symmetry

MDPI

Article

Another Perspective on Automatic Construction of Integral Distinguishers for ARX Ciphers

Kai Zhang [1,2,*] and Xuejia Lai [2,*]

[1] PLA SSF Information Engineering University, Zhengzhou 450001, China
[2] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
* Correspondence: zhkai2010@139.com (K.Z.); lai-xj@cs.sjtu.edu.cn (X.L.)

Abstract: This paper introduces a method to construct integral distinguishers for ARX ciphers. The basic idea of this method is to utilize the symmetry between the zero-correlation linear distinguishers and integral distinguishers. Combined with an automatic searching method on zero-correlation linear distinguishers of ARX ciphers, a subspace for the distinguishers is constructed. This subspace can finally be turned into an integral distinguisher based on the symmetry between these two distinguishers. Three ARX block ciphers, HIGHT, LEA and SPECK, are used to validate the effectiveness of this method. For LEA, four nine-round integral distinguishers are constructed, which is one more round than the previous best result derived with division property. For SPECK32, two more six-round integral distinguishers are constructed, whose number of active bits is reduced by one bit.

Keywords: cryptanalysis; block cipher; integral cryptanalysis; zero-correlation linear cryptanalysis

Citation: Zhang, K.; Lai, X. Another Perspective on Automatic Construction of Integral Distinguishers for ARX Ciphers. *Symmetry* **2022**, *14*, 461. https://doi.org/10.3390/sym14030461

Academic Editor: Alexander Shelupanov

Received: 20 January 2022
Accepted: 14 February 2022
Published: 24 February 2022

1. Introduction

Large numbers of cryptographic primitives using only addition, rotation and XOR three operations have been proposed for the past several years, which are generally denoted as ARX ciphers. As these operations can be implemented efficiently in both software and hardware platforms, the ARX ciphers usually have good performance. To meet the great security demand in constrained resource devices such as sensor nodes and RFID tags, ARX cipher is a good choice for the design of lightweight primitives. ARX ciphers have penetrated into many areas of symmetric key primitives, and there are many famous ARX ciphers such as HIGHT (ISO standard, Korean national standard, 2006) [1], SPECK (United States National Security Agency, 2013) [2], BLAKE (SHA-3 Finalists, 2014) [3], Skein (SHA-3 Finalists, 2010) [4], Threefish (underlying block cipher of Skein, 2010) [4], TEA family ciphers (TEA, 1994 [5]/XTEA, 1997 [6]/XXTEA, 1998 [7]), and Salsa20 (eSTREAM Finalists, 2008) [8].

Integral cryptanalysis was first proposed by Daemen, Knudsen and Rijmen to attack the SQUARE block cipher [9] and was further unified by Knudsen and Wagner as integral cryptanalysis [10]. There are usually two phases for integral cryptanalysis, one is to construct integral distinguishers, and the other one is to recover the key with the distinguisher. Integral cryptanalysis has proven to be effective against a wide variety of block ciphers.

For the construction of integral distinguishers, there are generally three approaches.

(1) Construction method based on traditional integral property

The focus of traditional integral distinguisher is to explore the propagation property through different cipher components for several states: C (CONSTANT), A (ALL), B (BALANCE), U (UNKNOWN) and then construct some integral distinguishers through deduction. There are some automatic approaches designed for integral distinguisher searching. In ACNS 2012, based on U-method [11], Zhang et al. proposed a unified method to search integral distinguishers for many block cipher structures [12]. In ICISC 2015,

Zhang et al. proposed a security evaluation framework against integral cryptanalysis for bit-oriented block ciphers based on match-through-the-Sbox technique [13].

(2) Construction method based on division property

For the past several years, the division property [14], which was proposed by Todo at Eurocrypt 2015, has led in the area of automatic construction for integral distinguishers for many block cipher structures. This property can explore the hidden properties between the traditional ALL and BALANCE properties in integral cryptanalysis. After the proposal of division property, many variants are proposed successively, such as bit-based division property [15] and three-subset division property [15]. Some corresponding automatic searching methods have been developed. At Asiacrypt 2016, with MILP (mixed integer linear programming), Xiang et al. introduced an automatic searching method for block ciphers with bitwise permutation based on bit-based division property [16]. In IET 2019, Sun et al. extended this framework to non-bit permutation-based block ciphers [17]. At Asiacrypt 2019, Wang et al. solved the problem of searching integral distinguishers based on bit-based division property using three subsets [18]. At Eurocrypt 2020, Hao et al. modeled three-subset division property without an unknown subset and improved cube attacks based on MILP [19]. At Latincrypt 2021, Ghosh and Dunkelman derived a more compact model for SAT (Boolean Satisfiability Problem)/CP (Constraint Programming) and realized the automatic search for bit-based division property [20]. At ACISP 2021, ElSheikh and Youssef solved the problem of bit-based division property for ciphers with large linear layers using MILP [21].

(3) Construction method based on the symmetry between different distinguishers

For Sbox-based designs, there are some links between the integral distinguishers and zero-correlation linear distinguishers. At Asiacrypt 2012, Bogdanov et al. revealed fundamental links of zero-correlation distinguishers to integral distinguishers and multidimensional linear distinguishers [22]. At Crypto 2015, Sun et al. illustrated the relationship between zero-correlation linear distinguishers and integral distinguishers for Sbox-based block ciphers [23]. For ARX-based designs, at ISP 2014, Wen et al. revealed a relation between the zero-correlation linear distinguishers and integral distinguishers [24]. This has made the foundation to construct integral distinguishers for ARX ciphers in the theoretical perspective.

