Advanced Zero-Sum Distinguishers for the Permutations of the PHOTON Family

DONG Le[1,2†], WU WenLing[1], WU Shuang[1] & ZOU Jian[1,2]

[1] State Key Lab of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;

[2] Graduate University of Chinese Academy of Sciences, Beijing 100149, China

Abstract. **PHOTON is a new collection of lightweight hash functions which use an extended sponge construction and AES-like permutations. The family has five members, and each of them has a corresponding permutation. The state sizes of these permutations are 100 bits, 144 bits, 196 bits, 256 bits and 288 bits, respectively. In this paper, we firstly estimate the upper bounds on the algebraic degrees of some round-reduced permutations and use the spectral properties to improve them. Then, some zero-sum distinguishers are constructed basing on these upper bounds. Applying the integral properties and the super-sbox technique used on AES-like block ciphers, we can extend one or two rounds in the middle of the previous zero-sum distinguishers. On the other side, the tighter upper bounds on algebraic degrees of these permutations are obtained by using some new results introduced by C. Boura etc. Basing on these new bounds, the full-round zero-sum distinguishers of the first four permutations can be constructed. Additionally, the results do not threat the security of the hash family.**

Keywords. PHOTON, zero-sum, higher-order differential, Walsh spectrum, integral attack, super-sbox.

1 Introduction

Nowadays, various smart devices such as RFID tags, smart cards, and wireless sensor nodes have become more and more important to our daily life and the security of them is a big challenge. As a result, many lightweight hash functions [1-4] and block ciphers [5-11] were designed in several years. The PHOTON family [4] introduced by J. Guo *etc.* in Crypto 2011 is a collection of lightweight hash functions. It consists of five members and each of them has their own permutations. Each permutation differs from the others in the state size and the S-box. There are two main techniques used by PHOTON: sponge-like construction [12] and AES-like permutation [13]. Both of them have been well-studied for years and their security seems reliable, which give us more confidence. All of the permutations used in PHOTON have 12 rounds and their states can be represented by the square matrices. For the security of PHOTON, designers gave two distinguishers: rebound distinguisher and integral distinguisher [14]. The rebound distinguisher is based on an 8-round differential path obtained by using the non-full-active super-sbox analysis [15]. The complexity of finding a solution pair is low, but it can not be extended to more rounds. The idea of integral distinguisher was firstly used on the known-key models of some block ciphers [16]. Applying the integral path introduced in [16], one can immediately obtain 7-round integral distinguishers for all the permutations of the PHOTON family. Whereas, no one can give a longer integral trial for these AES-like permutations to this day so that it can not be extended to more rounds as well.

In [17], X. Lai considered higher order derivatives of discrete functions and the concept of higher order differentials was introduced to analyze some block ciphers. In the last few years, researchers constructed many zero-sum distinguishers for some hash functions, which is based on the concept of the higher order derivative. In [18], J.-P. Aumasson and W. Meier firstly use this method to the permutations of three

† Corresponding author (email: dongle127@163.com)

SHA-3 candidates: KECCAK, Luffa and Hamsi. In 2010, C. Boura and A. Canteaut studied some special properties for iterated permutations and applied them to KECCAK-f and Hamsi-256 [19]. Later C. Boura *etc.* improved the method and used them to attack 24-round KECCAK-f permutation and Luffa [20]. Besides, J.-P. Aumasson *etc.* gave some 2^i-sum distinguishers for Hamsi-256 by estimating the upper bounds on the algebraic degrees of compression function and output permutation [21]. On the other hand, KECCAK team showed a generic method to construct a zero-sum for a given function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ [29] inspired by the algorithm for the generalized birthday problem [30] and by the attack on XHASH [31]. Most of the times, the complexity of this method is lower than the complexity of zero-sum attacks based on the higher-order differential if the round number of target function is large. However, there is a essential difference between the two methods. The generic method is a probability algorithm, and the higher-order differential attack is deterministic, *i.e.* it can distinguish the given function from the ideal functions with probability one.

Table 1 Summary of results for PHOTON. The targets $P_{100}, P_{144}, P_{196}, P_{256}, P_{288}$ are the permutations used in hash functions PHOTON-80, PHOTON-128, PHOTON-160, PHOTON-224, PHOTON-256, respectively

Target	Hash	Rounds	Time compl.	Memory compl.	Type	Source
P_{100}	PHOTON-80	8/12	2^8	2^4	rebound distinguisher	[14]
P_{144}	PHOTON-128	8/12	2^8	2^4	rebound distinguisher	[14]
P_{196}	PHOTON-160	8/12	2^8	2^4	rebound distinguisher	[14]
P_{256}	PHOTON-224	8/12	2^8	2^4	rebound distinguisher	[14]
P_{288}	PHOTON-224	8/12	2^{15}	2^8	rebound distinguisher	[14]
P_{100}	PHOTON-80	7/12	2^{36}	-	integral distinguisher	[14]
P_{144}	PHOTON-128	7/12	2^{44}	-	integral distinguisher	[14]
P_{196}	PHOTON-160	7/12	2^{52}	-	integral distinguisher	[14]
P_{256}	PHOTON-224	7/12	2^{60}	-	integral distinguisher	[14]
P_{288}	PHOTON-224	7/12	2^{88}	-	integral distinguisher	[14]
P_{100}	PHOTON-80	12/12	2^{97}	-	zero-sum distinguisher	5
P_{144}	PHOTON-128	12/12	2^{137}	-	zero-sum distinguisher	5
P_{196}	PHOTON-160	12/12	2^{167}	-	zero-sum distinguisher	5
P_{256}	PHOTON-224	12/12	2^{223}	-	zero-sum distinguisher	4.4

