\mathbb{K}}$ propagates to $\mathcal{D}^{1^m}_{\mathbb{K}'}$, which is denoted by $\mathcal{D}^{1^n}_{\mathbb{K}} \xrightarrow{\mathbf{F}} \mathcal{D}^{1^m}_{\mathbb{K}'}$, or $\mathbb{K} \xrightarrow{\mathbf{F}} \mathbb{K}'$.

Definition 2 (Division Trail (Xiang et al., 2016))**.** *Let* $\mathbf{F}$ *be the round function of an iterated block cipher. Assume that the input multi-set to the block cipher has initial division property* $\mathcal{D}^{1^n}_{\mathbb{K}_0}$ *with* $\mathbb{K}_0 = \{\mathbf{k}\}$*. This initial division property propagates through the round function which forms a chain*

$$\mathcal{D}^{1^n}_{\mathbb{K}_0} \xrightarrow{\mathbf{F}} \mathcal{D}^{1^n}_{\mathbb{K}_1} \xrightarrow{\mathbf{F}} \mathcal{D}^{1^n}_{\mathbb{K}_2} \xrightarrow{\mathbf{F}} \cdots$$

For any vector $\mathbf{k}_i^* \in \mathbb{K}_i (i \geq 1)$*, there must exist a vector* $\mathbf{k}_{i-1}^*$ *in* $\mathbb{K}_{i-1}$ *such that* $\mathbf{k}_{i-1}^*$ *can propagate to* $\mathbf{k}_i^*$ *according to the rules of division property propagation. Furthermore, for* $(\mathbf{k}_0, \mathbf{k}_1, \cdots, \mathbf{k}_r) \in \mathbb{K}_0 \times \mathbb{K}_1 \times \cdots \times \mathbb{K}_r$*, if* $\mathbf{k}_{i-1}$ *can propagate to* $\mathbf{k}_i$ *for all* $i \in \{1, 2, \cdots, r\}$*, we call* $(\mathbf{k}_0, \mathbf{k}_1, \cdots, \mathbf{k}_r)$ *an r-round division trail.*

Given $\mathbf{k}$ and $\mathbf{k}'$, whether there is a division trail $\mathbf{k} \to \mathbf{k}'$ for $\mathbf{F}$ can be determined by the resolution of a Mixed-Integer Linear Programming (MILP) model encoding the propagation rules of the division properties (Xiang et al., 2016). We refer the reader to (Xiang et al., 2016) for more information on MILP-aided analysis of division properties.

Besides its natural application in finding integral distinguishers, it turns out that the division property can be a very generic tool for probing the structure of boolean functions whose explicit ANFs are not available due to resource limitation. In particular, the propagation of division properties can be used to evaluate the degree of a boolean function (Todo et al., 2017).

***Lemma* 1** (Todo, Isobe, Hao, and Meier (Todo et al., 2017))**.** *Let* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be a boolean function whose ANF coefficients are denoted by* $a_{\mathbf{v}}^f$ $(\mathbf{v} \in \mathbb{F}_2^n)$*, and* $\mathbf{k} \in \mathbb{F}_2^n$*. Then* $a_{\mathbf{v}}^f = 0$ *for all* $\mathbf{v} \succcurlyeq \mathbf{k}$ *if there is no division trail such that* $\mathbf{k} \xrightarrow{f} 1$.

Lemma 1 leads to the following two propositions for evaluating the degrees of (vectorial) boolean functions.

***Proposition* 1.** *Let* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be a boolean function. Then the degree of* f *is upper bounded by* $d+1$ *where* $d = \max_{\mathbf{k} \in \mathbb{F}_2^n} \{wt(\mathbf{k}) : \mathbf{k} \xrightarrow{f} 1 \text{ is a division trail}\}$.

***Proposition* 2.** *Let* $\mathbf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be a vectorial boolean function. Then the degree of* $\mathbf{F}$ *is upper bounded by* $d+1$ *where* $d = \max_{\mathbf{k} \in \mathbb{F}_2^n} \{wt(\mathbf{k}) : \mathbf{k} \xrightarrow{\mathbf{F}} \mathbf{e}_j \text{ is a division trail for some } j \in \{0, \cdots, n-1\}\}$ *and* $\mathbf{e}_j$ *is the* j*th unit vector.*

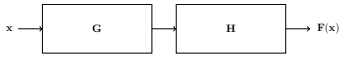

Fig 3: $\mathbf{F} = \mathbf{H} \circ \mathbf{G}$.