1.1. Related Work

There are some integral distinguisher-related construction or automatic searching methods targeted at ARX ciphers. At Asiacrypt 2017, based on SAT (Boolean Satisfiability Problem)/SMT (Satisfiability Modulo Theory), Sun et al. introduced a method to detect ARX ciphers' division property at the bit level and some specific ciphers' division property at the word level [25]. In 2017, based on MILP, Sun et al. investigated bit-based division property for ARX ciphers [26]. At SAC 2018, based on SAT and bit-based division property, Eskandari et al. introduced a tool based on SAT, which focuses on the usability and describing of the cryptographic primitives at a high level, and the target also involves ARX ciphers [27]. At ICICS 2018, Han et al. proposed an automatic searching method for ARX block ciphers with three-subset division property based on SAT/SMT [28].

Generally speaking, in the area of integral cryptanalysis for ARX ciphers, on the first perspective, the majority of construction or automatic searching methods are based on division property, and these automations are all utilized with different solvers. On the second perspective, for some ARX ciphers, the length of longest integral distinguishers derived with division property is not as long as zero-correlation linear distinguishers, which means there is a gap according to the symmetry of these two cryptanalytic methods. (A concrete example is for ARX block cipher LEA, the current longest integral distinguisher is eight-round [25,27], which is derived with bit-based division property. But the current longest zero-correlation linear distinguisher is nine-round [29]). This motivates us to fill this gap.

However, the starting point of this paper can be viewed as a modification, and it borrows from previous automatic searching tools for zero-correlation linear distinguishers on ARX ciphers to solve the problem of integral distinguisher construction. However, this idea of borrowing from another cryptanalytic method is not new. At Eurocrypt 2017, Sasaki et al. proposed a new tool to search impossible differential distinguishers, and the new tool is slightly modified from the previous differential searching tool [30]. This transfer borrows the tool of differential cryptanalysis to improve the impossible differential distinguishers.

Problem statement: For evaluating the security level on ARX ciphers against integral cryptanalysis, the key problem is how to construct longer and more useful integral distinguishers.

Idea flow: Our framework follows the third approach for the construction of integral distinguishers. The idea originates from the relationship between the integral and zero-correlation linear distinguishers for ARX ciphers, applied with a previous automatic searching tool designed for zero-correlation linear distinguishers on ARX ciphers.

Highlight: The highlight is using an automatic tool designed for zero-correlation linear distinguishers to realize the automatic construction of integral distinguishers for ARX ciphers.

1.2. Our Contributions

The main purpose of this paper is to introduce a method to construct integral distinguishers for ARX ciphers without a solver. The basic idea of this method is to use the relationship between the integral and zero-correlation linear distinguishers, combined with a previous automatic searching tool designed for zero-correlation linear distinguishers on ARX ciphers. The main contributions can be concluded as follows.

- Based on establishing a subspace of zero-correlation linear distinguishers (short for ZCLDs) and the relationship between the zero-correlation linear distinguishers and integral distinguishers (short for INTDs) of ARX ciphers, a unified method is proposed to construct theoretical integral distinguishers for ARX ciphers. For any ARX ciphers, if a subspace of ZCLDs can be constituted with our method, a corresponding length of integral distinguisher is developed. In addition, the number of active bits for the integral distinguisher can be controlled through the scale of the subspace.
- To validate the effectiveness of this method, we take three ARX ciphers—HIGHT, SPECK and LEA as examples. For LEA, four nine-round integral distinguishers are constructed, which is one round longer than previous distinguishers derived with bit-based division property. For SPECK32, two more six-round integral distinguishers are derived, the number of active bits is one bit less than previous best distinguishers. For HIGHT, four 17-round new integral distinguishers are discovered.

The comparison for some new or longer integral distinguishers with previous results are illustrated in Table 1 below.

Paper Outline. This paper is organized as follows. In Section 2, some preliminaries are presented. Section 3 proposes an automatic method to construct integral distinguishers on ARX ciphers. In Section 4, some applications on HIGHT, LEA and SPECK are presented. Section 5 provides a validation on the new integral distinguishers on LEA, and Section 6 concludes this paper.

Table 1. Summary of integral distinguishers for some typical ARX ciphers.

Algorithm	Longest Round	Least Dimension ♣	Number	Reference	Remark
HIGHT	12	8	1	[1]	Traditional Integral Property
	17	56	2	[31]	Traditional Integral Property
	17	**57**	**4**	**This paper**	**Relation between different distinguishers**
	18	63	2	[25–27]	Bit-Based Division Property
LEA	6	32	1	[32]	Traditional Integral Property
	7	96	1	[26]	Bit-Based Division Property
	8	118	2	[25,27]	Bit-Based Division Property
	9 *	**126**	**4**	**This paper**	**Relation between different distinguishers**
SPECK32	6	31	1	[25]	Word-Based Division Property
	6	31	2	[28]	Three Subsets Bit-Based Division Property
	6	**30**	**2**	**This paper**	**Relation between different distinguishers**

♣ Dimension represents the number of active bits for the integral distinguisher; * In Ref. [33], a 9-round integral distinguisher for LEA is also introduced. However, it is an invalid integral distinguisher, the reason is illustrated in Section 5.

2. Preliminary

2.1. Relationship between the ZCLDs and INTDs for ARX Ciphers

In Ref. [22], Bogdanov et al. illustrated that any zero-correlation linear distinguisher can be transformed into an integral distinguisher for Sbox-based designs. In Ref. [24], Wen et al. introduced the transformation rules for ARX ciphers between these two kinds of distinguishers. The transformation rule is illustrated as follows.

