Hindawi
IET Information Security
Volume 2024, Article ID 2939486, 15 pages
https://doi.org/10.1049/2024/2939486

Research Article

Unveiling the Neutral Difference and Its Automated Search

Guangqiu Lv, Chenhui Jin, Zhen Shi, and Ting Cui

PLA SSF Information Engineering University, Zhengzhou 450000, Henan, China

Correspondence should be addressed to Ting Cui; cuiting_1209@126.com

Received 15 February 2024; Revised 24 April 2024; Accepted 26 April 2024; Published 14 May 2024

Academic Editor: Qichun Wang

Given a differential characteristic and an existing plaintext pair that satisfies it (referred to as a right pair), generating additional right pairs at a reduced cost is an appealing prospect. The neutral bit technique, referred to as neutral differences throughout this paper, provides a solution to this challenge. Traditionally, the search for neutral differences has heavily depended on experimental testing, leading to limitations in the search range. In this work, we propose the neutral difference table and establish a link between boomerang cryptanalysis and neutral differences. Furthermore, we propose an automated search for neutral differences to address the problem of a limited search range of neutral differences, as previous approaches relied on experimental testing. This approach provides a basis for the subspace spanned by the neutral differences, and we apply this technique to both SPECK32 and LEA, where the predicted results closely match the experimental ones. Consequently, we present the improved differential-linear distinguishers for SPECK32 and LEA, along with the 18-round attacks on LEA192 and LEA256 with the lowest time complexity up to date.

1. Introduction

Differential cryptanalysis, proposed by Biham and Shamir [1], is one of the most powerful cryptanalysis techniques nowadays. As cryptanalysis progresses, an intriguing phenomenon related to differentials has captured the attention of researchers. For a differential $\Delta \rightarrow \Delta'$, when flipping a single bit or a set of bits simultaneously for an input x, the resulted input $x \oplus \nabla$ makes the differential $\Delta \rightarrow \Delta'$ established if and only if x makes it satisfied. In this paper, ∇ is referred to as a neutral difference. Previous literatures [2, 3] referred to it as a neutral bit when the Hamming weight of ∇ is 1 and a neutral set otherwise. The neutral difference technique holds significant prominence today, having contributed to the advancement of numerous cryptanalysis records [3–8].

However, the search for neutral differences of a differential lacks elegant methods except for exhaustion with experiments based on its definition [3–5, 9, 10]. This has led to the difficulty in finding more neutral differences. Therefore, there is an urgent need to develop automatic tools for searching neutral differences. We aim to dedicate ourselves to this problem and related cryptanalysis. The neutral probability of a neutral difference ∇ for a differential $\Delta \rightarrow \Delta'$ is defined as follows:

$$p = \frac{\#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta) = \Delta', S(x \oplus \nabla) \oplus S(x \oplus \nabla \oplus \Delta) = \Delta'\}}{\#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta) = \Delta'\}}, \tag{1}$$

where # represents the size of the set and S is a substitution.

1.1. Contribution. We establish links between neutral differences and boomerang cryptanalysis, thereby providing a theoretical foundation for the search of neutral differences. Based on this, we introduce an automatic search method for linearly independent neutral differences. As for applications, we present the neutral spaces for two differentials of SPECK32, which are spanned by all neutral differences with non-zero neutral probabilities. Experimental results confirm

Table 1: Comparison of our distinguishers with previous ones.

Cipher	Weak keys	Type	Round	Prob./Cor.	Ref.
SPECK32	Full	Linear	9	2^{-14}	[11]
		DL	9	$2^{-8.93}$	[12]
		Differential	10	$2^{-30.39}$	[13]
		Boomerang	10	$2^{-29.15}$	[14]
		DL	10	$2^{-13.90}$	[12]
		DL (ND)	10	-2^{-11}	[9]
		DL	11	$2^{-16.0}$	[9]
		DL (ND)	11	$-2^{-14.5}$	[9]
		DL (ND)	11	$-2^{-14.18}$	This work
		DL (ND)	11	$-2^{-13.07}$	This work
LEA	Full	Boomerang	16	$2^{-117.11}$	[15]
		DL (ND)	16	$-2^{-28.04}$	[6]
		DL	17	$-2^{-59.04}$	[6]
		DL (ND)	17	$-2^{-52.79}$	This work

DL = differential-linear distinguishers, DL (ND) = DL distinguishers combined with neutral difference technique, DC = differential characteristic, LC = linear characteristic.

Table 2: Key recovery attacks on round-reduced LEA.

Cipher	Round	Type	Data (CP)	Time	Ref.
LEA192	14/28	DC	$2^{124.79}$	$2^{124.79}$	[16]
	18/28	DL	$2^{126.63}$	$2^{189.63}$	[6]
	18/28	DL (ND)	$2^{124.96}$	$2^{180.80}$	This work
LEA256	15/32	DC	$2^{124.79}$	$2^{252.79}$	[16]
	18/32	DL	$2^{126.63}$	$2^{189.63}$	[6]
	18/32	DL (ND)	$2^{124.96}$	$2^{180.80}$	This work

DL = differential-linear distinguishers, DL (ND) = DL distinguishers combined with neutral difference technique, DC = differential cryptanalysis, CP = chosen-plaintexts.

Table 3: Notations.

Symbol	Description
$x[i]$	The ith bit of x, written as x_i for simplicity. x_{n-1} (resp. x_0) is the most (resp. least) significant bit of x
$x \lll t$	Rotation of x by t-bit to the left, written as $\overleftarrow{x}$ for simplicity
$x \ggg t$	Rotation of x by t-bit to the right, written as $\overrightarrow{x}$ for simplicity
$\cdot$	The inner product of two vectors
$\#\mathcal{X}$ or $\lvert\mathcal{X}\rvert$	The size of a set $\mathcal{X}$
$Pr[x=0]$	Probability that x equals 0
$Cor[x]$	The correlation of x, i.e., $Cor[x]=Pr[x=0]-Pr[x=1]$
$x\|y$	Concatenation operation. x_{n-1} is the most significant bit of the new binary vector

the validity of our method. Furthermore, we present improved differential-linear distinguishers for 11-round SPECK32 and 17-round LEA (illustrated in Table 1), as well as the 18-round attacks on LEA192 and LEA256 with the lowest time complexity (outlined in Table 2) up to date.

1.2. Organization. The remainder of this paper is organized as follows: Section 2 introduces the notations and concepts that will be used throughout the paper. Section 3 establishes the links between boomerang cryptanalysis and neutral differences and presents an automatic method for discovering neutral differences. Sections 4 and 5 apply the automatic search method to the SPECK32 and LEA ciphers. Finally, Section 6 concludes this paper.

2. Notations and Preliminaries

The notations we use in this paper are summarized in Table 3.

2.1. Preliminaries

Definition 1 (Differential Probability [1]). The probability of a differential $\Delta \rightarrow \Delta'$ for function $S:\mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is defined by the following:

$$p(\Delta,\Delta') = \frac{\#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta) = \Delta'\}}{2^n}. \tag{2}$$

Definition 2 (DDT). Let S be a substitution. The value of differential distribution table (DDT) at (Δ,Δ') is defined as follows:

$$\mathrm{DDT}_S(\Delta,\Delta') = \#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta) = \Delta'\}. \tag{3}$$

Definition 3 (NDT). Let S be a substitution. The value of neutral difference table (NDT) at (Δ,Δ',∇) is defined as follows:

$$\begin{aligned}\mathrm{NDT}\ _S(\Delta,\Delta',\nabla) = \#\{x \in \mathbb{F}_2^n |\ S(x) \oplus S(x \oplus \Delta) \\ = \Delta', S(x \oplus \nabla) \oplus S(x \oplus \nabla \oplus \Delta) = \Delta'\}\end{aligned} \tag{4}$$

Here, ∇ is called a neutral difference throughout this paper.

Definition 4 (Neutral Probability). Let S be a substitution. For a differential of S, denoted by $\Delta \rightarrow \Delta'$, ∇ is called a neutral difference for this differential, and the corresponding neutral probability is defined as follows:

$$\begin{aligned}p &= \frac{\#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta) = \Delta', S(x \oplus \nabla) \oplus S(x \oplus \nabla \oplus \Delta) = \Delta'\}}{\#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta) = \Delta'\}} \\ &= \frac{\mathrm{NDT}_S(\Delta,\Delta',\nabla)}{\mathrm{DDT}_S(\Delta,\Delta')}\end{aligned}. \tag{5}$$

In general, the higher the neutral probability p becomes, the more useful a neutral difference ∇ is for an attack. Bao et al. [3] have further suggested a way to amplify the neutral probability by introducing conditional neutral differences, which necessitate specific conditions to be met by input pairs. These proposed conditions are evaluated through experiments in [3].

Definition 5 (Plaintext Pair Structure). Denote m linearly independent neutral differences of a differential $(\Delta_{in},\Delta_{out})$ by $M_1, M_2, \ldots, M_m$. Let Ω be the linear subspace spanned by $M_1, M_2, \ldots, M_m$. Given a plaintext x, we define the plaintext pair structure $P_{x,\Omega,\Delta_{in}}$ as the set $\{(x \oplus y, x \oplus y \oplus \Delta_{in}) | y \in \Omega\}$.