4 THE INSIDE-OUT TECHNIQUE FOR FINDING ZERO-SUM DISTINGUISHERS

The so-called zero-sum distinguisher was proposed by Aumasson and Meier in (Aumasson and Meier, 2009), which can be regarded as a generalization of the integral property (*a.k.a.* saturation property) (Daemen et al., 1997; Knudsen and Wagner, 2002).

Definition 3 (Zero-Sum Distinguisher (Aumasson and Meier, 2009; Boura and Canteaut, 2010))**.** *Let* $\mathbf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be a permutation. A zero-sum is a set* $\mathcal{X} \subseteq \mathbb{F}_2^n$ *of inputs such that*

$$\bigoplus_{\mathbf{x} \in \mathcal{X}} \mathbf{x} \equiv 0 \quad \text{and} \quad \bigoplus_{\mathbf{x} \in \mathcal{X}} \mathbf{F}(\mathbf{x}) \equiv 0\,.$$

Since it is expected that a randomly chosen permutation does not have many zero-sums, the existence of many such sets of inputs can be seen as a distinguishing property of $\mathbf{F}$.

The zero-sum distinguishers are intimately related to the integral distinguishers whose existence has a close connection with the degree of the underlying boolean functions.

Let I be a subset of $\{0, \cdots, n-1\}$ with cardinality $|I|$, and $\delta(I)$ be the subspace spanned by $\{\mathbf{e}_i : i \in I\}$. For a vector $\mathbf{a} \in \mathbb{F}_2^n$, $\delta_{\mathbf{a}}(I)$ is defined to be the set $\{\mathbf{x} + \mathbf{a} : \mathbf{x} \in \delta(I)\}$. That is, $\delta_{\mathbf{a}}(I)$ is the set of all vectors whose values indexed by I traverse all possible values while the values at other positions are fixed to constants according to $\mathbf{a}$. It is easy to check that for any $\mathbf{a} \in \mathbb{F}_2^n$, and any I whose cardinality is strictly greater than 1, $\oplus_{\mathbf{x} \in \delta_{\mathbf{a}}(I)} \mathbf{x} \equiv 0$. Moreover, if $deg(\mathbf{F}) < n$, and $|I| > deg(\mathbf{F})$, then for any $\mathbf{a} \in \mathbb{F}_2^n$,

$$\bigoplus_{\mathbf{x} \in \delta_{\mathbf{a}}(I)} \mathbf{F}(\mathbf{x}) \equiv 0.$$

Therefore, many zero-sums $\delta_{\mathbf{a}}(I)$ for $\mathbf{F}$ with $deg(\mathbf{F}) < n$ can be identified. Since $\mathbf{F}$ is a permutation, we can construct zero-sums from the middle (the inside-out technique (Aumasson and Meier, 2009; Boura and Canteaut, 2010)) by exploiting the knowledge of the degrees of both the forward and backward directions of $\mathbf{F}$ as depicted in Fig. 3.

Firstly, $\mathbf{F}$ is decomposed into $\mathbf{H} \circ \mathbf{G}$, where $\mathbf{G}$ and $\mathbf{H}$ are n-bit permutations. Assuming that $deg(\mathbf{G}^{-1}) < n$ and $deg(\mathbf{H}) < n$, then for any $\mathbf{a} \in \mathbb{F}_2^n$ and I with

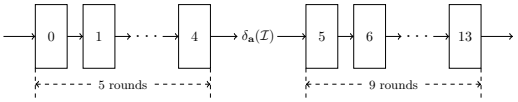

Fig 4: Apply the inside-out technique to 14-round GIMLI.

$|I| = \max\{deg(\mathbf{G^{-1}}), deg(\mathbf{H})\} + 1$, $\delta_{\mathbf{a}}(I)$ is a zero-sum for both $\mathbf{G}^{-1}$ and $\mathbf{H}$. Consequently, we have

$$\bigoplus_{\mathbf{x}\in\mathbf{G}^{-1}(\delta_{\mathbf{a}}(I))} \mathbf{x} \equiv 0$$

and

$$\begin{aligned}\bigoplus_{\mathbf{x}\in\mathbf{G}^{-1}(\delta_{\mathbf{a}}(I))} \mathbf{F}(\mathbf{x}) &= \bigoplus_{\mathbf{x}\in\mathbf{G}^{-1}(\delta_{\mathbf{a}}(I))} \mathbf{H}\circ\mathbf{G}(\mathbf{x}) \\ &= \bigoplus_{\mathbf{y}\in\delta_{\mathbf{a}}(I)} \mathbf{H}(\mathbf{y}) \\ &= 0\end{aligned}$$

which indicates that $\mathbf{G}^{-1}(\delta_{\mathbf{a}}(I))$ is a zero-sum for $\mathbf{F}$.

