IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 0, No. 0, pp. 0–0. DOI:10.46586/tosc.v0.i0.0-0

Mix-Basis Geometric Approach to Boomerang Distinguishers

Chengcheng Chang[1,3,4,5], Hosein Hadipour[2], Kai Hu[1,3,4,5,6(✉)], Muzhou Li[1,3,4,5] and Meiqin Wang[1,4,5]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China
kai.hu@sdu.edu.cn, chengcheng.chang@mail.sdu.edu.cn, muzhouli@mail.sdu.edu.cn,
[2] Ruhr University Bochum, Bochum, Germany
Hossein.Hadipour@ruhr-uni-bochum.de
[3] Quancheng Laboratory, Jinan 250103, China
mqwang@sdu.edu.cn
[4] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China
[5] State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, Qingdao, 266237, China
[6] Suzhou Research Institute, Shandong University, Suzhou, 215123, China

Abstract. Differential cryptanalysis relies on assumptions like *Markov ciphers* and *hypothesis of stochastic equivalence*. The probability of a differential characteristic estimated by classical methods is the key-averaged probability under the two assumptions. However, the real probability can vary significantly between keys. Hence, tools for differential cryptanalysis in the fixed-key model are desirable. Recently, Beyne and Rijmen applied the geometric approach to differential cryptanalysis and proposed a systematic framework called *quasi-differential* (CRYPTO 2022).

As a variant of differential cryptanalysis, boomerang attacks rely on similar assumptions, so it is important to study their probability in the fixed-key model as well. A direct extension of the quasi-differential for boomerang attacks leads to the quasi-3-differential framework (IEEE-IT 2024). However, such a straightforward approach is difficult in practical applications because there are too many quasi-3-differential trails.

We tackle this problem by applying the mix-basis style geometric approach (CRYPTO 2025) to the boomerang attacks and construct the quasi-boomerang framework. By choosing a suitable pair of bases, the boomerang probability can be computed by summing correlations of *quasi-boomerang characteristics*. The transition matrix of the key-XOR operation is also a diagonal matrix; thus, the influence of keys can be analyzed in a similar way to the quasi-differential framework.

We apply the quasi-boomerang framework to `SKINNY`-64 and `GIFT`-64. For `SKINNY`-64, we check and confirm 4 boomerang distinguishers with high probability (2 with probability 1 and 2 with probability 2^{-4}) generated from Hadipour, Bagheri, and Song's tool (ToSC 2021/1), through the analysis of key dependencies and the probability calculation from *quasi-boomerang characteristics*. We also propose a divide-and-conquer approach following the sandwich framework for boomerangs with small probability or long rounds to apply the quasi-boomerang framework. After checking 2/1 boomerang distinguisher(s) of `SKINNY`-64/`GIFT`-64, we find that the previously considered invalid 19-round distinguisher of `GIFT`-64 is valid.

In addition, as a contribution of independent interest, we revisit Boura, Derbez, and Germon's work by extending the quasi-differential framework to the related-key scenario (ToSC 2025/1), and show an alternative way to derive the same formulas in their paper by regarding the key-XOR as a normal cipher component.

Keywords: Boomerang, Fixed-Key, Mix-Basis, Geometric Approach

1 Introduction

Many modern cryptanalytic techniques, such as differential attack [BS90] and boomerang attack [Wag99], practically rely on independence assumptions as the *Markov cipher* and *hypothesis of stochastic equivalence assumptions* [LMM91]. Although these assumptions may sometimes seem fairly reliable, the community has been continuously working to verify or circumvent them.

The efforts on the validity of these assumptions can be roughly categorized into three categories. The first type of method is based on automatic search tools such as MILP or SAT. Usually, both the value and difference transitions of a differential characteristic (DC) are described in certain forms with proper constraints and fed to the search tools. The results of the search tool can reflect the validity of the target DC. For example, Liu et al. [LIMY20] developed an MILP tool to verify the DCs for `Gimli` permutation and found that many of them were invalid. Li et al. [LZH+24] proposed the AlgSAT tool that can check if a DC has at least one right pair. Very recently, Nageler et al. [NGJE25] proposed AutoDiVer based on the SAT tool, which can be used to verify a DC and compute its probability for different key spaces considering the key schedule.

