


Research Article

Zero-Correlation Linear Cryptanalysis on SPARX-64

Dawei Zhou,¹ Huaifeng Chen ,^{2,3} Rui Zong,⁴ and Ningning Song^{2,3}

¹Department of Information Security, Naval University of Engineering, Wuhan, China

²The 6th Research Institute of China Electronics Corporation, Beijing, China

³National Engineering Laboratory for Industrial Control System Information Security Technology, China

⁴Verification & Validation Technology co., Ltd, Shenzhen, China

Correspondence should be addressed to Huaifeng Chen; chenhf@ncse.com.cn

Received 19 September 2021; Accepted 29 November 2021; Published 27 December 2021

Academic Editor: Chao Wang

Copyright © 2021 Dawei Zhou et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

SPARX is a family of ARX-based block ciphers designed according to the long-trail strategy, which has 32-bit ARX-based SBoxes and has provable bounds against single-differential and single-linear cryptanalysis. Since its proposition, some third-party cryptanalysis methods have been presented. As far as we know, the best attacks against SPARX-64 covered 16 (out of 24) rounds. In this paper, we propose zero-correlation linear attacks on SPARX-64. At first, we construct some new zero-correlation linear distinguishers covering 14-round and 15-round SPARX-64. Then, 15,16,17 and 18-round versions can be attacked using multidimensional or multiple zero-correlation linear attack models, under DKP(distinct known plaintexts) settings. These are the best attacks against SPARX-64 up to now, regarding to the number of attacked rounds. Finally, we transform the zero-correlation distinguishers into integral ones using existing methods, which are also longer than the ones proposed by the designers.

1. Introduction

SPARX [1], introduced by Dinu et al. at ASIACRYPT'16, is the first ARX based family of block ciphers with the aim of providing provable security against single-trail differential and linear cryptanalysis. To achieve this target, the designers developed the long trail strategy which is different from the well-studied wide trail strategy [2] used in the design of AES. The long trail strategy advocates the use of large and comparatively expensive SBoxes in conjunction with cheaper and weaker linear layers. All the instances of SPARX, (SPARX-64/128, SPARX-128/128 and SPARX-128/128) use three or four rounds of SPECK [3] with subkeys as the big SBox, which can be specified using three simple operations: addition modulo 2^{16} (\boxplus), 16-bit rotations ($\ll\ll 2$ and $\gg\gg 7$) and 16-bit Xor (\boxplus).

There have been some cryptanalysis results on the family of SPARX. The designers gave the provable bounds on the probability of differential characteristic and the bias of linear trail. There is no differential or linear trail with significant probability for 5 (or more) steps. Also, they made integral

attacks with the help of Todo's division property [4]. For SPARX-64/128, the attack covers 15 rounds and recovers the key in time 2^{101} using 2^{37} chosen plaintexts. Moreover, the integral attacks cover 22-round SPARX-128/128 and 24-round SPARX-128/256. Then Abdelkhalek et al. [5] attacked 16-round SPARX64-128 using impossible differential attack, with the help of one 13-round distinguisher and the dependencies between the subkeys. Later, Tolba et al. [6] proposed multidimensional zero-correlation linear attacks on up to 25 rounds of SPARX-128/256 and 22 rounds of SPARX-128/128. Recently, Ankele and List [7] presented chosen-ciphertext differential attacks on 16-round SPARX-64/128. Previous attack results on SPARX-64/128 are compared in Table 1.

There is no zero-correlation cryptanalysis results on SPARX-64/128 from the literatures and we focus on this method in this paper. Zero-correlation [8] is one powerful tool in the cryptanalysis of block ciphers. Similar to that the impossible differential distinguisher uses a differential with probability zero, the zero-correlation distinguisher uses a linear hull with correlation zero. Then this technique

TABLE 1: Attacks on SPARX-64/128.

#rounds	Attack types	Data	Time	Ref.
15	Integral	2^{37} CP	$2^{101.0}$	[1]
15	Impossible differential	$2^{51.0}$ CP	$2^{94.1}$	[5]
16	Impossible differential	$2^{61.5}$ KP	$2^{94.0}$	[5]
16	Truncated differential	2^{32} CC	2^{93}	[7]
16	Rectangle	$2^{59.6}$ CC	2^{122}	[7]
16	Yoyo	2^{64} CP	2^{126}	[7]
15	Multidimensional zero-correlation	$2^{58.6}$ DKP	2^{106}	Sect. 4.1
16	Multidimensional zero-correlation	$2^{62.5}$ DKP	2^{101}	Sect. 4.2
17	Zero-correlation	$2^{63.6}$ DKP	2^{127}	Sect. 5.1
18	Zero-correlation	$2^{63.6}$ DKP	$2^{127.2}$	Sect. 5.2

* CP: Chosen Plaintext; KP: Known Plaintext; * CC: Chosen Ciphertext; DKP: Distinct Known Plaintext. * In KP settings, the samples are obtained randomly while in DKP settings there is a restriction that the plaintext-ciphertext samples are non-repeating.

develops a lot and some new models have been proposed, such as the multiple zero-correlation linear cryptanalysis [9], the multidimensional zero-correlation linear cryptanalysis [10] and some improved versions [11, 12]. In particular, Sun et al. [12] removed the approximation from the χ^2 -distribution to the normal distribution during the construction of multiple and multidimensional zero-correlation linear attack (MPZC and MDZC) models, which released the restriction on the number ‘ ℓ ’ of zero-correlation linear hulls, *i.e.*, ‘ ℓ ’ should be large enough. The new models were called χ^2 -MPZC and χ^2 -MDZC.

To improve the time complexity of linear attacks using *algorithm 2*, FFT technique was proposed in [13]. When the target bit for the linear distinguisher is a function of $x \oplus k$ where x, k are both n -bit values, the time can be improved from 2^{2^n} to $3 \cdot n \cdot 2^n$ simple calculations.

Our Contributions. We evaluate the security of SPARX-64/128 using the zero-correlation cryptanalysis in this paper:

- (1) We find some new zero-correlation distinguishers. By extending the existing simple zero-correlation distinguisher proposed in [6], we construct several multidimensional zero-correlation distinguishers covering 14-round SPARX-64. Moreover, with careful selection of the input mask, we can extend some distinguishers by one more round and get three 15-round zero-correlation distinguishers. These are the longest zero-correlation linear distinguishers of SPARX-64 as we know
- (2) Using the new zero-correlation distinguishers, we make zero-correlation linear attacks with the help of multiple/multidimensional zero-correlation linear cryptanalysis model in [12]. The multidimensional zero-correlation attack covers 15-round and 16-round using 14-round distinguishers. Then the zero-correlation attack with one single 15-round linear hull covers 17-round. What’s more, with the help of FFT technique, we also can attack 18-round

SPARX-64. These are the best attacks from the view of number of rounds attacked

- (3) Also, we transform the zero-correlation linear distinguishers into integral distinguishers. As a result, we can get some 14-round and 15-round integral distinguishers with balanced properties. The balanced property means that the numbers of each value in the output sets are equal for the integral distinguisher, while the zero-sum property means the Xor-sum is zero

Outline. First, we describe the target block cipher SPARX-64/128 and the zero-correlation linear attack models in Sect.2. In Sect.3, we show how to construct the 14-round and 15-round zero-correlation linear distinguishers for SPARX-64. Then we give the multidimensional zero-correlation and multiple zero-correlation linear cryptanalysis against SPARX in Sect.4 and 5. Sect.6 describes some new integral distinguishers and finally, Sect.7 concludes this paper.