5 ZERO-SUM DISTINGUISHERS FOR ROUND-REDUCED GIMLI

To apply the inside-out technique, We split the 14-round GIMLI into the first 5 rounds (denoted by $\mathbf{G}$) and the last 9 rounds (denoted by $\mathbf{H}$) as depicted in Fig. 4. Then the degrees of $\mathbf{G}^{-1}$ and $\mathbf{H}$ are evaluated with the method introduced in Sect. 3. Therefore, we need to set up MILP models encoding the propagation of division properties for round-reduced GIMLI and its inverse. According to the specification of GIMLI presented in Algorithm 1 (also see Appendix 6 for its inverse), the MILP models can be constructed by properly assembling the MILP models for the following three operations.

Modeling S-box. We treat the non-linear operation $(x',y',z') = (y\wedge z, x\vee z, x\wedge y)$ in GIMLI as a 3×3 S-box, and use the method presented in (Boura and Canteaut, 2016) to retrieve its propagation rules (see Table 1) of the division property. Using the convex hull computation approach (Sun et al., 2014), the propagation rule shown in Table 1 can be transformed into the following linear inequalities

$$\begin{cases} x+z-2x'-3y'-2z'+2\geq 0 \\ -x+y'+z'\geq 0 \\ -z+x'+y'\geq 0 \\ -y+x'+z'\geq 0 \\ x+y+z-x'-y'-z'\geq 0 \end{cases}$$

where all variables involved are binaries.

Table 1: Propagation rule of $(x',y',z') = (y\wedge z, x\vee z, x\wedge y)$.

Input	Output
$(0,0,0)$	$(0,0,0)$
$(0,0,1)$	$(0,1,0)$ $(1,0,0)$
$(0,1,0)$	$(0,0,1)$ $(1,0,0)$
$(0,1,1)$	$(1,0,0)$
$(1,0,0)$	$(0,0,1)$ $(0,1,0)$
$(1,0,1)$	$(0,1,0)$ $(1,0,1)$
$(1,1,0)$	$(0,0,1)$
$(1,1,1)$	$(1,0,1)$

Modeling COPY. Let $a \xrightarrow{\text{COPY}} (b_0,\cdots,b_{m-1})$ be a division trail of COPY. Then $a = b_0+\cdots+b_{m-1}$, where all variables involved are binaries.

Modeling XOR. Let $(a_0,\cdots,a_{m-1}) \xrightarrow{\text{XOR}} b$ be a division trail of XOR. Then $a_0+\cdots+a_{m-1} = b$, where all variables involved are binaries.

After assembling the above constraints for all operations involved in the underlying permutation, we can check whether d is an upper bound of the degree of the permutation as follows. We impose additional constraints dictating that

$$\sum_{i=0}^{n-1} u_i \geq d \text{ and } \sum_{i=0}^{n-1} v_i = 1, \quad (1)$$

where u_i's and v_i's are the variables representing the input and output division properties, respectively ($n = 384$ for GIMLI). If the resulting model is infeasible, then the algebraic degree of the underlying permutation is upper bounded by d due to Proposition 2.

Firstly, we evaluate the degree of $\mathbf{H}$. Note that the degree evaluation of $\mathbf{H}$ has already been done by the design team. However, we still perform this process to verify our implementation against the results provided by the designers. The upper bounds of the degrees for round reduced versions of $\mathbf{H}$ (up to 9 rounds) are summarized in Table 2, which match the results provided in (Bernstein et al., 2017).

We then evaluate the degrees of round-reduced $\mathbf{G}^{-1}$, and the results are listed in Table 3. Note that the bounds we get are not necessarily tight. In our experiment, we observed that when we set the d in equation (1) to be a very small value, the resolution time of the MILP model can be very long. Therefore, we prefer to choose a d which may be much larger than the degree of the analyzed permutation.

According to the above results and the discussion of Sect. 4, We can conclude that $\mathbf{G}^{-1}(\delta_{\mathbf{a}}(I))$ with $|I| > 350$ is a zero-sum of 14-round GIMLI for any $\mathbf{a}\in\mathbb{F}_2^n$. Finally, we note that all models are solved by the Gurobi optimizer (Gurobi Optimization, 2013) and all experiments are performed on a com-

Table 2: The upper bounds of the degrees of round-reduced GIMLI.