Definition 6 (BCT [17]). Let S be a substitution and S^{-1} be its inverse. The value of boomerang connectivity table (BCT) at (Δ,∇) is defined as follows:

$$\begin{aligned}&\mathrm{BCT}_S(\Delta,\nabla) \\ &\quad = \#\{x \in \mathbb{F}_2^n | S^{-1}(S(x)) \oplus \nabla \oplus S^{-1}(S(x \oplus \Delta) \oplus \nabla) = \Delta\}.\end{aligned} \tag{6}$$

Definition 7 (UBCT/LBCT/EBCT [18]). Let S be a substitution and S^{-1} be its inverse. The values of three variants of BCT, namely upper BCT, lower BCT, and extended BCT, are defined, respectively, as follows:

$$\begin{aligned}&\mathrm{UBCT}_S(\Delta,\Delta',\nabla) \\ &= \#\left\{ x \in \mathbb{F}_2^n \middle| \begin{array}{l} S(x) \oplus S(x \oplus \Delta) = \Delta', \\ S^{-1}(S(x) \oplus \nabla) \oplus S^{-1}(S(x \oplus \Delta) \oplus \nabla) = \Delta \end{array} \right\},\end{aligned} \tag{7}$$

$$\begin{aligned}&\mathrm{LBCT}_S(\Delta,\nabla',\nabla) \\ &= \#\left\{ x \in \mathbb{F}_2^n \middle| \begin{array}{l} S(x) \oplus S(x \oplus \nabla') = \nabla, \\ S^{-1}(S(x) \oplus \nabla) \oplus S^{-1}(S(x \oplus \Delta) \oplus \nabla) = \Delta \end{array} \right\},\end{aligned} \tag{8}$$

$$\begin{aligned}&\mathrm{EBCT}_S(\Delta,\Delta',\nabla',\nabla) \\ &= \#\left\{ x \in \mathbb{F}_2^n \middle| \begin{array}{l} S(x) \oplus S(x \oplus \Delta) = \Delta', \\ S(x) \oplus S(x \oplus \nabla') = \nabla, \\ S^{-1}(S(x) \oplus \nabla) \oplus S^{-1}(S(x \oplus \Delta) \oplus \nabla) = \Delta \end{array} \right\}.\end{aligned} \tag{9}$$

If the substitution S can be known from the context, the symbol S will be omitted. For example, DDT_S will be abbreviated as DDT.

3. Links to Boomerang Cryptanalysis and the Automated Search for Neutral Differences

In this section, we prove that the NDT is the LBCT in Boomerang cryptanalysis, which provides a foundation for automated search of neutral differences. Furthermore, we introduce an automatic search method for linearly independent neutral differences.

3.1. Links between Boomerang Cryptanalysis and Neural Difference. In this section, we present the links between neutral difference and boomerang cryptanalysis in Theorem 1 and how to calculate the neutral probability of neutral differences through LBCT in Corollary 1.

Theorem 1. *Let S be a substitution. There holds*

$$\mathrm{NDT}_S(\Delta,\Delta',\nabla) = \mathrm{LBCT}_S(\nabla,\Delta,\Delta'). \tag{10}$$

Proof. It is obvious that $S(x) \oplus S(x \oplus \Delta) = \Delta'$ if and only if $S^{-1}(S(x) \oplus \Delta') = x \oplus \Delta$. If x satisfies that $S(x) \oplus S(x \oplus \Delta) = \Delta'$, then we have the following:

$$\begin{aligned} &S(x \oplus \nabla) \oplus S(x \oplus \nabla \oplus \Delta) \\ &\quad = \Delta' \Leftrightarrow S^{-1}(S(x) \oplus \Delta') \oplus S^{-1}(S(x \oplus \nabla) \oplus \Delta') = \nabla. \end{aligned} \tag{11}$$

Therefore, there holds $\mathrm{NDT}_S(\Delta, \Delta', \nabla) = \mathrm{LBCT}_S(\nabla, \Delta, \Delta')$. □

Theorem 2. *Let S be a substitution and S^{-1} be its inverse. There holds*

$$\mathrm{NDT}_S(\Delta, \Delta', \nabla) = \mathrm{UBCT}_{S^{-1}}(\Delta', \Delta, \nabla). \tag{12}$$

Proof. We have

$$\begin{aligned} \mathrm{LBCT}_S(\Delta, \nabla', \nabla) &= \# \left\{ x \in \mathbb{F}_2^n \,\middle|\, \begin{array}{c} S(x) \oplus S(x \oplus \nabla') = \nabla, \\ S^{-1}(S(x) \oplus \nabla) \oplus S^{-1}(S(x \oplus \Delta) \oplus \nabla) = \Delta \end{array} \right\} \\ &\overset{y=S(x)}{=} \# \left\{ y \in \mathbb{F}_2^n \,\middle|\, \begin{array}{c} y \oplus \nabla = S(S^{-1}(y) \oplus \nabla'), \\ S^{-1}(y \oplus \nabla) \oplus S^{-1}(S(S^{-1}(y) \oplus \Delta) \oplus \nabla) = \Delta \end{array} \right\} \\ &= \# \left\{ y \in \mathbb{F}_2^n \,\middle|\, \begin{array}{c} S^{-1}(y \oplus \nabla) \oplus S^{-1}(y) = \oplus \nabla', \\ S^{-1}(S(S^{-1}(y) \oplus \Delta) \oplus \nabla) = S^{-1}(y \oplus \nabla) \oplus \Delta \end{array} \right\} \\ &= \# \left\{ y \in \mathbb{F}_2^n \,\middle|\, \begin{array}{c} S^{-1}(y \oplus \nabla) \oplus S^{-1}(y) = \oplus \nabla', \\ S(S^{-1}(y) \oplus \Delta) \oplus S(S^{-1}(y \oplus \nabla) \oplus \Delta) = \nabla \end{array} \right\} \\ &= \mathrm{UBCT}_{S^{-1}}(\nabla, \nabla', \Delta) \end{aligned} \quad . \tag{13}$$

According to Theorem 1, we have $\mathrm{NDT}_S(\Delta, \Delta', \nabla) = \mathrm{UBCT}_{S^{-1}}(\Delta', \Delta, \nabla)$. □

Theorem 1 demonstrates that the NDT entries of a substitution S are the entries of LBCT. A similar result connecting the NDT with the UBCT is provided in Theorem 2. For notational simplicity, we shall primarily focus on LBCT in our subsequent theoretical developments. Consequently, one can identify neutral differences with a high neutral probability by concurrently constructing models/programs for LBCT and DDT, as presented in Section 3.2, where an automated method of searching for neutral differences is introduced.

Corollary 1. *For a differential $\Delta \to \Delta'$ of a substitution S, the neutral probability of a neutral difference ∇ can be calculated as follows:*

$$p = \frac{\mathrm{NDT}_S(\Delta, \Delta', \nabla)}{\mathrm{DDT}_S(\Delta, \Delta')} = \frac{\mathrm{LBCT}_S(\nabla, \Delta, \Delta')}{\mathrm{DDT}_S(\Delta, \Delta')} . \tag{14}$$

Lemma 1. *Let $S: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a bijection. For a neutral difference ∇ of a differential (Δ, Δ') with a non-zero probability, if $\mathrm{BCT}_S(\nabla, \Delta') = 2^n$ or $\mathrm{DDT}_S(\Delta, \Delta') = 2^n$, then the corresponding neutral probability p is 1.*

Proof. Let $\mathrm{DDT}_S(\Delta, \Delta') = 2^n$. For each $x \in \mathbb{F}_2^n$, it holds that $S(x) \oplus S(x \oplus \Delta) = \Delta'$. Hence, we have $S(x \oplus \nabla) \oplus S(x \oplus \nabla \oplus \Delta) = \Delta'$, which indicates $p = 1$ by Definition 4.

Let $\mathrm{BCT}_S(\nabla, \Delta') = 2^n$. For each $x \in \mathbb{F}_2^n$, it holds $S^{-1}(S(x) \oplus \Delta') \oplus S^{-1}(S(x \oplus \nabla) \oplus \Delta') = \nabla$. By Theorem 1, we have $\mathrm{NDT}_S(\Delta, \Delta', \nabla) = \mathrm{DDT}_S(\Delta, \Delta')$. Hence, $p = 1$ by Definition 4. □

By constraining the input variable x to a small set $\mathcal{X}$ instead of $x \in \mathbb{F}_2^n$, we can increase the neutral probability p. In this case, the neutral difference ∇ is referred to as a conditional neutral difference, which was first proposed in [3]. Lemma 2 provides sufficient conditions, under which the neutral probability is 1, by imposing restrictions on the input variable x.

Lemma 2. *Let $S: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a bijection. For a non-zero probability differential (Δ, Δ'), the neutral probability of a conditional neutral difference ∇, which requires the input of S limited to a set $\mathcal{X}$, will be 1 if $\mathrm{BCT}_S(\nabla, \Delta') = |\mathcal{X}|$ or $\mathrm{DDT}_S(\Delta, \Delta') = |\mathcal{X}|$.*

Proof. The proof process is similar to that of Lemma 1. □

3.2. Basic Framework for Automated Search of Neutral Differences

3.2. Basic Framework for Automated Search of Neutral Differences. In this section, we aim to merge the automated search for differentials and EBCT characteristics in order to effectively find neutral differences with a higher probability for a given differential $\Delta \to \Delta'$. Experimental results in Section 4 confirm the validity of our method, with the predicted neural probabilities being close to the experimental ones.

