Chinese Journal of Electronics
vol. 33, no. 3, pp. 672–682, May 2024
https://doi.org/10.23919/cje.2022.00.419

RESEARCH ARTICLE

Related-Key Zero-Correlation Linear Attacks on Block Ciphers with Linear Key Schedules

Yi ZHANG, Kai ZHANG, and Ting CUI

PLA SSF Information Engineering University, Zhengzhou 450000, China

Corresponding author: Ting CUI, Email: cuiting_1209@hotmail.com

Manuscript Received December 7, 2022; Accepted March 13, 2023

Abstract — Related-key model is a favourable approach to improve attacks on block ciphers with a simple key schedule. However, to the best of our knowledge, there are a few results in which zero-correlation linear attacks take advantage of the related-key model. We ascribe this phenomenon to the lack of consideration of the key input in zero-correlation linear attacks. Concentrating on the linear key schedule of a block cipher, we generalize the zero-correlation linear attack by using a related-key setting. Specifically, we propose the creation of generalized linear hulls (GLHs) when the key input is involved; moreover, we indicate the links between GLHs and conventional linear hulls (CLHs). Then, we prove that the existence of zero-correlation GLHs is completely determined by the corresponding CLHs and the linear key schedule. In addition, we introduce a method to construct zero-correlation GLHs by CLHs and transform them into an integral distinguisher. The correctness is verified by applying it to SIMON16/16, a SIMON-like toy cipher. Based on our method, we find 12/13/14/15/15/17/20/22-round related-key zero-correlation linear distinguishers of SIMON32/64, SIMON48/72, SIMON48/96, SIMON64/96, SIMON64/128, SIMON96/144, SIMON128/192 and SIMON128/256, respectively. As far as we know, these distinguishers are one, two, or three rounds longer than current best zero-correlation linear distinguishers of SIMON.

Keywords — Zero-correlation linear attack, Related-key model, Linear key schedule, Block cipher, SIMON.

Citation — Yi ZHANG, Kai ZHANG, and Ting CUI, “Related-Key Zero-Correlation Linear Attacks on Block Ciphers with Linear Key Schedules,” *Chinese Journal of Electronics*, vol. 33, no. 3, pp. 672–682, 2024. doi: 10.23919/cje.2022.00.419.

I. Introduction

Related-key attacks were independently proposed by Knudsen in 1992 [1] and Biham in 1994 [2]. This type of attack improves the attackers’ permissions to control the relation of keys without obtaining their specific values. Consequently, combined with other attack methods, such as differential attacks, impossible differential attacks and rectangle attacks, many results on ciphers, such as AES and KASUMI, are improved under the related-key model.

For linear attacks, Bogdanov *et al.* in 2013 [3] found an invariant bias of some linear approximations of block ciphers under certain key differences, which provides access to applying related-key linear attacks. Later, several works developed this idea. At SAC 2019, Lee *et al.* [4] introduced related-key linear approximations obtained from a linear trail of block ciphers with a linear key schedule under arbitrary known key differences. In 2021, Cao and Zhang [5] combined multidimensional linear cryptanalysis with key difference invariant bias.

Zero-correlation linear attack, proposed by Bogdanov, utilizes zero-correlation linear approximations instead of linear approximations with a large bias, and can be regarded as a dual attack of impossible differential attacks [6]. It also inherit the idea of multidimensional linear attacks in [7], which establishes the link with the integral attack [8]. However, only a few related-key zero-correlation linear attacks have appeared. At FSE 2019, Ankele *et al.* [9] proposed a novel idea to construct zero-correlation linear hulls by making contradictions in the linear tweakey schedules. Niu *et al.* [10] generalized the idea to key schedules at CT-RSA 2021. The scope of their methods is limited to linear (twea)key schedules using only word-wise operations. Thus, related-key zero-correlation linear attacks need be further extended to ciphers with bitwise operation.

Note that a key schedule determines the attackers’

Associate Editor: Prof. Debiao HE, Wuhan University.

controlling abilities of keys under the related-key model. The key schedule is usually regarded as a major factor of security against related-key attacks. Inspired by previous works, we concentrate on linear schedules as well and construct related-key zero-correlation linear distinguishers at the bitwise level.

The family of the lightweight block cipher SIMON [11], proposed by the National Security Agency in 2013, is exactly a favourable type of objective for bit-oriented research. It is a Feistel-structure block cipher with its round function only consisting of AND, rotation and XOR operations. While its various versions provide high performance across a range of devices, its security strength have attracted numerous cryptanalysts' eyes. A larger number of results such as differential, linear and integral attacks have been published. To date, differential attacks and linear attacks combined with automatic search tools and Mastui's search algorithm [12] have achieved the remarkable results and are producing further results constantly [13], [14]. Integral attacks are not only theoretically enriched by division property [15], but also practically boosted by automatic search tools [16], [17]. In contrast, recently, the results from zero-correlation attacks seem to stagnate after the work in [18]–[20].

The main results of zero-correlation linear distinguishers of SIMON are shown in Table 1.

Table 1 Zero-correlation linear distinguishers on SIMON

Cipher	Attack model	Rounds	Ref.
SIMON32	SK	10	[19]
	SK	11	[20]
	RK	12	This work
SIMON48	SK	11	[19]
	SK	12	[20]
SIMON48/72	RK	13	This work
SIMON48/96	RK	14	This work
SIMON64	SK	12	[19]
	SK	13	[18]
	RK	15	This work
SIMON96	SK	15	[19]
	SK	16	[18]
SIMON96/144	RK	17	This work
SIMON128	SK	18	[19]
	SK	19	[18]
SIMON128/192	RK	20	This work
SIMON128/256	RK	22	This work

Note: SK represents a single key model; RK represents a related-key model.

In this paper, we are devoted to taking full advantage of previous work on conventional linear hulls, and improving the results of zero-correlation linear attacks with the aid of the related-key model.

Our contribution In the theoretical aspect, for block ciphers with a linear schedule, we first introduce their zero-correlation generalized linear hulls (GLHs) when the key input mask is considered. We establish the relation between GLHs and conventional linear hulls (CLHs), which indicates that some zero-correlation GLHs come from a CLH. Then, we prove that the correlation of a GLH is completely determined by the linear key schedule and its corresponding CLH.

In the practical aspect, we propose a method to construct a series of zero-correlation GLHs at the bitwise level with their corresponding CLHs, which are verified by applying the method to SIMON16/16, a SIMON-like toy cipher. Based on this method, we obtain a series of 12/13/14/15/15/17/20/22-round zero-correlation GLHs of SIMON32/64, SIMON48/72, SIMON48/96, SIMON64/96, SIMON64/128, SIMON96/144, SIMON128/192, and SIMON128/256, respectively, which can be transformed into equal-length integral distinguishers.

Note that the motivation to transform ZCGLHs into integral distinguishers is to reduce the high data complexity of the zero-correlation linear attack. Since the distinguishers originate from zero-correlation GLHs, our attack is essentially a zero-correlation linear attack. More clear relation between zero-correlation linear attack and integral attack is demonstrated by Bogdanov *et al.* in [8].

In some sense, our theory might inspire research to find longer zero-correlation GLHs that have never been discovered, even if the corresponding CLHs are not zero-correlation. Our method could also be applied to several block ciphers with different structures, such as SKINNY (AES-like structure), QARMA (PRINCE-like structure) and CHAM (generalized Feistel-structure).

Organization In Section II, we recall some basic concepts of linear cryptanalysis. Then, in Section III, we introduce generalized linear hulls and establish a related-key zero-correlation linear attack. Next, in Section IV, we propose a method to construct zero-correlation GLHs and apply the method to the block cipher SIMON. Finally, we conclude in Section V.

II. Preliminaries

In this section, we recall the basic concepts of linear cryptanalysis and multidimensional zero-correlation linear distinguishers.

Definition 1 (Canonical scalar product) For column vector $x, y \in \mathbb{F}_2^n$, the canonical scalar product of x and y is defined as $\langle x, y\rangle = x^{\mathrm{T}} y$.

Definition 2 (Adjoint linear mapping) For a linear mapping $h : \mathbb{F}_2^m \to \mathbb{F}_2^n$, if the binary matrix $\boldsymbol{M}_{n\times m}$ is its matrix form (under some basis) and the input variable x is treated as a column vector, i.e., $h(x) = \boldsymbol{M}x$, then the adjoint linear mapping of h is defined by

$$\begin{aligned} h^{\mathrm{T}} : \mathbb{F}_2^n &\to \mathbb{F}_2^m \\ y &\mapsto \boldsymbol{M}^{\mathrm{T}} y \end{aligned}$$

Definition 3 (Correlation) [21] Given a function F :

$\mathbb{F}_2^m \to \mathbb{F}_2^n$ and a pair of input and output masks $(\alpha, \gamma) \in \mathbb{F}_2^m \times \mathbb{F}_2^n$, we call $\langle \alpha, x \rangle \oplus \langle \gamma, F(x) \rangle$ a linear approximation of function F ($\alpha \to \gamma$ for short). Then the correlation of the linear approximation is defined as

$$\mathrm{cor}_F(\alpha, \gamma) = \frac{1}{2^m} \sum_{x \in \mathbb{F}_2^m} (-1)^{\langle \alpha, x \rangle \oplus \langle \gamma, F(x) \rangle}$$

Definition 4 (Linear trail) [22] Let function F be the composition of r functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$ $(i = 1, 2, \dots, r)$, i.e.,

$$F(x) = f_r \circ f_{r-1} \circ \cdots \circ f_1(x)$$

For the pair of input and output masks $(\Gamma_{i-1}, \Gamma_i) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ of f_i, we called the concatenation

$$\Gamma = (\Gamma_0, \Gamma_1, \dots, \Gamma_r)$$

of the masks an r-round linear trail of F. Then the correlation of the linear trail is defined by

$$C_\Gamma = \prod_{i=1}^{r} \mathrm{cor}_{f_i}(\Gamma_{i-1}, \Gamma_i)$$

For iterative block ciphers, the two following propositions are deduced from Definition 3 when the keys are treated differently.