2. Preliminaries

2.1. Notations. The following symbols and notations are used throughout this paper:

- (i) \boxplus : addition modulo 2^{16}
- (ii) \oplus : bit-wise Xor
- (iii) $\ll\ll$: 16-bit rotation to the left
- (iv) $\gg\gg$: 16-bit rotation to the right
- (v) \parallel : concatenation of two bit strings
- (vi) x_L : left half (16-bit) of the word x (32-bit).
- (vii) x_R : right half (16-bit) of the word x (32-bit).
- (viii) SPECKEY-3R: three rounds of SPECKEY

- (ix) K^{2i}, K^{2i+1} : the subkeys used in the left and, respectively, right SPECKEY-3R of the i -th step of SPARX-64. Each has three 32-bit words $K^{*,1}, K^{*,2}, K^{*,3}$, used in three rounds of SPECKEY-3R, respectively
- (x) $1_b^x(0_b^x, ?_b^x)$: x -bit of '1'('0', '?'). '?' is one undetermined bit
- (xi) $x[i]$: the i -th bit of bit string x . $x[0]$ is the least significant bit
- (xii) $x[j \sim i]$: the concatenation of $x[j], x[j-1], \dots, x[i]$, $j > i$

2.2. Brief Description of SPARX-64/128. SPARX-64/128 is the lightest instance of the SPARX family. It operates on two 32-bit words and uses a 128-bit key. There are 8 steps and 3 rounds per step. A high level view of SPARX-64/128 and the general structure of a step is shown in Figure 1. Both branches have non-linear operations SPECKEY-3R, which means three rounds of SPECKEY, involving three 32-bit subkeys. SPECKEY splits the state into two 16-bit branches and xor the left and right half key bits, *i.e.*, K_L^{ij} and K_R^{ij} , in each branch before the non-linear operations. The linear layer \mathcal{L} operates 32-bit value as follows,

$$\mathcal{L}(x) = x_L \oplus ((x_L \oplus x_R) \lll 8) \parallel x_R \oplus ((x_L \oplus x_R) \lll 8). \quad (1)$$

In the i -th step of SPARX-64, six 32-bit subkeys $K^{2i,1}, K^{2i,2}, K^{2i,3}, K^{2i+1,1}, K^{2i+1,2}, K^{2i+1,3}$ are involved. In particular, $K^{2i,1}, K^{2i,2}, K^{2i,3}$ are used in the left SPECKEY-3R and $K^{2i+1,1}, K^{2i+1,2}, K^{2i+1,3}$ are used in the right SPECKEY-3R.

The 128-bit permutation used in the key schedule is simple, which is shown in Algorithm 1. For more details, please refer to [1].

2.3. χ^2 - Multiple/Multidimensional Zero-Correlation Cryptanalysis. We start this section with the introduction of MPZC and MDZC models. Suppose that there are N plaintext-ciphertext samples and ℓ zero-correlation linear approximations for an n -bit block cipher. For the i -th approximation, the adversary counts the samples which make the linear approximation hold and gets the corresponding counter T_i . Under the model of MPZC cryptanalysis, the adversary evaluates the following statistic:

$$T^{MP} = N \sum_{i=1}^{\ell} \left(2 \frac{T_i}{N} - 1 \right)^2. \quad (2)$$

For MDZC model, the ℓ zero-correlation linear approximations form a linear space (considering the zero vector in) with dimension m and then $\ell = 2^m - 1$. For each plaintext-ciphertext sample, the adversary evaluates the m base linear approximation and obtains an m -bit value z . By iterating all N samples, the adversary would get a counter vector $V[z]$ with $z = 0, 1, \dots, 2^m - 1$. The statistic

used in MDZC is:

$$T^{MD} = \sum_{z=0}^{2^m-1} \frac{(V[z] - N2^{-m})^2}{N2^{-m}}. \quad (3)$$

To estimate the data complexity and success probability, researchers [14] considered two sampling models, *i.e.*, KP and DKP. In KP settings, the samples are obtained randomly while in DKP settings there is a restriction that the plaintext-ciphertext samples are non-repeating. In [14], Blondeau and Nyberg proved T^{MP} and T^{MD} followed the same distribution when the same sampling method are applied. They gave the estimation method of data complexity under these two sampling models for MPZC and MDZC. Later, Sun et al. proposed the χ^2 -MPZC and MDZC, in which they use the χ^2 -distributions to model the statistics [12], instead of the normal distributions.

Considering two types of errors:

- (i) *Type-1 error*: made by wrongfully discarding the cipher (false negative) and suppose the probability is α_0 . This is related to the success probability P_S and $P_S = 1 - \alpha_0$
- (ii) *Type-2 error*: made by wrongfully accepting a randomly chosen permutation as the cipher (false positive) and suppose the probability is α_1 . This is related to the time complexity T_S of the exhaustive search phase and $T_S = 2^k \cdot \alpha_1$ where k is the length of the main key

Then the χ^2 -MPZC and MDZC evaluate the data complexity as follows. where $\chi_{1-\alpha_0}^{(l)}$ and $\chi_{\alpha_1}^{(l)}$ are the respective quantiles of the χ^2 -distribution with l degrees of freedom evaluated on the points $1 - \alpha_0$ and α_1 . In the attacks, the threshold value to distinguish the cipher and randomly chosen permutation is calculated as $\tau = \chi_{1-\alpha_0}^{(l)}$.

Theorem 1. *in ([12])*

Suppose that the linear approximations involved satisfy the hypotheses in [14]. The number N^{KP} of KPs requires in a MPZC or MDZC linear attack is

$$N^{KP} \approx \frac{2^n \left(\chi_{1-\alpha_0}^{(l)} - \chi_{\alpha_1}^{(l)} \right)}{\chi_{\alpha_1}^{(l)}}, \quad (4)$$

and the number N^{DKP} of DKPs required in a MPZC or MDZC linear attack is

$$N^{DKP} \approx \frac{2^n \left(\chi_{1-\alpha_0}^{(l)} - \chi_{\alpha_1}^{(l)} \right)}{\chi_{1-\alpha_0}^{(l)}}, \quad (5)$$

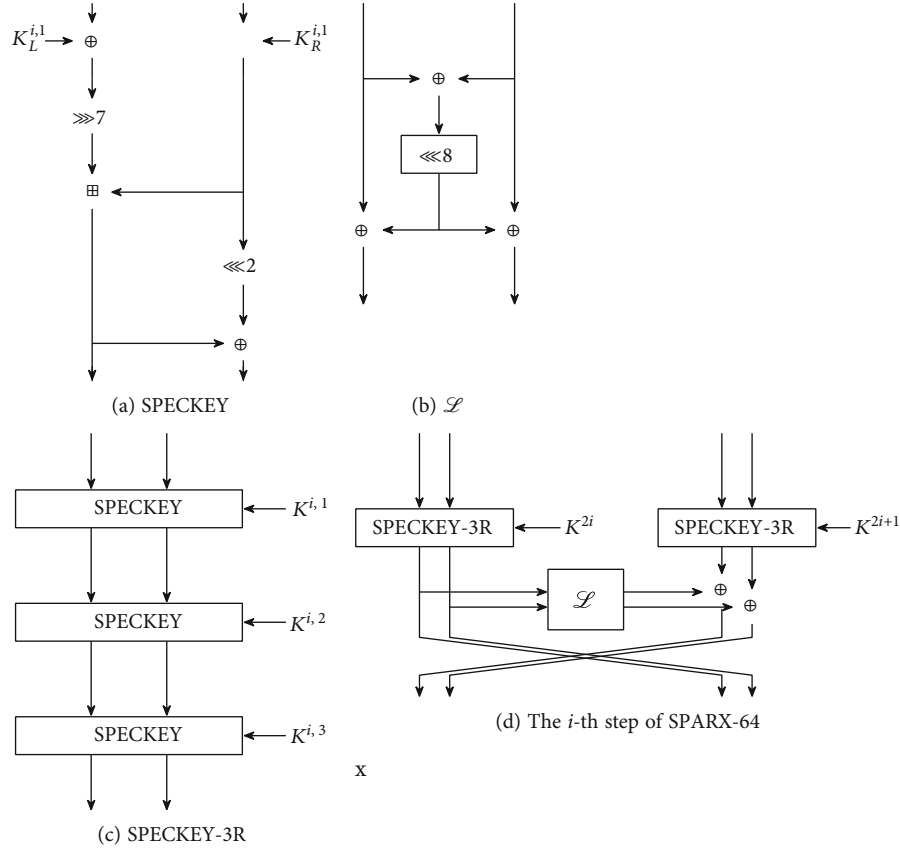
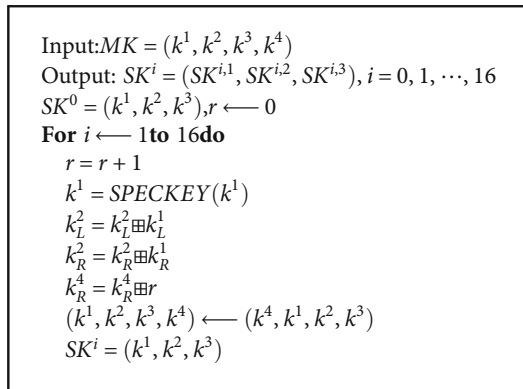