The second type studies the local internal dependencies between different rounds or components of a cipher, sometimes with the key schedule. Linear or non-linear constraints would be obtained, so the validity can be known by checking if these constraints are solvable. For example, Peyrin and Tan analyzed the key dependencies arising from DCs in `GIFT` and `SKINNY` [PT22]. This work has been extended recently by Peyrin et al., who proposed an automated verifier `Trail-Estimator` to identify and analyze constraints within differential trails for word-oriented block ciphers in [PTZZ25] and applied it to `SKINNY`, `LBLOCK`, and `TWINE`. Their algorithm can also find the probability of a DC in different key spaces.

The third one is the quasi-differential techniques proposed by Beyne and Rijmen [BR22]. This method is an application of the geometric approach [Bey23] to various attacks such as the linear [Bey21], differential [BR22], (ultrametric) integral cryptanalysis [BV23, BV24a] and some combined attacks [HZC+25]. In this method, differential cryptanalysis is described by a transition matrix under the quasi-differential basis. The exact probability of a DC can be calculated by summing *correlations* of all quasi-differential characteristics (quasi-DCs) corresponding to this DC. If the sum of the correlations is zero, then the target DC is invalid. Additionally, for key-alternating ciphers, the round keys will only affect the positive/negative sign of a quasi-DC's correlation, but not influence the absolute value. Thus, a set of linear equations can usually be easily obtained by analyzing the signs. Different solutions of the linear equations lead to different key subspaces, where the probability of the DC in the corresponding key subspaces can be calculated. Very recently, Boura et al. [BDG25] extended the quasi-differential framework from the single-key to the related-key scenario and presented an approach to verify the validity of some related-key DCs of `AES` [DR20] and `SKINNY` [BJK+16] that takes the key schedule into account.

To date, the primary focus of the above methods has been on DCs, whereas boomerang distinguishers [Wag99], a significant variant of differential cryptanalysis, have remained relatively underexplored.

Boomerang attacks [Wag99] regard the target F as a composition of two sub-ciphers, i.e., $\mathsf{F} = \mathsf{F}_1 \circ \mathsf{F}_0$, assuming the upper DC of F_0 and the lower DC of F_1 are independent. There are many works that handle the independence assumption between the upper DC and lower DC of a boomerang. Cid et al. [CHP+18] proposed the Boomerang Connectivity Table (BCT) to study the incompatibility of the two DCs based on the sandwich framework (regarding F as $\mathsf{F} = \mathsf{F}_2 \circ \mathsf{F}_1 \circ \mathsf{F}_0$ in [DKS10]) when the middle part F_1 is only a single S-box

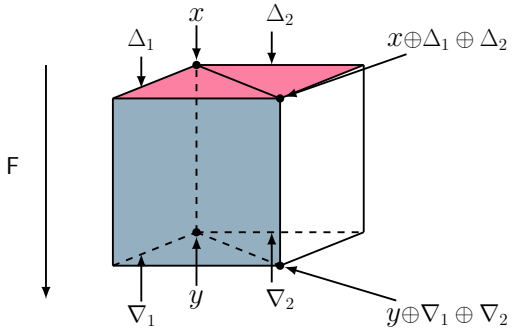

Figure 1: The input and output of a boomerang distinguisher. For the input, Δ_1 is known, and x, Δ_2 can be any value. For the output, ∇_2 is known, and y, ∇_1 can be any value. For the input (resp. output), the four values in a quartet sum to zero as the four values are $x, x \oplus \Delta_1, x \oplus \Delta_2, x \oplus \Delta_1 \oplus \Delta_2$ (resp. $y, y \oplus \nabla_1, y \oplus \nabla_2, y \oplus \nabla_1 \oplus \nabla_2$), to make it a 3rd-order space.

layer. Song et al. [SQH19], Wang and Peyrin [WP19] both revisited the BCT and evaluate the dependency between two DCs through multiple rounds. However, no similar efforts that analyze the independence assumptions for all rounds for boomerang distinguishers have been reported.

Boomerang attacks (including the rectangle attacks [BDK01, BDK02]) are important, as they often keep the longest attack records for many ciphers. For example, in the related-key setting, the full-round boomerang/rectangle attack on `AES`-192 in [DEFN22, YSZ+24], the 25/26/32-round rectangle attacks on `SKINNY`-64-128/`SKINNY`-128-256/`SKINNY`-128-384 in [YSZ+24, SYC+24, DQSW22], the 11-round boomerang attack on `Deoxys-BC`-256 in [YSZ+24], the 15-round rectangle attack on `Deoxys-BC`-384 in [SYC+24], and the 26-round rectangle attack on `GIFT`-64 in [DQSW22]. Without doubts, the validity of the independence assumptions of these boomerang distinguishers is as important as that of DCs. Thus, it is equally desirable to have some methods to find dependencies of boomerang distinguishers. However, tools that are useful to check DCs are not trivially applicable to boomerang distinguishers.