Proposition 1 [21] Given an iterative block cipher:

$$E_k(x) = G_r(\cdots(G_2(G_1(x \oplus k_0) \oplus k_1) \oplus k_2 \cdots) \oplus k_r$$

where $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are its round functions $(i = 1, 2, \dots, r)$ and $k = (k_0, k_1, \dots, k_r)$ is fixed. Then, for the pair of input and output masks (α, γ), we have

$$\mathrm{cor}_{E_k}(\alpha, \gamma) = \sum_{\substack{\Gamma = (\Gamma_0, \dots, \Gamma_r) \\ \Gamma_0 = \alpha, \Gamma_r = \gamma}} (-1)^{\langle \Gamma, k \rangle} \prod_{i=1}^{r} \mathrm{cor}_{G_i}(\Gamma_{i-1}, \Gamma_i)$$

For the completeness of the paper, we provide a brief proof of Proposition 1 in Appendix A.

We call the linear approximation $\alpha \to \gamma$ a conventional linear hull of E_k (CLH for short), which contains all possible linear trails of E_k from α to γ.

The linear approximation $\alpha \to \gamma$ is called a zero-correlation conventional linear hull (ZCCLH for short) if and only if $\prod_{i=1}^{r} \mathrm{cor}_{G_i}(\Gamma_{i-1}, \Gamma_i) = 0$ holds for any linear trail $\Gamma = (\alpha_1, \Gamma_1, \dots, \Gamma_{r-1}, \gamma)$.

Note that $\mathrm{cor}_{E_k}(\alpha, \gamma) = 0$ does not mean $\alpha \to \gamma$ is a ZCGLH because of the sign of C_Γ, which is controlled by k. Only when $\mathrm{cor}_{E_k}(\alpha, \gamma) = 0$ holds for any k, is $\alpha \to \gamma$ a ZCCLH.

Proposition 2 [23] Let an r-round iterative block cipher $E : \mathbb{F}_2^n \times \mathbb{F}_2^t \to \mathbb{F}_2^n$ be the composition of r round functions $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$ $(i = 1, 2, \dots, r)$ with a linear key schedule $L : \mathbb{F}_2^t \to (\mathbb{F}_2^n)^{r+1}$, i.e.,

$$\begin{aligned} E(x, k) :&= F(x, L(k)) \\ &= G_r(\cdots(G_2(G_1(x \oplus k_0) \oplus k_1) \oplus k_2 \cdots) \oplus k_r \end{aligned}$$

where the key is one of input variable of E and $L(k) = (k_0, k_1, \dots, k_r)$. Then for the pair of plaintext input, key input and output masks $((\alpha_1, \alpha_2), \gamma) \in (\mathbb{F}_2^n \times \mathbb{F}_2^t) \times \mathbb{F}_2^n$,

$$\mathrm{cor}_E((\alpha_1, \alpha_2), \gamma) = \sum_{\substack{\Gamma = (\Gamma_0, \dots, \Gamma_r) \in (\mathbb{F}_2^n)^{r+1} \\ \Gamma_0 = \alpha_1, \Gamma_r = \gamma, L^{\mathrm{T}}(\Gamma) = \alpha_2}} \prod_{i=1}^{r} \mathrm{cor}_{G_i}(\Gamma_{i-1}, \Gamma_i)$$

A brief proof of Proposition 2 is also presented in Appendix A.

We call the linear approximation $(\alpha_1, \alpha_2) \to \gamma$ a generalized linear hull (GLH) of E. Then, $(\alpha_1, \alpha_2) \to \gamma$ is a zero-correlation generalized linear hull (ZCGLH) if and only if $\prod_{i=1}^{r} \mathrm{cor}_{G_i}(\Gamma_{i-1}, \Gamma_i) = 0$ holds for any linear trail $\Gamma = (\alpha_1, \Gamma_1, \dots, \Gamma_{r-1}, \gamma)$ that satisfies $L^{\mathrm{T}}(\Gamma) = \alpha_2$.

According to the definitions and propositions of CLHs, GLHs and ZCGLHs, when the key input is treated as a constant, we are discussing CLHs, and the key value only influences the sign of the correlation of linear trails in a linear approximation; when the key input is treated as a variable, we are discussing GLHs, and the correlation of a linear approximation is restricted by the key's mask.

Definition 5 (Balance of vectorial Boolean function) Let $H : \mathbb{F}_2^m \to \mathbb{F}_2^n$ be a mapping $(m \geq n)$ and $A \subseteq \mathbb{F}_2^m$. If the size of the set $H_A^{-1}(y) = \{x \in A | H(x) = y\}$ is independent of $y \in \mathbb{F}_2^n$, we call H is balanced on A.

Definition 6 (Dual space) Let A be a subspace of $\mathbb{F}_2^m$. The set $A^\perp = \{x \in \mathbb{F}_2^m | \langle a, x \rangle = 0, a \in A\}$ can be proven to be a subspace. We call $A^\perp$ is a dual subspace of A.

Theorem 1 [24] Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function on $\mathbb{F}_2^n$, and let A be a subspace of $\mathbb{F}_2^n$ and $b \in \mathbb{F}_2^n \backslash \{\mathbf{0}_n\}$. Suppose that for any $a \in A$, $a \to b$ is a zero-correlation linear hull of F; then, for any constant $\lambda \in \mathbb{F}_2^n$, $\langle b, F(x \oplus \lambda) \rangle$ is balanced on $A^\perp = \{x \in \mathbb{F}_2^n | \langle a, x \rangle = 0, a \in A\}$.

Theorem 1 shows that one can transform several zero-correlation linear hulls ($A \to b$) into an integral distinguisher. Hence, if the input x of the function F goes through $A^\perp$, then the sum of XORing all $\langle b, F(x \oplus \lambda) \rangle$ is zero. And the data complexity of the distinguishing attack can be reduced up to the size of $A^\perp$ from the size of $\mathbb{F}_2^n$.

III. On the Existence of ZCGLHs

In this section, the relation between CLHs and GLHs is established. Then the question about whether a GLH is zero-correlation is transformed into an analysis of linear trails of a corresponding CLH. Subsequently, the theorem presented below indicates the existence of ZCGLHs. It turns out that the existence of ZCGLHs is only relevant to the corresponding CLHs and the linear key schedule.

1. Relation between ZCCLH and ZCGLH

For an r-round iterative block cipher

$$\begin{aligned} E(x,k) :&= F(x, KS(k)) \\ &= G_r(\cdots(G_2(G_1(x \oplus k_0) \oplus k_1) \oplus k_2 \cdots) \oplus k_r \end{aligned}$$

where $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$ $(i=1,2,\ldots,r)$ and $KS : \mathbb{F}_2^t \to (\mathbb{F}_2^n)^{r+1}$ are its round functions and linear key schedule, respectively; and $KS(k) = (k_0, k_1, \ldots, k_r)$.

Given a pair of masks $((\alpha_1, \alpha_2), \gamma) \in (\mathbb{F}_2^n \times \mathbb{F}_2^t) \times \mathbb{F}_2^n$ of E, let

$$\Omega_0(\alpha_1 \to \gamma) = \{\Gamma \in (\mathbb{F}_2^n)^{r+1} | (\Gamma_0, \Gamma_r) = (\alpha_1, \gamma) \text{ and } C_\Gamma \neq 0\}$$

be the subset consisting of all possible linear trails of E_k from α to γ (here k is fixed).

And let

$$\Omega_1((\alpha_1, \alpha_2) \to \gamma) = \{\Gamma \in \Omega_0(\alpha_1 \to \gamma) | KS^{\mathrm{T}}(\Gamma) = \alpha_2\}$$

Thus, $\Omega_1((\alpha_1, \alpha_2) \to \gamma)$ is actually the subset of $\Omega_0(\alpha_1 \to \gamma)$, in which any linear trail satisfies $KS^{\mathrm{T}}(\Gamma) = \alpha_2$.

According to Propositions 1 and 2, the trails in $\Omega_0(\alpha_1 \to \gamma)$ are exactly all trails contributing to the correlation of the CLH $\alpha_1 \to \gamma$, while the trails in $\Omega_1((\alpha_1, \alpha_2) \to \gamma)$ are exactly all trails contributing to the correlation of the GLH $(\alpha_1, \alpha_2) \to \gamma$. We conclude this property as the following theorems.

Theorem 2 Given an r-round iterative cipher E_k with a fixed key k, the CLH $\alpha_1 \to \gamma$ of E_k is zero-correlation if and only if $\Omega_0(\alpha_1 \to \gamma) = \varnothing$.

Proof Based on Proposition 1, $\alpha_1 \to \gamma$ is a ZCCLH if and only if no possible trails of E_k from α_1 to γ exist, i.e., $\Omega_0(\alpha_1 \to \gamma)$ has no elements.□

Theorem 3 Given an r-round iterative cipher E with a linear key schedule $KS : \mathbb{F}_2^t \to (\mathbb{F}_2^n)^{r+1}$, the GLH $(\alpha_1, \alpha_2) \to \gamma$ of E is zero-correlation if and only if $\Omega_1((\alpha_1, \alpha_2) \to \gamma) = \varnothing$.