First, we introduce the notations that will be used in this discussion. Let the cipher S be a composition of $S_0, S_1, \ldots, S_{l-1}$. Throughout this paper, the term "characteristic" refers to a differential/boomerang path, which not only specifies the input and output differences but also specifies the intermediate differences. For clarity, we will use $\varDelta_0$, $\varDelta_l$, and ∇_0 to refer to $\varDelta$, $\varDelta'$, and ∇, respectively.

Assuming that the cipher is a Markov cipher and the characteristic with the largest probability for a differential $\varDelta_0 \rightarrow \varDelta_l$ determines the differential probability, it is well-known [19] that:

$$p(\varDelta_0 \rightarrow \varDelta_l) \approx \max_{\varDelta_1,\ldots,\varDelta_{l-1}\in\mathbb{F}_2^n} \prod_{0\leq i\leq l-1} p(\varDelta_i \rightarrow \varDelta_{i+1}). \tag{15}$$

Delaune et al. [18] used Equation (16) to estimate $\mathrm{LBCT}_S(\nabla_0, \varDelta_0, \varDelta_l)$.

$$\begin{aligned}&\mathrm{LBCT}_{\,S}(\nabla_0, \varDelta_0, \varDelta_l)\\ &\quad\approx \sum_{\nabla_1,\ldots,\nabla_l,\varDelta_1,\ldots,\varDelta_{l-1}\in\mathbb{F}_2^n} \prod_{0\leqslant i\leqslant l-1} \mathrm{EBCT}_{\,S_i}(\nabla_i, \nabla_{i+1}, \varDelta_i, \varDelta_{i+1}).\end{aligned} \tag{16}$$

In other words, LBCT characteristics can be approximated by a cluster of EBCT characteristics. According to Definitions 1 and 2, there holds $p(\varDelta_0, \varDelta_l) = \frac{\mathrm{DDT}_S(\varDelta_0, \varDelta_l)}{2^n}$. Based on Equations (15) and (16), the neutral probability of the neutral difference ∇_0 for a differential $\varDelta_0 \rightarrow \varDelta_l$ can be calculated by the following:

$$\begin{aligned}p &= \frac{\mathrm{LBCT}_S(\nabla_0, \varDelta_0, \varDelta_l)}{\mathrm{DDT}_S(\varDelta_0, \varDelta_l)} = \frac{\mathrm{LBCT}_S(\nabla_0, \varDelta_0, \varDelta_l)/2^n}{\mathrm{DDT}_S(\varDelta_0, \varDelta_l)/2^n} = \frac{\mathrm{LBCT}_S(\nabla_0, \varDelta_0, \varDelta_l)/2^n}{p(\varDelta_0, \varDelta_l)}\\ &\approx \frac{2^{-n} \sum\limits_{\nabla_1,\ldots,\nabla_l\in\mathbb{F}_2^n} \prod\limits_{0\leqslant i\leqslant l-1} \mathrm{EBCT}_{\,S_i}(\nabla_i, \nabla_{i+1}, \varDelta_i, \varDelta_{i+1})}{\prod\limits_{0\leq i\leq l-1} p(\varDelta_i \rightarrow \varDelta_{i+1})}.\end{aligned} \tag{17}$$

Here, $\varDelta_0 \rightarrow \varDelta_1 \rightarrow \cdots \rightarrow \varDelta_l$ refers to the differential characteristic that dominantly determines the probability of the differential $\varDelta_0 \rightarrow \varDelta_l$, and also partially determines the EBCT characteristics.

The objective of the automated search is to identify a set of differences that maximizes the neutral probability, as defined by Equation (17). This neutral probability serves as the objective function for this automated search problem. By leveraging Equation (17), we can integrate the automated search for differential characteristics and extended boomerang characteristics to uncover a neural difference ∇. The problem of automatically finding differential characteristics $\varDelta_0 \rightarrow \varDelta_l$ has been effectively addressed in previous works such as [11, 19–23]. Similarly, the automatic search for boomerang characteristics has been successfully tackled in [14, 17, 18]. Since this paper does not focus on facilitating the automatic search for boomerang or differential cryptanalysis, we will omit the specific details related to these methods.

Let $\varDelta_0 \rightarrow \varDelta_1 \rightarrow \cdots \rightarrow \varDelta_l$ be the differential characteristic that dominantly determines the probability of the differential $\varDelta_0 \rightarrow \varDelta_l$. Additionally, let $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ be m linearly independent neutral differences for this differential $\varDelta_0 \rightarrow \varDelta_l$ and $\varOmega = Span\{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$. The following framework outlines the process for searching for a new neutral difference that is linearly independent of $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$.

Step 1: In the search model, specify the differences used in the EBCT trail, namely $(\nabla_0, \varDelta_0), (\nabla_1, \varDelta_1), \ldots, (\nabla_l, \varDelta_l)$. To ensure the expected propagation of differences, set $\varDelta_0, \varDelta_1, \ldots, \varDelta_l$ as known values.

Step 2: Introduce constraints to prevent ∇_0 from being selected in $\varOmega$. This ensures that the newly discovered neutral difference will be linearly independent of $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$. An efficient approach for achieving this is presented in Section 3.3.

Step 3: Characterize the relationships between differences in the EBCT trails and differential trails. Using this search model, the solvers will return a solution of $(\nabla_0, \varDelta_0), (\nabla_1, \varDelta_1), \ldots, (\nabla_l, \varDelta_l)$ with the maximum neutral probability.

Upon completion of the above process, a new neutral difference for the differential $\varDelta_0 \rightarrow \varDelta_l$, denoted by α_m, will be obtained. The neutral probability is estimated through an EBCT trail, and Equation (17) suggests that intermediate differences should be enumerated. Consequently, to obtain a more precise estimation of the neutral probability, one can iterate the aforementioned process to discover additional EBCT trails. In such cases, Step 2 is modified as follows:

Step 2: Set $\nabla_0 = \alpha_m$ and introduce constraints to exclude the previously found EBCT trails.

We constructed an automatic search model based on the Boolean satisfiability problem (SAT), and the source code of this paper is publicly available at https://github.com/PigInTheSky1234/Unveiling-the-Neutral-Difference-and-Its-Automated-Search.

Remark 1. It is possible to calculate the probability of LBCT by directly connecting a single LBCT trail for one round with a differential trail for the remaining rounds. However, at FSE 2022, Kidmose and Tiessen [24] pointed out a crucial issue with this approach: when calculating boomerang probabilities, directly connecting differential trails may result in trails with a zero probability. To address this, they introduced the concept of 3-difference trails. Notably, a 3-difference trail can be viewed as a manifestation of an EBCT trail. Therefore, to achieve a more precise probability estimation, we use EBCT trails to calculate the probabilities of LBCT trails.

3.3. The Method of Excluding a Linear Space from $\mathbb{F}_2^n$. As far as we know, in differential-linear/neural cryptanalysis, it is common to use multiple neutral differences simultaneously, which forms a neutral space spanned by these differences. If one wants to exclude all 2^m neutral differences point by point with 2^m constraints to find a neutral difference, the computational burden of the solver would be greatly increased. Next, we will give a solution to this problem with only one constraint. Let m linearly independent neutral differences be $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$. Denote the neutral space spanned by these neutral differences as Ω and the remaining space as $\mathbb{F}_2^n/\Omega$. In this section, we will demonstrate how to identify neutral differences for a given differential $\varDelta_0 \rightarrow \varDelta_l$ within $\mathbb{F}_2^n/\Omega$ using existing solvers.

Theorem 3. *Let $e_i = 1 \lll i$ and $\Omega = Span\{e_0, e_1, \ldots, e_{m-1}\}$. There holds that*

$$x \in \mathbb{F}_2^n/\Omega \Leftrightarrow \sum_{i=m}^{n-1} x[i] > 0. \tag{18}$$

Proof. The necessary and sufficient condition for $x \in \Omega$ is that $x[m] = x[m+1] = \cdots = x[n-1] = 0$, which proves the above. □

Theorem 4. *Let $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ be m linearly independent neutral differences and $\Omega = Span\{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$. Let φ: $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a linear bijection and $\varphi(\alpha_i) = e_i$ for $0 \leq i < m$. There holds that*

$$x \in \mathbb{F}_2^n/\Omega \Leftrightarrow \left[\sum_{i=m}^{n-1} \varphi(x)[i]\right] > 0. \tag{19}$$

Proof. Let $V = Span\{e_0, e_1, \ldots, e_{m-1}\}$. Since φ is a linear bijection, it holds that $x \in \Omega \Leftrightarrow \varphi(x) \in \varphi(\Omega) = V$. By Theorem 3, this theorem holds. □

The following is a construction method for the linear bijection $\varphi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. Let $\varphi(x) = Ax$ and $B = A^{-1}$. A is a $n \times n$ binary inverse matrix. $\varphi(\alpha_i) = e_i$ indicates that $\alpha_i = \varphi^{-1}(e_i) = Be_i = B_i$, where B_i is the ith column of B. Therefore, $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ are the first m columns of B. Ensuring the matrix B is invertible means that the linear bijection $\varphi(x) = B^{-1}x$ is obtained, which is easy by the linear algebra techniques.

Once another neutral difference α_m is obtaining, the $(m+1)$-th column of B is replaced by α_m. Once again, ensuring the matrix B to be invertible will lead to an updated linear bijection $\varphi(x) = B^{-1}x$. The number of constraints excluding Ω spanned by m neutral differences is reduced from the original 2^m to 1, as stated in Theorem 4.