In this paper, we study the higher-order differential properties of PHOTON, and the Walsh spectrum of the PRESENT S-box which is used in most members of the PHOTON family. Applying the result in [22, 19], we obtain the tighter upper bounds on algebraic degrees of some PHOTON permutations. Then the zero-sum distinguishers of them can be constructed. The integral attack is a well-known tool to analyze AES-like block cipher. Applying some integral properties, we extend one round into the distinguishers for some permutations used in the PHOTON family. Besides, two rounds are added into the distinguishers of some permutations by using the super-sbox idea which was introduced to attack some SHA-3 candidates. Note that we utilize the super-sbox technique in a different approach from the rebound attack. At last, we obtain some new upper bounds on algebraic degrees of the permutations by applying the result in [20] and construct three new full-round distinguishers basing on them. Totally, we construct the full-round zero-sum distinguishers for the first four permutations in the PHOTON family. Table 1 presents the main results in this paper and some previous results showed by the designer of PHOTON in [14]. Note that one only need to find some inputs, which forms a zero-sum of the given permutation, when he construct a zero-sum distinguisher. Consequently, we only need to compute backward from some states in some middle rounds so that the time complexity in Table 1 is half the data complexity.

This paper is organized as follows: in Section 2, we show four concepts: zero-sum, zero-sum partition, zero-sum structure and zero-sum distinguisher. In Section 3, we give the description of the PHOTON

family and the definition of higher-order differential. Some zero-sum distinguishers are constructed for the permutations of all PHOTON members. In Section 4, we improve the upper bounds on the degrees of some permutations basing on the spectral properties and some advanced zero-sum distinguishers are constructed by using some integral properties and the super-sbox idea. In Section 5, we present some tighter upper bounds on the degrees of the permutations and construct some full-round distinguishers. Section 6 concludes the paper.

2 Zero-Sum, Zero-Sum Partition, Zero-Sum Structure and Zero-Sum Distinguisher

2.1 Zero-Sum, Zero-Sum Partition and Zero-Sum Structure

In 2009, J.-P. Aumasson and W. Meier firstly presented the concept of zero-sum distinguisher, and applied it to round-reduced versions of the KECCAK-f permutation [18]. C. Boura and A. Canteaut gave the definitions for zero-sum and zero-sum partition in [19].

Definition 1. Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. A zero-sum for F of size K is an input set of F, $\{x_1, \cdots, x_K\} \subset \mathbb{F}_2^n$, satisfying both following conditions

1. The sum of all elements in the set is zero.
2. The sum of the corresponding images of all elements in the set is zero.

We can express them by

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

Note that it is easy to obtain a zero-sum from an integral path [23]. Indeed, an integral distinguisher used on the known-key model of a block cipher constructs a zero-sum as the input set.

Definition 2. Let P be a permutation from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. A zero-sum partition for P of size $K = 2^k$ is a collection of 2^{n-k} subsets $X_i = \{x_{i,1}, \cdots, x_{i,2^k}\} \subset \mathbb{F}_2^n$, $1 \leqslant i \leqslant 2^{n-k}$, satisfying the following conditions

1. The intersection of any two zero-sums is a null set, *i.e.*

$$X_i \cap X_j = \varnothing, i \neq j, 1 \leqslant i, j \leqslant 2^{n-k}.$$

2. The union of these zero-sums is $\mathbb{F}_2^n$, *i.e.* $\bigcup_{i=1}^{2^{n-k}} X_i = \mathbb{F}_2^n$.
3. Each subset is a zero-sum for P of size 2^k, *i.e.*

$$\bigoplus_{j=1}^{2^k} x_{i,j} = \bigoplus_{j=1}^{2^k} P(x_{i,j}) = 0, 1 \leqslant i \leqslant 2^{n-k}.$$

Each X_i is called a zero-sum structure for the permutation P.

2.2 Zero-Sum Distinguisher

As described in [18], if we find some distinct values that sum to zero such that their images by a given function f also sum to zero, we can construct a zero-sum distinguisher for the function f. In some cases, the images of a intermediate state structure sum to zero for i permutation rounds, and the sum of its preimages for j rounds also vanishes. Then, these preimages construct a zero-sum for $i + j$ permutation rounds and we can build a zero-sum distinguisher from it.

3 Higher-Order Differentials for PHOTON

Higher-order differential is an efficient tool to construct zero-sum distinguishers. In this section, we firstly introduce the concept of higher-order differential and then show how to build a zero-sum distinguisher for a permutation by estimating the upper bound on its algebraic degree. Next, the description of the PHOTON family is given. At last, we present the higher-order differential attack on each PHOTON permutation and construct the zero-sum distinguishers for them.

3.1 Constructing Zero-Sum Distinguishers from the Higher-Order Derivatives

In [17], X. Lai gave the definition of the derivatives of cryptographic functions. For a permutation from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, the definition can be formulated as follows.

Definition 3. Let P be a permutation from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. For any $a \in \mathbb{F}_2^n$ the derivative of P at the point a is the function

$$D_a P(x) = P(x \oplus a) \oplus P(x).$$

The i-th order derivative of P at the point $a_1, \cdots, a_i$ is defined by

$$D_{a_1,\cdots,a_i} P(x) = D_{a_i}(D_{a_{i-1}}(\cdots D_{a_1} P(x))) = \bigoplus_{(k_1,\cdots,k_i)\in\mathbb{F}_2^i} P(x \oplus \bigoplus_{j=1}^{i} k_j a_j).$$

For any m-dimensional subspace V of $\mathbb{F}_2^n$, the m-th order derivative of P with respect to V is the function defined by

$$D_V P(x) = D_{a_m}(D_{a_{m-1}}(\cdots D_{a_1} P(x))) = \bigoplus_{v\in V} P(x \oplus v),$$

where $a_1, \cdots, a_m$ is a basis of V.