Proof (Necessity) If $(\alpha_1, \alpha_2) \to \gamma$ is a ZCGLH of E, then there are two cases as follows:

Case 1: $\Omega_0(\alpha_1 \to \gamma) = \varnothing$, then $\Omega_1((\alpha_1, \alpha_2) \to \gamma) = \varnothing$;

Case 2: $\Omega_0(\alpha_1 \to \gamma) \neq \varnothing$ but no trails in $\Omega_0(\alpha_1 \to \gamma)$ satisfies $KS^{\mathrm{T}}(\Gamma) = \alpha_2$, then $\Omega_1((\alpha_1, \alpha_2) \to \gamma) = \varnothing$.

(Sufficiency) If $\Omega_1((\alpha_1, \alpha_2) \to \gamma) = \varnothing$, then one of the above two cases holds. Each of the cases indicates that $(\alpha_1, \alpha_2) \to \gamma$ of E is a ZCGLH according to Proposition 2.

Corollary 1 $(\alpha_1, \alpha_2) \to \gamma$ is a ZCGLH of E, if one of the following two conditions holds:

1) $\Omega_0(\alpha_1 \to \gamma) = \varnothing$;

2) $\Omega_0(\alpha_1 \to \gamma) \neq \varnothing$ but $KS^{\mathrm{T}}(\Gamma) \neq \alpha_2$ holds for any $\Gamma \in \Omega_0(\alpha_1 \to \gamma)$.

Corollary 2 If $\alpha_1 \to \gamma$ is a ZCCLH of E_k, then for any $\alpha_2 \in \mathbb{F}_2^t$, $(\alpha_1, \alpha_2) \to \gamma$ is a ZCGLH of E.

According to the above theorems and corollaries, a ZCCLH can deduce its corresponding ZCGLHs. However, a nonzero-correlation CLH could not ensure all its corresponding GLHs are nonzero-correlation. Based on such a conclusion, we present a theorem to demonstrate the existence of ZCGLHs.

2. The existence of ZCGLHs

Theorem 4 Let $E : \mathbb{F}_2^n \times \mathbb{F}_2^t \to \mathbb{F}_2^n$ be an r-round iterative cipher, and let its key schedule $KS : \mathbb{F}_2^t \to (\mathbb{F}_2^n)^{r+1}$ be linear. Given a CLH $\alpha_1 \to \gamma$ of E_k (k is a fixed key), the corresponding GLH $(\alpha_1, \alpha_2) \to \gamma$ is a ZCGLH of E if and only if $\alpha_2 \notin KS^{\mathrm{T}}(\Omega_0(\alpha_1 \to \gamma))$.

Proof The theorem can be proved by Corollary 1.

According to Theorem 4, given a CLH $\alpha_1 \to \gamma$, all ZCGLHs are exactly determined by the set $KS^{\mathrm{T}}(\Omega_0(\alpha_1 \to \gamma))$. Even though the CLH is not zero-correlation, one can choose a mask of the key input ($\alpha_2 \notin KS^{\mathrm{T}}(\Omega_0(\alpha_1 \to \gamma))$) to generate a ZCGLH $(\alpha_1, \alpha_2) \to \gamma$. Thus, once we consider the key input (in the related-key model), the previous upper bound of ZCCLHs might be broken through, which inspires us to explore a new upper bound of ZCGLHs.

In addition, we can give a general description of the existence of ZCGLHs.

Corollary 3 All ZCGLHs come from the set $\mathbb{ZC} = \{(\alpha_1, \alpha_2) \to \gamma | \alpha_2 \in \mathbb{F}_2^t \backslash KS^{\mathrm{T}}(\Omega_0(\alpha_1 \to \gamma))\}\}$.

Corollary 4 Given a CLH $\alpha_1 \to \gamma$ of the cipher E_k, if $\Omega_0(\alpha_1 \to \gamma) \bigcap \ker KS^{\mathrm{T}} = \varnothing$, then $(\alpha_1, 0) \to \gamma$ is a ZCGLH of E, where $\ker KS^{\mathrm{T}}$ represents the kernel of the linear map KS^{T}.

Corollary 4 supports the transformation of ZCGLHs into an integral distinguisher.

3. Zero-correlation linear attack based on ZCGLHs

The correlation of the ZCGLH $(\alpha_1, \alpha_2) \to \gamma$ is

$$\mathrm{cor}_E((\alpha_1, \alpha_2), \gamma) = \frac{1}{2^{n+t}} \sum_{(x,k) \in \mathbb{F}_2^n \times \mathbb{F}_2^t} (-1)^{\langle \alpha_1, x \rangle \oplus \langle \alpha_2, k \rangle \oplus \langle \gamma, E(x,k) \rangle}$$

According to the zero-correlation linear attack [6], we need nearly 2^{n+t} data to distinguish E from a random permutation. Obviously, it is not a valid attack when we only use one ZCGLH. However, a multidimensional zero-correlation linear attack [8], [24] provides us with the idea of taking advantage of ZCGLHs, i.e., combining several ZCGLHs to attack ciphers.

Suppose that we obtain a linear subspace $A \subset \mathbb{F}_2^{n+t}$ and an output mask $b \in \mathbb{F}_2^n$ such that any $a \in A$ leads the GLHs $a \to b$ to be zero-correlation. According to Theorem 1, we obtain an integral distinguisher of which the data complexity is only $2^{n+t}/|A|$.

Example 1 Let $\alpha_1 \to \gamma$ be a CLH of the cipher $E(x, K)$, let $KS : \mathbb{F}_2^t \to (\mathbb{F}_2^n)^r$ be the key schedule of the cipher and let $A_2 \subset \mathbb{F}_2^t$ be a linear subspace spanned by $s-1$ linearly independent elements $\{\alpha_2^{(1)}, \alpha_2^{(2)}, \ldots, \alpha_2^{(s-1)}\}$. Suppose that $\Omega_0(\alpha_1 \to \gamma) \bigcap \ker KS^{\mathrm{T}} = \varnothing$, and for each $\alpha_2 \in A_2$, $(\alpha_1, \alpha_2) \to \gamma$ is a ZCGLH. Then a subspace $A \subset$

$\mathbb{F}_2^n \times \mathbb{F}_2^t$ spanned by $\{(\alpha_1, \mathbf{0}_t), (\mathbf{0}_n, \alpha_2^{(1)}), (\mathbf{0}_n, \alpha_2^{(2)}), \ldots, (\mathbf{0}_n, \alpha_2^{(s-1)})\}$ satisfies that $(\alpha_1, \alpha_2) \to \gamma$ is a ZCGLH for any $(\alpha_1, \alpha_2) \in A$. Hence, according to Theorem 1, the cipher E is balanced on $A^{\perp}$. In other words, we only need to use $2^{(n+t-s)}$ data under $(t-s+1)$-bit related-key to distinguish the cipher from a random permutation.

Thus, one can first obtain several ZCGLHs from CLHs by Theorem 4, and then transforms these ZCGLHs into a related-key zero-correlation linear distinguisher. The required data complexity is determined by the number of valid ZCGLHs.

In the next section, we present an attack instance to illustrate the details of our zero-correlation linear attack based on ZCGLHs. Our theory above can also be verified.

IV. Application to SIMON

In this section, we apply our theory to construct zero-correlation linear distinguishers of SIMON, an And-RX block cipher.

We first briefly describe the specifics of SIMON. Next, we establish the propagation rules of mask propagation in the round functions of SIMON and collect all truncated linear trails propagation forward (or backward). After linking a forward trail and a backward trail, we obtain a rough set containing an Ω_0 discussed above. The rest of this section presents a method to construct a series of ZCGLHs of SIMON and to transform them into integral distinguishers. The correctness is verified by applying the method to SIMON16/16, a SIMON-like toy cipher.

Finally, we obtain 12-round, 13-round, 13-round, 15-round, 15-round, 17-round, 20-round, and 21-round related-key integral distinguishers of SIMON32/64, SIMON48/72, SIMON48/96, SIMON64/96, SIMON64/128, SIMON96/144, SIMON128/192 and SIMON128/256, respectively.

1. Brief description of SIMON

The SIMON block cipher is an r-round Feistel block cipher with an n-bit word and an mn-bit master key, denoted by SIMON$2n/mn$, where $n \in \{16, 24, 32, 48, 64\}$, $m \in \{2, 3, 4\}$ and $r \in \{32, 36, 36, 42, 44, 52, 54, 68, 69, 72\}$. There are ten versions in the SIMON family, and the corresponding parameters are listed in Table 2.