FIGURE 1: (a) The SPECKEY function; (b) The linear layer \mathcal{L} ; (c) SPECKEY-3R; (d) The i -th step of SPARX-64.



ALGORITHM 1: Key schedule of SPARX-64/128

3. Zero-Correlation Linear Hulls of SPARX-64

The 12-round zero-correlation linear hull of SPARX-64 proposed in [6] is shown in Figure 2, which is $(\alpha, 0) \rightarrow (0, \beta)$, $\alpha \neq 0, \beta \neq 0$. α_1, α_2 are linear masks derived from the input mask α , while β_1, β_2 are linear masks derived from the output mask β . The contradiction appears in the second linear permutation \mathcal{L} , where the corresponding input mask is zero while the output mask is non-zero value $\alpha_2 (= \beta_2)$. This distinguisher is like the 5-round zero-correlation linear hull of Feistel structure [8] with bijected F functions, which only takes advantage of the properties of the structures. In the fol-

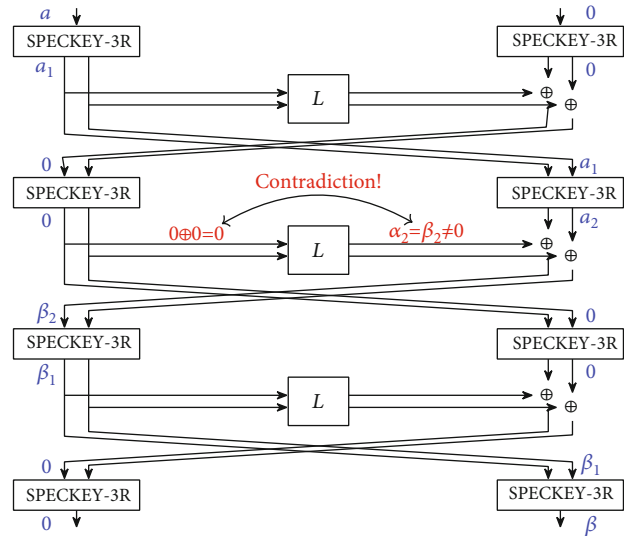


FIGURE 2: 12-Round Zero Correlation Linear Hull of SPARX64.

lowing subsections, we will study the detailed property of linear mask's propagation in SPECKEY and construct longer zero-correlation linear hulls.

Since there are only XOR (\oplus), Modulo Addition (\boxplus), Branch (\vdash) and Rotation (\ll or \gg), we review how the linear masks propagate through these operations. Let x, y, z be values and $\Gamma_x, \Gamma_y, \Gamma_z$ be the corresponding masks.

TABLE 2: Linear Masks' Relations among Some Simple Operations.

Operation	Values' relation	Masks' relation
\oplus	$z = x \oplus y$	$\Gamma_x = \Gamma_y = \Gamma_z$
\vdash	$y = x, z = x$	$\Gamma_x \oplus \Gamma_y \oplus \Gamma_z = 0.$
$\ll\ll$	$y = x \ll\ll i$	$\Gamma_y = \Gamma_x \ll\ll i$
$\gg\gg$	$y = x \gg\gg i$	$\Gamma_y = \Gamma_x \gg\gg i$
\boxplus	$z = x \boxplus y$	$MSB^1(\Gamma_x) = MSB^1(\Gamma_y) = MSB^1(\Gamma_z)$

Suppose the position of the first bit '1' from the MSB is $MSB^1(x)$ for x . Then the masks' relations are shown in Table 2.

Only the Modulo Addition (\boxplus) is non-linear and the corresponding correlation may be not one. However, when $\Gamma_x = \Gamma_y = \Gamma_z = 0x0000$ or $\Gamma_x = \Gamma_y = \Gamma_z = 0x0001$, the correlation at \boxplus is equal to 1.

3.1. Expand the Linear Hull with Input Mask $(\alpha, 0)$ Backward with Correlation One. In fact, by limiting the values of α and β , we can expand the number of rounds of zero-correlation linear hull. The main idea is to make the input mask (or output mask) go back (or forward) one more round with correlation one. The only non-linear operation in one SPECK round is \boxplus , so we hope the corresponding input mask or output mask of \boxplus is $0x0000$ or $0x0001$, which leads to linear approximations with correlation one.

For the case of input mask α , we expect that Γ_1, Γ_2 be $0x0001$ or $0x0000$, where Γ_1, Γ_2 are the output masks of the \boxplus in Figure 3. It's easy to know that $\Gamma_2 = \alpha_L \oplus \alpha_R$ and $\Gamma_1 = (L^T \alpha)_L \oplus (L^T \alpha)_R$ where L^T is the transform of the linear layer. So we can get the following four equations:

$$(1) \begin{cases} \alpha_L \oplus \alpha_R = 0x0000 \\ (L^T \alpha)_L \oplus (L^T \alpha)_R = 0x0000 \end{cases} \quad (2) \begin{cases} \alpha_L \oplus \alpha_R = 0x0000 \\ (L^T \alpha)_L \oplus (L^T \alpha)_R = 0x0001 \end{cases}$$

$$(3) \begin{cases} \alpha_L \oplus \alpha_R = 0x0001 \\ (L^T \alpha)_L \oplus (L^T \alpha)_R = 0x0000 \end{cases} \quad (4) \begin{cases} \alpha_L \oplus \alpha_R = 0x0001 \\ (L^T \alpha)_L \oplus (L^T \alpha)_R = 0x0001 \end{cases} \quad (6)$$

According to $L^T \alpha = ((L^T \alpha)_L, (L^T \alpha)_R) = (\alpha_L \oplus (\alpha_L \oplus \alpha_R)_{\gg\gg 8}, \alpha_R \oplus (\alpha_L \oplus \alpha_R)_{\gg\gg 8})$, we know that only the first and forth equations have possible solutions.

(i) Equation Equation (4). holds when $\alpha_L = \alpha_R$

(ii) Equation Equation (7) holds when $\alpha_L = \alpha_R \oplus 0x0001$

We set the condition $\alpha_L = \alpha_R$ (See the left part of Figure 3) and then we can derive that the linear mask becomes

$$(\Gamma_1^{in1}, \Gamma_2^{in1}, \Gamma_3^{in1}, \Gamma_4^{in1}) = (0, (\alpha_R)_{\gg\gg 2}, 0, (\alpha_R)_{\gg\gg 2}) \quad (7)$$

after one decrypted round. In a further step, there is $\Gamma_3 = (\alpha_R \gg\gg 2) = \Gamma_4$. To expand one more round with correlation one, we hope the corresponding masks Γ_3, Γ_4 also be $0x0000$ or $0x0001$. Then we obtain the only non-zero solution

$\alpha_L = \alpha_R = 0x0004$. At last, we get the linear mask

$$(\Gamma_1^{in0}, \Gamma_2^{in0}, \Gamma_3^{in0}, \Gamma_4^{in0}) = (0x0080, 0x4001, 0x0080, 0x4001). \quad (8)$$

after two decrypted rounds.