Note that the degree of any first order derivative of a function has the property $\deg(D_a P(x)) \leqslant \deg P(x) - 1$. Therefore, for every subspace V of dimension $(\deg P + 1)$ or any $(\deg P + 1)$ points $a_1, \cdots, a_{\deg P+1}$ the value of the $(\deg P + 1)$-order derivative of the permutation P is zero, *i.e.*

$$D_V P(x) = \bigoplus_{v\in V} P(x \oplus v) = 0,$$

$$D_{a_1,\cdots,a_{\deg P+1}} P(x) = \bigoplus_{(k_1,\cdots,k_{\deg P+1})\in\mathbb{F}_2^{\deg P+1}} P(x \oplus \bigoplus_{j=1}^{\deg P+1} k_j a_j) = 0.$$

Recalling the zero-sum distinguisher we mentioned in the last section, we find that if we can obtain $(\deg P + 1)$ points $a_1, \cdots, a_{\deg P+1}$ satisfying the condition

$$\bigoplus_{(k_1,\cdots,k_{\deg P+1})\in\mathbb{F}_2^{\deg P+1}} \bigoplus_{j=1}^{\deg P+1} k_j a_j = 0,$$

we can construct a zero-sum distinguisher and for a given $x \in \mathbb{F}_2^n$,

$$\{x \oplus \bigoplus_{j=1}^{\deg P+1} k_j a_j, (k_1, \cdots, k_{\deg P+1}) \in \mathbb{F}_2^{\deg P+1}\}$$

is a zero-sum of size $2^{\deg P+1}$ for the permutation P.

J.-P. Aumasson and W. Meier introduced the method to construct a zero-sum distinguisher for an iterated permutation in [18]. We denote the permutation by $P = R_r \circ \cdots \circ R_1$, where r denotes the round number of P. Let n be the size of state. The process can be presented as follows:

Step 1. Determine the algebraic degrees of one round and one inverse round for the iterated permutation, denoted by d_1 and d_2 respectively.

Step 2. For $i = 1, 2, \cdots$, estimate the upper bound on the degree of i-round iterated permutation based on the degree of one round d_1, until find a positive integer r_1 satisfying the condition that

$$d_1^{r_1} < n - 1, \text{and } d_1^{r_1+1} \geqslant n - 1.$$

In addition, apply the method in the opposite direction and find the corresponding integer r_2.

Step 3. Fix $n - l - 1$ bits of the intermediate state after r_2 rounds to some arbitrary value, where $l = \max(d_1^{r_1}, d_2^{r_2})$. For each of the values of the bits left (we call them *active bits* in this paper), compute r_2 rounds backwards to obtain 2^{l+1} initial states $x_1, \cdots, x_{2^{l+1}}$. Then, the set $\{x_1, \cdots, x_{2^{l+1}}\}$ is a zero-sum of size 2^{l+1} for the permutation P or its round-reduced version.

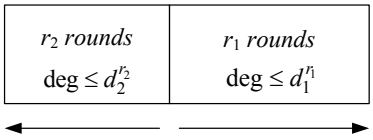

Fig. 1. Structure of the zero-sum distinguisher

Remark. In the second step, a trivial method is applied to estimate the upper bound on the degrees of some permutations. The method is rooted in the fact: for two mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, named G and F, we can obtain an upper bound on the degree of the composition $G \circ F$ by $\deg(G \circ F) \leqslant \deg(G)\deg(F)$. Specifically, the bound on the degree of i-round iterated permutation is d^i if the degree of one round is d. In the later sections of [18], Aumasson *etc.* improved the method for the KECCAK-f permutation. If we choose at most one bit in each row as the active bit, the first round backwards has degree one because only one variable enters into the nonlinear part of this round. Besides, Aumasson *etc.* show a higher-order differential attack on another SHA-3 candidate Hamsi-256 [21].

3.2 Description of the PHOTON Family

The PHOTON family [4] is a series of lightweight hash functions, announced by J. Guo *etc.* in Crypto 2011. There are two main techniques used in PHOTON: (1) extended sponge construction and (2) AES-like primitive as internal permutation.

Sponge function [12] is a new choice to design a hash function from a fixed permutation. In order to allow more flexibility, PHOTON adopts the framework of extending the original sponge construction (see Figure 2). It allows the number r' of bits extracted after each permutation P in the squeezing part to be different from the bit rate r in the absorbing part, in order to reduce the time spent in the squeezing process.

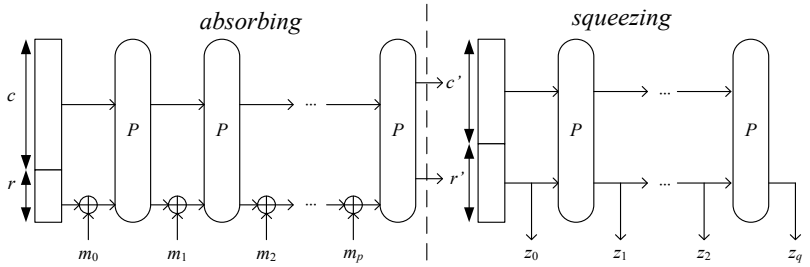

Fig. 2. The extended sponge framework used by the PHOTON family

The internal permutation P used by PHOTON is a fixed key AES-like function. The state can be represented as a $d \times d$ matrix and its size is sd^2, where s denotes the size of each entry in the matrix, equaling to the size of each S-box. Each round in PHOTON includes four basic operations:

AddConstants (AC). each entry in the first column of the internal state XORs a constant to distinguish each round in the permutation and destroy the classical symmetry between columns.