For an ARX cipher H, the inputs are split into three parts and the outputs into two parts.

$$H: \mathbb{F}_2^r \times \mathbb{F}_2 \times \mathbb{F}_2^s \to \mathbb{F}_2^t \times \mathbb{F}_2^u$$

$$H(x,y,z) = (H_1(x,y,z), H_2(x,y,z))$$

The function $T_{\lambda||\lambda'}$ is defined as

$$T_{\lambda||\lambda'}: \mathbb{F}_2^s \to \mathbb{F}_2^t$$

$$T_{\lambda||\lambda'}(z) = H_1(\lambda,\lambda',z)$$

Theorem 1 ([24]). *If the input and output linear mask a and b are independent and the approximation for H has correlation of zero for any $a = (a_1 \,||\, 1, 0)$, $a_1 \in \mathbb{F}_2^r$ and any $b = (b_1, 0)$, $b_1 \neq 0, b_1 \in \mathbb{F}_2^t$, the sum of XOR of the function $H(x,y,z)$ is zero for any λ,*

$$\bigoplus_{y||z} H_1(\lambda,y,z) = 0$$

which represents an integral distinguisher.

If the output linear mask is a fixed constant, Corollary 1 can be easily derived from Theorem 1.

Corollary 1. *If the input and output linear mask a and b are independent and the approximation for H has correlation of zero for any $a = (a_1 \,||\, 1, 0)$, $a_1 \in \mathbb{F}_2^r$ and a fixed $b = (b_1, 0)$, $b_1 \neq 0, b_1 \in \mathbb{F}_2^t$, the sum of XOR of the function $H(x,y,z)$ is zero for any λ,*

$$\bigoplus_{y||z} b_1 \cdot H_1(\lambda,y,z) = 0$$

which represents an integral distinguisher.

2.2. Automatic Search of Zero-Correlation Linear Hulls for ARX Ciphers

In Ref. [29], Zhang et al. introduced an automatic search method targeted at deriving longer zero-correlation linear distinguishers for ARX ciphers (Algorithm 1 in [29]). In this method, a modified operation is used to model the property of non-zero-correlation linear approximations for the internal states. Combined with a miss-in-the-middle approach, some current longest zero-correlation linear distinguishers are derived.

In the following section, these two methods will be united to construct integral distinguishers on ARX ciphers.

3. Automatic Construction of Integral Distinguishers

The target of this construction method are two-fold. Regarding the first perspective, the round for the constructed integral distinguisher is as long as current longest zero-correlation linear distinguishers. Regarding the second perspective, the number of active bits for the integral distinguisher should be as small as possible.

To reach the first target, a subspace of current longest zero-correlation linear distinguishers should be constructed. To reach the second target, this subspace should be as large as possible; the reason is as follows.

- Through Theorem 1, it is found that with more free bits, the less the dimension of the corresponding integral distinguisher is. A free bit represents the linear mask bit, which can take any value on $\mathbb{F}_2$, the dimension represents the number of active bits for the integral distinguisher.

Thus, the problem of constructing integral distinguishers can be changed into a problem of constructing a subspace for the longest zero-correlation linear distinguishers, and the subspace should be as large as possible.

3.1. Basic Idea of Our Automatic Method

This automatic method mainly consists of the following four steps.

(1) Based on the automatic ZCLD searching method, construct a long zero-correlation linear distinguisher $\alpha \to \beta$ and derive the contradiction bit for this distinguisher.
(2) Change the zero of linear mask for the input/output into one that is bit by bit. If the change does not affect the contradiction bit, store the position of this input/output bit. All the stored positions can constitute a subspace for the input linear mask and a subspace for the output linear mask.
(3) Test whether all the linear masks in the subspace can be zero-correlation linear distinguishers with the same contradiction bit as $\alpha \to \beta$. If, after adding some bits, not all linear approximations in the subspace are zero-correlation, remove the positions of these bits.
(4) Construct integral distinguishers with the remaining subspace.

3.2. An Automatic Construction Method of Integral Distinguishers for ARX Ciphers

Following the four steps in Section 3.1, Algorithm 1 is proposed to solve the problem of automatic construction of integral distinguishers on ARX ciphers.

The core of this method is to construct a subspace of long zero-correlation linear distinguishers with the same contradiction bit and then use the relationship between INTDs and ZCLDs for ARX ciphers to construct integral distinguishers.

There are some issues to be addressed as follows.

- The length of the zero-correlation linear distinguisher should be as long as possible. As the length of the constructed INTD is the same as the length of the ZCLDs, if we want the length of the INTD to be longer, the ZCLDs used should be as long as possible.
- If there is only one longest zero-correlation linear distinguisher, the integral distinguisher derived is a trivial integral distinguisher, and it is infeasible to construct an

integral distinguisher. Some shorter zero-correlation linear distinguishers should be considered to construct integral distinguishers.

➢ This method can also be used to construct a subspace of long impossible differential distinguishers or zero-correlation linear distinguishers.

Algorithm 1 An automatic construction method of integral distinguishers.

Step 1: Construct a long ($r_1 + r_2$-round) zero-correlation linear distinguisher $\alpha \to \beta$, denote the contradiction bit of the distinguisher as A_1.

Step 2: Construct a set $\Omega_{in} = \varnothing$. Add the positions for the nonzero bits of α to the set Ω_{in} according to the following rule.

➢ Set zeros of α to one bit by bit, and add those bit positions that do not affect the contradiction bit A_1 to set Ω_{in}.

Step 3: Test whether for any $\gamma_i \in \mathbb{F}_2$, $\alpha \underset{i\in\Omega_{in}}{\oplus} \gamma_i \cdot e_i \to \beta$ is an $r_1 + r_2$ round zero-correlation linear distinguisher. Delete those bit positions that do not pass this test from set Ω_{in}. e_i represents the single bit linear mask, which has one at the i-th bit.

➢ Construct a subspace based on Ω_{in}. In this subspace, all the linear approximations are $r_1 + r_2$-round zero-correlation.

Step 4: Turn the subspace of zero-correlation linear distinguishers into an integral distinguisher.