Similarly, when the condition is $\alpha_L = \alpha_R \oplus 0x0001$ (See right part of Figure 3), we can derive that

$$(\Gamma_1^{in1}, \Gamma_2^{in1}, \Gamma_3^{in1}, \Gamma_4^{in1}) = (0x0080, (\alpha_R)_{\gg\gg 2} \oplus 0x0041, 0, (\alpha_R)_{\gg\gg 2} \oplus 0x0001) \quad (9)$$

Then there is $\Gamma_3 = (\alpha_R \gg\gg 2) \oplus 0x00c1, \Gamma_4 = (\alpha_R \gg\gg 2) \oplus 0x0081$. In this situation, there is no value of α satisfying $\Gamma_3, \Gamma_4 \in \{0x0000, 0x0001\}$ at the same time. This means that when $\alpha_L = \alpha_R \oplus 0x0001$, we can only expand the linear hull backward one more round and can not expand the linear hull two more rounds backward with correlation one.

3.2. Expand the Linear Hull with Output Mask $(0, \beta)$ Forward with Correlation One. For the output linear mask $(0, \beta)$, we follow the similar method. See Figure 4. At first, we hope that the linear masks Γ_5, Γ_6 taking value $0x0000$ or $0x0001$. So we can list the following equations.

$$(1) \begin{cases} \beta_L \gg\gg 7 = 0x0000 \\ (L^T \beta)_L \gg\gg 7 = 0x0000 \end{cases} \quad (2) \begin{cases} \beta_L \gg\gg 7 = 0x0000 \\ (L^T \beta)_L \gg\gg 7 = 0x0001 \end{cases}$$

$$(3) \begin{cases} \beta_L \gg\gg 7 = 0x0001 \\ (L^T \beta)_L \gg\gg 7 = 0x0000 \end{cases} \quad (4) \begin{cases} \beta_L \gg\gg 7 = 0x0001 \\ (L^T \beta)_L \gg\gg 7 = 0x0001 \end{cases} \quad (10)$$

According to $L^T \beta = ((L^T \beta)_L, (L^T \beta)_R) = (\beta_L \oplus (\beta_L \oplus \beta_R)_{\gg\gg 8}, \beta_R \oplus (\beta_L \oplus \beta_R)_{\gg\gg 8})$, we know that only the solutions are as follows.

(i) Equation Equation (4). holds when $\beta_L = \beta_R = 0x0000$

(ii) Equation Equation (5) holds when $\beta_L = 0x0000, \beta_R = 0x8000$

(iii) Equation Equation (7) holds when $\beta_L = 0x0080, \beta_R = 0x8080$

(iv) Equation Equation (8) holds when $\beta_L = 0x0080, \beta_R = 0x0080$

Figure 4 gives the detailed propagation of output linear mask $(0, \beta)$ when $\beta_L = 0x0000, \beta_R = 0x8000$ or $\beta_L = 0x0080, \beta_R = 0x8080$. The output mask after one more round is

$$(\Gamma_1^{out0}, \Gamma_2^{out0}, \Gamma_3^{out0}, \Gamma_4^{out0}) = (0x0002, 0x0002, 0x0207, 0x0206), (\Gamma_1^{out0}, \Gamma_2^{out0}, \Gamma_3^{out0}, \Gamma_4^{out0}) = (0x0207, 0x0206, 0x0002, 0x0002), \quad (11)$$

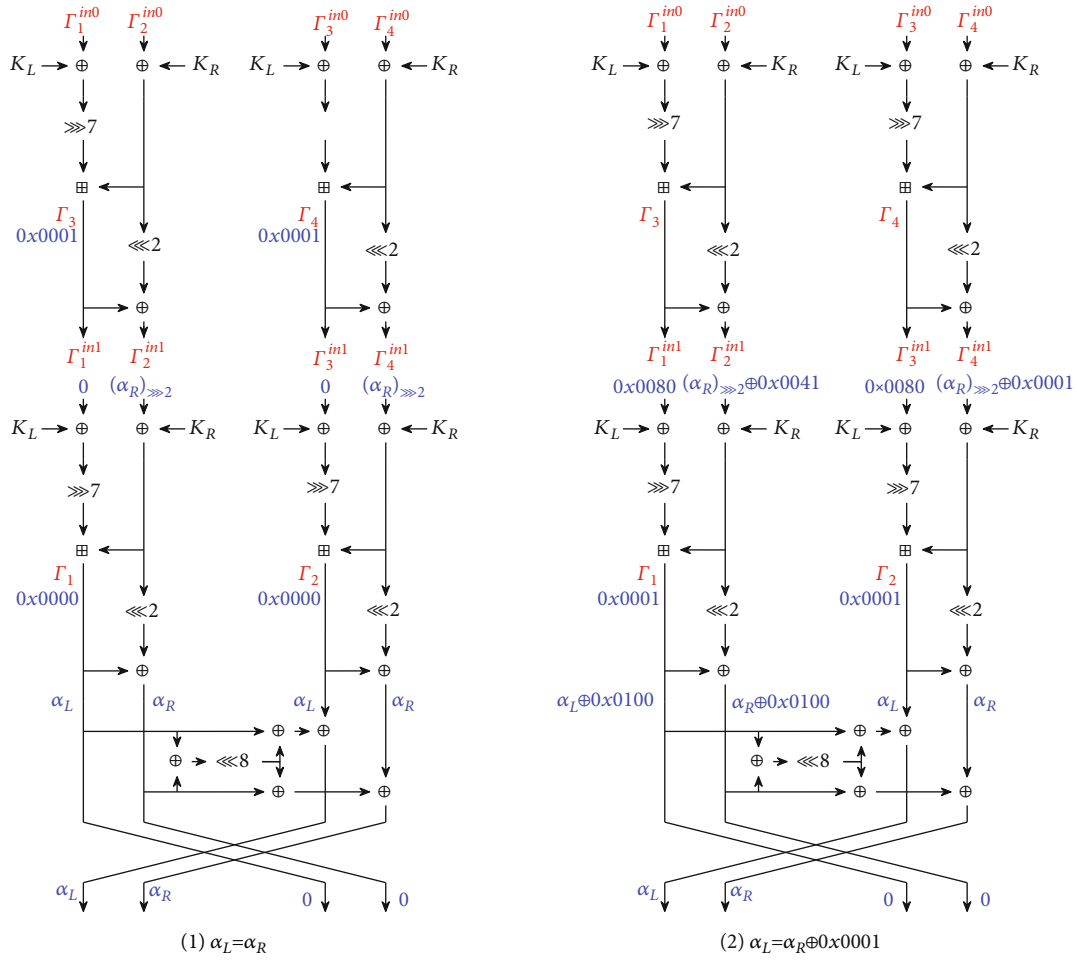


FIGURE 3: Expand the input mask $(\alpha, 0)$ by two more rounds. Red signals represent the variable names and the blue are the corresponding values.