In [WSW+24], Wang et al. extended the quasi-differential framework to theoretical quasi-d-differential cryptanalysis and revisited the boomerang attack from the perspective of 3-differential ($d = 3$) [Tie16]. However, the quasi-3-differential framework is hard to use in practice, as the correlation of each quasi-3-differential trail is too small. The deep reason is that a boomerang distinguisher is actually a *specially truncated* 3-differential where parts of input and output differences can be any values. Hence, to describe a boomerang distinguisher, countless quasi-3-differential trails have to be accumulated. Due to limited computing power, computing probabilities for boomerang distinguishers via quasi-3-differential remains highly impractical. In fact, the authors of [WSW+24] only searched and verified a part of the 2-round 3-differentials of the distinguisher of `GIFT`-64.

Recently, Hu et al. extended the geometric approach by allowing the use of different bases for the input and output spaces [HZC+25], a flexibility that has been implied in Beyne's doctoral thesis [Bey23] but not utilized in any real cryptanalysis before. Using different bases brings much more convenience in describing attacks. In [HZC+25], the authors summarized three bases from previous geometric approach papers and extended them to an additional four bases. They also described the principles to choose bases from the seven bases for attacks of different *orders*, but they only provided examples for up to second-order attacks.

Our contributions. This paper applies the geometric approach to the boomerang attack

by choosing a pair of proper bases, presenting a much more practical tool for studying boomerang attacks in the fixed-key model. The main contributions include the theory and the applications.

We propose the quasi-boomerang framework as a theoretical tool to study the boomerang attack in the fixed-key model. This framework includes three key points, as follows,

3rd-order attack for describing boomerang attacks. Since the boomerang attack handles 4 values (a quartet), according to [HZC+25], we should describe it as a 4th-order attack. However, the transition matrix of a 4th-order attack will have a size of 4 times the cipher size, which is too heavy for searching trails. Instead, we notice that the boomerang attacks make an implicit assumption that the sum of the four values in a boomerang quartet is always zero. This inspires us to describe the boomerang attack as a 3rd-order attack. That is, for $\mathsf{F}:\mathbb{F}_2^n\to\mathbb{F}_2^n$, we will trace a linearly dependent quartet like $(x_0,x_1,x_2,x_0\oplus x_1\oplus x_2)$ where $x_0,x_1,x_2\in\mathbb{F}_2^n$ and the rank of these four values is 3. For the sake of convenient reference, we call it the *3rd-order assumption*. In addition, in boomerang attacks, what we care about more is the difference rather than the values. Hence, as shown in Figure 1, for the input, output of F, we consider the following propagation

$$(x,\Delta_1,\Delta_2,x\oplus\Delta_1\oplus\Delta_2)\xrightarrow{\mathsf{F}}(y,\nabla_1,\nabla_2,y\oplus\nabla_1\oplus\nabla_2).$$

Choice of the bases. Next, we choose suitable bases for this propagation to perform change-of-basis operations. The input basis is chosen as

$$b_{in}=[(-1)^{u_0^\top x}]_{x,u_0}\otimes[\delta_{u_1}(\Delta_1)]_{\Delta_1,u_1}\otimes[(-1)^{u_2^\top\Delta_2}]_{\Delta_2,u_2}.$$

The output basis is chosen as

$$b_{out}=[(-1)^{u_0^\top x}]_{x,u_0}\otimes[(-1)^{u_1^\top\Delta_1}]_{\Delta_1,u_1}\otimes[\delta_{u_2}(\Delta_2)]_{\Delta_2,u_2}.$$

Under these two bases, the coordinate of the transition matrix for the boomerang attack is

$$B^{\mathsf{F}}_{(v_0,v_1,v_2),(u_0,u_1,u_2)}=\frac{1}{2^{2n}}\sum_{x\in\mathbb{F}_2^n,\Delta_1=u_1,\nabla_2=v_2}(-1)^{u_0^\top x}(-1)^{u_2^\top\Delta_2}(-1)^{v_0^\top y}(-1)^{v_1^\top\nabla_1},$$

where $y=\mathsf{F}(x),\nabla_1=\mathsf{F}(x)\oplus\mathsf{F}(x\oplus\Delta_1),\nabla_2=\mathsf{F}(x)\oplus\mathsf{F}(x\oplus\Delta_2)$ and $\mathsf{F}(x\oplus\Delta_1\oplus\Delta_2)=y\oplus\nabla_1\oplus\nabla_2$.