3.3. A Toy Example

Suppose the size of the target block cipher is $n = 16$, $(P_1, P_2, \cdots, P_{16})$ represents the plaintext, and $(C_1, C_2, \cdots, C_{16})$ represents the ciphertext.

As illustrated in Figure 1, after step 1 in Algorithm 1, an eight-round zero-correlation linear distinguisher $\alpha \to \beta$ is constructed, and the contradiction bit is $A_1 = S_{13}^3$ (S_{13}^3 represents the 13th bit of the third round).

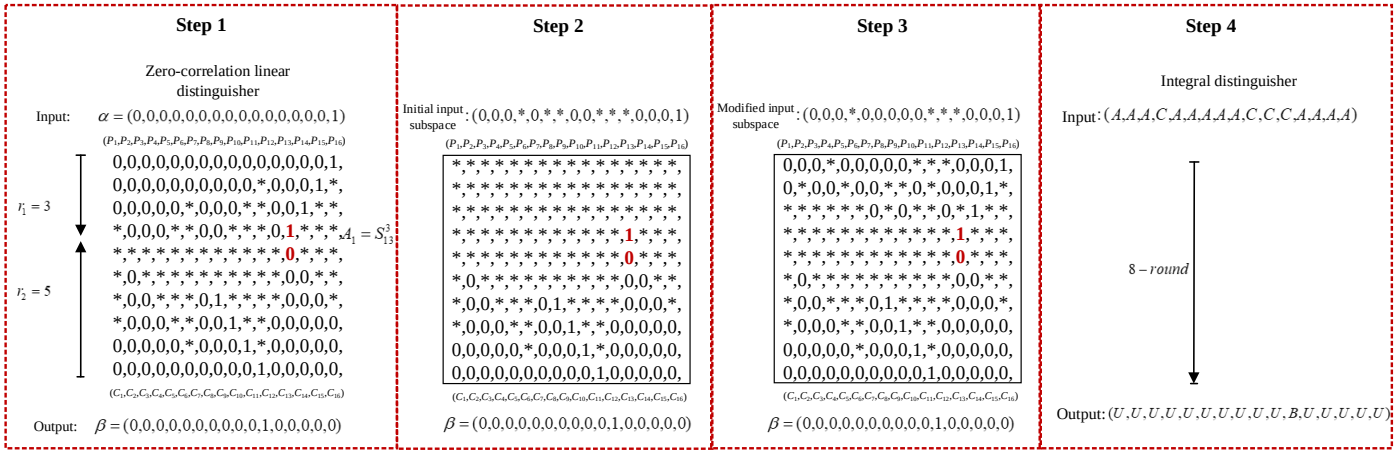

Figure 1. An illustration for a toy example.

After step 2, an initial input subspace of potential zero-correlation linear distinguishers are constructed. In this step, only the linear mask value of S_{13}^3 is concerned.

Based on step 3, some "bad positions" are eliminated from the initial input subspace, and a modified input subspace is derived. In this subspace, all the linear masks are eight-round zero-correlation linear distinguishers.

After step 4, this subspace is transformed to an integral distinguisher based on Theorem 1 or Corollary 1.

4. Applications

In this section, Algorithm 1 is applied to three ARX block ciphers—HIGHT, LEA and SPECK. In Section 4.1, the round functions for these block ciphers are briefly introduced. In Section 4.2, the constructed integral distinguishers for these ciphers are presented.

4.1. Brief Descriptions on HIGHT, LEA and SPECK

HIGHT is a lightweight block cipher proposed in CHES 2006 [1], which has been adopted as an ISO standard. It was designed by the Korea Information Security Agency. HIGHT has 32 rounds, with a 64 bit block and 128 bit key. The structure is a generalized Feistel network, and the round function of HIGHT is illustrated in Figure 2.

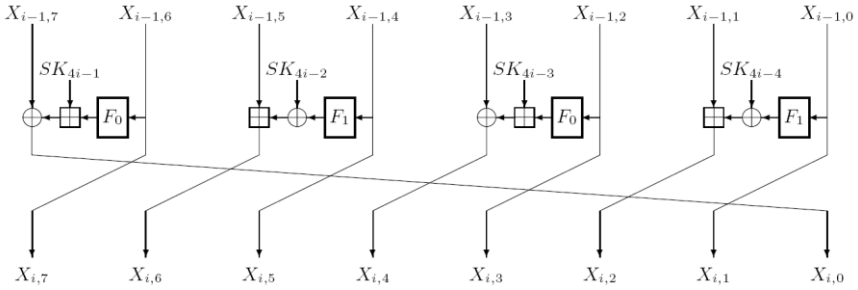

Figure 2. Round function of HIGHT.

LEA was proposed by Electronics and Telecommunications Research Institute of Korea in 2013 [32]. It provides a high-speed software encryption on general-purpose processors. LEA has a 128 bit block size and 128, 192, or 256 bit key sizes. The round function of LEA is depicted in Figure 3.

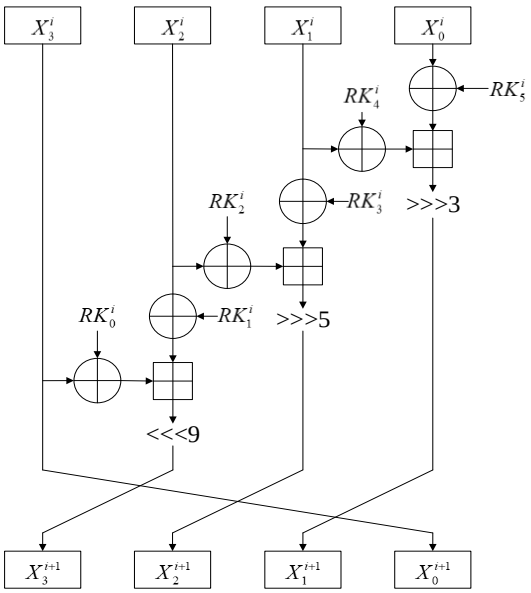

Figure 3. Round function of LEA.