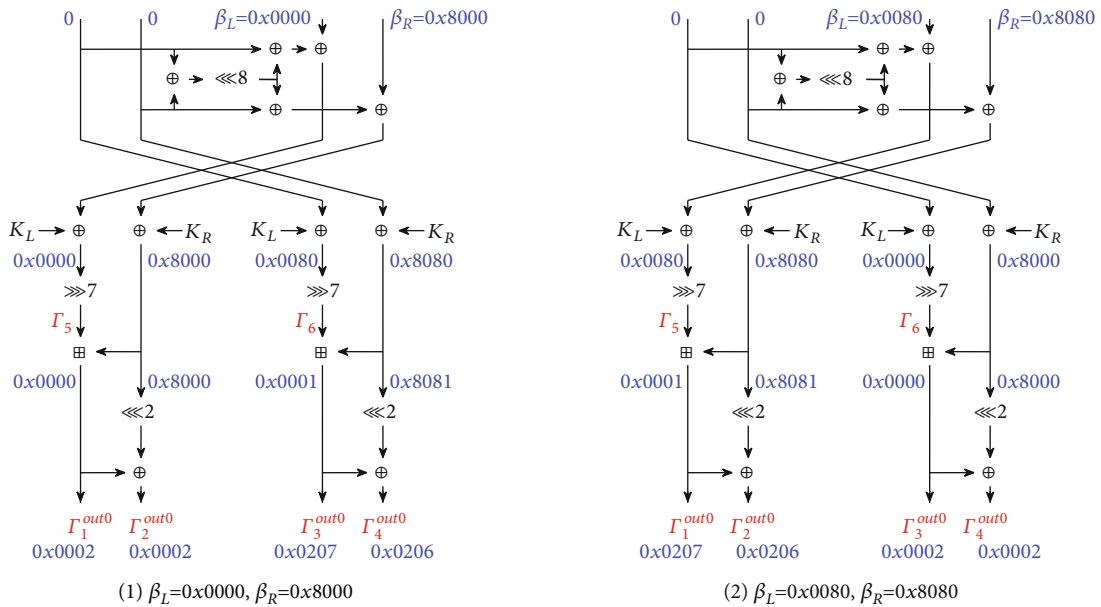


FIGURE 4: Expand the linear hull with output mask $(0, \beta)$ by one more round. Red signals represent the variable names and the blue are the corresponding values.

TABLE 3: Zero Correlation Linear Hulls of SPARX.

#R	Input mask(s)	Rounds covered	Output mask(s)
12	$(\alpha_L, \alpha_R, 0, 0)$	$\left(\underbrace{\text{SPECKEY} - 3\text{R}}_{4\text{steps}} \right)$	$(0, 0, \beta_L, \beta_R)$
14	$(0, \gamma, 0, \gamma),$ $(0, \gamma, 0, \gamma) \oplus$ $(0x0080, 0x0040, 0x0000, 0x0000)$	$\left(\text{SPECKEY} - 1\text{R}, \underbrace{\text{SPECKEY} - 3\text{R}}_{4\text{steps}}, \text{SPECKEY} - 1\text{R} \right)$	$(0x0207, 0x0206, 0x0002, 0x0002),$ $(0x0002, 0x0002, 0x0207, 0x0206),$ $(0x0205, 0x0204, 0x0205, 0x0204)$
15	$(0x0080, 0x4001, 0x0080, 0x4001)$	$\left(\text{SPECKEY} - 2\text{R}, \underbrace{\text{SPECKEY} - 3\text{R}}_{4\text{steps}}, \text{SPECKEY} - 1\text{R} \right)$	$(0x0207, 0x0206, 0x0002, 0x0002),$ $(0x0002, 0x0002, 0x0207, 0x0206),$ $(0x0205, 0x0204, 0x0205, 0x0204)$

γ : any 16-bit non-zero linear mask.

respectively. Otherwise, when $\beta_L = 0x0080, \beta_R = 0x0080$, there is

$$(\Gamma_1^{\text{out}0}, \Gamma_2^{\text{out}0}, \Gamma_3^{\text{out}0}, \Gamma_4^{\text{out}0}) = (0x0205, 0x0204, 0x0205, 0x0204). \quad (12)$$

We list the zero-correlation linear hulls in Table 3. #R denotes the number of rounds of the distinguishers.

4. Multidimensional Zero-Correlation Cryptanalysis of SPARX-64 Using 14-round Distinguishers

In this section, we give 15-round and 16-round multidimensional attacks with 14-round zero-correlation distinguishers in DKP sampling setting.

4.1. 15-Round Multidimensional Zero-Correlation Attack with One 14-round Distinguisher. Wu use one 14-round multidimensional zero-correlation distinguisher

$$(0, \gamma, 0, \gamma) \longrightarrow (0x0207, 0x0206, 0x0002, 0x0002) \quad (13)$$

to mount the attack. By adding one round at the top, the attack would cover 15 rounds. The symbols X_i, Y_i denote the corresponding states derived from the plaintexts or ciphertexts (See Figure 5). For enough plaintext-ciphertext samples, we need to guess the corresponding subkeys and get the numbers of all possible values of

$$[X_{1,1} \oplus X_{1,3}, (0x0207, 0x0206, 0x0002, 0x0002) \cdot Y_{1,1}]. \quad (14)$$

Since the MSB of $X_{1,1}$, i.e., $X_{1,1}[15]$, is linear with $K_L^{2i,2}[15]$ and $K_R^{2i,2}[15]$, in the attack there is no need guessing these two key bits. For simplicity, we can set them as 0. Similarly, we can also set $K_L^{2i+1,2}[15]$ and $K_R^{2i+1,2}[15]$ as constant values. So in the round before the distinguisher, the keys need to be guessed are $k_1 = (K_L^{2i,2}[14 \sim 0], K_R^{2i,2}[14 \sim 0])$ and $k_2 = (K_L^{2i+1,2}[14 \sim 0], K_R^{2i+1,2}[14 \sim 0])$. Since Y_1 is linear with

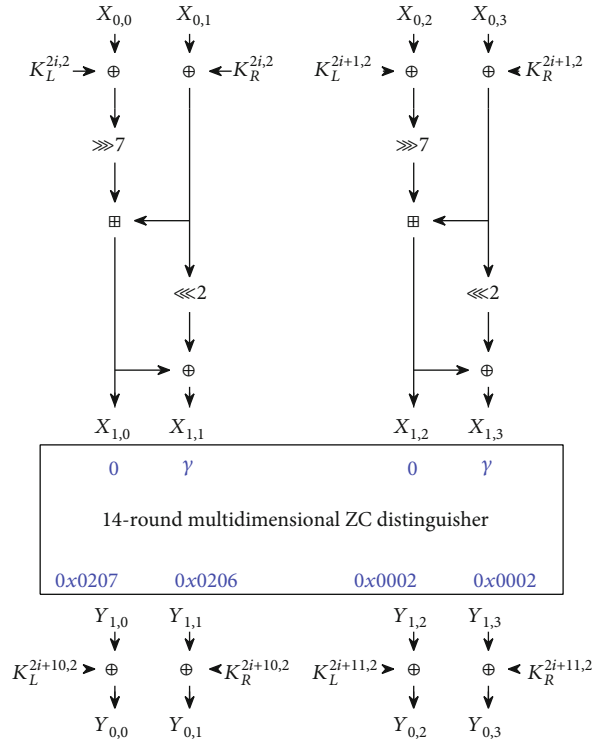


FIGURE 5: 15-Round Multidimensional Zero Correlation Linear Cryptanalysis on SPARX64.

$K_L^{2i+10,2}$ and $K_R^{2i+11,2}$, no key bits need to be guessed in the backward rounds.

Suppose the number of samples in the attack is N , the attack procedure is as follows.

- (i) Step 1. For N values of $[X_0, Y_0]$, suppose $K_L^{2i+10,2}, K_R^{2i+11,2} = 0$, then $Y_0 = Y_1$. We can compute

$$t_{\text{out}} = (0x0207, 0x0206, 0x0002, 0x0002) \cdot Y_0. \quad (15)$$

We get N values of $[X_0, t_{\text{out}}]$.

