Improved Zero-sum Distinguisher for Full Round KECCAK-f Permutation

Ming Duan[12] and Xuejia Lai[1]

[1] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, China.*

[2] *Basic Courses Department, University of Foreign Language, Luoyang, China.*

Abstract

KECCAK is one of the five hash functions selected for the final round of the SHA-3 competition and its inner primitive is a permutation called KECCAK-f. In this paper, we find that for the inverse of the only one nonlinear transformation of KECCAK-f, the algebraic degrees of any output coordinate and of the product of any two output coordinates are both 3 and also 2 less than its size 5. Combining the observation with a proposition from an upper bound on the degree of iterated permutations, we improve the zero-sum distinguisher of full 24 rounds KECCAK-f permutation by lowering the size of the zero-sum partition from 2^{1590} to 2^{1579}.

Keywords: hash functions, higher order differentials, algebraic degree, zero-sum, SHA-3.

1. Introduction

Zero-sum distinguisher, introduced by Aumasson and Meier in [1], is a method to generate zero-sum structures for iterated permutation, which combines higher order differentials with inside-out technique and is mainly decided by the algebraic degree of the permutation. Zero-sum distinguisher is deterministic and valid although it generate zero-sum structures with a small advantage relatively to generic method[3]. Zero-sum distinguisher can also be used to create partitions of inputs in many different zero-sum structures for the permutation[3][5].

KECCAK [2] is a family of cryptographic sponge functions which is one of the five hash functions selected for the third(and final) round of the SHA-3 competition and its core component is a permutation named KECCAK-f,

which is composed of several iterations of 5 round transformations. In 2009, a zero-sum distinguisher for the 16 rounds KECCAK-f permutation is given in [1]. Since then, the zero-sum distinguishers for more rounds KECCAK-f permutation are obtained [4][5][6] and the known lowest size of zero-sum partition of full 24 rounds KECCAK-f is 2^{1590}.

In this paper, we study the property of the inverse of the nonlinear transformation of KECCAK-f and observe that the algebraic degree of the product of any two output coordinates of the inverse of the nonlinear transformation is 2 less than its size, which helps us lower the size of zero-sum partition of full 24 rounds KECCAK-f from 2^{1590} to 2^{1579}.

The rest of the paper is organized as follows. Section 2 simply shows the description of the permutation KECCAK-f. In Section 3, zero-sum distinguishers of iterated permutation are recalled. An improved zero-sum distinguisher for full 24 rounds KECCAK-f permutation is presented in Section 4 and Section 5 concludes our results.

2. Description of the permutation KECCAK-f

The size of permutation KECCAK-f[2] is 1600 and the state can be represented by a 3-dimensional binary matrix of size $5 \times 5 \times 64$. The 5 round transformations are called θ, ρ, π, χ *and* ι. Only the transformation χ is nonlinear and its degree is 2 while the degree of its inverse is 3. The Boolean components of χ are listed in table 1 and more details of permutation KECCAK-f are available in [2].

Table 1. Boolean components of χ

Output	Corresponding Boolean function
χ_0	$x_0 + x_2 + x_1x_2$
χ_1	$x_1 + x_3 + x_2x_3$
χ_2	$x_2 + x_4 + x_3x_4$
χ_3	$x_0 + x_3 + x_0x_4$
χ_4	$x_1 + x_4 + x_0x_1$

3. Zero-sum distinguishers for iterated permutation

Firstly, we introduce the notions of higher order derivatives relation to zero-sum distinguisher.

3.1. Higher order derivatives

Higher order derivatives was introduced into cryptography by Lai in 1994[9] and their properties are investigated in [9][8].

Definition 1: Let $f(x)$ be a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, the derivative of f at point $a \in \mathbb{F}_2^n$ is defined as

$$\Delta_a f(x) = f(x \oplus a) \oplus f(x).$$

The i-th($i > 1$) derivative of the f at points $\{a_1, a_2, ..., a_i\}$ is defined as

$$\Delta^{(i)}_{a_1,...,a_i} f(x) = \Delta_{a_i}(\Delta^{(i-1)}_{a_1,...,a_{i-1}}),$$

where $\Delta^{(i-1)}_{a_1,...,a_{i-1}}$ is the $(i-1)$-th derivative of f at points $\{a_1, a_2, ..., a_{i-1}\}$. The 0-th derivative of f is defined to be $f(x)$ itself.