SPECK is a lightweight block cipher proposed by the US National Security Agency in 2013 [2]. The SPECK family is an ARX-based Feistel-type network, which processes the input as two words. The round function of SPECK is depicted in Figure 4 below. In this paper, we use SPECK32 as an example; thus, the rotation constants α/β are defined as 7/2, and L^i and R^i are both 16-bit words.

4.2. Constructing Integral Distinguishers

In Ref. [29], Zhang et al. proposed some long zero-correlation linear distinguishers for HIGHT, LEA and SPECK. The main target of this subsection is to construct integral distinguishers with Algorithm 1.

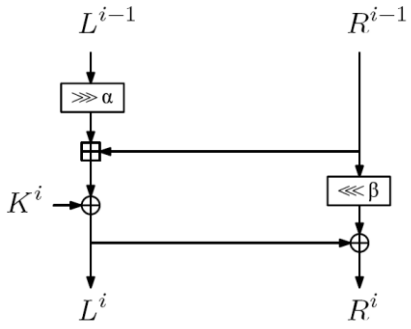

Figure 4. Round function of SPECK.

4.2.1. Integral Distinguishers for HIGHT

For HIGHT, a 17-round zero-correlation linear distinguisher is utilized, and the deduction for this distinguisher is illustrated in the Appendix A:

$$\alpha \to \beta: (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 10_7) \to (0,\ 0,\ 0,\ 0,\ 0, e_0,\ e_{2,4,5},\ 0)$$

If the plaintext and ciphertext for HIGHT are denoted as $(P_7, P_6, \cdots, P_0)$ and $(C_7, C_6, \cdots, C_0)$, respectively, $P_i(j)/C_i(j)$ represents the j-th bit for P_i/C_i. After the application of Algorithm 1, $\Omega_{in} = \{\Gamma P_0(0 \sim 6)\}$.

Thus $(A_8, A_8, A_8, A_8, A_8, A_8, A_8, AC_7) \overset{17-round}{\to} \oplus\{C_1(2) \oplus C_1(4) \oplus C_1(5) \oplus C_2(0)\}$ is a 17-round integral distinguisher for HIGHT, where A_i represents I consecutive active bits, and C_i represents i consecutive constant bits for the integral distinguisher.

In addition, there are three more 17-round integral distinguishers for HIGHT.

$$(A_8,\ A_8,\ A_8,\ A_8,\ A_8,\ AC_7,\ A_8,\ A_8) \overset{17-round}{\to} \oplus\{C_3(1) \oplus C_3(6) \oplus C_3(7) \oplus C_4(0)\}$$
$$(A_8,\ A_8,\ A_8,\ AC_7,\ A_8,\ A_8,\ A_8,\ A_8) \overset{17-round}{\to} \oplus\{C_5(2) \oplus C_5(4) \oplus C_5(5) \oplus C_6(0)\}$$
$$(A_8,\ AC_7,\ A_8,\ A_8,\ A_8,\ A_8,\ A_8,\ A_8) \overset{17-round}{\to} \oplus\{C_7(1) \oplus C_7(6) \oplus C_7(7) \oplus C_0(0)\}$$

4.2.2. Integral Distinguishers for LEA

For LEA, a nine-round zero-correlation linear distinguisher is utilized, and the deduction for this distinguisher is illustrated in the Appendix B:

$$\alpha \to \beta: (0,\ e_0,\ 0,\ 0) \to (e_9,\ 0,\ 0,\ e_0)$$

If the plaintext and ciphertext for LEA are denoted as (P_3, P_2, P_1, P_0) and (C_3, C_2, C_1, C_0), respectively, after the application of Algorithm 1, $\Omega_{in} = \{\Gamma P_3(0, 1)\}$.

Thus $(A_{30}C_2,\ A_{32},\ A_{32},\ A_{32}) \overset{9-round}{\to} \oplus\{C_3(9) \oplus C_0(0)\}$ is a nine-round integral distinguisher for LEA.

Using a similar approach, another three nine-round integral distinguishers for LEA can be constructed:

$$(A_{31}C_1,\ A_{32},\ A_{32},\ A_{32}) \overset{9-round}{\to} \oplus\{C_3(9) \oplus C_0(0)\}$$
$$(A_{32},\ A_{31}C_1,\ A_{32},\ A_{32}) \overset{9-round}{\to} \oplus\{C_3(9) \oplus C_0(0)\}$$
$$(A_{32},\ A_{30}C_2,\ A_{32},\ A_{32}) \overset{9-round}{\to} \oplus\{C_3(9) \oplus C_0(0)\}$$

4.2.3. Integral Distinguishers for SPECK32

For SPECK32, a six-round zero-correlation linear distinguisher is utilized, and the deduction for this distinguisher is illustrated in the Appendix C:

$$\alpha \to \beta: (0,\ e_7) \to (e_3,\ e_3)$$

If the plaintext and ciphertext for SPECK32 are denoted as (P_1, P_0) and (C_1, C_0), according to Algorithm 1, $\Omega_{in} = \{\Gamma P_0(5,6)\}$.

Thus, $(A_{16},\ A_9C_2A_5) \overset{6-round}{\rightarrow} \oplus\{C_1(3) \oplus C_0(3)\}$ is a six-round integral distinguisher for SPECK32.

Using a similar approach, another six-round integral distinguisher for SPECK32 can be derived.

$$(A_{16},\ A_9C_2A_5) \overset{6-round}{\rightarrow} \oplus\{C_1(2) \oplus C_0(2)\}$$

5. Validation on LEA

In this section, the flaw in Ref. [33] on nine-round integral distinguisher for LEA is presented, and the validation on our nine-round integral distinguishers are illustrated.