- (ii) Step 2. Guess 30 valid bits of k_1 , encrypt $X_{0,0}, X_{0,1}$ by one round and we can get $X_{1,1}$. Store the numbers of $[X_{1,1}, X_{0,2}, X_{0,3}, t_{out}]$.
- (iii) Step 3. Guess 30 valid bits of k_2 , encrypt $X_{0,2}, X_{0,3}$ by one round and we can get $X_{1,3}$. Store the numbers of $[X_{1,1} \oplus X_{1,3}, t_{out}]$.
- (iv) Step 4. For each guessed key, compute the statistic value used in the multidimensional zero-correlation attack, *i.e.*,

$$T = \sum_{X_{1,1} \oplus X_{1,3}, t_{out}} \frac{(V[X_{1,1} \oplus X_{1,3}, t_{out}] - N \cdot 2^{-m})^2}{N \cdot 2^{-m}}, \quad (16)$$

where $m = 17$. When T is smaller than the threshold value τ , the key is supposed to be a right key candidate and can then be checked using two plaintext-ciphertext pairs.

By setting $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-23}$, we can compute that the data complexity $N \approx 2^{58.616}$ and threshold $\tau = 131593$. The first three steps need

$$N \cdot \frac{1}{15} + (N \cdot 2^{30} + 2^{49} \cdot 2^{30+30}) \cdot \frac{1}{15} \cdot \frac{1}{2} \approx 2^{105} \quad (17)$$

encryptions. The last step needs $2^{128} \cdot \alpha_1 = 2^{105}$ times encryption. So the total time complexity is about 2^{106} encryptions.

4.2. 16-Round Multidimensional Zero-Correlation Attack with One 14-round Distinguisher. We can append one more round at the bottom to attack 16 rounds (See Figure 6). To control the time complexity, we use part of the above distinguisher. In detail, we only consider the input mask with form $\gamma = (0^{16-t} *^t)$, which means the distinguisher has dimension $t + 1$. So $k_1 = (K_L^{2i,2}[t-2 \sim 0], K_R^{2i,2}[t-2 \sim 0], K_L^{2i+1,2}[t-2 \sim 0], K_R^{2i+1,2}[t-2 \sim 0])$ need to be guessed.

For the output mask $(0x0207, 0x0206, 0x0002, 0x0002)$, we expand it by one round. The mask pattern at Y_0 would become $(0^2 1^? 1^3, 0^2 1^? 1^1 0^2, 0^3 1^? 1^2, 0^3 1^? 1^0 0^2)_b$. Only the non-linear key bits need to be guessed for the last round, which means we only consider $k_2 = (K_L^{2i+10,3}[12 \sim 0], K_R^{2i+10,3}[12 \sim 2])$, $k_3 = (K_L^{2i+11,3}[11 \sim 0], K_R^{2i+11,3}[11 \sim 2])$.

The attack procedure is as follows.

- (1) For N values of $[X_0, Y_0]$, compress Y_0 by one round and get $Y_{st1} = (Y_{0,0}[13 \sim 0], Y_{0,1}[13 \sim 2])$ and $Y_{st2} = (Y_{0,2}[12 \sim 0], Y_{0,3}[12 \sim 2])$.
- (2) Guess $4t - 4$ bits of k_1 , encrypt X_0 by one round and get $X_{1,1} \oplus X_{1,3}$. Store the numbers of $[X_{1,1} \oplus X_{1,3}, Y_{st1}, Y_{st2}]$.
- (3) Guess 24 valid bits of k_2 , decrypt Y_{st1} by one round and we can get $\beta_1 = (0x0207, 0x0206) \cdot (Y_{2,0}, Y_{2,1})$. Store the numbers of $[X_{1,1} \oplus X_{1,3}, \beta_1, Y_{st2}]$.

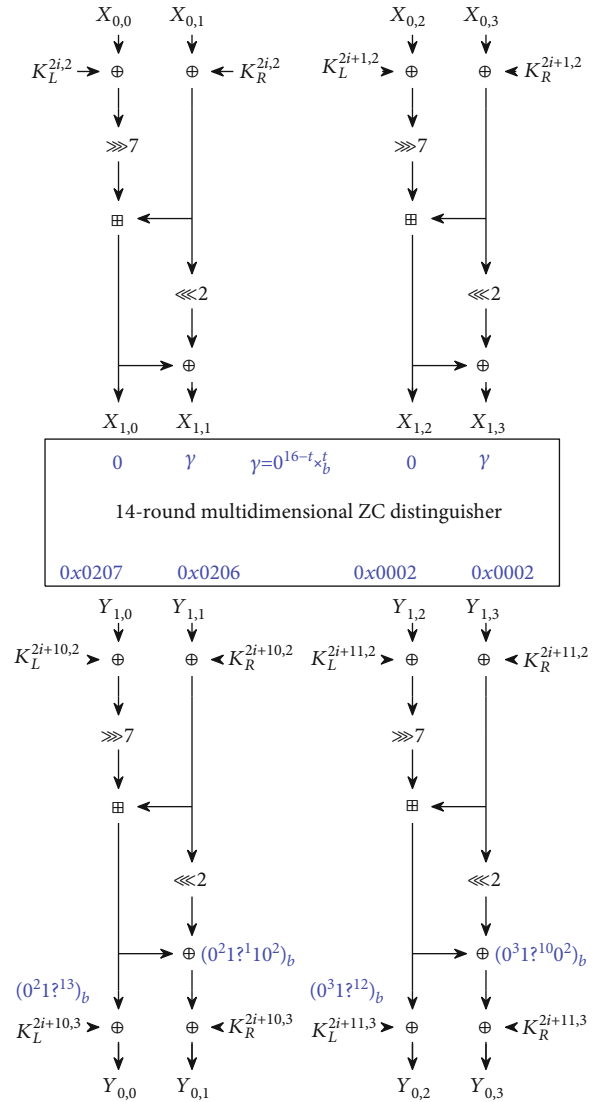


FIGURE 6: 16-Round Multidimensional Zero Correlation Linear Cryptanalysis on SPARX64.

- (4) Guess 22 valid bits of k_3 , decrypt Y_{st2} by one round and we can get $\beta_{out} = \beta_1 \oplus (0x0002, 0x0002) \cdot (Y_{2,2}, Y_{2,3})$. Store the numbers of $[X_{1,1} \oplus X_{1,3}, \beta_{out}]$.
- (5) For each guessed key, compute the statistic value used in the multidimensional zero-correlation attack, *i.e.*,

$$T = \sum_{X_{1,1} \oplus X_{1,3}, \beta_{out}} \frac{(V[X_{1,1} \oplus X_{1,3}, \beta_{out}] - N \cdot 2^{-m})^2}{N \cdot 2^{-m}}, \quad (18)$$

where $m = t + 1$. When T is smaller than the threshold value τ , the key is supposed to be a right key candidate and can then be checked using two plaintext-ciphertext pairs.

By setting $t = 8$, $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-28}$, we can compute that the data complexity $N \approx 2^{62.531}$ and threshold $\tau = 543$.

The first four steps need

$$N \cdot \frac{1}{16} + N \cdot 2^{4t-4} \cdot \frac{1}{16} + 2^{4t-4} \cdot (2^{54} \cdot 2^{24} + 2^{31} \cdot 2^{24+22}) \cdot \frac{1}{16} \cdot \frac{1}{2} \approx 2^{100} \quad (19)$$

encryptions. The last step needs $2^{128} \cdot \alpha_1 = 2^{100}$ times encryption. So the total time complexity is about 2^{101} encryptions.

5. Zero-Correlation Cryptanalysis of SPARX-64 Using 15-round Distinguisher

In this section, we give 17-round and 18-round attacks with 15-round zero-correlation distinguisher in DKP sampling setting. Notice that there is only one single zero-correlation linear hull. However, we also can use the multiple zero-correlation linear attack model to estimate the data complexity, as shown in [12].

5.1. 17-Round Zero-Correlation Attack with One 15-round Distinguisher. We use the 15-round zero-correlation distinguisher

$$(0x0080, 0x4001, 0x0080, 0x4001) \longrightarrow (0x0207, 0x0206, 0x0002, 0x0002) \quad (20)$$

to attack 17-round SPARX64/128.