One can check when setting $u_0=u_2=v_0=v_1=0$, $B^{\mathsf{F}}_{(0,0,v_2),(0,v_1,0)}$ counts the number of quartets that satisfy $\Delta_1=u_1,\nabla_2=v_2$. Under the 3rd-order assumption, this is exactly the probability of a rectangle distinguisher. The corresponding boomerang distinguisher's probability is 2^n times the rectangle's.

Boomerang characteristics and quasi-boomerang characteristics. Since the chosen bases are different, the boomerang attack is described as a mix-basis attack [HZC+25]. Let $\mathsf{F}=\mathsf{F}_2\circ\mathsf{F}_1\circ\mathsf{F}_0$. For F_0 and F_2, two same-basis attacks are derived with b_{in} and b_{out} as the bases, respectively. For F_1, a mix-basis attack applies.

Inherited from the geometric approach, the boomerang attack is now ready to be studied with trails. Analogous to the quasi-differential framework, the boomerang characteristics (BCs) and quasi-boomerang characteristics (quasi-BCs) are defined. The probability of a boomerang distinguisher (corresponding to a differential) is the sum of correlations of all quasi-BCs (corresponding to quasi-differential trails). However, the number of quasi-BCs can be huge, so we want to search for these trails in two phases, like we did in the quasi-differential framework. In b_{in} (resp. b_{out}), when we set $u_0=u_2=0$ (resp. $u_0=u_1=0$), the round-independence assumption is naturally introduced, as some intermediate values and differences have no limitations now. The probability of a BC is the

sum of the correlations of all quasi-BCs related to it. Therefore, we can first search for all BCs related to the boomerang distinguishers, then search for all quasi-BCs for each BC. Such a two-phase framework makes the search easier.

For applications, the quasi-boomerang framework is useful to compute the boomerang's probability in the fixed-key model and study the influence of keys similar to the quasi-differential framework [BR22]. We apply this framework to SKINNY-64 and GIFT-64, obtaining the following results, which are summarized in Table 1 also.

First, in the application to SKINNY-64, we find that the four boomerang distinguishers with high probabilities (2 with probability 1 and 2 with probability 2^{-4}) generated by tools in [HBS21] are all key-independent, and their probability can be calculated by summing the correlations of quasi-BCs. Next, for the boomerang distinguishers with small probability or long rounds, a divide-and-conquer approach is proposed to divide the boomerang into three parts to apply the quasi-boomerang framework. Two boomerangs of SKINNY-64 and one boomerang of GIFT-64 are checked using this approach, and the probability of the 19-round boomerang distinguisher is larger than 2^{-64}, which can be considered valid.

One interesting application of the quasi-boomerang framework is to address an open question raised by Hadipour at FSE 2023. At FSE 2023, Hadipour et al. [HNE22] presented a deterministic boomerang distinguisher for 11 rounds of SKINNY-64-128 (see Figure 3)[1]. This distinguisher was deliberately constructed using two differential trails that should be impossible according to the verification tool in [PT22], due to the dependency issue within the individual underlying differential trails. The goal was to demonstrate that the tool in [PT22] is limited to ordinary differential trails and cannot be used to verify boomerang distinguishers. However, the proposed boomerang distinguisher by Hadipour et al. was only verified experimentally for a limited number of random keys, and the authors posed the development of an analytical method for verifying boomerang distinguishers as an open question. Our quasi-boomerang framework addresses this question using the mix-basis geometric approach.

Finally, in Section 5, we discuss the influence of the key schedule on the quasi-boomerang framework. By regarding the key-XOR as a standard cipher component, the quasi-boomerang framework can be applied to key-alternating ciphers, considering the key schedule in a natural way. We provide theories and formulas for this. Similarly, we revisit Boura et al.'s work in [BDG25], where the authors defined two asymmetric functions for constructing the transition matrix for the key-XOR operation in the related-key setting, and provide an alternative way to get the same theorems.

We have made all source code and experimental results related to this paper available at https://github.com/ccc53021/quasi-boomerang.

Outline. In Section 2, we briefly recall the related works of differential, boomerang attacks, Beyne's geometric approach, and the generalization of the geometric approach by Hu et al.. In Section 3, we generalize the geometric approach to boomerang distinguishers in both single-key and related-key scenarios. In Section 4, we apply the quasi-boomerang framework to several boomerang distinguishers of SKINNY-64 and GIFT-64. Section 5 discusses the quasi-boomerang framework for key-alternating ciphers with the key schedule being considered. Section 6 concludes this paper.