4. Application to SPECK

First, we apply the automatic search technique of neutral difference to SPECK32 and experimentally validate its effectiveness. Second, we enhance the differential-linear distinguishers for 11-round SPECK32 by incorporating neutral differences, resulting in increased absolute values of correlations.

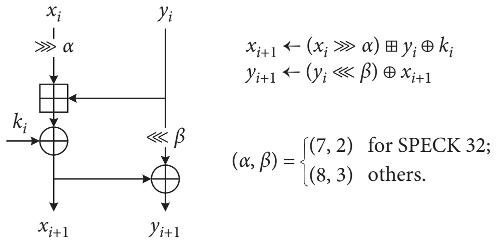

x_i
y_i
$\ggg \alpha$
k_i
$\lll \beta$
x_{i+1}
y_{i+1}
$x_{i+1} \leftarrow (x_i \ggg \alpha) \boxplus y_i \oplus k_i$
$y_{i+1} \leftarrow (y_i \lll \beta) \oplus x_{i+1}$
$(\alpha, \beta) = \begin{cases} (7,2) & \text{for SPECK 32;} \\ (8,3) & \text{others.} \end{cases}$

FIGURE 1: The SPECK instance.

4.1. SPECK. SPECK is a lightweight block cipher designed by the US National Security Agency, whose round function is depicted in Figure 1. For word size $n \in \{16, 24, 32, 48, 64\}$, each variant is identified by SPECK$2n/mn$, where $2n$ is its block size and mn is the key size. The rotation constants are $\alpha = 7$ and $\beta = 2$ for SPECK32 with 64-bit key, while $\alpha = 8$ and $\beta = 3$ for the others. Since we do not facilitate properties of the key schedules, their details are omitted.

4.2. The Neutral Subspaces for Two 2-Round Differentials. For SPECK32, there is a 2-round differential characteristic $0x0209\_0604 \rightarrow 0x1800\_0010 \rightarrow 0x0040\_0000$ with a probability of 2^{-8}. Table 4 shows the neutral space for this differential, which is spanned by the linearly independent neutral differences.

The following is an example to illustrate the search process introduced in Section 3.2. To search for a neutral difference for this differential trail, we specify the differences used in the EBCT trail in the search model, namely $(\nabla_0, \varDelta_0), (\nabla_1, \varDelta_1), (\nabla_2, \varDelta_2)$. To ensure that the differences propagate as expected, we set $\varDelta_0 = 0x0209\_0604$, $\varDelta_1 = 0x1800\_0010$, and $\varDelta_2 = 0x0040\_0000$ in the search model. Suppose that the neutral difference $0x0219\_0604$ is known, one can find a linear bijection φ where $\varphi(0x0209\_0604) = 1$ and $\varphi(0x0219\_0604) = 2$. According to Theorem 4, one can introduce the following constraint to prevent ∇_0 from being chosen from the linear space spanned by $0x0209\_0604$ and $0x0219\_0604$.

$$\left[\sum_{i=2}^{n-1} \varphi(\nabla_0)[i]\right] > 0. \tag{20}$$

Furthermore, one needs to characterize the relationships between differences in EBCT trails and differential trails. Using this search model, the solvers will yield a solution of $(\nabla_0, \varDelta_0), (\nabla_1, \varDelta_1), (\nabla_2, \varDelta_2)$ with the maximum neutral probability. Here, ∇_0 represents the newly discovered neutral difference. Suppose that $0x0040\_0000$ is the newly discovered neutral difference. By employing an EBCT trail, the neutral probability is estimated as $\widehat{Pr} = 2^{-1}$. By setting $\nabla_0 = 0x0040\_0000$ and repeating the aforementioned process, we discovered a total of 8 EBCT trails. By using these EBCT

Table 4: The subspace for 2-round differential $0x0209\_0604 \xrightarrow{2^{-8}} 0x0040\_0000$ of SPECK32, which is spanned by the first 26 neutral differences with non-zero neutral probabilities.

No.	Neutral diff.	$\widehat{Pr}$[1]	N	Pr EST	Pr EXP	Pr $\overline{\text{EXP}}$	No.	Neutral diff.	$\widehat{Pr}$	N	Pr EST	Pr EXP	Pr $\overline{\text{EXP}}$
1	0x0209_0604	–	–[5]	1.00[2]	1.00[3]	1.00[4]	17	0x2800_0010	2^{-2}	256	0.68	0.75	1.00
2	0x0219_2604	2^{-1}	45	1.00[5]	1.00	1.00	18	0x0a5d_3e14	2^{-3}	69	0.75	0.75	1.00
3	0x0040_0000	2^{-1}	8	1.00	1.00	1.00	19	0x6800_0010	2^{-3}	256	0.62	0.75	1.00
4	0x0249_8604	2^{-1}	4	1.00	1.00	1.00	20	0x0e09_060c	2^{-2}	3	0.38	0.37	1.00
5	0x4000_0080	2^{-2}	111	1.00	1.00	1.00	21	0x0a00_0004	2^{-2}	7	0.75	0.75	1.00
6	0x0030_2000	2^{-2}	53	1.00	1.00	1.00	22	0x1800_0010	2^{-3}	256	0.45	0.50	1.00
7	0x8000_0100	2^{-2}	42	1.00	1.00	1.00	23	0x0500_0002	2^{-3}	24	0.50	0.50	1.00
8	0x8002_0100	2^{-2}	30	1.00	1.00	1.00	24	0x0400_0008	2^{-1}	1	0.50	0.51	0.00
9	0x0020_4000	2^{-2}	45	1.00	1.00	1.00	25	0x1000_0000	2^{-2}	2	0.50	0.50	0.00
10	0x2000_0040	2^{-2}	256	0.99	1.00	1.00	26	0x1000_0020	2^{-2}	9	0.50	0.50	0.00
11	0xc209_0684	2^{-3}	114	1.00	1.00	1.00	27	0x0000_0004	–	–	No	No	No
12	0x021d_1e04	2^{-3}	61	1.00	1.00	1.00	28	0x0000_0200	–	–	No	No	No
13	0x0289_0605	2^{-2}	135	0.88	0.87	1.00	29	0x0000_0400	–	–	No	No	No
14	0x00a0_4000	2^{-3}	256	0.79	0.87	1.00	30	0x0000_0800	–	–	No	No	No
15	0x0140_8000	2^{-2}	70	0.75	0.75	1.00	31	0x0000_1000	–	–	No	No	No
16	0x0100_0002	2^{-2}	26	0.75	0.75	1.00	32	0x0001_0000	–	–	No	No	No[6]

[1] $\widehat{Pr}$ represents the theoretical estimation of the neutral probability obtained from a single EBCT trial. [2] $Pr =$ neutral probability. EST is a theoretical estimation of the neutral probability using N EBCT trails. The search program is set to find 256 single trails, while $N < 256$ indicates that there are only N EBCT trails found. [3] EXP represents the empirical results of the neutral probabilities for these neutral differences. The neutral probability is verified using 2^{15} plaintext pairs that satisfy the expected differential characteristic. [4] $\overline{\text{EXP}}$ represents the empirical results of the neutral probabilities for these neutral differences under the conditions specified in Table 5. These conditions are common for all 32 neutral differences. [5] The input difference is definitely a neutral difference with a probability of 1, but it is generally of no value for further cryptanalysis. Consequently, the input difference should be excluded out of the neutral space used for subsequent cryptanalysis. [6] No represents the neutral probability is 0. These 32 differences form a basis for the vector space $\mathbb{F}_2^{32}$.

trails, the theoretical estimation of neutral probability is 1, and the experimental result is 1 as well. Additionally, Table 5 presents the corresponding conditions that improve the neutral probabilities. Similar results for another 2-round differential $0x2a10\_0004 \rightarrow 0x2050\_2040 \rightarrow 0x8000\_0100$ with a probability of 2^{-6} are shown in Tables 6 and 7.

The input difference is definitely a neutral difference with a probability of 1. However, it is generally not useful for further cryptanalysis as exchanging two plaintexts in a pair of plaintext holds little value. It is crucial to note that not only should we avoid using the input difference as a neutral difference but also include it in the neutral space used, which is inappropriate.

4.3. Enhanced Differential-Linear Distinguishers by Neutral Differences. This section reviews how to construct a more effective distinguisher by a simple DL approximation when enough neutral differences are given. Furthermore, we present the improved distinguishers for 11-round SPECK32.

Table 5: The conditional neutral differences and corresponding conditions for 2-round differential $0x0209\_0604 \xrightarrow{2^{-8}} 0x0040\_0000$, where $x_l \| x_r$ be a plaintext of SPECK32.

Neutral diff.	Pr EXP	Pr $\overline{\text{EXP}}$	Condition
0x0289_0605	0.87	1.00	$x_l[10] \oplus x_r[3] = 0$
0x00a0_4000	0.87	1.00	
0x0140_8000	0.75	1.00	
0x0100_0002	0.75	1.00	
0x2800_0010	0.75	1.00	$x_l[11] \oplus x_r[4] = 1$
0x0a5d_3e14	0.75	1.00	
0x6800_0010	0.75	1.00	
0x0e09_060c	0.37	1.00	$x_l[12] \oplus x_r[5] = 0$
0x0a00_0004	0.75	1.00	
0x1800_0010	0.50	1.00	$x_l[10] = 0,\ x_l[12] = 1$
0x0500_0002	0.50	1.00	$x_l[8] = 1,\ x_r[1] = 1$

EXP (resp. $\overline{\text{EXP}}$) represents the empirical results of the neutral probabilities (under the conditions specified in the last column).