Table 2 Parameters in the family of SIMON block cipher

Variants	Word size (n)	Key word number (m)	Constant (z_j)	Rounds (r)
SIMON32/64	16	4	z_0	32
SIMON48/72	24	3	z_0	36
SIMON48/96	24	4	z_1	36
SIMON64/96	32	3	z_2	42
SIMON64/128	32	4	z_3	44
SIMON96/96	48	2	z_2	52
SIMON96/144	48	3	z_3	54
SIMON128/128	64	2	z_2	68
SIMON128/192	64	3	z_3	69
SIMON128/256	64	4	z_4	72

Round function Figure 1 shows the i-th round function round Function. As shown in Figure 1, the i-th round function of SIMON$2n$ is defined by

$$\begin{aligned} F_{RK_{i-1}} &: \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n} \\ &(X_L^{i-1}, X_R^{i-1}) \mapsto (X_L^i, X_R^i) \end{aligned}$$

and

$$\begin{cases} X_R^i = X_L^{i-1} \\ X_L^i = F(X_L^{i-1}) \oplus X_R^{i-1} \oplus RK_{i-1} \end{cases}$$

where RK_{i-1} is the i-th roundkey, $S(X_L) := X_L \lll 1$,

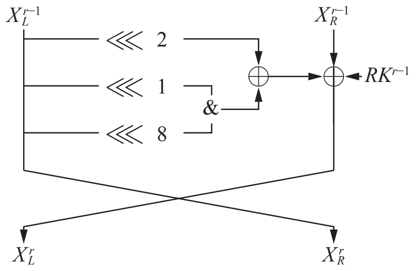

Figure 1 Round function of SIMON.

and

$$F(X_L) := S^8(X_L) \ \& \ S^1(X_L) \oplus S^2(X_L)$$

is the F function in the Feistel structure. Therefore, the round function can also be written as

$$F_{RK_{i-1}}(X_L^{i-1}, X_R^{i-1}) \triangleq G_{i-1}(X_L^{i-1} \oplus 0_n, X_R^{i-1} \oplus RK_{i-1})$$

Key schedule The roundkeys RK_i are derived from the master key by a key schedule chosen by the parameters m and n. It can be written as

$$\begin{aligned} KS : \mathbb{F}_2^{mn} &\to (\mathbb{F}_2^n)^r \\ K &\mapsto (RK_0, RK_1, \ldots, RK_{r-1}) \end{aligned}$$

The following five constant sequences z_0, z_1, z_2, z_3, z_4 with a period of 62 are used in different key schedules to generate round keys.

$$\begin{aligned} z_0 &= z_{0\{0\}} z_{0\{1\}} z_{0\{2\}} \cdots \\ &= 11111010001001010110000111 \\ &\quad\ 001011111010001001010110000011100110 \ldots \end{aligned}$$

$$\begin{aligned} z_1 &= z_{1\{0\}} z_{1\{1\}} z_{1\{2\}} \cdots \\ &= 10001110111110010011000010 \\ &\quad 110101000111011111001001100001011010 \ldots \end{aligned}$$

$$\begin{aligned} z_2 &= z_{2\{0\}} z_{2\{1\}} z_{2\{2\}} \cdots \\ &= 10101111011100000011010010 \\ &\quad 011000101000010001111110010110110011 \ldots \end{aligned}$$

$$\begin{aligned} z_3 &= z_{3\{0\}} z_{3\{1\}} z_{3\{2\}} \cdots \\ &= 11011011101011000110010111 \\ &\quad 100000010010001010011100110100001111 \ldots \end{aligned}$$

$$\begin{aligned} z_4 &= z_{4\{0\}} z_{4\{1\}} z_{4\{2\}} \cdots \\ &= 11010001111001101011011000 \\ &\quad\ 1000000101110000110010100100111011111\ldots \end{aligned}$$

Let the master key be $K = (k_0, k_1 \ldots, k_{m-1}) \in (\mathbb{F}_2^n)^m$; then, $(RK_0, RK_1, \ldots, RK_{m-1}) = K$ and we have RK_{i+m} as follows:

$$RK_{i+m} = \begin{cases} c \oplus z_{j_{\{i\}}} \oplus RK_i \oplus (I \oplus S^{-1})(S^{-3}(RK_{i+1})), & m = 2 \\ c \oplus z_{j_{\{i\}}} \oplus RK_i \oplus (I \oplus S^{-1})(S^{-3}(RK_{i+2})), & m = 3 \\ c \oplus z_{j_{\{i\}}} \oplus RK_i \oplus (I \oplus S^{-1})(RK_{i+1} \oplus S^{-3}(RK_{i+3})), & m = 4 \end{cases}$$

where $c = 2^n - 4 = \mathrm{0xff\ldots fc}$, $z_{j_{\{i\}}}$ is the i-th bit of the sequence z_j and $i = 0, 1, \ldots, r - m - 1, j \in \{0, 1, 2, 3, 4\}$.

Hence, SIMON is an iterative cipher

$$\begin{aligned} E(P, K) = G_{r-1}(\circ \cdots \circ G_1 \circ G_0(P \oplus (\mathbf{0}_n, RK_0)) \\ \oplus (\mathbf{0}_n, RK_1) \oplus \cdots \oplus (\mathbf{0}_n, RK_{r-1})) \oplus \mathbf{0}_{2n} \end{aligned}$$

whose linear key schedule satisfies the conditions of Proposition 2. The i-th round key of SIMON is $K_i = (\mathbf{0}_n, RK_i) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ when we apply the proposition, so the key schedule should be written as

$$\begin{aligned} L : \mathbb{F}_2^{mn} &\to (\mathbb{F}_2^{2n})^{r+1} \\ K &\mapsto (\mathbf{0}_{2n}, K_{r-1}, \ldots, K_0) \end{aligned}$$

2. Propagation rules for linear masks

According to Theorem 4, the key point to construct ZCGLHs is to ascertain Ω_0. Although it is impractical to accurately target all elements in Ω_0, narrowing down Ω_0 to a rough set is sometimes enough.

Here, we adapt the idea of truncated differences to compute truncated linear trails propagating with probability 1, where the truncated linear trails mean the mask values are replaced by asterisks if we fail to determine their specific values. Thus, such trails do not stop until there are asterisks covering all bits of one-round masks.

Hence, the collection of all linear trails following the form of the truncated linear trail is a roughly description of Ω_0.

The following four lemmas are easily proven.

Lemma 1 [25] Given a linear mapping $h(x_1, x_2) = x_1 \oplus x_2$, then for a pair of input masks (α, β) and an output mask γ, $\mathrm{cor}_h((\alpha, \beta), \gamma) \neq 0$ if and only if $\alpha = \beta = \gamma$.

Lemma 2 [25] Given a linear mapping $h(x) = (x, x)$, then for an input mask α and a pair of output masks (β, γ), $\mathrm{cor}_h(\alpha, (\beta, \gamma)) \neq 0$ if and only if $\alpha \oplus \beta \oplus \gamma = 0$.

Lemma 3 [6] Given a linear mapping $h^a(x) = x \lll a$, a is a constant, then for a pair of input and output masks (α, γ), $\mathrm{cor}_h(\alpha, \gamma) \neq 0$ if and only if $\alpha \lll a = \gamma$.

Lemma 4 Given a nonlinear mapping:

$$\begin{aligned} g : \mathbb{F}_2 \times \mathbb{F}_2 &\to \mathbb{F}_2 \\ (x, y) &\mapsto x \ \& \ y \end{aligned}$$

when the output mask $\gamma \neq 0$, no matter values the input masks (α, β) take, $\mathrm{cor}_h((\alpha, \beta), \gamma) \neq 0$; when the output mask $\gamma = 0$, $\mathrm{cor}_h((\alpha, \beta), \gamma) \neq 0$ if and only if $\alpha = \beta = 0$.

Based on the lemmas above, we can compute truncated linear trails of SIMON after given specific plaintext input and output masks.

Example 2 As shown in Tables 3–6, given a CLH $\alpha_1 \to \gamma$ of SIMON32, it derives an r_1-round forward truncated linear trail Γ^+ and an r_2-round backward truncated linear trail Γ^- (where $r_1 = 6, r_2 = 6$). An r-round truncated linear trail Γ can be generated by connecting them. If $r < r_1 + r_2$ (e.g., an 11-round trail in Table 5), the overlapping parts (Γ_5 and Γ_6) of the forward and backward trails take the intersection; otherwise, if $r > r_1 + r_2$ (e.g., an 15-round trail in Table 6), the vacant parts (Γ_7 and Γ_8) are filled with asterisks (unknown bits).

Table 3 Forward truncated linear trail Γ^+

Γ_0^+	0000000000000100 0000000000000000
Γ_1^+	0000000000000000 0000000000000100
Γ_2^+	0000000000000100 00000*00000000*1
Γ_3^+	00000*00000000*1 *10000**00000*0*
Γ_4^+	*10000**00000*0* ***10*0***0000**
Γ_5^+	***10*0***0000** *****1******0*0*
Γ_6^+	*****1******0*0* ****************

Table 4 Backward truncated linear trail Γ^-

Γ_0^-	0000000000000000 0000000000000010
Γ_1^-	0000000000000010 0000000000000000
Γ_2^-	100000*00000000* 0000000000000010
Γ_3^-	**10000**00000*0 100000*00000000*
Γ_4^-	****10*0***0000* **10000**00000*0
Γ_5^-	******1******0*0 ****10*0***0000*
Γ_6^-	**************** ******1******0*0

3. Method to construct ZCGLHs

Since all linear trails included in a CLH can be roughly estimated by the corresponding truncated linear trails, we present a method to construct ZCGLHs by computing target key input masks with these trails.

Given a pair of specific plaintext input and output masks $(\alpha_1, \gamma) \in \mathbb{F}_2^{2n} \times \mathbb{F}_2^n$, we can compute an r-round truncated linear trail $\Gamma \in (\mathbb{F}_2^{2n})^r$. The collection of all possible linear trails of the CLH $\alpha_1 \to \gamma$ is denoted by Ω_0.