SubCells (SC). two types of well-analyzed S-boxes are adopted to build the substitution layer: the 4-bit PRESENT S-box and the 8-bit AES S-box. Especially, the AES S-box of size 8-bit is only used in one hash function of the PHOTON family.

ShiftRows (SR). this layer is very similar to the ShiftRows used by AES. In short, the i-th row will classically be rotated by i positions to the left, i counts from 0.

MixColumnsSerial (MC). for implementing in an extremely compact way, the mixed layer of PHOTON uses a matrix with many zero entries and a serial way to update the column vectors. It is equivalent to multiply an MDS matrix.

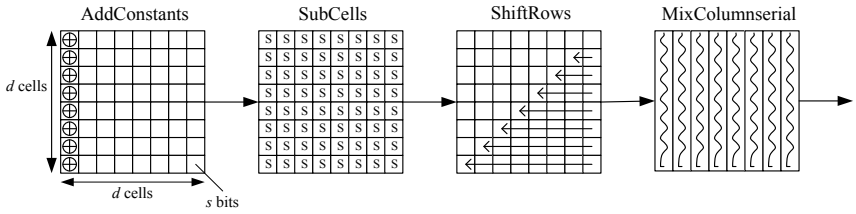

Fig. 3. One round of a PHOTON permutation

There are five members in the PHOTON hash function family: PHOTON-80/20/16, PHOTON-128/16/16, PHOTON-160/36/36, PHOTON-224/32/32 and PHOTON-256/32/32. Each of them was denoted by the form PHOTON-$n/r/r'$, where n, r and r' are the hash output size, the input bitrate and the output bitrate respectively. Accordingly, they use internal permutations P_{100}, P_{144}, P_{196}, P_{256} and P_{288} respectively. We can use a table (see Table 2) to enumerate the size of the internal state t, the number of cells d in each row or each column, the size of the S-boxes s and the round number N_r for each internal permutation.

Table 2 The parameters of the internal permutations P_t

	t	d	s	N_r
P_{100}	100	5	4	12
P_{144}	144	6	4	12
P_{196}	196	7	4	12
P_{256}	256	8	4	12
P_{288}	288	6	8	12

We notice that except the last permutation P_{288}, others adopt the 4×4 S-box and the round number of each permutation is twelve.

If one uses them to hash a message M of size l bits, the message is firstly padded to be a multiple of the bitrate r. The bit 1 is appended to the end of the message, followed by $r - 1 - (l \mathrm{mod} r)$ zeros (possibly none). Finally, the padded message is split into r-bit blocks $m_0, \cdots, m_p$. In each iteration of the absorbing part, the state absorbs the message block m_i and then applies the permutation P_t to update the state by

$$S_{i+1} = P_t(S_i \oplus (m_i \parallel \{0\}^c)).$$

Once all l message blocks have been absorbed, it enters into the squeezing part. The hash value can be computed by concatenating the successive r'-bit output blocks z_i until we reach the appropriate output size n.

3.3 Zero-Sum Distinguishers for the Permutations of the PHOTON Family

As previously mentioned, the algebraic degree of a permutation P provides some particular zero-sums. Accordingly, we should estimate the algebraic degrees of the permutations used in the PHOTON family. For one round of these permutations, the only nonlinear operation is SubCells. Other operations are linear and have algebraic degree one. Additionally, there are two types of S-boxes used in PHOTON, the PRESENT S-box and the AES S-box, each of algebraic degree 3 and 7 respectively. Furthermore, the algebraic degree of each inverse is the same. Then, we can estimate the degrees for some permutation rounds and construct some zero-sum distinguishers for the members of the PHOTON family.

- P_{100}: for this permutation, the degree of one round or one inverse round is 3 so that the 4-round permutation has degree at most $3^4 = 81$ ($3^5 = 243$ exceeds the bit number of the state). As a result, we can randomly choose 82 bits of the intermediate state after 4 rounds as the active bits and compute backward to obtain 2^{82} initial values to compose a zero-sum. In other words, we construct a zero-sum distinguisher of 8 permutation rounds with the complexity 2^{82}.
- P_{144}: it is obviously that we can construct a zero-sum distinguisher for this permutation by randomly choosing 82 bits of the intermediate state after 4 rounds with complexity 2^{82}. Whereas, we notice that there are 36 parallel S-boxes in one round. We can choose at most one active bit entering into a single S-box to ensure that one round is free. In this case, the degree of 4 (inverse) rounds is at most $1 \times 2^3 = 27$. We need to choose 28 active bits from 28 different elements in the state matrix. As a result, the complexity of constructing an 8-round zero-sum distinguisher decreases from 2^{82} to 2^{28}.
- P_{196}: we can use the same technique to P_{196} to construct an 8-round zero-sum distinguisher with complexity 2^{28};
- P_{256}: for this permutation, the algebraic degree of one round is also 3, but it has a larger state. Notice that the bit number in intermediate state is greater than 3^4. Therefore, we can construct a zero-sum distinguisher of 10 permutation rounds with complexity 2^{244}.
- P_{288}: the permutation uses the AES S-box which has the algebraic degree 7. Additionally, the degree of its inverse is also 7. Hence, 2-round permutation has degree at most 49 (the upper bound on the degree of 3-round permutation is greater than the state size) and we can obtain a 4-round zero-sum distinguisher with complexity 2^{50}.

Commonly, it is hard to build a zero-sum distinguisher for an AES-like permutation if it uses an 8×8 S-box, because the algebraic degree becomes very large in few rounds.