The correlation [25] of a differential-linear approximation (Δ, Γ) for a vectorial Boolean function $E: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is defined as follows:

$$Cor(\Delta, \Gamma) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\Gamma \cdot (E(x) \oplus E(x \oplus \Delta))}, \tag{21}$$

where $\Delta \in \mathbb{F}_2^n$ and $\Gamma \in \mathbb{F}_2^m$. Assuming that a DL trail (Δ_{in}, Γ) has a correlation pq, we aim to enhance the correlation by incorporating m neutral differences of the prepended short-round differential $(\Delta_{in}, \Delta_{out})$ with a probability of p. Under the condition that $2^m \geq q^{-2}$, Beierle et al. [5] pointed out that the DL distinguisher (Δ_{in}, Γ) would work as follows:

Step 1: Randomly generate a plaintext x, and then use m neutral differences to generate the corresponding plaintext pair structure $P_{x,\Omega,\Delta_{in}} = \{(x \oplus y, x \oplus y \oplus \Delta_{in}) | y \in \Omega\}$, where Ω is the space spanned by these m neutral differences.

Table 6: The subspace for 2-round differential $0x2a10\_0004 \xrightarrow{2^{-6}} 0x8000\_0100$ of SPECK32, which is spanned by the first 29 linearly independent neutral differences with non-zero neutral probabilities.

No.	Neutral diff.	$\widehat{Pr}$	N	Pr EST	Pr EXP	Pr $\overline{\text{EXP}}$	No.	Neutral diff.	$\widehat{Pr}$	N	Pr EST	Pr EXP	Pr $\overline{\text{EXP}}$
1	0x2a10_0004	–	–	1.00	1.00	1.00	17	0x0140_8000	2^{-2}	173	0.75	0.75	1.00
2	0x2810_0000	2^{-1}	10	1.00	1.00	1.00	18	0x2b10_0006	2^{-2}	65	0.75	0.75	1.00
3	0x2a30_0004	2^{-3}	38	1.00	1.00	1.00	19	0x0a04_0804	2^{-1}	22	0.75	0.75	1.00
4	0x0040_0000	2^{-1}	7	1.00	1.00	1.00	20	0x2a58_3004	2^{-3}	22	0.50	0.50	1.00
5	0x0040_8000	2^{-1}	13	1.00	1.00	1.00	21	0x2a16_0404	2^{-3}	102	0.75	0.75	1.00
6	0x0060_4000	2^{-2}	70	1.00	1.00	1.00	22	0x5000_0060	2^{-4}	256	0.45	0.49	1.00
7	0x6a10_0084	2^{-2}	256	0.93	0.98	1.00	23	0x201c_0800	2^{-2}	22	0.50	0.50	0.52
8	0x6a10_0004	2^{-3}	256	0.83	0.98	1.00	24	0x3a10_0004	2^{-2}	16	0.50	0.50	0.50
9	0x8000_0100	2^{-2}	256	0.93	0.97	1.00	25	0x1e10_001c	2^{-2}	9	0.25	0.25	0.50
10	0xea10_0084	2^{-3}	256	0.86	0.97	1.00	26	0x2e10_0004	2^{-2}	27	0.50	0.50	0.49
11	0x4001_0080	2^{-3}	256	0.62	0.94	1.00	27	0x1000_0020	2^{-3}	8	0.50	0.50	0.00
12	0x2a11_0204	2^{-2}	256	0.93	0.94	1.00	28	0x0008_1000	2^{-3}	2	0.50	0.50	0.00
13	0x2a12_0404	2^{-2}	93	0.88	0.87	1.00	29	0x0400_0008	2^{-3}	9	0.50	0.50	0.00
14	0x2a90_0005	2^{-2}	256	0.87	0.88	1.00	30	0x0000_0004	–	–	No	No	No
15	0x0002_0000	2^{-3}	256	0.85	0.88	1.00	31	0x0000_0010	–	–	No	No	No
16	0x2ab0_4004	2^{-3}	256	0.78	0.88	1.00	32	0x0000_0800	–	–	No	No	No

The notations are the same as Table 4.

Table 7: The conditional neutral differences and corresponding conditions for 2-round differential $0x2a10\_0004 \xrightarrow{2^{-6}} 0x8000\_0100$, where $x_l \| x_r$ be a plaintext of SPECK32.

Neutral diff.	Pr EXP	Pr $\overline{\text{EXP}}$	Condition
0x0140_8000	0.75	1.00	$x_l[10] \oplus x_r[3] = 0$
0x2b10_0006	0.75	1.00	
0x0a04_0804	0.75	1.00	$x_l[3] \oplus x_r[12] = 0$
0x2a58_3004	0.50	1.00	
0x2a16_0404	0.75	1.00	
0x5000_0060	0.49	1.00	$x_l[12] \oplus x_r[5] = 0$

EXP (resp. $\overline{\text{EXP}}$) represents the empirical results of the neutral probabilities (resp. under the conditions specified in the last column).

Step 2: The corresponding cipher pair structure of $P_{x,\Omega,\Delta_{in}}$ is denoted by $\{(c_0, c_0'), (c_1, c_1'), \dots, (c_{2^m-1}, c_{2^m-1}')\}$. Then, one can compute

$$Cor = \frac{1}{2^m} \sum_{0 \le i < 2^m} (-1)^{\Gamma \cdot \left(c_i \oplus c_i'\right)}. \tag{22}$$

Step 3: If the correlation observed using 2^m pairs is approximately q, the distinguisher succeeds. Otherwise, go to Step 1.

The essential requirement for this distinguisher to be effective is to identify sufficient neutral differences so that $2^m \geq \frac{1}{q^2}$. With probability p, the plaintext pair structure $P_{x,\Omega,\Delta_{in}}$ makes the short-round differential satisfied. Denote the product of the neutral probabilities of the neutral differences utilized by $\bar{p}$. With probability $p\bar{p}$, the distinguisher succeeds in Step 3. Thus, the data complexity of (Δ_{in}, Γ) required is $\mathcal{O}(p^{-1}\bar{p}^{-1}q^{-2})$ instead of $\mathcal{O}(p^{-2}q^{-2})$. Note that the statistical value Cor is derived from 2^m ciphertext pairs. When comparing with the DL distinguishers without using the neutral difference technique, we regard the (equivalent) correlations of DL (ND) as $p^{\frac{1}{2}}\bar{p}^{\frac{1}{2}}q$, since the data complexity required is $\mathcal{O}(p^{-1}\bar{p}^{-1}q^{-2})$. Table 8 summarizes the differential-linear distinguishers for 11-round SPECK32.

5. Application to LEA

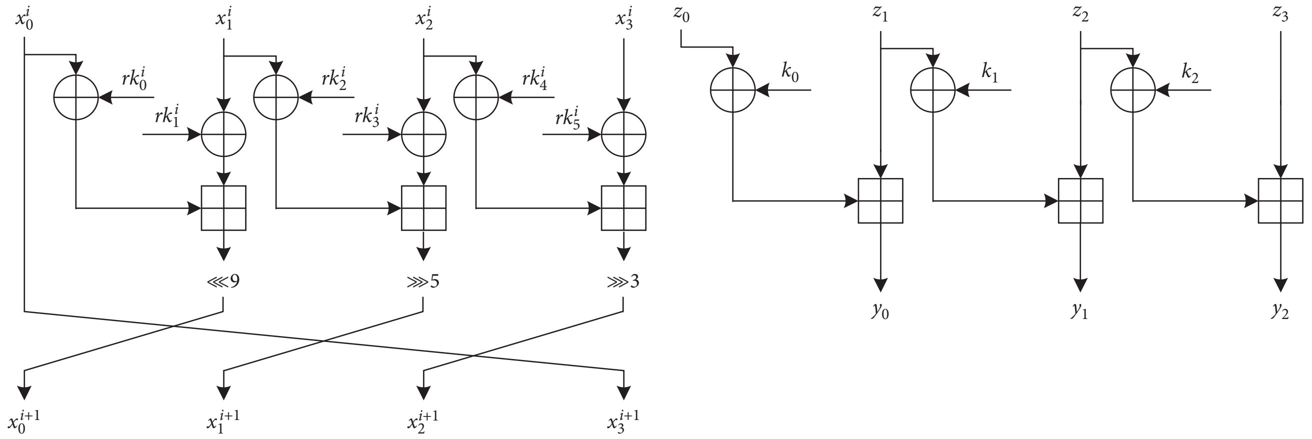
5.1. LEA. The LEA family of block ciphers not only serves as the national standard of the Republic of Korea but also is included in the ISO/IEC 29192-2:2019 standard. The LEA family has a block size of 128 bits and consists of three different key sizes: 128, 192, and 256 bits, denoted by LEA128, LEA192, and LEA256, respectively. Figure 2(a) provides a schematic view of the round function of LEA. The inputs/outputs of each round of LEA consist of four 32-bit words.

5.2. Enhanced Differential-Linear Distinguishers by Neutral Differences. For LEA, there is a 4-round differential characteristic shown in Table 9, with a probability of 2^{-33}. Table 10 of Appendix A outlines 61 linearly independent neutral differences for this differential. Since not all of the neutral probabilities are 1, it is significant to know the probability of obtaining a plaintext structure consisting of 2^{61} right pairs from a right pair. In this case, the statistical variable will clearly demonstrate advantages when the key is guessed correctly. Though it is computationally infeasible to verify it directly, we randomly select subspaces spanned by five neutral differences and verify the probability of obtaining 2^5 right pairs from a right pair. Denote the product of the five individual neutral probabilities by p, and let the empirical probability of obtaining 2^5 right pairs be $\widehat{p}$. We utilized 2^{12} right pairs to repeat the above experiments 100 times and

Table 8: DL distinguishers combined with the neutral difference technique, denoted by DL (ND).