Higher order derivatives should be computed at points that are linearly independent, otherwise the derivative will trivially be zero. Note that the degree of the derivative of a function is at least 1 less than the degree of the function. This implies that the $(d+1)$-th derivative of n-variable Boolean function of degree d is zero, which is used in many cryptanalysis methods, such as zero-sum distinguisher.

3.2. Zero-sum properties

Note that the permutation used in a hash function does not depend on any secret parameter, the property of the permutation can be exploited from the middle. The zero-sum property introduced by Aumasson and Meier in [1] is based on higher order differentials and inside-out technique. Its main idea is taking higher order derivatives at initial states inverted from an intermediate internal state subspace, which is different from traditionally higher order differential distinguisher taking derivatives directly at initial state subspace. So zero-sum distinguisher lowers the order of higher order derivatives nearly a half with the cost of some inverted computations.

Here we give the definitions of zero-sum and zero-sum partition and more details are revised to [1][6].

Definition 2: Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. A *zero-sum* for F of size K is a subset $\{x_1, ..., x_K\} \subset \mathbb{F}_2^n$ of elements which sum to zero and for which the corresponding images by F also sum to zero, i.e.,

$$\sum_{i=1}^{K} x_i = \sum_{i=1}^{K} F(x_i) = 0.$$

Definition 3: Let P be a permutation from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. A *zero-sum partition* for P of size $K = 2^k$ is a collection of 2^{n-k} disjoint zero-sums $X_i = \{x_{i,1}, ..., x_{i,2^k}\} \subset \mathbb{F}_2^n$, i.e.,

$$\bigcup_{i=1}^{2^{n-k}} X_i = \mathbb{F}_2^n \text{ and } \sum_{j=1}^{2^k} x_{i,j} = \sum_{j=1}^{2^k} P(x_{i,j}) = 0, \forall 1 \leq i \leq 2^{n-k}.$$

4. Improved Zero-Sum Distinguisher for KECCAK-f

4.1. An Observation of permutation KECCAK-f

We respectively give the Boolean components of χ^{-1} and the product of any two output coordinates of χ^{-1} in table 2 and 3.

Table 2. Boolean components of χ^{-1}

Output	Corresponding Boolean function
χ_0^{-1}	$0+2+4+12+14+34+134$
χ_1^{-1}	$0+1+3+02+04+23+024$
χ_2^{-1}	$1+2+4+01+13+34+013$
χ_3^{-1}	$0+2+3+04+12+24+124$
χ_4^{-1}	$1+3+4+01+03+23+023$

where $12\cdots n$ means that $x_1x_2\cdots x_n$.

Table 3. Product of any two output coordinates of χ^{-1}

Product	Corresponding Boolean function
$\chi_0^{-1}\chi_1^{-1}$	$0+01+02+03+04+023+024$
$\chi_0^{-1}\chi_2^{-1}$	$2+4+02+04+12+14+34+034+134$
$\chi_0^{-1}\chi_3^{-1}$	$0+2+03+04+12+23+24+34+123+124$
$\chi_0^{-1}\chi_4^{-1}$	$4+03+04+14+24+124+134$
$\chi_1^{-1}\chi_2^{-1}$	$1+01+12+13+14+013+134$
$\chi_1^{-1}\chi_3^{-1}$	$0+3+01+02+04+13+23+014+024$
$\chi_1^{-1}\chi_4^{-1}$	$1+3+01+03+14+23+34+023+234$
$\chi_2^{-1}\chi_3^{-1}$	$2+02+12+23+24+024+124$
$\chi_2^{-1}\chi_4^{-1}$	$1+4+01+12+13+24+34+012+013+034+234$
$\chi_3^{-1}\chi_4^{-1}$	$3+03+13+23+34+013+023$

where $12\cdots n$ means that $x_1x_2\cdots x_n$.

From the table 3, An interesting observation of the inverse of the nonlinear layer of permutation KECCAK-f is obtained.