The binary matrix form of L^{T} is denoted by

$$[L_0, L_1, \ldots, L_{2nr-1}]$$

where L_j is the j-th mn-dimensional column vector in

Table 5 11-round truncated linear trail

Γ_0	0000000000000100 0000000000000000
Γ_1	0000000000000000 0000000000000100
Γ_2	0000000000000100 00000*00000000*1
Γ_3	00000*00000000*1 *10000**00000*0*
Γ_4	*10000**00000*0* ***10*0***0000**
Γ_5	***10*0***0000** *****11*****0000
Γ_6	*****11*****0000 ****10*0***0000*
Γ_7	****10*0***0000* **10000**00000*0
Γ_8	**10000**00000*0 100000*00000000*
Γ_9	100000*00000000* 0000000000000010
Γ_{10}	0000000000000010 0000000000000000
Γ_{11}	0000000000000000 0000000000000010

Table 6 15-round truncated linear trail

Γ_0	0000000000000100 0000000000000000
Γ_1	0000000000000000 0000000000000100
Γ_2	0000000000000100 00000*00000000*1
Γ_3	00000*00000000*1 *10000**00000*0*
Γ_4	*10000**00000*0* ***10*0***0000**
Γ_5	***10*0***0000** *****1******0*0*
Γ_6	*****1******0*0* ****************
Γ_7	**************** *****1******0*0*
Γ_8	******1******0*0 ****************
Γ_9	**************** ******1******0*0
Γ_{10}	******1******0*0 ****10*0***0000*
Γ_{11}	****10*0***0000* **10000**00000*0
Γ_{12}	**10000**00000*0 100000*00000000*
Γ_{13}	100000*00000000* 0000000000000010
Γ_{14}	0000000000000010 0000000000000000
Γ_{15}	0000000000000000 0000000000000010

the matrix.

Let $J=\{j|\mathit{\Gamma}_{\{j\}}\equiv 1 \text{ or } 0, \mathit{\Gamma}\in\mathit{\Omega}_0\}$, and $\eta_0=\oplus_{j\in J}(\mathit{\Gamma}_{\{j\}}\cdot L_j)$, where $\mathit{\Gamma}_{\{j\}}$ is the j-th bit of $\mathit{\Gamma}$ and the operation "$\cdot$" is a scalar product in the vector space.

Then, for $\mathit{\Gamma}\in\mathit{\Omega}_0$,

$$L^{\mathrm{T}}(\mathit{\Gamma})=\oplus_{j=0}^{2nr-1}(\mathit{\Gamma}_{\{j\}}\cdot L_j)=\eta_0\oplus(\oplus_{j\notin J}(\mathit{\Gamma}_{\{j\}}\cdot L_j))\in\mathbb{F}_2^t$$

The following theorem helps us to find the ZCGLHs that are used in our attack.

Theorem 5 If the vector η_0 above is linearly independent with the vector group $\{L_j\}_{j\notin J}$, then there exists a $(t-1)$-dimensional subspace A_2 that satisfies $A_2\bigcap L^{\mathrm{T}}(\mathit{\Omega}_0)=\varnothing$; otherwise, there exists an $(t-s)$-dimensional subspace A_2 that satisfies $A_2\bigcap L^{\mathrm{T}}(\mathit{\Omega}_0)=\varnothing$, where s is the rank of the group $\{L_j\}_{j\notin J}$.

Proof Suppose that the vector group $\{L_{j_1},L_{j_2},\dots,L_{j_s}\}$ is a maximal linearly independent group of $\{L_j\}_{j\notin J}$.

In the first case, the vector group $\{L_{j_1},L_{j_2},\dots,L_{j_s}\}$ can be extended to be a basis group of the vector space $\mathbb{F}_2^t$. Then the basis group could be denoted by

$$\{L_{j_1},L_{j_2},\dots,L_{j_s},\eta_0,\eta_1,\dots,\eta_{t-s-1}\}$$

And let the subspace spanned by the group $\{L_{j_1},L_{j_2},\dots,L_{j_s},\eta_1,\eta_2,\dots,\eta_{t-s-1}\}$ be denoted by A_2, then $L^{\mathrm{T}}(\mathit{\Omega}_0)\subset\eta_0\oplus A_2$. Since $A_2\bigcap(\eta_0\oplus A_2)=\varnothing$, we have $A_2\bigcap L^{\mathrm{T}}(\mathit{\Omega}_0)=\varnothing$.

In the second case, let $\{L_{j_1},L_{j_2},\dots,L_{j_s},\eta_1,\eta_2,\dots,\eta_{t-s}\}$ be a basis group of $\mathbb{F}_2^t$, then the group $\{\eta_1,\eta_2,\dots,\eta_{t-s}\}$ could span to be a subspace A_2 that satisfies $(A_2\backslash\{\mathbf{0}_t\})\bigcap L^{\mathrm{T}}(\mathit{\Omega}_0)=\varnothing$.

The proof of Theorem 5 indicates that $L^{\mathrm{T}}(\mathit{\Omega}_0)$ is a subset of the space W spanned by the vector group $\{L_0,L_1,\dots,L_{2nr-1}\}$. In addition, $W=\eta_0\oplus A_2$ in the first case, while W is spanned by $\{L_{j_1},L_{j_2},\dots,L_{j_s}\}$ in the second case. In both cases, we can easily construct a space A_2 to feed the condition of Theorem 4, i.e. $\alpha_2\notin L^{\mathrm{T}}(\mathit{\Omega}_0)$ holds for any $\alpha_2\in A_2$. Hence, we obtain a class of ZCGLHs to construct zero-correlation linear distinguishers.

In most cases, $s=t$ because of the pursuance for longer ZCGLHs. Thus, we often expect the first case in Theorem 5 to happen. If it happens, we could follow the steps in Example 1 to construct ZCGLHs and transform them into an integral distinguisher.

Finally, according to Theorem 5, we propose a method to construct r-round ZCGLHs from a CLH $\alpha_1\to\gamma$ as follows.

Step 1 Generate a truncated linear trail $\mathit{\Gamma}$ from an input CLH $\alpha_1\to\gamma$ based on the lemmas in Section IV, then the index set J can be determined.

Step 2 Compute the matrix of L^{T} with the key schedule L.

Step 3 Compute the vector $\eta_0=\oplus_{j\in J}(\mathit{\Gamma}_{\{j\}}\cdot L_j)$.

Step 4 Compute a maximal linearly independent group of $\{L_j\}_{j\notin J}$, and we denote it by $\{L_{j_1},L_{j_2},\dots,L_{j_s}\}$.

Step 5 Determine the linear dependence between η_0 and $\{L_{j_1},L_{j_2},\dots,L_{j_s}\}$. If they are linearly independent, continue the procedure; otherwise, terminate the procedure and the CLH cannot be used to construct ZCGLHs by this method.

Step 6 Extend the vector group $\{L_{j_1},L_{j_2},\dots,L_{j_s},\eta_0\}$ to be a basis group of $\mathbb{F}_2^t$, and we denote the basis group by $\{L_{j_1},L_{j_2},\dots,L_{j_s},\eta_0,\eta_1,\dots,\eta_{t-s-1}\}$. Then let the subspace A_2 be spanned by the group $\{L_{j_1},L_{j_2},\dots,L_{j_s},\eta_1,\eta_2,\dots,\eta_{t-s-1}\}$.

Step 7 Let $A_1=\{\alpha_1,\mathbf{0}_t\}$ and let $A=A_1\times A_2\subset\mathbb{F}_2^{2n}\times\mathbb{F}_2^t$. Terminate the procedure and we construct ZCGLHs that can be transformed into an integral distinguisher. Specifically,

$$\underset{(x,K)\in A^{\perp}}{\oplus}\langle\gamma,E(x\oplus\lambda_1,K\oplus\lambda_2)\rangle=0$$

where $(\lambda_1,\lambda_2)\in\mathbb{F}_2^{2n}\times\mathbb{F}_2^t$ is any constant.

After obtaining ZCGLHs from a CLH by the method above and transform them into an integral distinguisher by Theorem 1, we can compute $\oplus_{(x,K)\in A^{\perp}}\langle\gamma, E(x\oplus\lambda_1, K\oplus\lambda_2)\rangle$ under the related-key setting. Since the subspace A consist of $2n-1$ basis vectors in $(A_1, \mathbf{0}_t)$ and one basis vector in $(\mathbf{0}_{2n}, A_2)$, the data complexity of the distinguisher is 2^{2n} with one-bit related-key.

The method above only involves CLHs and the key schedule, so it can also be utilized in a number of block ciphers with different structures, (such as SKINNY, QARMA, and CHAM), as long as the description of their linear hulls are relatively clear and the key schedule is linear. The clearer the description is, the better this method works.

4. Experimental verification

To verify our theory (especially Theorem 4) and the method above, we present two experiments.

The first experiment This experiment is to verify Theorem 4 by testing ZCGLHs of SIMON16/16. In this paper, relative to SIMON, we set $n=8, m=2, r=8$ and the constant to be z_2, and let the F-function be $F(X_L) := S^4(X_L)\ \&\ S^1(X_L)\oplus\ S^2(X_L)$.

Firstly, we store all 2^{32} 3-tuples $(K, P, E(P,K))$ of SIMON16/16, where K, P and $E(P,K)$ represent key, plaintext and ciphertext, respectively.