4 Advanced Zero-Sum Distinguishers for the Permutations of the PHOTON Family

In the last section, we show a method to find zero-sums and construct zero-sum distinguishers for an iterated permutation. The key point of this method is to estimate the algebraic degrees of a composed permutation and its inverse. Though, the upper bound obtained by the trivial way is often very little representative of the real degree of the permutation. For some iterated permutation, the bound may reduce if we use some spectral properties. In this section, the definition of Walsh spectrum is firstly introduced, and then the upper bounds on the algebraic degrees of some round-reduced permutations are improved by using the result in [19, 22]. Furthermore, we improve our attacks by using the properties of integral

cryptanalysis and super-sbox idea. We give some integral properties used in our next attacks, and then exploit the structure and extend one round to distinguishers. In order to construct zero-sum distinguishers with more rounds, we introduce the super-sbox technique and show some advanced distinguishers at last.

4.1 Exploiting the Bound on the Degree of SubCells Layer of PHOTON

Definition 4. The Walsh spectrum of a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is the multiset

$$\{\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+\alpha\cdot x}, \alpha\in\mathbb{F}_2^n\}.$$

The Walsh spectrum of a vectorial function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ corresponds to the multiset

$$\{\sum_{x\in\mathbb{F}_2^n}(-1)^{\beta\cdot f(x)+\alpha\cdot x}, \alpha\in\mathbb{F}_2^n, \beta\in\mathbb{F}_2^n\setminus\{0\}\},$$

where $x\cdot y$ denotes the dot product between two vectors x and y, *i.e.* $\sum x_i y_i$.

We call the Walsh spectrum of a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ be 2^l-*divisible* if all its values are divisible by 2^l. Then, we may obtain an improved upper bound on the degree of $G\circ F$ if all the Walsh spectrum of F is divisible by a large power of 2.

Theorem 1.[19, 22] Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ such that its Walsh spectrum is 2^l-divisible. Then, for any function G from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, we have

$$\deg(G\circ F)\leqslant n-l+\deg(G).$$

In [19], C. Boura and A. Canteaut consider the hash function whose nonlinear part consists of some parallel applications of a small permutation. For these permutations, there are two results as following.

1. If the Walsh spectrum of the small nonlinear component is 2^{l_0}-divisible, the Walsh spectrum of the whole nonlinear layer is $2^{l_0 n_r}$-divisible, where n_r denotes the number of the small nonlinear components in a nonlinear layer.

2. The Walsh spectrum is invariant under composition with a linear transformation.

As we mentioned before, the only nonlinear part is the SubCells layer and it has d^2 parallel S-boxes. In addition, P_{196} and P_{256} use the 4-bit PRESENT S-box whose Walsh spectrum is 2^2-divisible. Accordingly, all the elements of the Walsh spectrum of the SubCells layer for P_{196} and P_{256} are divisible by 2^{98} and 2^{128} respectively. Since the Walsh spectrum is invariant under composition with a linear transformation, the Walsh spectrum of a whole round for each of the two permutations is invariable. We can improve the attacks on both permutations.

- P_{196}: as we computed before, the four (inverse) rounds permutation has degree at most $3^4 = 81$. Besides, the Walsh spectrum of one-round is divisible by 2^{98}. Applying Theorem 1, we can obtain that the algebraic degree of five (inverse) rounds permutation has degree at most $196-2\times 49+81 = 179$. We can construct a 10-round zero-sum distinguisher for P_{196} with complexity 2^{180};

- P_{256}: in the last section, we construct a 10-round zero-sum distinguisher for the permutation in a trivial way with complexity 2^{244}. Notice that the Walsh spectrum of one-round P_{256} is 2^{98}-divisible. The algebraic degree of five (inverse) rounds permutation has degree at most $256-2\times 64+81 = 209$. The complexity of constructing a 10-round zero-sum distinguisher decreases to 2^{210}.

Since the Walsh spectrum and the algebraic degree have close relationship for a function, we can improve the upper bound on the degree by the spectral properties. Moreover, an improved zero-sum distinguisher can be constructed.

4.2 Exploiting the Structure from the Integral Properties

Integral attack [23-26] is well-known to be effective against byte-based block ciphers. The basic idea of the attack is to consider the propagation of sums of (many) values and to use the existence of that property to verify key guesses.

In this attack some bytes of the plaintext are chosen to be constant, denoted by C, and others, called active bytes, take on all values through the set of texts which were denoted by A. For these active bytes, it is unaffected by the application of a bijective S-box substituting bytes. In other words, the image of an active byte after a bijective S-box is also an active byte, *i.e.* a byte taking on all values. Furthermore, applying AddConstants the active bytes and constant bytes are invariant. If ShiftRow is applied, some active bytes may be transposed. In this subsection, we utilize these integral properties to extend one round in the middle of the previous distinguishers. It should be stressed here that it is a different approach from the known-key integral distinguishers presented in [14].

In the higher-order differential attack, the algebraic degree may have a great increase when a nonlinear layer is added. For these AES-like permutations, we show how to extend a round of our distinguishers by passing through an S-box layer freely. We can choose the active bits used in our high-order differential attacks with the following method: if we need to choose m active bits in previous attack, we should randomly choose $\lceil m/s \rceil$ entries in the state matrix, where s is the size of an entry, and all bits in these entries are active (we call them active bytes or active nibbles for PHOTON) in the improved attack. Since the images of active bytes and active nibbles after a bijective S-box are also active, the two intermediate states on both sides of the nonlinear layer in the extended round can be the starting points of the higher-order differential attack (see Figure 4). Note that the complexity may increase to $2^{s\lceil m/s \rceil}$ in the attack. Specially, the process leads to a failure if the whole state is active, *i.e.* $\lceil m/s \rceil = d^2$. For the PHOTON family, the bound on algebraic degree of some rounds permutation we estimated equals to the algebraic degree bound of its inverse. Therefore, this method is suitable for the permutation with odd round number. We can construct the zero-sum distinguishers with 9 rounds for P_{100} and P_{144}, and with 11 rounds for P_{196} and P_{256}. For instance, we already know that the 5-round P_{256} has degree at most 209. Choose 53 nibbles as the active nibbles in the input state of SubCells layer of the sixth round, and then its output state has 53 active nibbles in the same state entries. Computing forward and backward, we can obtain two balance states: the input state of the first round and the output state of the eleventh round. In other words, we construct a zero-sum distinguisher of 5+1+5=11 rounds P_{256} with complexity 2^{212}. By the same method, 9-round, 9-round and 11-round zero-sum distinguishers of P_{100}, P_{144} and P_{196} can be constructed with complexities $2^{84}, 2^{84}$ and 2^{180}, respectively.