# Rounds	1	2	3	4	5	6	7	8	9
Bounds	2	4	8	16	29	52	95	163	266

Table 3: The upper bounds of the degrees of round-reduced $\mathbf{G}^{-1}$.

# rounds	1	2	3	4	5
Bounds	32	63	141	170	350

puter running Ubuntu 16.04 TLS system with Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz.

6 CONCLUSION AND DISCUSSION

In this work, by analyzing the degrees of round-reduced versions of the GIMLI permutation and its inverse, we obtained a set of 14-round zero-sum distinguishers, which achieves one-round improvement compared with the results offered by the designers. More specifically, the 14-round zero-sum distinguishers are constructed with the knowledge of the algebraic degree of the vectorial boolean function representing the output of 9-round GIMLI permutation and the upper bound of the degree of the inverse of 5-round GIMLI permutation, where the evaluation of the algebraic degrees is performed by solving MILP models encoding the propagation of the division properties. Note that we are only able to get the upper bound of the algebraic degrees under our current computational resources. Therefore, it is interesting to investigate whether tighter bounds can be obtained. We expect that a more accurate degree evaluation may help to extend the zero-sum distinguisher one more round.

ACKNOWLEDGEMENTS

The authors thank the anonymous reviewers for many helpful comments. The work is supported by the Chinese Major Program of National Cryptography Development Foundation (Grant No. MMJJ20180102), the National Natural Science Foundation of China (61732021, 61802400, 61772519, 61802399), the Youth Innovation Promotion Association of Chinese Academy of Sciences, and the Institute of Information Engineering, CAS (Grant No. Y7Z0251103).

REFERENCES

Aumasson, J.-P. and Meier, W. (2009). Zero-sum distinguishers for reduced Keccak-f and for the core functions of Luffa and Hamsi. Available at http://131002.net/data/papers/AM09.pdf.

Bernstein, D. J. (2008). The salsa20 family of stream ciphers. In *New Stream Cipher Designs - The eSTREAM Finalists*, pages 84–97. https://cr.yp.to/snuffle/salsafamily-20071225.pdf.

Bernstein, D. J., Kölbl, S., Lucks, S., Massolino, P. M. C., Mendel, F., Nawaz, K., Schneider, T., Schwabe, P., Standaert, F., Todo, Y., and Viguier, B. (2017). Gimli : A cross-platform permutation. In *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, pages 299–320.

Bertoni, G., Daemen, J., Peeters, M., and Assche, G. V. (2013). Keccak. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 313–314. https://keccak.team/files/Keccak-reference-3.0.pdf.

Boura, C. and Canteaut, A. (2010). A zero-sum property for the Keccak-f permutation with 18 rounds. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2488–2492.

Boura, C. and Canteaut, A. (2016). Another view of the division property. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 654–682.

Cui, T., Jia, K., Fu, K., Chen, S., and Wang, M. (2016). New automatic search tool for impossible differentials and zero-correlation linear approximations. *IACR Cryptology ePrint Archive*, 2016:689.

Daemen, J., Knudsen, L. R., and Rijmen, V. (1997). The block cipher square. In *Fast Software Encryption, 4th International Workshop, FSE 1997, Haifa, Israel, January 20-22, 1997, Proceedings*, pages 149–165.

Fu, K., Wang, M., Guo, Y., Sun, S., and Hu, L. (2016). Milp-based automatic search algorithms for differential and linear trails for speck. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 268–288.

Gurobi Optimization (2013). Gurobi optimizer reference manual. http://www.gurobi.com.

Hamburg, M. (2017). Cryptanalysis of $22\frac{1}{2}$ rounds of Gimli. Cryptology ePrint Archive, Report 2017/743. https://eprint.iacr.org/2017/743.

Knudsen, L. R. and Wagner, D. A. (2002). Integral cryptanalysis. In *Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers*, pages 112–127.

Mouha, N., Mennink, B., Herrewege, A. V., Watanabe, D., Preneel, B., and Verbauwhede, I. (2014). Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, pages 306–323.

Mouha, N., Wang, Q., Gu, D., and Preneel, B. (2012). Differential and linear cryptanalysis using mixed-integer linear programming. In *Information Security and Cryptology –ISC 2012*, pages 57–76. Springer.