In Ref. [33], six nine-round zero-correlation linear distinguishers are used to construct a nine-round integral distinguisher on LEA. These nine-round zero-correlation linear distinguishers are as follows:

$$(0,\ e_0,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0)$$

$$(0,\ e_1,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0)$$

$$(0,\ e_2,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0)$$

$$(e_0,\ 0,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0)$$

$$(e_1,\ 0,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0)$$

$$(e_2,\ 0,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0)$$

It can be seen that these distinguishers are all single bit input linear masks. It is expected that these linear masks can constitute a big subspace that can be turned into an integral distinguisher. However, on the first perspective, the problem of subspace is not considered, which is an essential condition for the input linear masks in Theorem 1. On the second perspective, if we use the positions of these single bits to construct a large subspace (it seems that the integral distinguisher in Ref. [33] are derived in this way), many linear approximations in this large subspace are not zero-correlation, which also violates the condition in Theorem 1. This will make the nine-round integral distinguisher proposed in Ref. [33] invalid.

After the application of Algorithm 1 on LEA, there are only 14 possible nine-round zero-correlation linear distinguishers, and the structures are as follows:

$$((0,0,..,0,0,1),\ 0,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0) \tag{1}$$

$$((0,0,..,0,1,*),\ 0,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0) \tag{2}$$

$$((0,..,0,1,*,*),\ 0,\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0) \tag{3}$$

$$(0,\ (0,0,..,0,0,1),\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0) \tag{4}$$

$$(0,\ (0,0,..,0,1,*),\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0) \tag{5}$$

$$(0,\ (0,..,0,1,*,*),\ 0,\ 0) \overset{9-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0) \tag{6}$$

The subspace of zero-correlation linear distinguishers for (6) is validated in Table 2.

Table 2. A subspace of zero-correlation linear distinguishers for 9-round LEA.

Round	$(\Gamma_3^r,\Gamma_2^r,\Gamma_1^r,\Gamma_0^r)$
0	00000000000000000000000000000000000000000000000000000000000000001**00000000000000000000000000000000000000000000000000000000000000000000
1	000000000000000000001**00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001**
2	000000000000000000001**000000000001**00000000000000000000000000001**00000000000000000000000000000000000000000000000001**0000001**
3	**********1**********1**********0000000000000000001********1**********
4	**1**
4	1*****************************1*****************************0000000000001*****************0000000000001*****************
5	00000000000000000000001*******000000000000000001**************000000000000000001**************000000000000000001************
6	0000000000000000000000000000000000000000000000000001*********000000000000000000001*********000000000000000000000001********
7	00000000000000000000000000000000000000000000000000001*****000000000000000000000001*****000000000000000000000000000000
8	000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
9	000000000000000000000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001

For the above distinguishers, it can be seen that four subspaces can be used to construct nontrivial integral distinguishers (i.e., subspaces 2, 3, 5 and 6), the results for these four circumstances are illustrated as follows.

$$(2)\ (A_{31}C_1,\ A_{32},\ A_{32},\ A_{32}) \overset{9-round}{\rightarrow} \oplus\{C_3(9) \oplus C_0(0)\}$$

$$(3)\ (A_{30}C_2,\ A_{32},\ A_{32},\ A_{32}) \overset{9-round}{\rightarrow} \oplus\{C_3(9) \oplus C_0(0)\}$$

$$(5)\ (A_{32},\ A_{31}C_1,\ A_{32},\ A_{32}) \overset{9-round}{\rightarrow} \oplus\{C_3(9) \oplus C_0(0)\}$$

$$(6)\ (A_{32},\ A_{30}C_2,\ A_{32},\ A_{32}) \overset{9-round}{\rightarrow} \oplus\{C_3(9) \oplus C_0(0)\}$$

However, XORing two bits of the ciphertext may be not intuitive, and another approach will be utilized to validate this distinguisher.

For LEA, the nine-round zero-correlation linear distinguisher can be decomposed as 8 + 1 round:

$$\alpha \overset{9-round}{\rightarrow} \beta : (0,\ (0,..,0,1,*,*),\ 0,\ 0) \overset{8-round}{\rightarrow} (0,\ e_0,\ 0,\ 0) \overset{1-round}{\rightarrow} (e_9,\ 0,\ 0,\ e_0)$$

According to Theorem 1, the output formed after eight-round encryption is

$$(U_{32},\ U_{31}B_1,\ U_{32},\ U_{32})$$

That is, $\oplus X_2^8[0]$ is balanced. According to the round function of LEA, $X_2^8[0] = X_3^9[9] \oplus \Delta X_0^9[0] \oplus K_0^8[0] = C_3(9) \oplus C_0(0) \oplus K_0^8[0]$, $K_0^8[0]$ is a key-related fixed constant, and it can be eliminated if it is added with even times; thus, $\oplus X_2^8[0] = \oplus\{C_3(9) \oplus C_0(0)\}$, which means the XOR of two ciphertext bits after nine-round is also balanced. This is consistent with our previous theorized construction method.

6. Conclusions

This paper investigates the methodology to construct integral distinguishers for ARX ciphers. Based on the idea of constructing a subspace of long zero-correlation linear distinguishers and the relationship between the INTDs and ZCLDs for ARX ciphers, a method is proposed to solve this problem. This paper takes three typical ARX ciphers, HIGHT, LEA and SPECK, as examples to show the effectiveness of our method. Some longer and better integral distinguishers are discovered. More applications of this method and the possible extension on Sbox-based designs are left for future work. However, although some longer or more integral distinguishers are derived, some of them are not friendly to key recovery attacks. Exploring better key recovery attacks is for other future work.