Secondly, given a CLH $\alpha_1\rightarrow\gamma$, compute and store 2^{32} 2-tuples (K, H_K), where

$$H_K = \sum_{P}(-1)^{\langle\alpha_1,P\rangle\oplus\langle\gamma,E(P,K)\rangle}$$

Thirdly, for each $\alpha_2\in\mathbb{F}_2^{16}$, compute

$$\mathrm{cor}_E((\alpha_1,\alpha_2),\gamma) = \sum_{K}(-1)^{\langle\alpha_1,K\rangle}H_K$$

Forthly, compute η_0 and A_2 from the CLH $\alpha_1\rightarrow\gamma$ by the method to construct ZCGLHs.

The first experiment cost about 2^{32} data complexity, $2^{32}+2^{16}\times 2^{16}=2^{33}$ time complexity and 2^{32} memory complexity. We repeat the experiment by using 10 different CLHs. It turns out that

$$\mathrm{cor}_E((\alpha_1,\alpha_2),\gamma) = \begin{cases} 0, & \alpha_2\notin\eta_0\oplus A_2 \\ \text{uncertain}, & \text{otherwise}\end{cases}$$

Therefore, the result strongly sustains our theory.

The second experiment This experiment is to verify the method to construct ZCGLHs by testing the integral distinguishers of SIMON32/64.

Firstly, given a CLH $\alpha_1\rightarrow\gamma$ of 12-round SIMON32/64, we get an integral distinguisher by using the method. Secondly, set 1000 different key values and go through the space $A^{\perp}$. It turns out that the integral distinguisher is valid for these 1000 keys. So the result promises the correctness of the method.

5. Related-key zero-correlation linear distinguishers of SMION

We apply our method to the SIMON family and the best results can be seen in Table 7. Please refer to the Appendix B for detailed intermediate results.

Our attacks on SIMON only need to use $2n$-bit data that involves $(2n-1)$-bit plaintext and 1-bit related-key. With the cost of a constant memory complexity and 2^{2n} time complexity to compute $\oplus_{(x,K)\in A^{\perp}}\langle\gamma, E(x\oplus\lambda_1, K\oplus\lambda_2)\rangle$, one can distinguish SIMON from a random permutation. Hence, our distinguishing attacks are valid.

Table 7 Related-key zero-correlation and integral distinguishers of SIMON

Version	Round	Related-key	Data	Time	Memory
SIMON32/64	12	1-bit	$O(2^{32})$	$O(2^{32})$	$O(1)$
SIMON48/72	13	1-bit	$O(2^{48})$	$O(2^{48})$	$O(1)$
SIMON48/96	14	1-bit	$O(2^{48})$	$O(2^{48})$	$O(1)$
SIMON64/96	15	1-bit	$O(2^{64})$	$O(2^{64})$	$O(1)$
SIMON64/128	15	1-bit	$O(2^{64})$	$O(2^{64})$	$O(1)$
SIMON96/144	17	1-bit	$O(2^{96})$	$O(2^{96})$	$O(1)$
SIMON128/192	20	1-bit	$O(2^{128})$	$O(2^{128})$	$O(1)$
SIMON128/256	22	1-bit	$O(2^{128})$	$O(2^{128})$	$O(1)$

V. Conclusions

In this paper, with the aid of the related-key model, we present a generalized zero-correlation linear attack both from the theoretical aspect and the practical aspect. More specifically, by studying block ciphers' linear key schedules, we establish the links between the conventional zero-correlation linear attack and the generalized attack. Then we prove that the existence of the generalized zero-correlation linear distinguisher is completely determined by conventional linear approximations and the linear key schedule. Hence, we present a method to construct generalized zero-correlation linear distinguishers. Based on this method, we find zero-correlation linear distinguishers of the SIMON family, which are at least one-round longer than previous zero-correlation linear distinguishers of SIMON.

Our theory further extends zero-correlation linear attacks to the related-key model, which should prompt reasearchers to more cautiously analyse the security of block ciphers with a linear key schedule against the zero-correlation linear attack.

Since the method only involves a cipher's conventional linear hulls and the key schedules, it not only can be applied to several other ciphers, such as SKINNY, QARMA and CHAM, but also works better along with recent developments in the research on linear hulls. Because a more clear discription on linear hulls provide us more possibility to construct zero-correlation and obtain the improvement.

By the way, we believe that the ciphers using nonlinear key schedule might be threatened by related-key zero-correlation linear attacks as well. For instance, Niu *et al.* [10] found related-key zero-correlation linear distinguishers of TWINE and Lblock, whose key schedules are both nonlinear. Though the nonlinear components in key schedules weaken the controlling force of related-key attacks, there might have some information that could be used to cause zero-correlation. It will be an interesting direction for us to do further research.

Acknowledgements

This work was supported by the Natural Science Foundation of Henan (Grant No. 222300420100), the Foundation of Key Laboratory of National Defense Science and Technology (Grant No. 61421030107), and the National Natural Science Foundation of China (Grant Nos. 61802437, 62372463, and 62302518).

Appendix A. Proof of Proposition 1

Lemma 5 Let $F:\mathbb{F}_2^n\times(\mathbb{F}_2^n)^{r+1}\to\mathbb{F}_2^n$ and $E_k(x):=F(x,k)$, then for $(\alpha,\gamma)\in\mathbb{F}_2^n\times\mathbb{F}_2^n$,

$$\mathrm{cor}_{E_k}(\alpha,\gamma)=\sum_{\varLambda\in(\mathbb{F}_2^n)^{r+1}}(-1)^{\langle\varLambda,k\rangle}\mathrm{cor}_F((\alpha,\varLambda),\gamma)$$

Proof

$$\begin{aligned}&\sum_{\varLambda\in(\mathbb{F}_2^n)^{r+1}}(-1)^{\langle\varLambda,k\rangle}\mathrm{cor}_F((\alpha,\varLambda),\gamma)\\&=\frac{1}{2^{nr+2n}}\sum_{\varLambda}(-1)^{\langle\varLambda,k\rangle}\sum_{x,k'}(-1)^{\langle\alpha,x\rangle\oplus\langle\varLambda,k'\rangle\oplus\langle\gamma,F(x,k')\rangle}\\&=\frac{1}{2^{nr+2n}}\sum_{x,k'}(-1)^{\langle\alpha,x\rangle\oplus\langle\gamma,F(x,k')\rangle}\sum_{\varLambda}(-1)^{\langle\varLambda,k\oplus k'\rangle}\\&=\frac{2^{nr+n}}{2^{nr+2n}}\sum_{x,k'=k}(-1)^{\langle\alpha,x\rangle\oplus\langle\gamma,F(x,k')\rangle}\\&=\mathrm{cor}_{E_k}(\alpha,\gamma)\end{aligned}$$

Corollary 5 Let $F:\mathbb{F}_2^n\times(\mathbb{F}_2^n)^{r+1}\to\mathbb{F}_2^n$ and $E_k(x):=F(x,k)$, then for $((\alpha_1,\varLambda),\gamma)\in(\mathbb{F}_2^n\times\mathbb{F}_2^{nr+n})\times\mathbb{F}_2^n$,

$$\mathrm{cor}_F((\alpha,\varLambda),\gamma)=\frac{1}{2^{nr+n}}\sum_{k\in(\mathbb{F}_2^n)^{r+1}}(-1)^{\langle\varLambda,k\rangle}\mathrm{cor}_{E_k}(\alpha,\gamma)$$

Lemma 6 Given

$$\begin{aligned}g_i:\mathbb{F}_2^n\times\mathbb{F}_2^n&\to\mathbb{F}_2^n\\(x,k_i)&\mapsto G_i(x)\oplus k_i\end{aligned}$$

and

$$\begin{aligned}f:\mathbb{F}_2^n\times(\mathbb{F}_2^n\times\mathbb{F}_2^n)&\to\mathbb{F}_2^n\\(x,(k_1,k_2))&\mapsto g_2(g_1(x,k_1),k_2)\end{aligned}$$

then for $((\varGamma_0,(\varLambda_1,\varLambda_2)),\varGamma_2)\in(\mathbb{F}_2^n\times(\mathbb{F}_2^n\times\mathbb{F}_2^n))\times\mathbb{F}_2^n$,

$$\begin{aligned}&\mathrm{cor}_f((\varGamma_0,(\varLambda_1,\varLambda_2)),\varGamma_2)\\&=\sum_{\varGamma_1\in\mathbb{F}_2^n}\mathrm{cor}_{g_1}((\varGamma_0,\varLambda_1),\varGamma_1)\mathrm{cor}_{g_2}((\varGamma_1,\varLambda_2),\varGamma_2)\end{aligned}$$

where $G_i:\mathbb{F}_2^n\to\mathbb{F}_2^n$, $k_i\in\mathbb{F}_2^n$ is constant and $i=1,2$.