[1] Page 10 in https://iacr.org/submit/files/slides/2023/fse/fse2023/tosc2022_3_36/slides.pdf.

Table 1: Our analysis results of the validity of Boomerang distinguishers. **#Keys** denotes the size of the key space. **KI** denotes Key-Independent.

Cipher	#R	KI?	#Keys	Prob.	Reference
SKINNY-64-128	11	✓	2^{128}	1	Section 4.1.1
	12	✓	2^{128}	2^{-4}	Section 4.1.2
	17†	✗	2^{128}	$2^{-48.72}$	[LGS17, Table 12]
			2^{126}	$2^{-43.42}$	Section 4.2.1
			2^{127}	$2^{-45.42}$	
			2^{126}	0	
SKINNY-64-192	15	✓	2^{192}	1	Section 4.1.3
	16	✓	2^{192}	2^{-4}	Section 4.1.4
	22†	✓	2^{192}	$2^{-54.94}$	[LGS17, Table 14]
			2^{192}	$2^{-53.79}$	Section 4.2.2
GIFT-64	19†‡	✓	2^{128}	2^{-50}	[CWZ19, Table 5]
			2^{128}	2^{-68}	[JZZD20]
			2^{128}	$2^{-54.19}$	Section 4.2.3

† denotes the joint boomerang distinguishers that follow the sandwich framework.
‡ The probability of the 19-round distinguisher of GIFT-64 is 2^{-68} in [JZZD20], which is smaller than 2^{-64}, thus considered invalid.

2 Preliminaries

In this section, we recall the differential cryptanalysis, the boomerang attacks and their related-key variants, Beyne's geometric approach theory, and Hu et al.'s mix-basis extension of the geometric approach.

2.1 Differential and Boomerang Cryptanalysis

Typically, differential cryptanalysis [BS91] focuses on functions F that are structured as compositions, specifically $\mathsf{F} = \mathsf{F}_r \circ \mathsf{F}_{r-1} \circ \cdots \circ \mathsf{F}_1$. Obtaining the input and output difference for F_i, say (a_i, a_{i+1}), and connecting them, we can get a DC as $(a_1, a_2, \ldots, a_{r+1})$. The estimation of probabilities associated with these characteristics often assumes independence between the intermediate differentials:

$$\Pr_{\mathrm{DC}}[a_0, \ldots, a_{r+1}] \approx \prod_{i=1}^{r} \Pr[\mathsf{F}_i(x_i \oplus a_i) \oplus \mathsf{F}_i(x_i) = a_{i+1}]. \tag{1}$$

In scenarios where the functions $\mathsf{F}_1, \ldots, \mathsf{F}_r$ depend on keys $k_1, \ldots, k_r$, the heuristic proposed in Equation 1 can be supported by the *Markov cipher* assumption [LMM91]. Specifically, it has been shown that if all round keys are uniformly random and independent, the *key-averaged probability* of a characteristic corresponds to the product of the intermediate key-averaged probabilities.

Wagner [Wag99] first introduced the boomerang attack, which can regard the target cipher F as a composition of two sub-ciphers F_0 and F_1, i.e., $\mathsf{F} = \mathsf{F}_1 \circ \mathsf{F}_0$. The boomerang attack is an adaptive chosen plaintext-ciphertext attack. We assume that there is a

differential $\alpha \xrightarrow{\mathsf{F}_0} \beta$ with probability p, and $\gamma \xrightarrow{\mathsf{F}_1} \delta$ with probability q, The expected probability of the boomerang attack is:

$$\Pr[\mathsf{F}^{-1}(\mathsf{F}(P_1) \oplus \delta) \oplus \mathsf{F}^{-1}(\mathsf{F}(P_1 \oplus \alpha) \oplus \delta) = \alpha] = p^2q^2. \tag{2}$$

The boomerang attack relies on an independent assumption between F_0 and F_1. But this assumption might be unreliable [Mur11]. Therefore, many papers have studied this problem thoroughly, including sandwich attack [DKS10] and boomerang connectivity table (BCT) technique [CHP+18], and the generalized BCT techniques for multiple rounds [SQH19, WP19, DDV20]. The BCT technique divides the cipher into three parts, say $\mathsf{F} = \mathsf{F}_2 \circ \mathsf{F}_1 \circ \mathsf{F}_0$. Assume F_1 is a layer of parallel small Sboxes. For each Sbox, a BCT can be established.