Author Contributions: Conceptualization, X.L.; methodology and validation, K.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by the National Natural Science Foundation of China under grant no. 61802437, 61972248, 61902428, 62102448 and China Postdoctoral Science Foundation under grant no. 2020M681314.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the anonymous reviewers for their helpful comments.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Zero-correlation linear distinguisher on HIGHT

$$\alpha \to \beta : (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 10_7) \to (0,\ 0,\ 0,\ 0,\ 0, e_0,\ e_{2,4,5},\ 0)$$

Table A1. Deduction of zero-correlation linear distinguisher for 17-round HIGHT.

Round	Γ_7^r	Γ_6^r	Γ_5^r	Γ_4^r	Γ_3^r	Γ_2^r	Γ_1^r	Γ_0^r
0	00000000	00000000	00000000	00000000	00000000	00000000	00000000	10000000
1	00000000	00000000	00000000	00000000	00000000	00000000	10000000	00000000
2	00000000	00000000	00000000	00000000	00000000	1*******	********	00000000
3	00000000	00000000	00000000	00000000	1*******	********	********	00000000
4	00000000	00000000	00000000	1*******	********	********	********	00000000
5	00000000	00000000	1*******	********	********	********	********	00000000
6	00000000	1*******	********	********	********	********	********	00000000
7	1*******	********	********	********	********	********	********	00000000
8	********	********	********	********	********	********	********	1*******
8	********	********	********	********	********	********	00000001	0*******
9	********	********	********	********	00000000	00000001	0*******	********
10	********	********	00000000	00000000	00000001	0*******	********	********
11	00000000	00000000	00000000	00000001	1*******	********	********	********
12	00000000	00000000	00000001	1*******	********	********	00000000	00000000
13	00000000	00000001	1*******	********	00000000	00000000	00000000	00000000
14	00000001	11000010	00000000	00000000	00000000	00000000	00000000	00000000
15	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000001
16	00000000	00000000	00000000	00000000	00000000	00000000	00000001	00000000
17	00000000	00000000	00000000	00000000	00000000	00000001	00110100	00000000

Appendix B

Zero-correlation linear distinguisher on LEA

$$\alpha \to \beta : (0,\ e_0,\ 0,\ 0) \to (e_9,\ 0,\ 0,\ e_0)$$

Table A2. Deduction of zero-correlation linear distinguisher for 9-round LEA.

Round	Γ_3^r	Γ_2^r	Γ_1^r	Γ_0^r
0	00000000000000000000000000000000	00000000000000000000000000000001	00000000000000000000000000000000	00000000000000000000000000000000
1	00000000000000000000000010000000	00000000000000000000000000000000	00000000000000000000000000000000	00000000000000000000000000000001
2	00000000000000000000001000000000	00001000000000000000000000000000	00100000000000000000000000000000	00000000000000000000001000000001
3	**********001******	*****001**********	***00000000000000000000001******	001**********
4	**********	**********	***001**********	**********
4	1**********	1**********	00000000001**********	00000000000001**********
5	00000000000000000000001*******	00000000000000001**********	00000000000000001**********	00000000000000001**********
6	00000000000000000000000000000000	00000000000000000001*********	00000000000000000001*********	00000000000000000000001********
7	00000000000000000000000000000000	00000000000000000000000001*****	00000000000000000000000001*****	00000000000000000000000000000000
8	00000000000000000000000000000000	00000000000000000000000000000001	00000000000000000000000000000000	00000000000000000000000000000000
9	00000000000000000000001000000000	00000000000000000000000000000000	00000000000000000000000000000000	00000000000000000000000000000001

Appendix C

Zero-correlation linear distinguisher on SPECK32

$$\alpha \rightarrow \beta : (0, e_7) \rightarrow (e_3, e_3)$$

Table A3. Deduction of zero-correlation linear distinguisher for 6-round SPECK32.

Round	Γ_1^r	Γ_0^r
0	0000000000000000	0000000010000000
1	0000001000000000	0000001000000000
2	000010000001****	000010000001**00
3	1***************	1**************00
3	*********1******	0***************
4	00000001*0000000	100000000000001*
5	0000000000000000	0000000000000010
6	0000000000001000	0000000000001000