Proof

$$\begin{aligned}&\sum_{\varGamma_1\in\mathbb{F}_2^n}\mathrm{cor}_{g_1}((\varGamma_0,\varLambda_1),\varGamma_1)\mathrm{cor}_{g_2}((\varGamma_1,\varLambda_2),\varGamma_2)\\&=\frac{1}{2^{4n}}\sum_{\varGamma_1\in\mathbb{F}_2^n}\sum_{x,k}(-1)^{\langle\varGamma_0,x\rangle\oplus\langle\varLambda_1,k\rangle\oplus\langle\varGamma_1,g_1(x,k)\rangle}\end{aligned}$$

$$\begin{aligned}&\sum_{y,k'}(-1)^{\langle\varGamma_1,y\rangle\oplus\langle\varLambda_2,k'\rangle\oplus\langle\varGamma_2,g_2(y,k')\rangle}\\&=\frac{1}{2^{4n}}\sum_{x,k,y,k'}(-1)^{\langle\varGamma_0,x\rangle\oplus\langle\varLambda_1,k\rangle\oplus\langle\varLambda_2,k'\rangle\oplus\langle\varGamma_2,g_2(y,k')\rangle}\\&\sum_{\varGamma_1\in\mathbb{F}_2^n}(-1)^{\langle\varGamma_1,y\rangle\oplus\langle\varGamma_1,g_1(x,k)\rangle}\\&=\frac{1}{2^{4n}}\sum_{x,k,k'}(-1)^{\langle\varGamma_0,x\rangle\oplus\langle\varLambda_1,k\rangle\oplus\langle\varLambda_2,k'\rangle\oplus\langle\varGamma_2,f(x,(k,k'))\rangle}\\&\sum_{\varGamma_1\in\mathbb{F}_2^n}(-1)^0=\mathrm{cor}_f((\varGamma_0,(\varLambda_1,\varLambda_2)),\varGamma_2)\end{aligned}$$

□

Lemma 7 Given

$$\begin{aligned}g_0:\mathbb{F}_2^n\times\mathbb{F}_2^n&\to\mathbb{F}_2^n\\(x,k_0)&\mapsto G_1(x\oplus k_0)\end{aligned}$$

and

$$\begin{aligned}g_1:\mathbb{F}_2^n\times\mathbb{F}_2^n&\to\mathbb{F}_2^n\\(x,k_1)&\mapsto G_1(x)\oplus k_1\end{aligned}$$

then for $((\varGamma_0,\varGamma_1),(\varLambda_0,\varLambda_1))\in(\mathbb{F}_2^n\times\mathbb{F}_2^n)\times(\mathbb{F}_2^n\times\mathbb{F}_2^n)$,

$$\mathrm{cor}_{g_0}((\varGamma_0,\varLambda_0),\varGamma_1)=\begin{cases}\mathrm{cor}_{G_1}(\varGamma_0,\varGamma_1), & \text{if } \varLambda_0=\varGamma_0\\0, & \text{otherwise}\end{cases}$$

and

$$\mathrm{cor}_{g_1}((\varGamma_0,\varLambda_1),\varGamma_1)=\begin{cases}\mathrm{cor}_{G_1}(\varGamma_0,\varGamma_1), & \text{if } \varLambda_1=\varGamma_1\\0, & \text{otherwise}\end{cases}$$

where $G_1:\mathbb{F}_2^n\to\mathbb{F}_2^n$, and $k_0,k_1\in\mathbb{F}_2^n$ are constants.

Proof

$$\begin{aligned}&\mathrm{cor}_{g_0}((\varGamma_0,\varLambda_0),\varGamma_1)\\&=\frac{1}{2^{2n}}\sum_{x,k}(-1)^{\langle\varGamma_0,x\rangle\oplus\langle\varLambda_0,k\rangle\oplus\langle\varGamma_1,G_0(x,k)\rangle}\\&=\frac{1}{2^{2n}}\sum_{x',k}(-1)^{\langle\varGamma_0,x'\oplus k\rangle\oplus\langle\varLambda_0,k\rangle\oplus\langle\varGamma_1,G_0(x')\rangle}\\&=\frac{1}{2^{2n}}\sum_{x'}(-1)^{\langle\varGamma_0,x'\rangle\oplus\langle\varGamma_1,G_0(x')\rangle}\sum_{k}(-1)^{\langle\varLambda_0\oplus\varGamma_0,k\rangle}\\&=\frac{1}{2^n}\mathrm{cor}_{G_0}(\varGamma_0,\varGamma_1)\sum_{k}(-1)^{\langle\varLambda_0\oplus\varGamma_0,k\rangle}\\&=\begin{cases}\mathrm{cor}_{G_1}(\varGamma_0,\varGamma_1), & \text{if } \varLambda_0=\varGamma_0\\0, & \text{otherwise}\end{cases}\end{aligned}$$

Similarly, we also get

$$\mathrm{cor}_{g_1}((\varGamma_0,\varLambda_1),\varGamma_1)=\begin{cases}\mathrm{cor}_{G_1}(\varGamma_0,\varGamma_1), & \text{if } \varLambda_1=\varGamma_1\\0, & \text{otherwise}\end{cases}$$

Proof of Proposition 1

Let $E(x,k):=E_k(x)$, so

$$E(x,k)=g_r(\cdots(g_2(g_1(x\oplus k_0),k_1),\cdots,k_r),$$

where $g_i(x,k_i)=G_i(x)\oplus k_i$. Then for $(\alpha,\gamma)\in\mathbb{F}_2^n\times\mathbb{F}_2^n$,

$$\begin{aligned}&\mathrm{cor}_{E_k}(\alpha,\gamma)\\&=\sum_{\varLambda\in(\mathbb{F}_2^n)^{r+1}}(-1)^{\langle\varLambda,k\rangle}\mathrm{cor}_E((\alpha,\varLambda),\gamma)\\&=\sum_{\varLambda\in(\mathbb{F}_2^n)^{r+1}}(-1)^{\langle\varLambda,k\rangle}\sum_{\substack{\varGamma=(\varGamma_0,\varGamma_1,\ldots,\varGamma_r)\\\varGamma_0=\alpha,\varGamma_r=\gamma}}\prod_{i=1}^{r}\mathrm{cor}_{g_i}((\varGamma_{i-1},\varLambda_i),\varGamma_i)\\&=\sum_{\substack{\varGamma=(\varGamma_0,\varGamma_1,\ldots,\varGamma_r)\\\varGamma_0=\alpha,\varGamma_r=\gamma}}(-1)^{\langle\varGamma,k\rangle}\prod_{i=1}^{r}\mathrm{cor}_{G_i}(\varGamma_{i-1},\varGamma_i)\end{aligned}$$

Proof of Proposition 2

Let $E(x,k) = F(x, L(k)) = E_{L(k)}(x)$, then

$$\begin{aligned}\mathrm{cor}_E((\alpha_1,\alpha_2),\gamma) &= \frac{1}{2^t}\sum_{mk\in\mathbb{F}_2^t}(-1)^{\langle\alpha_2,mk\rangle}\mathrm{cor}_{E_{L(mk)}}(\alpha_1,\gamma) = \frac{1}{2^t}\sum_{mk\in\mathbb{F}_2^t}(-1)^{\langle\alpha_2,mk\rangle}\sum_{\Lambda=(\Lambda_0,\ldots,\Lambda_r)\in\mathbb{F}_2^{nr+n}}(-1)^{\langle\Lambda,L(mk)\rangle}\mathrm{cor}_F((\alpha_1,\Lambda),\gamma)\\ &= \frac{1}{2^t}\sum_{\Lambda=(\Lambda_0,\ldots,\Lambda_r)\in\mathbb{F}_2^{nr+n}}\mathrm{cor}_F((\alpha_1,\Lambda),\gamma)\sum_{mk\in\mathbb{F}_2^t}(-1)^{\langle\Lambda,L(mk)\rangle\oplus\langle\alpha_2,mk\rangle}\\ &= \frac{1}{2^t}\sum_{\Lambda=(\Lambda_0,\ldots,\Lambda_r)\in\mathbb{F}_2^{nr+n}}\mathrm{cor}_F((\alpha_1,\Lambda),\gamma)\sum_{mk\in\mathbb{F}_2^t}(-1)^{\langle L^{\mathrm{T}}(\Lambda),mk\rangle\oplus\langle\alpha_2,mk\rangle} = \sum_{\substack{\Lambda=(\Lambda_0,\ldots,\Lambda_r)\in\mathbb{F}_2^{nr+n}\\ L^{\mathrm{T}}(\Lambda)=\alpha_2}}\mathrm{cor}_F((\alpha_1,\Lambda),\gamma).\end{aligned}$$

Based on the proof of Proposition 1, we obtain

$$\sum_{\Lambda=(\Lambda_0,\ldots,\Lambda_r)\in\mathbb{F}_2^{nr+n} L^{\mathrm{T}}(\Lambda)=\alpha_2}\mathrm{cor}_F((\alpha_1,\Lambda),\gamma) = \sum_{\Gamma=(\Gamma_0,\ldots,\Gamma_r)\in\mathbb{F}_2^{nr+n}\Gamma_0=\alpha_1,\Gamma_r=\gamma,L^{\mathrm{T}}(\Gamma)=\alpha_2}\prod_{i=1}^{r}\mathrm{cor}_{G_i}(\Gamma_{i-1},\Gamma_i).$$

Appendix B. Distinguishers of SIMON

Here, we display the details of some of the best results we obtained for SIMON32/64, SIMON48/72, SIMON48/96, SIMON64/96, SIMON64/128, SIMON96/144, SIMON128/192, and SIMON128/256.

According to the method to construct ZCGLHs in Section IV.3, given a CLH $\alpha_1 \to \gamma$, we figure out the $A_2^{\perp}$ that satisfies $A_2 \bigcap L^{\mathrm{T}}(\Omega_0) = \varnothing$. In the results below, all η_0 are linearly independent with $\{L_j\}_{j\notin J}$. So we denote the rank of $L^{\mathrm{T}}(\Omega_0)$ by $(s+1)$.

Since $A_2^{\perp}$ is a $(t-1)$-dimensional subspace, we can also figure out a vector ξ that satisfies $\{\xi, \mathbf{0}_t\} = A_2^{\perp}$. Then $A^{\perp} = A_1^{\perp} \times A_2^{\perp}$, where $A_1^{\perp} = \{\alpha_1, \mathbf{0}_{2n}\}$. Therefore, we only list the vector ξ instead of the basis of $A^{\perp}$ for brevity. Note that, the dual subspace of A is not unique when $s < t-1$. It means we can get more plaintext structures to distinguish the cipher when a single plaintext structure is not enough to distinguish.