We add one round at the top and one round at the bottom to make the attack which is similar to the 16-round attack, except that the distinguisher here is 15-round (See Figure 7). The key bits involved in this attack are $k_1 = (K_L^{2i,1}[15 \sim 7, 4 \sim 0], K_R^{2i,1}[13 \sim 0], K_L^{2i+1,1}[15 \sim 7, 4 \sim 0], K_R^{2i+1,1}[13 \sim 0])$ and $k_2 = (K_L^{2i+10,3}[12 \sim 0], K_R^{2i+10,3}[12 \sim 2]), k_3 = (K_L^{2i+11,3}[11 \sim 0], K_R^{2i+11,3}[11 \sim 2])$.

The attack procedure is as follows.

- (1) For N values of $[X_0, Y_0]$, compress Y_0 by one round and get $Y_{st1} = (Y_{0,0}[13 \sim 0], Y_{0,1}[13 \sim 2])$ and $Y_{st2} = (Y_{0,2}[12 \sim 0], Y_{0,3}[12 \sim 2])$.
- (2) Guess 56 bits of k_1 , encrypt X_0 by one round and get $\beta_0 = (0x0080, 0x4001, 0x0080, 0x4001) \cdot X_1$. Calculate the numbers of $[Y_{st1}, Y_{st2}]$ according to the sign of β_0 (+1 if $\beta_0 = 0$, -1 if $\beta_0 = 1$).
- (3) Guess 24 valid bits of k_2 , decrypt Y_{st1} by one round and we can get $\beta_1 = (0x0207, 0x0206) \cdot (Y_{2,0}, Y_{2,1})$. Calculate the numbers of $[Y_{st2}]$ according to the sign of β_1 .
- (4) Guess 22 valid bits of k_3 , decrypt Y'_{st2} by one round and we can get $\beta_2 = (0x0002, 0x0002) \cdot (Y_{2,2}, Y_{2,3})$. Calculate the final counter C according to the sign of β_2 .
- (5) For each guessed key, compute the statistic value used in the multiple zero-correlation attack, *i.e.*,

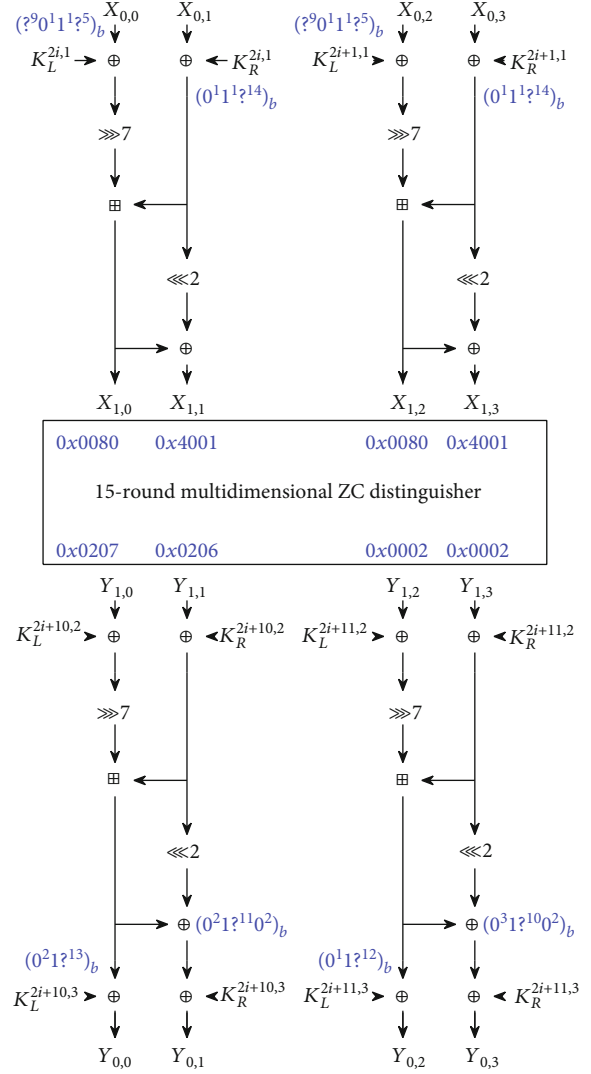


FIGURE 7: 17-Round Multidimensional Zero Correlation Linear Cryptanalysis on SPARX64.

$$T = N \left(\frac{C}{N} \right)^2. \quad (21)$$

When T is smaller than the threshold value τ , the key is supposed to be a right key candidate and can then be checked using two plaintext-ciphertext pairs.

By setting $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-1}$, we can compute that the data complexity $N \approx 2^{63.634}$ and threshold $\tau = 2$. The first four steps need

$$N \cdot \frac{1}{17} + N \cdot 2^{56} \cdot \frac{1}{17} + 2^{56} \cdot (2^{46} \cdot 2^{24} + 2^{22} \cdot 2^{24+22}) \cdot \frac{1}{17} \cdot \frac{1}{2} \approx 2^{121.15} \quad (22)$$

encryptions. The last step needs $2^{128} \cdot \alpha_1 = 2^{127}$ times encryption. So the total time complexity is $T \approx 2^{127}$ encryptions.

TABLE 4: Integral Distinguishers of SPARX.

#R	Input sets($(x_0, x_1, x_2, x_3) \in \mathcal{S}$)	Rounds covered(f)	Active bit(s)($(y_0, y_1, y_2, y_3) \in f(\mathcal{S})$)
12	(C_0, C_1, A_0, A_1)	$\left(\underbrace{\text{SPECKEY} - 3\text{R}}_{4\text{steps}} \right)$	$(*, *, A_3, A_4)$
14	$(A_0, A_1, A_2, A_1 \oplus C)$	$\left(\text{SPECKEY} - 1\text{R}, \underbrace{\text{SPECKEY} - 3\text{R}}_{4\text{steps}}, \text{SPECKEY} - 1\text{R} \right)$	$(0x0207 \cdot y_0) \oplus (0x0206 \cdot y_1) \oplus (0x0002 \cdot y_2) \oplus (0x0002 \cdot y_3)$
15	$(0x0080 \cdot x_0) \oplus (0x4001 \cdot x_1) \oplus (0x0080 \cdot x_2) \oplus (0x4001 \cdot x_3) = '0'$ (or = '1')	$\left(\text{SPECKEY} - 2\text{R}, \underbrace{\text{SPECKEY} - 3\text{R}}_{4\text{steps}}, \text{SPECKEY} - 1\text{R} \right)$	$(0x0207 \cdot y_0) \oplus (0x0206 \cdot y_1) \oplus (0x0002 \cdot y_2) \oplus (0x0002 \cdot y_3)$

5.2. 18-Round Zero-Correlation Attack with One 15-round Distinguisher. By adding one more round before the 17-round attack, we can extend the attack to 18 rounds. The key bits involved in the first round are $K^{2i-2,3}$ and $K^{2i-1,3}$. According to the key schedule, we know that

$$K^{2i-2,3} = K^{2i,1}, K^{2i-1,3} = K^{2i+1,1}. \quad (23)$$

Let P, Y_0 be the plaintext-ciphertext pair. The attack procedure is as follows.