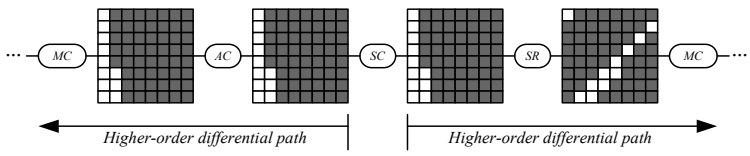

Fig. 4. Part of the one extended round of the structure of the improved zero-sum distinguisher for P_{256}. White nibbles are constant. Black nibbles denote the active nibbles.

4.3 Exploiting the Structure from the Super-Sbox Idea

In [27], two-round AES differential was studied, and a composition of serial operations is called a super-sbox. Actually, if we consider 4-byte permutations instead of the usual 8-bit S-boxes, two rounds of an AES permutation can be represented by using only one nonlinear layer with a large size. In 2010, H. Gilbert and T. Peyrin apply the idea to some AES-like hash functions to reach a more efficient use of

the freedom degrees [28]. Specifically, for a fixed permutation, two AES-like permutation rounds can be expressed as

$$MC \circ SR \circ SB \circ AC \circ MC \circ SR \circ SB \circ AC.$$

Since ShiftRows and SubBytes are commutative, it can also be represented by

$$MC \circ SR \circ (SB \circ AC \circ MC \circ SB) \circ SR \circ AC.$$

The part in the middle $SB \circ AC \circ MC \circ SB$ can be viewed a super-sbox which only involve in a single column.

In this paper, we utilize the super-sbox technique in a different approach. For rebound attack, it was applied to constructed a differential path with one more round which exploits the differential properties in a match-in-the-middle way. Nonetheless, we use the technique to guarantee that certain active nibbles are also active after two rounds, even if some positions change in the original operations order.

We will firstly show the method to extend two rounds to the trivial zero-sum distinguisher and apply it to some permutations of the PHOTON family. Using the super-sbox idea, the active bits need to be chosen columnwise: if we need to choose m active bits attacking on an r-rounds permutation, we should randomly choose $\lceil m/ds \rceil$ columns in the state matrix in the advanced attack, and all bits in these columns are active. If $\lceil m/ds \rceil < d$, we can construct an $(r+2)$-round zero-sum distinguisher by adding two rounds in the middle.

At first, for the two rounds in the middle, swap ShiftRows and SubCells of the first round, and then we can write the two rounds

$$MC \circ SR \circ (SC \circ AC \circ MC \circ SC) \circ SR \circ AC.$$

Choose $\lceil m/ds \rceil$ columns in the intermediate state after the ShiftRows layer in the first round. It is easy to deduce that the super-sbox makes an active column become an active column. Therefore, the selected columns in the state after the super-sbox layer are also active and other columns are still constants. We obtain two starting points for the higher-order differential attacks backward and foreword (see Figure 5). Applying this method to PHOTON, we can improve some distinguishers which were constructed before.

- P_{144}: there are 36 nibbles in the state and the algebraic degree of 4 permutation rounds is at most 81. Consequently, selecting $\lceil 82/24 \rceil = 4$ columns, we can construct a zero-sum distinguisher of $4 + 2 + 4 = 10$ rounds with complexity 2^{96};
- P_{196}: the state has 49 nibbles and the algebraic degree of 5 permutation rounds is at most 179. In this case, we have to choose $\lceil 180/28 \rceil = 7$ columns and it leads to a trivial zero-sum;
- P_{256}: for this permutation, there are 64 nibbles in the state and the algebraic degree of 5 rounds permutation is at most 209. Thus, we need to choose $\lceil 210/32 \rceil = 7$ active columns. We can construct a 12-round zero-sum distinguisher with complexity 2^{224} (see Figure 5).;

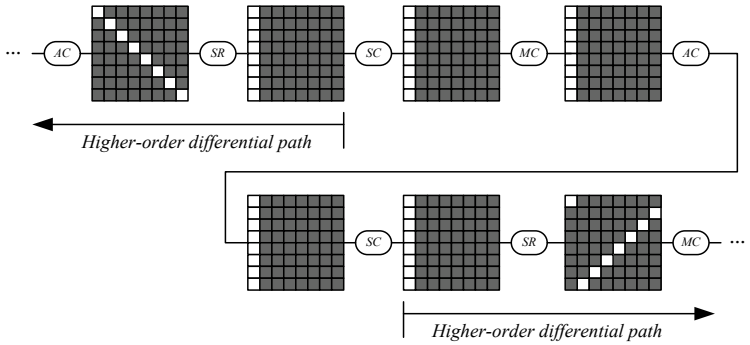

Fig. 5. Part of the two extended rounds of the structure of the advanced zero-sum distinguisher for P_{256}

5 Exploiting the Upper Bounds on the Algebraic Degrees

Utilizing integral property and super-sbox idea, we construct some zero-sum distinguishers for some PHOTON permutations, which adopt PRESENT S-box. The key point of this method is to match two middle states, which have some active nibbles, and then compute forward and backward to reach the balance. On the other hand, if we only estimate the algebraic degrees of a permutation and its inverse to construct distinguishers we can apply the result in [20].