Observation: For the inverse of the only one nonlinear transformation of KECCAK-f, the algebraic degrees of any output coordinate and of the product of any two output coordinates are both 3 and also 2 less than its size 5.

4.2. Discussion of the upper bound on the degree of iterated permutations

High algebraic degree is an important design principle for cryptographic algorithm. It is difficult to determine the algebraic degree when the round of the algorithm is too big. Estimating the upper bound of the algebraic degree is a relatively feasible way. In [7], Canteaut and Videau gave an upper bound of the degree of composition of nonlinear functions and used it to estimate algebraic degree of the whole algorithm. In the rump session of Crypto 2010, Boura, Canteaut and Cannière proposed an improved upper bound for iterated permutation with a nonlinear layer composed of parallel applications of small balanced Sboxes[6]. Here we discuss the latter upper bound and give a proposition with visualized bound in some case.

Theorem 1[6]**:** Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ corresponding to the concatenation of m smaller balanced Sboxes, $S_1, ..., S_m$, defined over $\mathbb{F}_2^{n_0}$. Let δ_k be the maximal degree of the product of any k coordinates of anyone of these smaller Sboxes. Then, for any function G from $\mathbb{F}_2^n$ into $\mathbb{F}_2^l$, we have

$$deg(G \circ F) \leq n - \frac{n - deg(G)}{\gamma},$$

where

$$\gamma = max_{1 \leq i \leq n_0 - 1} \frac{n_0 - i}{n_0 - \delta_i}.$$

Most notably, we have

$$deg(G \circ F) \leq n - \frac{n - deg(G)}{n_0 - 1}.$$

Moreover, if $n_0 \geq 3$ and all Sboxes have degree at most $n_0 - 2$, we have

$$deg(G \circ F) \leq n - \frac{n - deg(G)}{n_0 - 2}.$$

Lemma 1: Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ corresponding to the concatenation of m smaller Sboxes, $S_1, ..., S_m$, defined over $\mathbb{F}_2^{n_0}$. Let δ_i be

the maximal degree of the product of any i coordinates of anyone of these Sboxes. If $n_0 \geq 2k-1$ $(k \geq 1)$ and $\delta_i \leq n_0 - 1$ for any i from 1 to $n_0 - 1$ and $\delta_i \leq n_0 - 2$ for any i from 1 to $k-1$ when $k \geq 2$, Then, we have

$$(n_0 - k)(n_0 - \delta_i) - (n_0 - i) \geq 0$$

for any i from 1 to $n_0 - 1$.

Proof: When $k = 1$, then we have

$$\begin{aligned}(n_0 - k)(n_0 - \delta_i) - (n_0 - i) &= (n_0 - 1)(n_0 - \delta_i) - (n_0 - i) \\ &\geq (n_0 - 1) - (n_0 - i) \\ &\geq (n_0 - 1) - (n_0 - 1) = 0.\end{aligned}$$

When $k \geq 2$, then we have

$$\begin{aligned}(n_0 - k)(n_0 - \delta_i) - (n_0 - i) &\geq (n_0 - k) \times 2 - (n_0 - i) \\ &\geq 2(n_0 - k) - (n_0 - 1) \\ &\geq n_0 - 2k + 1 \geq 0.\end{aligned}$$

Firstly, from the proof of theorem 1, one can know that the condition that the Sboxes are balanced in the theorem is to confirm that the inequation $\delta_i \leq n_0 - 1$ is satisfied for any i from 1 to $n_0 - 1$, but it is not a necessary condition for that, so it is not necessary to limit the condition to balanced Sboxes, i.e., the condition in theorem 1 can be generalized.

Secondly, the parameter γ in the theorem is also used to confirm that the inequation $(n_0 - k)(n_0 - \delta_i) - (n_0 - i) \geq 0$ is satisfied for any i from 1 to $n_0 - 1$ and lemma 1 tells us that the positive integer $n_0 - k$ also does in some case, so we have the following visualized upper bound.