Cipher	Round[1]	Weak keys	Input diff.	Intermediate diff.	Output mask	p	q	M	$m/\bar{p}$	$p^{\frac{1}{2}}q$	Ref.
SPECK32	1 + 9	Full	0*x*2050_2040	0*x*8000_0100	0*x*3854_3844	2^{-2}[2]	-2^{-10}	28[3]	21/1.0[3]	-2^{-11}[4]	[9]
	1 + 10		0*x*2*a*10_0004	0*x*2050_2040	0*x*3854_3844	2^{-4}	-2^{-12}	25	$25/2^{-1}$	$-2^{-14.5}$	[9]
	2 + 9		0*x*0209_0604	0*x*0040_0000	0*x*2240_4280	2^{-8}	$-2^{-10.18}$	25	21/1.0	$-2^{-14.18}$	This work
	2 + 9		0*x*2*a*10_0004	0*x*8000_0100	0*x*3854_3844	2^{-6}	$-2^{-10.07}$	28	21/1.0	$-2^{-13.07}$	This work
LEA	4 + 12	Full	♢	0x8000_0000	[0,9,61,91,105]	2^{-33}	$-2^{-10.97}$	34	$21/2^{-1.14}$	$-2^{-28.04}$	[6]
	4 + 13				[0,29,37,38,61,68,88, 91,101,102,105,114]	2^{-33}	$-2^{-26.04}$	61	$53/2^{-20.50}$	$-2^{-52.79}$	This work

[1] $A+B$ indicates a DL (ND) that combines an A-round differential and a B-round DL trail, where the A-round differential starts from input diff. and ends at intermediate diff. [2] p = theoretical probability of the prepended short-round differential. q is the experimental correlation of the bottom DL trail. [3] The number of (conditional) neutral differences for the above A-round differential presented in the original paper is denoted by M. $m/\bar{p}$ denotes the current DL distinguisher utilizing m (conditional) neutral differences simultaneously, where the product of the probabilities of these neutral differences is $\bar{p}$. To evaluate the DL (ND) using the same criteria, we set m as the smallest integer such that $2^m > q^{-2}$. [4] Denote the overall correlation of the differential-linear trails by pq. Here, we regard the (equivalent) correlations of DL (ND) as $p^{\frac{1}{2}}\bar{p}^{\frac{1}{2}}q$, since the data complexity required is $\mathcal{O}(p^{-1}\bar{p}^{-1}q^{-2})$. ♢ represents the input difference listed in Table 9.



(a)

(b)

FIGURE 2: The LEA instance: (a) the round function of LEA; (b) parallel modular additions.

TABLE 9: A 4-round differential characteristic for LEA.

r	Differences	$-\log(p_i)$
0	0x8a000080_80402080_80402210_c0402234	
1	0x80400014_80000014_88000004_8a000080	17
2	0x80000000_80400000_80400010_80400014	10
3	0x80000000_80000000_80000000_80000000	6
4	0x00000000_00000000_00000000_80000000	0
$-\sum_{i=1}^{4}\log(p_i)$		33

found $0.398 \leq \widehat{p}/p \leq 3.061$, and the average of $\widehat{p}/p$ is 1.033. In summary, this experiment indicates that the probability of obtaining 2^m right pairs using m neutral differences can be approximated by the product of the individual neutral probability experimental values of these neutral differences, which has been verified in [6]. Consequently, the theoretical probability of obtaining 2^{61} right pairs from a right pair using these 61 neutral differences is $2^{-29.96}$. The differential-linear distinguisher that employs the neutral difference technique is presented in Table 8.

5.3. The 18-Round Key Recovery Attack on LEA. To attack the 18-round LEA with key sizes of 192 and 256 bits, we employ the 17-round DL (ND) distinguisher described in Table 8 by adding an additional round. The attack program is outlined in Algorithm 1, which recovers 60 bits of subkey in the last round.

For the convenience of introducing the 18-round key recovery attack, we use the following notations (see Figure 2(b)):

$$
\begin{aligned}
&(z_0^i, z_1^i, z_2^i, z_3^i)\\
&=(x_0^{17}, x_1^{17} \oplus rk_1^{17}, x_2^{17} \oplus rk_3^{17}, x_3^{17} \oplus rk_5^{17});\\
&(k_0, k_1, k_2)\\
&=(rk_0^{17}, rk_1^{17} \oplus rk_2^{17}, rk_3^{17} \oplus rk_4^{17});\\
&(y_0^i, y_1^i, y_2^i)\\
&=(x_0^{18} \ggg 9, x_1^{18} \lll 5, x_2^{18} \lll 3);\\
&(c_0^i, c_1^i, c_2^i)\\
&=(y_0^i \oplus z_0^i \oplus z_1^i \oplus k_0, y_1^i \oplus z_1^i \oplus z_2^i \oplus k_1, y_2^i \oplus z_2^i \oplus z_3^i \oplus k_2);
\end{aligned}
\tag{23}
$$

where i indicates the current ciphertext comes from the ith ciphertext pair. If i is obvious in the context, i will be omitted. Similarly, let $(\bar{z}_0^i, \cdots, \bar{z}_3^i, \bar{y}_0^i, \bar{y}_1^i, \bar{y}_2^i, \bar{c}_0^i, \bar{c}_1^i, \bar{c}_2^i)$ represent the other ciphertext for the ith ciphertext pair.

Consider the linear mask $[0, 29, 37, 38, 61, 68, 88, 91, 101, 102, 105, 114]$. The statistical value Cor is calculated as follows:

$$
Cor_{(k_0,k_1,k_2)} = \sum_{0 \leqslant i < 2^m} (-1)^{\left(z_3^i \oplus \bar{z}_3^i\right)[0,29] \oplus \left(z_2^i \oplus \bar{z}_2^i\right)[5,6,29] \oplus \left(z_1^i \oplus \bar{z}_1^i\right)[6,26,29] \oplus \left(z_0^i \oplus \bar{z}_0^i\right)[5,6,9,18]},
\tag{24}
$$

```
Input: $m$ neutral differences $M_1, \dots, M_m$ and corresponding subspace $\Omega \leftarrow Span\{M_1, \dots, M_m\}$, number of replications $R$, plaintext structures $P_{x_j,\Omega,\Delta_{in}} = \{(x_j \oplus y, x \oplus y \oplus \Delta_{in}) | y \in \Omega\}$ for $0 \leq j < R$, threshold $\Theta$.
Output: List of key candidates, denoted by $\mathscr{K}$.
$\mathscr{K} \leftarrow \emptyset$
for $1 \leq j \leq R$ do
    Choose the $j$th plaintext structure $P_{x_j,\Omega,\Delta_{in}}$
    /* Denote the ciphertext pairs, encrypted from $P_{x_j,\Omega,\Delta_{in}}$, by $\{(c_0, c'_0), (c_1, c'_1), \dots, (c_{2^m-1}, c'_{2^m-1})\}$ */
    for each possible $k$ do
      $Cor_k = 0$
      for $0 \leq i < 2^m$ do
        // A filtering process that enhances advantages.
        /* $Dec_k$ represents one round decryption with $k$. $\Gamma$ represents the output mask, and $N$ is the
          number of ciphertext pairs to calculate this correlation. */
        if $(c_i, c'_i)$ is useful for current $k$ then
          $Cor_k + = \frac{1}{N}(-1)^{\Gamma \cdot (Dec_k(c_i) \oplus Dec_k(c'_i))}$ end
        else
            Continue
    // Without losing generality, let the correlation of the bottom DL distinguisher be less
      than 0 and $\Theta < 0$.
     if $Cor_k < \Theta$ then
        Store the key candidate $k$ to $\mathscr{K}$.
```

Algorithm 1: Pseudocode for the Key Recovery of Differential-Linear Attack.

where $(z_3^i \oplus \bar{z}_3^i)[0, 29] = z_3^i[0] \oplus \bar{z}_3^i[0] \oplus z_3^i[29] \oplus \bar{z}_3^i[29]$. Here, $z_0^i, y_0^i, y_1^i, y_2^i, \bar{z}_0^i, \bar{y}_0^i, \bar{y}_1^i$ and $\bar{y}_2^i$ can be directly obtained from the ith ciphertext pair. We guess the least significant 29 bits of both k_0 and k_1 to obtain the least significant 29 bits of $z_1, z_2, \bar{z}_1, \bar{z}_2$, i.e., $z_1 = y_0 \boxminus (z_0 \oplus k_0), z_2 = y_1 \boxminus (z_1 \oplus k_1)$. In this scenario, we also obtain the least significant 30 bits of c_0, c_1. For example, $c_0[0] = 0$ and $c_0[j+1] = (z_0 \oplus k_0)[j] \& c_0[j] \oplus (z_0 \oplus k_0)[j] \& z_1[j] \oplus c_0[j] \& z_1[j]$ for $0 \leq j < 29$. Due to the nature of the additions, we have the following:

$$\begin{aligned} z_3[0] \oplus \bar{z}_3[0] &= (z_0 \oplus y_0 \oplus y_1 \oplus y_2)[0] \oplus (k_0 \oplus k_1 \oplus k_2)[0] \\ &\quad \oplus (\bar{z}_0 \oplus \bar{y}_0 \oplus \bar{y}_1 \oplus \bar{y}_2)[0] \oplus (k_0 \oplus k_1 \oplus k_2)[0] \\ &= (z_0 \oplus y_0 \oplus y_1 \oplus y_2)[0] \oplus (\bar{z}_0 \oplus \bar{y}_0 \oplus \bar{y}_1 \oplus \bar{y}_2)[0] \end{aligned} \tag{25}$$

and

$$\begin{aligned} z_1[29] \oplus \bar{z}_1[29] &= z_0[29] \oplus c_0[29] \oplus k_0[29] \oplus y_0[29] \oplus \bar{z}_0[29] \oplus \bar{c}_0[29] \oplus k_0[29] \oplus \bar{y}_0[29] \\ &= z_0[29] \oplus \bar{z}_0[29] \oplus c_0[29] \oplus \bar{c}_0[29] \oplus y_0[29] \oplus \bar{y}_0[29]. \end{aligned} \tag{26}$$