Theorem 2. [20] Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ corresponding to the concatenation of m smaller balanced S-boxes, $S_1, \cdots, S_m$, defined over $\mathbb{F}_2^{n_0}$. Then, for any function G from $\mathbb{F}_2^n$ into $\mathbb{F}_2^l$, we have

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

Obviously, the theorem provides a tighter upper bound on the algebraic degree of a iterative permutation when the round number is large enough. Note that when representing $\deg(G \circ F)$ as a function of $\deg G$, the upper bound in Theorem 2 states that the degree of $G \circ F$ is upper-bounded by a line with slope $1/(n_0 - 1)$. However, the upper bound introduced in [19] corresponds to a line with slope one. As a result, the former increases slower than the later when $n_0 > 2$ (but the former corresponds to a higher starting point). Applying the theorem, we can obtain that the upper bounds on the degrees of five PHOTON permutations and the tighter bounds are presented in Table 3.

Table 3 Upper bounds on the algebra degrees of the output of r rounds permutations

round	bound on degree				
	P_{100}	P_{144}	P_{196}	P_{256}	P_{288}
1	3	3	3	3	7
2	9	9	9	9	49
3	27	27	27	27	253
4	75	81	81	81	283
5	91	123	157	197	-
6	97	137	183	236	-

From the table, we can find that when the round number is six the upper bound on degree of each of the first four permutations, denoted by P_n, is less than $n - 1$. Therefore, besides permutation P_{256} we can construct full-round distinguishers for P_{100}, P_{144} and P_{196} basing on these new upper bounds. As a result, full-round zero-sum distinguishers for permutations $P_{100}, P_{144}, P_{196}$, and P_{256} can be constructed with complexity $2^{98}, 2^{138}, 2^{184}$ and 2^{237}, respectively. Note that the complexity of attacking on P_{256} is larger than the previous complexity 2^{224}. Furthermore, we can also obtain a zero-sum distinguisher for 8-round P_{288} with complexity 2^{284}.

Applying the super-sbox idea, we can improve the complexity of attacking on P_{196}. For this permutation, there are 49 nibbles in the state and the new upper bound on algebraic degree of 5 rounds permutation is 157. Thus, we need to choose $\lceil 158/28 \rceil = 6$ active columns. As a result, the complexity of constructing a 12-round zero-sum distinguisher decreases to 2^{168}.

6 Conclusion

In this paper, we presented the cryptanalysis results of PHOTON hash function family by using the higher-order differential properties, the spectral properties, the integral properties and the super-sbox. For AES-like hash functions, it seems to be an efficient way to construct the integral distinguishers for the permutations used in these functions. However, if they adopt some small S-boxes, the higher-order

differential attack may be a better choice. We study the Walsh spectrum of the PRESENT S-box and exploit improved upper bounds on the degrees of some round-reduced PHOTON permutations. It permits us to attack some permutations with more rounds and makes our next attack available.

Notice that a structure of integral attack involves in some active bytes and some constant bytes. It is similar to the structure used in higher-order differential attack. So we can firstly choose the active bits nibble by nibble for the state of PHOTON. The active nibbles pass through the SubCells layer freely because the S-boxes used in PHOTON are bijective. The zero-sum distinguisher can be extended one more round by using this idea. In addition, we can improve this method based on the super-sbox technique and choose the active bits column by column. Applying this method, it is feasible to extend two rounds to some distinguishers in the middle.

On the other hand, we exploit the tighter upper bounds on the degrees of these permutations and find that the full-round distinguishers can be constructed for the permutations P_{100}, P_{144} and P_{196}. Utilizing the super-sbox idea, we improve the complexity of attacking on P_{196}. All in all, we have attacked all permutations used by the PHOTON family. Additionally, the results do not threat the security of the hash family.

1 Aumasson J P, Henzen L, Meier W, Naya-Plasencia M. Quark: A Lightweight Hash. In: Mangard S, Standaert F X, eds. CHES 2010, LNCS 6225. Heidelberg: Springer-Verlag, 2010. 1-15

2 Badel S, Dagtekin N, Nakahara J, Ouafi K, Reffé N, Sepehrdad P, Susil P, Vaudenay S. ARMADILLO: A Multi-purpose Cryptographic Primitive Dedicated to Hardware. In: Mangard S, Standaert F X, eds. CHES 2010, LNCS 6225. Heidelberg: Springer-Verlag, 2010. 398-412

3 Yoshida H, Watanabe D, Okeya K, Kitahara J, Wu H, Küçük Ö, Preneel B. MAME: A Compression Function with Reduced Hardware Requirements. In: Paillier P, Verbauwhede I, eds. CHES 2007, LNCS 4727. Heidelberg: Springer-Verlag, 2007. 148-165

4 Guo J, Peyrin T, Poschmann A. The PHOTON Family of Lightweight Hash Functions. In: Rogaway P, ed. CRYPTO 2011, LNCS 6841. Heidelberg: Springer-Verlag, 2011. 222-239

5 Cannière C D, Dunkelman O, Knezevic M. KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Clavier C, Gaj K, eds. CHES 2009, LNCS 5747. Heidelberg: Springer-Verlag, 2009. 272-288

6 Bogdanov A, Knudsen L R, Leander G, Paar C, Poschmann A, Robshaw M J B, Seurin Y, Vikkelsoe C. PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P, Verbauwhede I, eds. CHES 2007, LNCS 4727. Heidelberg: Springer-Verlag, 2007. 450-466