Definition 1 (**Boomerang Connectivity Table**, [CHP+18])**.** Let $\mathsf{S} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an invertible Sbox, and $\beta, \gamma \in \mathbb{F}_2^n$. The Boomerang Connectivity Table (BCT) of S is given by a $2^n \times 2^n$ table, in which the entry for the (β, γ) position is given by

$$BCT(\beta, \gamma) = \frac{\#\{x \in \mathbb{F}_2^n | \mathsf{S}^{-1}(\mathsf{S}(x) \oplus \gamma) \oplus \mathsf{S}^{-1}(\mathsf{S}(x \oplus \beta) \oplus \gamma) = \beta\}}{2^n}.$$

If there is a differential $\alpha \xrightarrow{\mathsf{F}_0} \beta$ with probability p, and $\gamma \xrightarrow{\mathsf{F}_2} \delta$ with probability q, the probability of a boomerang distinguisher of F is p^2q^2r where $r = \Pr_{BCT}[\beta, \gamma] = BCT(\beta, \gamma)$.

Although these techniques have managed to handle the connecting point of F_0 and F_2, however, the independent assumptions in other rounds still exist, such as the propagations for F_0 and F_2. This paper verifies the boomerang distinguishers considering all these independent assumptions.

The amplified boomerang attack, later renamed as the rectangle attack [BDK01, BDK02], is proposed by Kelsey et al. [KKS00], turning the boomerang attack into the chosen-plaintext scenario. In [KT22], Kidmose and Tiessen proved that the probability of a boomerang distinguisher is 2^n times that of the corresponding rectangle distinguisher, with a formal analysis using 3-differential cryptanalysis, where n is the length of the block. In this paper, we do not strictly distinguish the terms boomerang and rectangle attacks. The geometric approach actually describes the rectangle attack; we will multiply a 2^n with the probability to make it satisfy the boomerang probability.

Boomerang attacks in the related-key setting. In [Bih94], Biham introduced related-key attacks, where the attacker knows the specific difference of the round keys. In the boomerang attacks, assume the key space is $\mathbb{K}$, the attacker can query four related-key oracles. Let Δk and ∇k denote the key differences for subciphers F_0 and F_1, respectively, and the base key is $k_1 \in \mathbb{K}$, the four keys generated from k_1 are: $k_1, k_2 = k_1 \oplus \Delta k, k_3 = k_1 \oplus \nabla k$, and $k_4 = k_1 \oplus \Delta k \oplus \nabla k$. Then the attacker queries a plaintext pair (P_1, P_2) with difference $P_1 \oplus P_2 = \alpha$ to the k_1 and k_2 encryption oracles, respectively, obtaining the corresponding ciphertext pair (C_1, C_2), and computes $C_3 = C_1 \oplus \delta, C_4 = C_2 \oplus \delta$. After that, the attacker queries the ciphertext pair (C_3, C_4) to the k_3 and k_4 decryption oracles, respectively, and gets the resulting plaintext pair (P_3, P_4). The probability that $P_3 \oplus P_4$ is equal to α is p^2q^2. In this setting, longer related-key DC and boomerang distinguishers might be obtained. The differential and boomerang attacks in the related-key setting depend on similar independent assumptions between adjacent rounds.

2.2 Beyne's Geometric Approach Theory and Its Mix-Basis Extension

The geometric approach was developed by Beyne [Bey23] as a novel and systematic method to understand cryptanalytic attacks. This theory has been successfully used in linear [Bey21], differential [BR22], (ultrametric) integral cryptanalysis [BV23, BV24b]

and some combined attacks [HZC+25]. This subsection briefly introduces the ideas of the geometric approach, as well as its most recent extension to the mix-basis attacks in [HZC+25]. The mix-basis geometric approach is closer to the techniques used in this paper.

Before we start, we first introduce the order of a space [2] and an attack that will play an important role in this paper.

Definition 2 (Order of a space and an attack [HZC+25](adapted))**.** If the rank of a subspace $\mathbb{S} = \{(x_0, x_1, \ldots, x_{s-1}) : x_i \in \mathbb{F}_2^n\}$ is d, i.e., any element in $\mathbb{S}$ can be computed by an element in $\mathbb{F}_2^{dn}$, we say the order of $\mathbb{S}$ is d. Consider $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Suppose an attack uses samples from d-th-order space, we call d the order of this attack.