Additionally, we utilize the conditional linear approximation proposed by Biham and Carmeli [26] to compute $z_3[29]$ and $\bar{z}_3[29]$. See Appendix B for more details. For clarity, let $b_0 \| b_1$ and $b_2 \| b_3$ represent $(z_2 \oplus k_2 \oplus y_2)[28:27]$ and $(\bar{z}_2 \oplus k_2 \oplus \bar{y}_2)[28:27]$, respectively. Then we have the following:

$$\begin{aligned} z_3[29] \oplus \bar{z}_3[29] = z_2[29] &\oplus \bar{z}_2[29] \oplus y_2[29] \oplus \bar{y}_2[29] \\ &\oplus (y_2[28] \& b_0) \oplus (y_2[27] \& (b_0 \oplus 1) \& b_1) \\ &\oplus (\bar{y}_2[28] \& b_2) \oplus (\bar{y}_2[27] \& (b_2 \oplus 1) \& b_3), \end{aligned} \tag{27}$$

where $b_0 \| b_1 \neq 0$ and $b_2 \| b_3 \neq 0$. We define $C_j^i = c_j^i \oplus \bar{c}_j^i$, $Z_j^i = z_j^i \oplus \bar{z}_j^i$, and $Y_j^i = y_j^i \oplus \bar{y}_j^i$ for simplicity. As a result, the statistical value can be rewritten as follows:

$$Cor_{(k_0,k_1,k_2)} = \sum_{\substack{0 \leq i < 2^m, \\ b_0 \| b_1 \neq 0,\, b_2 \| b_3 \neq 0}} (-1)^{\substack{Z_2^i[5,6] \oplus Z_1^i[6,26] \oplus Z_0^i[0,5,6,9,18,29] \\ \oplus Y_3^i[0] \oplus Y_2^i[0,29] \oplus Y_1^i[0] \oplus Y_0^i[0,29] \oplus C_0^i[29] \oplus \mathcal{S}}}, \tag{28}$$

where

$$\mathcal{S} = (y_2[28]\&b_0) \oplus (y_2[27]\&(b_0 \oplus 1)\&b_1) \oplus (\bar{y}_2[28]\&b_2) \oplus (\bar{y}_2[27]\&(b_2 \oplus 1)\&b_3). \tag{29}$$

Note that only $\frac{3}{4} \times \frac{3}{4} = 2^{-0.83}$ of the generated plaintext–ciphertext pairs are used simultaneously. Consequently, we need to guess 60 bits of the subkey, i.e., $k_2[28]$, $k_2[27]$, $k_1[28:0]$, and $k_0[28:0]$.

The 18-round attack utilizes all 61 neutral differences in Table 10 simultaneously and sets the parameter R as $2^{33+29.96} = 2^{62.96}$. Let $N = 2^{61-0.83} = 2^{60.17}$ and $c = -2^{-26.04}$ represent the correlation of the bottom DL approximation (see the last row of Table 8). If the guessed subkey is correct and each pair of $P_{x,\Omega,\Delta_{in}}$ satisfies the prepended short-round differential, the statistical variable $Cor_{(k_0,k_1,k_2)}$ follows the normal distribution with mean of c and variance of $\frac{(1+c)(1-c)}{N}$. Otherwise, $Cor_{(k_0,k_1,k_2)}$ follows the normal distribution with mean of 0 and variance of $\frac{1}{N}$. When the threshold Θ is set to $-2^{-26.26}$, the right key will pass through Line 9 of Algorithm 1 with a probability of $\Phi(\frac{\Theta - c}{\sqrt{(1+c)(1-c)/N}}) = 0.99$ while a wrong key will pass with a probability of $\Phi(\frac{\Theta - 0}{\sqrt{1/N}}) = 2^{-145}$. Here, $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{-x^2}{2}} dx$ is the distribution function of the standard normal distribution. The expected number of wrong keys in key candidates is $2^{62.96} \times 2^{60} \times 2^{-145} \approx 0$. The data complexity should be $2^{62.96} \times 2^{61} \times 2 = 2^{124.96}$ chosen plaintext pairs and the time complexity should be $2^{124.96} \times 2^{60} = 2^{184.96}$ operations. Each operation consists of a partial decryption for one round, a dot product, and an addition. Roughly estimated, we assume that the time complexity for one operation is approximately equal to that of one round of decryption. Therefore, the final time complexity for our 18-round attack is $2^{184.96}/18 = 2^{180.80}$ full encryptions of 18-round LEA. The success rate is determined by the probability of obtaining a plaintext structure, where each plaintext pair satisfies the prepended short-round differential characteristic, i.e., $Succ = 1 - (1 - 2^{-33-29.96})^{2^{33+29.96}} = 0.632$. The comparison of our attack with previous attacks on LEA is shown in Table 2.

6. Conclusion

In this paper, we have investigated the link between neutral difference and boomerang cryptanalysis. Based on it, we introduce an automated approach for identifying linearly independent neutral differences. Consequently, we present the improved differential-linear distinguishers for SPECK32 and LEA, along with the 18-round attacks on LEA192 and LEA256 with the lowest time complexity up to date.

Appendix

A. Neural Differences for 4-Round Differential on LEA

Table 10: The neutral differences for 4-round differential, as shown in Table 9.

No.	Neutral diff.	*Pr*
1	0*x*8*a*000080_80402080_80402210_*c*0402234	1.00
2	0*x*00000000_00000000_00000000_00000004	1.00
3	0*x*00000000_00000000_00000010_00000010	0.99
4	0*x*00000000_00400000_00400000_00400000	1.00
5	0*x*00000000_00000000_00000000_80000000	0.89
6	0*x*00000000_00000000_00000000_00004000	0.99
7	0*x*00000000_00000000_00000000_00008000	0.99
8	0*x*00000000_00000000_00000000_00010000	0.99
9	0*x*00000000_00000000_00000000_00020000	0.99
10	0*x*00004000_00000000_00000000_00000000	0.99
11	0*x*00008000_00000000_00000000_00000000	0.99
12	0*x*00010000_00000000_00000000_00000000	0.98
13	0*x*00000000_00000000_00000000_00040000	0.98
14	0*x*00000000_00000000_00000000_00080000	0.97
15	0*x*00020000_00000000_00000000_00000000	0.96
16	0*x*10000000_00000000_00000000_00000000	0.94
17	0*x*00000000_00000000_00080000_00000000	0.94
18	0*x*20000000_00000000_00000000_00000000	0.94

Table 10: Continued.

No.	Neutral diff.	*Pr*
19	0x00000000_00000000_00000000_00100000	0.95
20	0x00040000_00000000_00000000_00000000	0.93
21	0x40000000_00000000_00000000_00000000	0.92
22	0x00000000_00000000_00000000_00200000	0.92
23	0x00000000_00000000_00100000_00000000	0.90
24	0x00000100_00000000_00000000_00000000	0.81
25	0x00000000_00040000_00040000_00000000	0.91
26	0x00000000_80000000_80000000_00000000	0.80
27	0x80000000_00000000_00000000_00000000	0.90
28	0x00080000_00000000_00000000_00000000	0.86
29	0x00000000_00000000_00000000_00800000	0.86
30	0x00000000_00000000_00200000_00000000	0.83
31	0x00000000_00004000_00004000_00000000	0.82
32	0x00000000_00080000_00000000_00000000	0.84
33	0x00000200_00000000_00000000_00000000	0.81
34	0x00000000_00008000_00008000_00000000	0.77
35	0x00000000_00000000_00000000_01000000	0.78
36	0x0a000080_00002080_00002200_40002221	0.74
37	0x0a010080_00012080_00012200_40012220	0.73
38	0x0a000080_00002080_00802200_40802220	0.73
39	0x00000000_00000000_00004000_00005000	0.74
40	0x8a000080_80502080_80502210_c0502234	0.68
41	0x8a000080_80402080_8040a210_c040a234	0.66
42	0x8a000080_80402080_81402210_c1402234	0.60
43	0x0a000080_00002080_00002600_40002620	0.57
44	0x00000000_00000020_00000000_00000000	0.65
45	0x00000000_00000000_00010000_00010000	0.55
46	0x00000000_00000000_00000000_04000000	0.51
47	0x80000000_80420000_80420010_80420014	0.48
48	0x00000000_00000000_00000002_00000002	0.39
49	0x80000000_90400000_90400010_90400014	0.46
50	0x8a000080_80402080_90402210_d0402234	0.44
51	0x0a200080_00202080_00202200_40202220	0.41
52	0x0a000480_00002480_00002600_40002620	0.47
53	0x8a000080_80402480_80402610_c0402634	0.43
54	0x80000020_80400000_80400010_80400114	0.43
55	0x0a000080_00002080_00002a00_40002a20	0.45
56	0x80000000_80000000_80000000_80000002	0.50
57	0x80000000_80400000_80401010_80401014	0.48
58	0x80000000_80400000_82400010_82400014	0.44
59	0x00000000_00200000_00200000_00200000	0.42
60	0x0a000081_00002081_00002201_40002221	0.41
61	0x00800000_00800000_00800000_00800000	0.40
62	0x80000000_80c00000_80c00010_80c00014	0.40

The 2nd to 35th neutral differences were proposed in [6]. The empirical results of the neutral probabilities are obtained from 2^{18} right pairs.