Sasaki, Y. and Todo, Y. (2017). New impossible differential search tool from design and cryptanalysis aspects - revealing structural properties of several ciphers. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, pages 185–215.

Shi, D., Sun, S., Derbez, P., Todo, Y., Sun, B., and Hu, L. (2018). Programming the demirci-selçuk meet-in-the-middle attack with constraints. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part II*, pages 3–34.

Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., and Song, L. (2014). Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, DES(L) and other bit-oriented block ciphers. In *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, pages 158–178.

Todo, Y. (2015). Structural evaluation by generalized integral property. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, pages 287–314.

Todo, Y., Isobe, T., Hao, Y., and Meier, W. (2017). Cube attacks on non-blackbox polynomials based on division property. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, pages 250–279.

Todo, Y. and Morii, M. (2016). Bit-based division property and application to SIMON family. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 357–377.

Xiang, Z., Zhang, W., Bao, Z., and Lin, D. (2016). Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, pages 648–678.

APPENDIX

Algorithm 2: The reversed GIMLI permutation

Input: $\mathbf{s} = (s_{i,j}) \in \mathcal{W}^{3\times 4}$
Output: $\mathsf{GIMLI}^{-1}(\mathbf{s}) = (\tilde{s}_{i,j}) \in \mathcal{W}^{3\times 4}$
for r from 24 downto 1 inclusive **do**
  if $r \mod 4 = 0$ **then**
    $s_{0,0} = s_{0,0} \oplus \mathsf{0x9e377900} \oplus r$
  end
  if $r \mod 4 = 0$ **then**
    $s_{0,0}, s_{0,1}, s_{0,2}, s_{0,3} \leftarrow s_{0,1}, s_{0,0}, s_{0,3}, s_{0,2}$
  else if $r \mod 4 = 2$ **then**
    $s_{0,0}, s_{0,1}, s_{0,2}, s_{0,3} \leftarrow s_{0,2}, s_{0,3}, s_{0,0}, s_{0,1}$
  end

  for $j \in \{0, \cdots, 3\}$ **do**
    $\tilde{s}_{0,j,0} \leftarrow s_{2,j,0}$
    $\tilde{s}_{1,j,0} \leftarrow s_{1,j,0} \oplus \tilde{s}_{0,j,0}$
    $\tilde{s}_{2,j,0} \leftarrow s_{0,j,0} \oplus \tilde{s}_{1,j,0}$
    $\tilde{s}_{0,j,1} \leftarrow s_{2,j,1} \oplus \tilde{s}_{2,j,0}$
    $\tilde{s}_{1,j,1} \leftarrow s_{1,j,1} \oplus \tilde{s}_{0,j,1} \oplus (\tilde{s}_{2,j,0} \vee \tilde{s}_{0,j,0})$
    $\tilde{s}_{2,j,1} \leftarrow s_{0,j,1} \oplus \tilde{s}_{1,j,1}$
    $\tilde{s}_{0,j,2} \leftarrow s_{2,j,2} \oplus \tilde{s}_{2,j,1} \oplus (\tilde{s}_{1,j,0} \wedge \tilde{s}_{2,j,0})$
    $\tilde{s}_{1,j,2} \leftarrow s_{1,j,2} \oplus \tilde{s}_{0,j,2} \oplus (\tilde{s}_{2,j,1} \vee \tilde{s}_{0,j,1})$
    $\tilde{s}_{2,j,2} \leftarrow s_{0,j,2} \oplus \tilde{s}_{1,j,2}$

    for $k \in \{3, \cdots, 31\}$ **do**
      $\tilde{s}_{0,j,k} \leftarrow s_{2,j,k} \oplus \tilde{s}_{2,j,k-1} \oplus (\tilde{s}_{1,j,k-2} \wedge \tilde{s}_{2,j,k-2})$
      $\tilde{s}_{1,j,k} \leftarrow s_{1,j,k} \oplus \tilde{s}_{0,j,k} \oplus (\tilde{s}_{2,j,k-1} \vee \tilde{s}_{0,j,k-1})$
      $\tilde{s}_{2,j,k} \leftarrow s_{0,j,k} \oplus \tilde{s}_{1,j,k} \oplus (\tilde{s}_{0,j,k-3} \wedge \tilde{s}_{1,j,k-3})$
    end

    $\tilde{s}_{0,j} \leftarrow \tilde{s}_{0,j} \lll -24$
    $\tilde{s}_{1,j} \leftarrow \tilde{s}_{1,j} \lll -9$
  end
end
return $(\tilde{s}_{i,j})$