For a d-th-order attack, the input and output can be generated by d linearly independent elements $x_0, x_1, \ldots, x_{d-1} \in \mathbb{F}_2^n$. Since $\mathbb{F}_2^{dn} \cong \prod_{i=1}^{d} \mathbb{F}_2^n$, we can also say that a d-th attack works for $\mathsf{F}^{\times d} : \mathbb{F}_2^{dn} \to \mathbb{F}_2^{dn}$ and denote the output as $\mathsf{F}^{\times d}(x) \in \mathbb{F}_2^{dn}$ for $x \in \mathbb{F}_2^{dn}$. When describing the basic ideas of the geometric approach or the order information is clear from the context, we will omit the superscript $\times d$ for the sake of simplicity. Actually, in most parts of this paper, the order information is clear.

Consider $\mathbb{F}_2^n$ (Note that in the following, n might be d times the block size of a cipher) and let $\mathbb{Q}$ be the rational number field. $\mathbb{Q}[\mathbb{F}_2^n]$ denotes the free vector space over $\mathbb{Q}$ generated by the elements of $\mathbb{F}_2^n$, where the basis vectors correspond to the elements of $\mathbb{F}_2^n$ and the scalars are taken from $\mathbb{Q}$, i.e.,

$$\mathbb{Q}[\mathbb{F}_2^n] = \left\{ \sum_u k_u \delta_u, k_u \in \mathbb{Q}, u \in \mathbb{F}_2^n \right\},$$

where δ_u represents the basis vector uniquely related to u.

For a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ that sends an element $u \in \mathbb{F}_2^n$ to $\mathsf{F}(u) \in \mathbb{F}_2^n$, we can induce a linear mapping T^{F} defined as

$$T^{\mathsf{F}} : \mathbb{Q}[\mathbb{F}_2^n] \to \mathbb{Q}[\mathbb{F}_2^n], \quad \sum_u k_u \delta_u \mapsto \sum_u k_u \delta_{\mathsf{F}(u)}.$$

$(\delta_u, 0 \le u < 2^n)$ is a standard basis. Following the notations in [HZC+25], when the elements of basis vectors can be represented by a function, we can use the function to represent the basis. For example, consider the Dirac delta function

$$\delta_u(\cdot) : \mathbb{F}_2^n \to \mathbb{Q}, \quad \delta_u(x) = \begin{cases} 1, \text{ if } x = u; \\ 0, \text{ otherwise.} \end{cases}$$

Putting every basis vector δ_u into the u-th column of a matrix, we can obtain a matrix, which can be written as $[\delta_u(x)]_{x,u}$, where $0 \le x < 2^n$ and $0 \le u < 2^n$ are respectively the indices of the rows and columns. Generally, given a function $f_u(\cdot) : \mathbb{F}_2^n \to \mathbb{Q}$, a matrix can be represented as $[f_u(x)]_{x,u}$ with the same style of $[\delta_u(x)]_{x,u}$. Regarding all its columns as a set of basis vectors (if the matrix is of full rank), $[f_u(x)]_{x,u}$ is a basis of $\mathbb{Q}[\mathbb{F}_2^n]$.

Remark. Here we use δ_u to represent a vector and $\delta_u(\cdot)$ a function. Note that $\delta_u = [\delta_u(x), x = 0, 1, \ldots, 2^n - 1]$, which justifies the usage of δ_u as a standard basis vector and $\delta_u(\cdot)$ a function.

T^{F} is a permutation matrix (when F is a permutation) called the transition matrix under the standard basis. When choosing a new basis for the input space and another for the

[2] The space here refers to any set, rather than a linear space.

Table 2: Seven bases of the first-order space listed in [HZC+25]. $\alpha_u(x)$ and $\beta^{\star}_{\mathsf{F}(x)}(v)$ are used in Equation 3.

Index	Basis	Effect of input $\alpha_u(x)$	Effect of output $\beta^{\star}_{\mathcal{E}(x)}(v)$
0	$[\delta_u(v)]_{v,u}$	$\delta_u(x)$	$\delta_{\mathcal{E}(x)}(v)$
1	$[(-1)^{u^\top v}]_{v,u}$	$(-1)^{u^\top x}$	$2^{-n}(-1)^{\mathcal{E}(x)^\top v}$
2	$[2^{-n}(-1)^{u^\top v}]_{v,u}$	$2^{-n}(-1)^{u^\top x}$	$(-1)^{\mathcal{E}(x)^\top v}$
3	$[u^v]_{v,u}$	u^x	$(-1)^{\mathrm{wt}(v\oplus\mathcal{E}(x))}\mathcal{E}^v(x)$
4	$[(-1)^{\mathrm{wt}(u\oplus v)}u^v]_{v,u}$	$(-1)^{\mathrm{wt}(u\oplus x)}u^x$	$\mathcal{E}^v(x)$
5	$[v^u]_{v,u}$	x^u	$(-1)^{\mathrm{wt}(v\oplus\mathcal{E}(x))}v^{\mathcal{E}(x)}$
6	$[(-1)^{\mathrm{wt}(u\oplus v)}v^u]_{v,u}$	$(-1)^{\mathrm{wt}(u\oplus x)}x^u$	$v^{\mathcal{E}(x)}$