B. Conditional Linear Approximations for Additions

This section introduces the conditional linear approximation technique, which is also known as the partitioning technique proposed by Biham and Carmeli [26]. This technique has the ability to amplify the bias of linear approximations of additions. Furthermore, it has been applied to the differential-linear attack on ARX ciphers [5, 6, 27]. The core of the conditional linear approximation technique is shown in Lemma B.1.

Lemma B.1 (Page 10, [5]). *Let* $y = x \boxplus z$ *and* $s = y \oplus x$, *where* $x, y, z \in \mathbb{F}_2^n$. *Let* $\mathcal{S}^i_{b_0 b_1} = \{(x, y) \in \mathbb{F}_2^{2n} | s[i-1] = b_0, s[i-2] = b_1\}$. *For* $i \geq 3$, *we have the following:*

$$z[i] = \begin{cases} x[i] \oplus y[i] \oplus y[i-1] \oplus 1, & \text{with corr. } 1, \text{ if } (x, y) \in \mathcal{S}^i_{1*} \\ x[i] \oplus y[i] \oplus y[i-2] \oplus 1, & \text{with corr. } 1, \text{ if } (x, y) \in \mathcal{S}^i_{01} \\ x[i] \oplus y[i] \oplus y[i-3] \oplus 1, & \text{with corr. } 0.5, \text{ if } (x, y) \in \mathcal{S}^i_{00} \end{cases}, \tag{B.1}$$

where $\mathcal{S}^i_{1*} = \mathcal{S}^i_{10} \cup \mathcal{S}^i_{11}$ *and* $\mathcal{S}^i_{0*} = \mathcal{S}^i_{00} \cup \mathcal{S}^i_{01}$.

Data Availability

The data that support the findings of this study are openly available at https://github.com/PigInTheSky1234/Unveiling-the-Neutral-Difference-and-Its-Automated-Search.

Conflicts of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article besides the funding that we already state and our affiliations.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (grant nos. 62302518 and 62372463) and the Natural Science Foundation of Henan (grant no: 222300420100).

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[2] E. Biham and R. Chen, "Near-collisions of SHA-0," in *Advances in Cryptology–CRYPTO 2004*, vol. 3152 of *Lecture Notes in Computer Science*, pp. 290–305, Springer, Berlin, Heidelberg, 2004.

[3] Z. Bao, J. Guo, M. Liu, L. Ma, and Y. Tu, "Enhancing differential-neural cryptanalysis," in *Advances in Cryptology–ASIACRYPT 2022*, vol. 13791 of *Lecture Notes in Computer Science*, pp. 318–347, Springer, 2022.

[4] A. Gohr, "Improving attacks on round-reduced speck32/64 using deep learning," in *Advances in Cryptology–CRYPTO 2019*, vol. 11693 of *Lecture Notes in Computer Science*, pp. 150–179, Springer, Cham, 2019.

[5] C. Beierle, M. Broll, F. Canale et al., "Improved differential-linear attacks with applications to ARX ciphers," *Journal of Cryptology*, vol. 35, no. 4, Article ID 29, 2022.

[6] Y. Chen, Z. Bao, and H. Yu, "Differential-linear approximation semi-unconstrained searching and partition tree: Application to lea and speck," in *Advances in Cryptology–ASIACRYPT 2023*, vol. 14440 of *Lecture Notes in Computer Science*, pp. 223–255, Springer, Singapore, 2023.

[7] O. Dunkelman, N. Keller, and A. Weizmann, "Practical-time related-key attack on GOST with secret S-boxes," in *Advances in Cryptology–CRYPTO 2023*, vol. 14083 of *Lecture Notes in Computer Science*, pp. 177–208, Springer, Cham, 2023.

[8] S. Wang, M. Liu, S. Hou, and D. Lin, "Moving a step of chacha in syncopated rhythm," in *Advances in Cryptology–ASIACRYPT 2022*, vol. 14083 of *Lecture Notes in Computer Science*, pp. 273–304, Springer, Cham, 2023.

[9] E. Bellini, D. Gerault, J. Grados, R. H. Makarim, and T. Peyrin, "Fully automated differential-linear attacks against ARX ciphers," in *Topics in Cryptology–CT-RSA 2023*, vol. 13871 of *Lecture Notes in Computer Science*, pp. 252–276, Springer, Cham, 2023.

[10] R. AlTawy and A. Hülsing, "Another look at differential-linear attacks," 2023, Cryptology ePrint Archive, Paper 2023/1675 (2023). https://doi.org/10.1007/978-3-030-99277-4, https://eprint.iacr.org/2023/1675.

[11] K. Fu, M. Wang, Y. Guo, S. Sun, and L. Hu, "MILP-based automatic search algorithms for differential and linear trails for speck," in *Fast Software Encryption. FSE 2016*, vol. 9783 of *Lecture Notes in Computer Science*, pp. 268–288, Springer, Berlin, Heidelberg, 2016.

[12] Z. Niu, S. Sun, Y. Liu, and C. Li, "Rotational differential-linear distinguishers of ARX ciphers with arbitrary output linear masks," in *Advances in Cryptology–CRYPTO 2022*, vol. 13507 of *Lecture Notes in Computer Science*, pp. 3–32, Springer, Cham, 2022.

[13] H. Lee, S. Kim, H. Kang, D. Hong, J. Sung, and S. Hong, "Calculating the approximate probability of differentials for ARX-based cipher using SAT solver," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 28, no. 1, pp. 15–24, 2018.

[14] D. Wang, B. Wang, and S. Sun, "SAT-aided automatic search of boomerang distinguishers for ARX ciphers," *IACR Transactions on Symmetric Cryptology*, vol. 2023, no. 1, pp. 152–191, 2023.

[15] D. Kim, D. Kwon, and J. Song, "Efficient computation of boomerang connection probability for ARX-based block ciphers with application to SPECK and LEA," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E103.A, no. 4, pp. 677–685, 2020.

[16] L. Song, Z. Huang, and Q. Yang, "Automatic differential analysis of ARX block ciphers with application to speck and LEA," in *Information Security and Privacy. ACISP 2016*, vol.

9723 of *Lecture Notes in Computer Science*, pp. 379–394, Springer, Cham, 2016.

[17] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song, *Advances in Cryptology–EUROCRYPT 2018*, vol. 10821 of Lecture Notes in Computer Science, pp. 683–714, Springer, Cham, 2018.

[18] S. Delaune, P. Derbez, and M. Vavrille, "Catching the fastest boomerangs," *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. 4, pp. 104–129, 2020.

[19] S. Sun, L. Hu, M. Wang et al., "Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties," Cryptology ePrint Archive, 2014.

[20] L. Sun, W. Wang, and M. Wang, "Accelerating the search of differential and linear characteristics with the SAT method," *IACR Transactions on Symmetric Cryptology*, vol. 2021, no. 1, pp. 269–315, 2021.

[21] T. Hou, J. Zhang, and T. Cui, "Recover the secret components in a ForkCipher," *Chinese Journal of Electronics*, vol. 32, no. 3, pp. 597–602, 2023.

[22] K. Taka, T. Ishikawa, K. Sakamoto, and T. Isobe, "An efficient strategy to construct a better differential on multiple-branch-based designs: application to orthros," in *Topics in Cryptology–CT-RSA 2023*, vol. 13871 of *Lecture Notes in Computer Science*, pp. 277–304, Springer, Cham, 2023.

[23] T. Cui, Y. Mao, Y. Yang, Y. Zhang, J. Zhang, and C. Jin, "Congruent differential cluster for binary SPN ciphers," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2385–2397, 2024.

[24] A. B. Kidmose and T. Tiessen, "Formal analysis of boomerang probabilities," *IACR Transactions on Symmetric Cryptology*, vol. 2022, no. 1, pp. 88–109, 2022.

[25] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis," in *Advances in Cryptology-CRYPTO'94*, pp. 17–25, Springer, Cham, 1994.

[26] E. Biham and Y. Carmeli, "An improvement of linear cryptanalysis with addition operations with applications to feal-8x," in *Selected Areas in Cryptography–SAC 2014*, vol. 8781 of *Lecture Notes in Computer Science*, pp. 59–76, Springer, Cham, 2014.

[27] G. Leurent, "Improved differential-linear cryptanalysis of 7-round chaskey with partitioning," in *Advances in Cryptology–EUROCRYPT 2016*, vol. 9665 of *Lecture Notes in Computer Science*, pp. 344–371, Springer, Berlin, Heidelberg, 2016.