1) SIMON32/64's 12-round distinguisher

α_1	:	0X 1 0000
γ	:	0X 4
s	:	56
η_0	:	0X E3F2 5045 477A AA78
ξ	:	0X 9224 5CC1 9DE7 7100

2) SIMON48/72's 13-round distinguisher

α_1	:	0X 1000 0000
γ	:	0X 8
s	:	70
η_0	:	0X 9F A120 2099 0743 8C3A
ξ	:	0X 2800 0000 8800 0000

3) SIMON48/96's 14-round distinguisher

α_1	:	0X 100 0000
γ	:	0X 8
s	:	95
η_0	:	0X C399 FD36 6747 7385 D9B4 ADD8
ξ	:	0X 2520 0037 1000 2CE8 001A

4) SIMON64/96's 15-round distinguisher

α_1	:	0X 1 0000 0000
γ	:	0X 400 0000
s	:	95
η_0	:	0X DE17 0DEF 1A0C 3923 29D8 EB04
ξ	:	0X 3C00 0000 0000 0000 0440 000C

5) SIMON64/128's 15-round distinguisher

α_1	:	0X 1 0000 0000
γ	:	0X 8
s	:	123
η_0	:	0X D1F3 BBC6 A7C6 F422 F858 B5AB 6EDF 884D
ξ	:	0X 9000 123B 5800 182A 2400 1E65 7D00 0E50

6) SIMON96/96's 15-round distinguisher

α_1	:	0x 1 0000 0000 0000
γ	:	0X 8
s	:	92
η_0	:	0X 6D17 2926 5D5F 56BC 9137 EA1C
ξ	:	0X E600 0010 D478 B2A0 0001 3212

7) SIMON96/144's 17-round distinguisher

α_1	:	0x 1 0000 0000 0000
γ	:	0X 2
s	:	139
η_0	:	0X 3A32 15F7 157D 4F52 5B11 15A4 A878 1849 1333
ξ	:	0X 2000 0000 0602 0000 0000 001E 6600 0000 00A0

8) SIMON128/128's 18-round distinguisher

α_1	:	0x 1 0000 0000 0000 0000
γ	:	0X 2
s	:	127
η_0	:	0X 199A 29F6 F325 A287 DB59 B9C9 8946 0741
ξ	:	0X 8280 0000 0280 2B83 5078 0000 287A A7D8

9) SIMON128/192's 20-round distinguisher

α_1	:	0x 1 0000 0000 0000 0000
γ	:	0X 200
s	:	187
η_0	:	0X 4164 B0FB 5103 0CF3 4799 E1A9 DF9B 4F15 E881 6FC9 E47B 7A08
ξ	:	0X 4000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0002

10) SIMON128/256's 22-round distinguisher

α_1	:	0x 1 0000 0000 0000 0000
γ	:	0x 400 0000 0000 0000
s	:	255
η_0	:	0X 4FD7 E1AB E9E5 EA7E FAB6 024B E569 FAA5 811D CD81 D617 8878 35DA F955 F003 7762
ξ	:	0x 2195 0000 0000 0003 9722 6000 0000 0002 227D 2000 0000 0000 7D4A

References

[1] L. R. Knudsen, "Cryptanalysis of loki 91," in *Proceedings of International Workshop on the Theory and Application of Cryptographic Techniques*, Queensland, Australia, pp.196–208, 1992.

[2] E. Biham, "New types of cryptanalytic attacks using related keys," *Journal of Cryptology*, vol. 7, no. 4, pp. 229–246, 1994.

[3] A. Bogdanov, C. Boura, V. Rijmen, *et al.*, "Key difference invariant bias in block ciphers," in *Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security*, Bengaluru, India, pp.357–376, 2013.

[4] J. K. Lee, B. Koo, and W. H. Kim, "A general framework for

the related-key linear attack against block ciphers with linear key schedules," in *Proceedings of the 26th International Conference on Selected Areas in Cryptography*, Waterloo, ON, Canada, pp.194–224, 2019.

[5] W. Q. Cao and W. T. Zhang, "Multidimensional linear cryptanalysis with key difference invariant bias for block ciphers," *Cybersecurity*, vol. 4, no. 1, article no. 32, 2021.

[6] 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.

[7] M. Hermelin, J. Y. Cho, and K. Nyberg, "Multidimensional linear cryptanalysis," *Journal of Cryptology*, vol. 32, no. 1, pp. 1–34, 2019.

[8] A. Bogdanov, G. Leander, K. Nyberg, *et al.*, "Integral and multidimensional linear distinguishers with correlation zero," in *Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security*, Beijing, China, pp.244–261, 2012.

[9] R. Ankele, C. Dobraunig, J. Guo, *et al.*, "Zero-correlation attacks on tweakable block ciphers with linear tweakey expansion," *IACR Transactions on Symmetric Cryptology*, vol. 2019, no. 1, pp. 192–235, 2019.

[10] C. Niu, M. Z. Li, S. W. Sun, *et al.*, "Zero-correlation linear cryptanalysis with equal treatment for plaintexts and tweakeys," in *Proceedings of Cryptographers' Track at the RSA Conference*, Virtual Event, pp.126–147, 2021.

[11] R. Beaulieu, D. Shors, J. Smith, *et al.*, "The simon and speck families of lightweight block ciphers," *Cryptology ePrint Archive*, in press, 2013.

[12] M. Matsui, "On correlation between the order of S-boxes and the strength of DES," in *Proceedings of Workshop on the Theory and Application of of Cryptographic Techniques*, Perugia, Italy, pp.366–375, 1994.

[13] Z. B. Liu, Y. Q. Li, L. Jiao, *et al.*, "On the upper bound of squared correlation of simon-like functions and its applications," *IET Information Security*, vol. 16, no. 3, pp. 220–234, 2022.

[14] Z. B. Liu, Y. Q. Li, and M. S. Wang, "Optimal differential trails in SIMON-like ciphers," *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 1, pp. 358–379, 2017.

[15] Y. Todo and M. Morii, "Bit-based division property and application to SIMON family," in *Proceedings of the 23rd International Conference on Fast Software Encryption*, Bochum, Germany, pp.357–377, 2016.

[16] Z. J. Xiang, W. T. Zhang, Z. Z. Bao, *et al.*, "Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers," in *Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security*, Hanoi, Vietnam, pp.648–678, 2016.

[17] S. P. Wang, B. Hu, J. Guan, *et al.*, "Exploring secret keys in searching integral distinguishers based on division property," *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. 3, pp. 288–304, 2020.

[18] L. Sun, K. Fu, and M. Q. Wang, "Improved zero-correlation cryptanalysis on SIMON," in *Proceedings of the 11th International Conference on Information Security and Cryptology*, Beijing, China, pp.125–143, 2015.

[19] X. L. Yu, W. L. Wu, Z. Q. Shi, *et al.*, "Zero-correlation linear cryptanalysis of reduced-round SIMON," *Journal of Computer Science and Technology*, vol. 30, no. 6, pp. 1358–1369, 2015.

[20] Q. J. Wang, Z. Q. Liu, K. Varıcı, *et al.*, "Cryptanalysis of reduced-round SIMON32 and SIMON48," in *Proceedings of the 15th International Conference on Cryptology in India*, New Delhi, India, pp.143–160, 2014.

[21] K. Nyberg, "Correlation theorems in cryptanalysis," *Discrete Applied Mathematics*, vol. 111, no. 1-2, pp. 177–188, 2001.

[22] M. Matsui, "The first experimental cryptanalysis of the data encryption standard," in *Proceedings of the 14th Annual International Cryptology Conference*, Santa Barbara, CA, USA, pp.1–11, 1994.

[23] T. Kranz, G. Leander, and F. Wiemer, "Linear cryptanalysis: Key schedules and tweakable block ciphers," *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 1, pp. 474–505, 2017.

[24] B. Sun, Z. Q. Liu, V. Rijmen, *et al.*, "Links among impossible differential, integral and zero correlation linear cryptanalysis," in *Proceedings of the 35th Annual Cryptology Conference*, Santa Barbara, CA, USA, pp.95–115, 2015.

[25] E. Biham, "On Matsui's linear cryptanalysis," in *Proceedings of Workshop on the Theory and Application of Cryptographic Techniques*, Perugia, Italy, pp.341–355, 1994.

Yi ZHANG received the B.S. degree in cryptology from PLA SSF Information Engineering University, Zhengzhou, China, in 2016. He is currently studing for the M.S. degree in the Department of Applied Mathematics, PLA SSF Information Engineering University, Zhengzhou, China. His current research interests include block cipher design and cryptanalysis.
(Email: yizhang0796@foxmail.com)

Kai ZHANG received the Ph.D. degree in cryptology from the Information Science and Technology Institute, Zhengzhou, China, in 2016. His main research interests include design and analysis of symmetric ciphers. His works have been published in several refereed journals and he has been serving as a referee for several famous international journals in the area of information security and cryptology.
(Email: zhkai2010@139.com)

Ting CUI is currently a Professor at the Department of Applied Mathematics, PLA SSF Information Engineering University, China. His current research interests include cryptography and cyberspace security. His works have been published in several refereed journals and he has been serving as a referee for several famous international journals in the area of information security and cryptology.
(Email: cuiting_1209@hotmail.com)