7 Engels D, Fan X, Gong G, Hu H, Smith E M. Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices. In: Sion R, Curtmola R, Dietrich S, Kiayias A, Miret J M, Sako K, Sebé, F, eds. Financial Cryptography Workshops, LNCS 6054. Heidelberg: Springer-Verlag, 2010. 3-18

8 Hong D, Sung J, Hong S, Lim J, Lee S, Koo B, Lee C, Chang D, Lee J, Jeong K, Kim H, Kim J, Chee S. HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin L, Matsui M, eds. CHES 2006, LNCS 4249. Heidelberg: Springer-Verlag, 2006. 46-59

9 Knudsen L R, Leander G, Poschmann A, Robshaw M J B. PRINTcipher: A Block Cipher for IC-Printing. In: Mangard S, Standaert F X, eds. CHES 2010, LNCS 6225. Heidelberg: Springer-Verlag, 2010. 16-32

10 Lim C H, Korkishko T. mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors. In: Song J, Kwon T, Yung M, eds. WISA 2005, LNCS 3786. Heidelberg: Springer-Verlag, 2006. 243-258

11 Standaert F X, Piret G, Gershenfeld N, Quisquater J J. SEA: A Scalable Encryption Algorithm for Small Embedded Applications. In: Domingo-Ferrer J, Posegga J, Schreckling D, eds. CARDIS 2006, LNCS 3928. Heidelberg: Springer-Verlag, 2006. 222-236

12 Bertoni G, Daemen J, Peeters M, Assche G V. Sponge functions. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.8103&rep=rep1type=pdf

13 National Institute of Standards and Technology. Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

14 Guo J, Peyrin T, Poschmann A. The PHOTON Family of Lightweight Hash Functions. http://www.ecrypt.eu.org/hash2011/proceedings/hash2011_04.pdf

15 Sasaki Y, Li Y, Wang L, Sakiyama K, Ohta K. Non-full-active Super-Sbox Analysis: Applications to ECHO and Grøstl. In: Abe M, ed. ASIACRYPT 2010. LNCS 6477. Heidelberg: Springer-Verlag, 2010. 38-55

16 Knudsen L R, Rijmen V. Known-Key Distinguishers for Some Block Ciphers. In: Kurosawa K, ed. ASIACRYPT 2007, LNCS 4833. Heidelberg: Springer-Verlag, 2007. 315-324

17 Lai X. Higher order derivatives and differential cryptanalysis. Communications and Cryptography: Two Sides of One Tapestry,

Kluwer Acadamic Publishers, 1994

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

19 Boura C, Canteaut A. Zero-Sum Distinguishers for Iterated Permutations and Application to Keccak- and Hamsi-256. In: Biryukov A, Gong G, Stinson D R, eds. SAC 2010. LNCS 6544. Heidelberg: Springer-Verlag, 2010. 1-17

20 Boura C, Canteaut A, Cannière, C D. Higher-order differential properties of Keccak and Luffa. In: Joux A, ed. FSE 2011, LNCS 6733. Heidelberg: Springer-Verlag, 2011. 252-269

21 Aumasson J P, Käsper E, Knudsen L R, Matusiewicz K, ∅ degård R S, Peyrin T, Schläffer, M. Distinguishers for the Compression Function and Output Transformation of Hamsi-256. In: Steinfeld R, Hawkes P, eds. ACISP 2010, LNCS 6168. Heidelberg: Springer-Verlag, 2010. 87-103

22 Canteaut A, Videau M. Degree of Composition of Highly Nonlinear Functions and Applications to Higher Order Differential Cryptanalysis. In: Knudsen L R, ed. EUROCRYPT 2002, LNCS 2332. Heidelberg: Springer-Verlag, 2002. 518-533

23 Knudsen L R, Wagner D. Integral Cryptanalysis. In: Daemen J, Rijmen V, eds. FSE 2002, LNCS 2365. Heidelberg: Springer-Verlag, 2002. 112-127

24 Daemen J, Knudsen L R, Rijmen V. The Block Cipher Square. In: Biham E, ed. FSE 1997, LNCS 1267. Heidelberg: Springer-Verlag, 1997. 149-165

25 Ferguson N, Kelsey J, Lucks S, Schneier B, Stay M, Wagner D, Whiting D. Improved Cryptanalysis of Rijndael. In: Schneier B, ed. FSE 2000, LNCS 1978. Heidelberg: Springer-Verlag, 2000. 213-230

26 Galice S, Minier M. Improving Integral Attacks Against Rijndael-256 Up to 9 Rounds. In: Vaudenay S, ed. AFRICACRYPT 2008, LNCS 5023. Heidelberg: Springer-Verlag, 2008. 1-15

27 Daemen J, Rijmen V. Understanding Two-Round Differentials in AES. In: Prisco R D, Yung M, eds. SCN 2006, LNCS 4116. Heidelberg: Springer-Verlag, 2006. 78-94

28 Gilbert H, Peyrin T. Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations. In: Hong S, Iwata T, eds. FSE 2010, LNCS 6147. Heidelberg: Springer-Verlag, 2010. 365-383

29 Bertoni G, Daemen J, Peeters M, Van Assche G. Note on zero-sum distinguishers of Keccak-f. Public comment on the NIST Hash competition, available at http://keccak.noekeon.org/NoteZeroSum.pdf

30 Wagner D. A Generalized Birthday Problem. In: Yung M, ed. CRYPTO 2002, LNCS 2442. Heidelberg: Springer-Verlag, 2002. 288-303

31 Bellare M, Micciancio D. A New Paradigm for Collision-Free Hashing: Incrementality at Reduced Cost . In: Fumy W, ed. EUROCRYPT 1997, LNCS 1233. Heidelberg: Springer-Verlag, 1997. 163-192