Proposition 1: Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ corresponding to the concatenation of m smaller Sboxes, $S_1, ..., S_m$, defined over $\mathbb{F}_2^{n_0}$. Let δ_i be the maximal degree of the product of any i coordinates of anyone of these Sboxes. If $n_0 \geq 2k-1$ $(k \geq 1)$ and $\delta_i \leq n_0 - 1$ for any i from 1 to $n_0 - 1$ and $\delta_i \leq n_0 - 2$ for any i from 1 to $k-1$ when $k \geq 2$, Then, for any function G from $\mathbb{F}_2^n$ into $\mathbb{F}_2^l$, we have

$$deg(G \circ F) \leq n - \frac{n - deg(G)}{n_0 - k}.$$

Actually, when the conditions of proposition 1 are satisfied and n_0 is an even number, then the parameter γ can be improved to $n_0 - k - \frac{1}{2}$ which is not relation to this paper.

4.3. Improved zero-sum partition for full round KECCAK-f

Let R denote the KECCAK-f round permutation. Note that χ is the only nonlinear transformation of R, Combining observation and proposition 1, we have

$$deg(G \circ R) \leq n - \frac{n - deg(G)}{3}$$

and

$$deg(G \circ R^{-1}) \leq n - \frac{n - deg(G)}{2},$$

where G is any function from F_2^5 into F_2^l. Our upper bounds on the degree of the inverse KECCAK-f is less than the bounds in [6] when the rounds is more than 7 and the comparison is listed in table 4.

Table 4. Comparison of the upper bounds on $deg(R^{-r})$.

round	bound in [6]	our bound
1	3	3
2	9	9
3	27	27
4	81	81
5	243	243
6	729	729
7	1309	1309
8	1503	1454
9	1567	1532
10	1589	1566
11	1596	1583
12	1598	1591
13	1599	1595
14		1597
15		1598
16		1599

Combing the same upper bounds on $deg(R^r)$ with that in [6] and our new lower upper bounds on $deg(R^{-r})$, we have a zero-sum partition of size 2^{1579} for the full KECCAK-f permutation less than the original size 2^{1590}. Indeed, one can consider the intermediate states after the 3 linear layers θ, ρ and π in the 11-th round because the upper bound of the backward 10 rounds 1566 and that of forward 13 rounds 1578[6] are both at least 1 less than 1579.

5. Conclusion and discussion

In this paper, we gave a lower size zero-sum partition of full 24 rounds KECCAK-f permutation which is based on an interesting observation on the inverse of the nonlinear transformation of the permutation. One can verify that some of the products of three output coordinates also have degree only 3, these properties may be used to more practical cryptanalysis on KECCAK in the future.

References

[1] J.-P. Aumasson and W. Meier. Zero-sum distinguishers for reduced KECCAK-f and for the core functions of Luffa and Hamsi. Presented at the rump session of Cryptographic Hardware and Embedded Systems-CHES 2009, 2009.

[2] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. KECCAK sponge function family main document. Submission to NIST (Round 2), 2009.

[3] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Note on zero-sum distinguishers of KECCAK-f. Public comment on the NIST Hash competition, available at http://KECCAK.noekeon.org/NoteZeroSum.pdf, 2010.

[4] C. Boura and A. Canteaut. A Zero-Sum property for the KECCAK-f Permutation with 18 Rounds. NIST mailing list, 2010.

[5] C. Boura and A. Canteaut. Zero-sum Distinguishers for Iterated Permutations and Application to KECCAK-f and Hamsi-256. In SAC 2010 - Selected Areas in Cryptography, Lecture Notes in Computer Science. Springer, 2010. To appear.

[6] C. Boura, A. Canteaut and C. D. Cannière, Higher-order differential properties of KECCAK and Luffa, Presented at the rump session of Crypto 2010, Paper 2010/589 in http://eprint.iacr.org/.

[7] A. Canteaut and M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. In Advances in Cryptology - EUROCRYPT 2002, volume 2332 of Lecture Notes in Computer Science, pages 518C533. Springer-Verlag, 2002.

[8] M. Duan, X. Lai, M. Yang, X. Sun and B. Zhu, Distinguishing properties of higher order derivatives of Boolean functions, Paper 2010/417 in http://eprint.iacr.org/.

[9] X. Lai. Higher order derivatives and differential cryptanalysis. In Proc. Symposium on Communication, Coding and Cryptography, in honor of J. L. Massey on the occasion of his 60th birthday. Kluwer Academic Publishers, 1994.