- (1) For N values of $[P, Y_0]$, guess 64 bits of $K^{2i-2,3}, K^{2i-1,3}$ and encrypt P by two rounds and get

$$\beta_0 = (0x0080, 0x4001, 0x0080, 0x4001) \cdot X_1 \oplus Y_{0,0}[13] \oplus Y_{0,1}[13] \oplus Y_{0,2}[12] \oplus Y_{0,3}[12]. \quad (24)$$

Calculate the numbers of $[Y']$ according to the value of β_0 (+1 if $\beta_0 = 0$, -1 if $\beta_0 = 1$), where

$$Y' = (Y_{0,0}[12 \sim 0], Y_{0,1}[12 \sim 2], Y_{0,2}[11 \sim 0], Y_{0,3}[11 \sim 2]). \quad (25)$$

- (2) It's clear that the target bit, *i.e.*, is a function of $Y' \oplus k$, where $k = (K_L^{2i+10,3}[12 \sim 0], K_R^{2i+10,3}[12 \sim 2], K_L^{2i+11,3}[11 \sim 0], K_L^{2i+11,3}[11 \sim 2])$. So the target counter C can be computed using FFT techniques for all possible keys
- (3) For each guessed key, compute the statistic value used in the multiple zero-correlation attack, *i.e.*,

$$T = N \left(\frac{C}{N} \right)^2. \quad (26)$$

When T is smaller than the threshold value τ , the key is

supposed to be a right key candidate and can then be checked using two plaintext-ciphertext pairs.

By setting $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-1}$, we can compute that the data complexity $N \approx 2^{63.634}$ and threshold $\tau = 2$. The first step needs $N \cdot 2^{64} \cdot 2/18 = 2^{124.464}$ encryptions. The second step needs $2^{64} \cdot 3 \cdot 46 \cdot 2^{46} = 2^{117.109}$ simple calculations. The last step needs $2^{128} \cdot \alpha_1 = 2^{127}$ times encryption. So the total time complexity is $T \approx 2^{127.2}$ encryptions.

6. Integral Distinguishers on SPARX

Zero-correlation linear distinguishers can be transformed into integral distinguishers according to the known results in [10, 15]. Theorem 6 describes the result given in [15].

Theorem 2. (Corollary 4, [15])

Let $F : F_2^n \rightarrow F_2^n$ be a function on F_2^n , and let A be a subspace of F_2^n and $b \in F_2^n \setminus \{0\}$. Suppose that $A \rightarrow b$ is a zero correlation linear hull of F , then for any $\lambda \in F_2^n$, $b \cdot F(x \oplus \lambda)$ is balanced on A^\perp .

As a result, we can transform the linear hulls in Table 3 to some integral distinguishers. Partial integral distinguisher are given in Table 4.

Suppose the state of SPARX64/128 is represented as $(x_0, x_{1,2}, x_3)$ where x_i is a 16-bit word. The 12-round integral distinguisher means if we set the value at x_0 and x_1 to constants and let the value at x_2, x_3 take all possible values, the values at x_2, x_3 after 4 steps (minus the last linear layer) will take all possible values. This is the same with that proposed in [1].

The 14-round distinguisher means that when letting the values at x_0, x_1, x_2 take all possible values and setting $x_3 = x_1$, after one SPECKEY round, four full steps and one SPECKEY round, the one bit result of $(0x0207 \cdot y_0) \oplus (0x0206 \cdot y_1) \oplus (0x0002 \cdot y_2) \oplus (0x0002 \cdot y_3)$ will be active, where (y_0, y_1, y_2, y_3) means the value after 14-round encryption. We can expand this distinguisher one more round forward with probability 1 to get one 15-round distinguisher. The input set has 2^{63} elements (x_0, x_1, x_2, x_3) which satisfy $(0x0080 \cdot x_0) \oplus (0x4001 \cdot x_1) \oplus (0x0080 \cdot x_2) \oplus (0x4001 \cdot x_3) = '0'$ (or = '1').

7. Conclusion

We have given zero-correlation cryptanalysis results against SPARX-64/128 in this paper. 14 and 15-round zero-correlation linear distinguishers have been proposed, which are the longest distinguishers as far as we know. Then, with the help of χ^2 -MTZD and MPZC models, we have given 15, 16, 17 and 18-round key recovery attacks of SPARX-64/128 with post-whitening key. Our attacks cover the most rounds, while the existing attack on SPARX-64/128 covers 16 rounds. Also, we have transformed the new zero-correlation linear distinguishers into integral distinguishers. The longest one is 15-round, which is three rounds longer than the existing 12-round zero-correlation distinguisher.

Data Availability

The data used to support the findings of this study are included within the article

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

- [1] D. Dinu, L. Perrin, A. Udovenko, V. Velichkov, J. Großschädl, and A. Biryukov, "Design strategies for arx with provable bounds: Sparx and lax," in *Advances in Cryptology – ASIACRYPT 2016*, J. H. Cheon and T. Takagi, Eds., pp. 484–513, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
- [2] J. Daemen and V. Rijmen, "Aes and the wide trail design strategy," in *Advances in Cryptology | EUROCRYPT 2002*, L. R. Knudsen, Ed., pp. 108–109, Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.
- [3] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, *The simon and speck families of lightweight block ciphers*, Cryptology ePrint Archive, Report 2013, 2013, <https://eprint.iacr.org/2013/404>.
- [4] Y. Todo, "Structural evaluation by generalized integral property," in *Advances in Cryptology – EUROCRYPT 2015*, I. E. Oswald and M. Fischlin, Eds., pp. 287–314, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.
- [5] A. Abdelkhalek, M. Tolba, and A. M. Youssef, "Impossible differential attack on reduced round sparx-64/128," in *Progress in Cryptology – AFRICACRYPT 2017*, M. Joye and A. Nitaj, Eds., pp. 135–146, Springer International Publishing, Cham, 2017.
- [6] M. Tolba, A. Abdelkhalek, and A. M. Youssef, "Multidimensional zerocorrelation linear cryptanalysis of reduced round sparx-128," in *Selected Areas in Cryptography – SAC 2017*, C. Adams and J. Camenisch, Eds., pp. 423–441, Springer International Publishing, Cham, 2018.
- [7] R. Ankele and E. List, "Differential cryptanalysis of round-reduced sparx-64/128," in *applied cryptography and network security*, B. Preneel and F. Vercauteren, Eds., pp. 459–475, Springer International Publishing, Cham, 2018.
- [8] A. Bogdanov and V. Rijmen, "Linear hulls with correlation zero and linear cryptanalysis of block ciphers," *Designs, Codes and Cryptography*, vol. 70, no. 3, pp. 369–383, 2014.
- [9] A. Bogdanov and M. Wang, "Zero correlation linear cryptanalysis with reduced data complexity," in *Fast Software Encryption*, A. Canteaut, Ed., pp. 29–48, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
- [10] A. Bogdanov, G. Leander, K. Nyberg, and M. Wang, "Integral and multidimensional linear distinguishers with correlation zero," in *Advances in Cryptology – ASIACRYPT 2012*, X. Wang and K. Sako, Eds., pp. 244–261, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
- [11] H. Chen, T. Cui, and Meiqin Wang, "Improving algorithm 2 in multidimensional (zero-correlation) linear cryptanalysis using χ^2 -method," *Designs, Codes and Cryptography*, vol. 81, no. 3, pp. 523–540, 2016.
- [12] L. Sun, H. Chen, and M. Wang, "Zero-correlation attacks: statistical models independent of the number of approximations," *Designs, Codes and Cryptography*, vol. 86, no. 9, pp. 1923–1945, 2018.
- [13] C. Baudoin, F. X. Standaert, and J.-J. Quisquater, "Improving the time complexity of matsui's linear cryptanalysis," in *Information Security and Cryptology - ICISC 2007*, K.-H. Nam and G. Rhee, Eds., pp. 77–88, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.
- [14] C. Blondeau and K. Nyberg, "Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity," *Designs, Codes and Cryptography*, vol. 82, no. 1-2, pp. 319–349, 2017.
- [15] B. Sun, Z. Liu, V. Rijmen et al., "Links among impossible differential, integral and zero correlation linear cryptanalysis," in *Advances in Cryptology–CRYPTO 2015*, R. Gennaro and M. Robshaw, Eds., vol. 14, pp. 95–115, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.