References

1. Hong, D.; Sung, J.; Hong, S.; Lim, J.; Lee, S.; Koo, B.S.; Lee, C.; Chang, D.; Lee, J.; Jeong, K.; et al. HIGHT: A new block cipher suitable for low-resource device. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Yokohama, Japan, 10–13 October 2006; pp. 46–59.
2. Beaulieu, R.; Shors, D.; Smith, J.; Treatman-Clark, S.; Weeks, B.; Wingers, L. The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 7–11 June 2015; pp. 1–6.
3. Aumasson, J.P.; Meier, W.; Phan, R.C.W.; Henzen, L. *The Hash Function BLAKE*; Springer: Berlin, Germany, 2014.
4. Ferguson, N.; Lucks, S.; Schneier, B.; Whiting, D.; Bellare, M.; Kohno, T.; Callas, J.; Walker, J. The Skein Hash Function Family. Submission to NIST (Round 3). 2010. Available online: https://www.schneier.com/wp-content/uploads/2016/02/skein.pdf (accessed on 10 January 2022).
5. Wheeler, D.J.; Needham, R.M. TEA, a tiny encryption algorithm. In Proceedings of the International Workshop on Fast Software Encryption, Cambridge, UK, 9–11 December 1993; pp. 363–366.
6. Needham, R.; Wheeler, D.J. *Extended Tiny Encryption Algorithm*; Technical Report; Computer Laboratory, University of Cambridge: Cambridge, UK, 1997.
7. Wheeler, D.; Needham, R. *XXTEA: Correction to XTEA*; Technical Report; Computer Laboratory, University of Cambridge: Cambridge, UK, 1998.
8. Bernstein, D.J. The Salsa20 family of stream ciphers. In *New Stream Cipher Designs*; Robshaw, M., Billet, O., Eds.; Springer: Berlin, Germany, 2008; Volume 4986, pp. 84–97.
9. Daemen, J.; Knudsen, L.; Rijmen, V. The block cipher Square. In Proceedings of the International Workshop on Fast Software Encryption, Haifa, Israel, 20–22 January 1997; pp. 149–165.
10. Knudsen, L.; Wagner, D. Integral cryptanalysis. In Proceedings of the International Workshop on Fast Software Encryption, Leuven, Belgium, 4–6 February 2002; pp. 112–127.
11. Kim, J.; Hong, S.; Sung, J.; Lee, S.; Lim, J.; Sung, S. Impossible differential cryptanalysis for block cipher structures. In Proceedings of the International Conference on Cryptology in India, New Delhi, India, 8–10 December 2003; pp. 82–96.
12. Zhang, W.; Su, B.; Wu, W.; Feng, D.; Wu, C. Extending higher-order integral: An efficient unified algorithm of constructing integral distinguishers for block ciphers. In Proceedings of the International Conference on Applied Cryptography and Network Security, Singapore, 26–29 June 2012; pp. 117–134.
13. Zhang, H.; Wu, W.; Wang, Y. Integral attack against bit-oriented block ciphers. In Proceedings of the Information Security and Cryptology, Seoul, Korea, 25–27 November 2015; pp. 102–118.
14. Todo, Y. Structural evaluation by generalized integral property. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015; pp. 287–314.
15. Todo, Y.; Morii, M. Bit-based division property and application to simon family. In Proceedings of the International Conference on Fast Software Encryption, Bochum, Germany, 20–23 March 2016; pp. 357–377.
16. Xiang, Z.; Zhang, W.; Bao, Z.; Lin, D. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ci-phers. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 4–8 December 2016; pp. 648–678.
17. Sun, L.; Wang, W.; Wang, M.Q. MILP-aided bit-based division property for primitives with non-bit-permutation linear layers. *IET Inf. Secur.* **2019**, *14*, 12–20. [CrossRef]
18. Wang, S.; Hu, B.; Guan, J.; Zhang, K.; Shi, T. MILP-aided method of searching division property using three subsets and applications. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, 8–12 December 2019; pp. 398–427.

19. Hao, Y.; Leander, G.; Meier, W.; Todo, Y.; Wang, Q. Modeling for three-subset division property without unknown subset and improved cube attacks. In Proceedings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 10–14 May 2020; pp. 466–495.
20. Ghosh, S.; Dunkelman, O. Automatic search for bit-based division property. In Proceedings of the International Conference on Cryptology and Information Security in Latin America, Bogotá, Colombia, 6–8 October 2021; pp. 254–274.
21. ElSheikh, M.; Youssef, A.M. On MILP-based automatic search for bit-based division property for ciphers with (large) linear layers. In Proceedings of the Australasian Conference on Information Security and Privacy, Perth, WA, Australia, 1–3 December 2021; pp. 111–131.
22. Bogdanov, A.; Leander, G.; Nyberg, K.; Wang, M. Integral and multidimensional linear distinguishers with correlation zero. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, 2–6 December 2012; pp. 244–261.
23. Sun, B.; Liu, Z.; Rijmen, V.; Li, R.; Cheng, L.; Wang, Q.; Alkhzaimi, H.; Li, C. Links among impossible differential, integral and zero correlation linear cryptanalysis. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015; pp. 95–115.
24. Wen, L.; Wang, M. Integral zero-correlation distinguisher for ARX block cipher, with application to SHACAL-2. In Proceedings of the Australasian Conference on Information Security and Privacy, Wollongong, NSW, Australia, 7–9 July 2014; pp. 454–461.
25. Sun, L.; Wang, W.; Wang, M. Automatic search of bit-based division property for ARX ciphers and word-based divi1sion property. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017; pp. 128–157.
26. Sun, L.; Wang, W.; Liu, R.; Wang, M. MILP-aided bit-based division property for ARX ciphers. *Sci. China Inf. Sci.* **2017**, *61*, 118102:1–118102:3. [CrossRef]
27. Eskandari, Z.; Kidmose, A.B.; Kölbl, S.; Tiessen, T. Finding integral distinguishers with ease. In Proceedings of the International Conference on Selected Areas in Cryptography, Calgary, AB, Canada, 15–17 August 2018; pp. 115–138.
28. Han, Y.; Li, Y.; Wang, M. Automatical method for searching integrals of ARX block cipher with division property using three subsets. In Proceedings of the International Conference on Information and Communications Security, Lille, France, 29–31 October 2018; pp. 647–663.
29. Zhang, K.; Guan, J.; Hu, B. Automatic search of impossible differentials and zero-correlation linear hulls for ARX ciphers. *China Commun.* **2018**, *15*, 54–66. [CrossRef]
30. Sasaki, Y.; Todo, Y. New impossible differential search tool from design and cryptanalysis aspects. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, 30 April–4 May 2017; pp. 185–215.
31. Zhang, P.; Sun, B.; Li, C. Saturation attack on the block cipher HIGHT. In Proceedings of the International Conference on Cryptology and Network Security, Kanazawa, Japan, 12–14 December 2009; pp. 76–86.
32. Hong, D.; Lee, J.K.; Kim, D.C.; Kwon, D.; Ryu, K.H.; Lee, D.G. LEA: A 128-bit block cipher for fast encryption on common processors. In Proceedings of the International Workshop on Information Security Applications, Jeju Island, Korea, 19–21 August 2013; pp. 3–27.
33. Li, H.; Ren, J.J.; Chen, S.Z. Integral attack on reduced-round LEA cipher. *Acta Electron. Sin.* **2020**, *48*, 17.