output space, we can get another transition matrix of the linear mapping corresponding to T^{F}, after the change-of-basis operations. Let the input basis be $[\alpha_u(x)]_{x,u}$, and output basis $[\beta_u(x)]_{x,u}$. In addition, we assume that $[\beta_u(x)]^{-1}_{x,u}$ can also be represented as $[\beta^{\star}_u(x)]_{x,u}$. According to [Bey23, HZC+25], the coordinate of the new matrix under the new bases is

$$B^{\mathsf{F}}_{v,u} = \sum_{x\in\mathbb{F}_2^n} \alpha_u(x)\beta^{\star}_{\mathsf{F}(x)}(v) \tag{3}$$

According to whether $[\alpha_u(x)]_{x,u} = [\beta_u(x)]_{x,u}$, the attacks described by the geometric approach can be divided into the same-basis attack and mix-basis attack.

Definition 3 (Same-basis and mix-basis attack [HZC+25])**.** An attack on $\mathsf{F}:\mathbb{F}_2^n\to\mathbb{F}_2^n$ is called a same-basis attack if the bases chosen for the input and output spaces are the same; otherwise, it is called a mix-basis attack.

First-order attacks. In [HZC+25], Hu et al. revisited three bases from existing geometric papers and generated four additional bases with simple rules. The seven bases are listed in Table 2. By choosing a pair of bases for the input and output spaces, we can derive the coordinate expression of the corresponding matrix, which is related to a certain attack.

Example 1. Consider $\mathsf{F}:\mathbb{F}_2^n\to\mathbb{F}_2^n$. We choose $[(-1)^{u^\top x}]_{x,u}$ as the basis of the input and output spaces, the transition matrix coordinate is then

$$A^{\mathsf{F}}_{v,u} = \sum_{x\in\mathbb{F}_2^n} \alpha_u(x)\beta^{\star}_{\mathsf{F}(x)}(v) = 2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x\oplus v^\top \mathsf{F}(x)}.$$

This is related to the linear cryptanalysis [Bey21].

Higher-order attacks. For $0\le i<d$, suppose $[\alpha_u(x)]^{(i)}_{x,u}$ is a basis of $\mathbb{Q}[\mathbb{F}_2^n]$, then $\bigotimes_{0\le i<d}[\alpha_u(x)]^{(i)}_{x,u}$ is a basis for $\mathbb{Q}[\mathbb{F}_2^{dn}] = \bigotimes_{0\le i<d}\mathbb{Q}[\mathbb{F}_2^n]$, where $\otimes$ is the Kronecker product. According to the rule of the Kronecker product, if $\left([\beta_u(x)]^{(i)}_{x,u}\right)^{-1} = [\beta^{\star}_u(x)]^{(i)}_{x,u}$, then

$$\left(\bigotimes_{0\le i<d}[\beta_u(x)]^{(i)}_{x,u}\right)^{-1} = \bigotimes_{0\le i<d}[\beta^{\star}_u(x)]^{(i)}_{x,u}.$$

Hence, for a d-th order on $\mathsf{F}_2^{\times d} : \mathbb{F}_2^{dn} \to \mathbb{F}_2^{dn}$, we can choose d first-order bases to generate a d-th-order basis, and further obtain the matrix coordinate expression according to Equation 3.

Example 2. Consider a second-order attack on $\mathsf{F}^{\times 2} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$. We select $[(-1)^{u_0^\top x}]_{x,u} \otimes [\delta_{u_1}(\Delta)]_{\Delta,u_1}$ as the basis for both the input and output spaces. The transition matrix coordinate is then

$$\begin{aligned} A^{\mathsf{F}^{\times 2}}_{(v_0,v_1),(u_0,u_1)} &= \sum_{(x,\Delta)\in\mathbb{F}_2^{2n}} (-1)^{u_0^\top x}\delta_{u_1}(\Delta)(-1)^{v_0^\top \mathsf{F}(x)}\delta_{v_1}(\mathsf{F}(x)\oplus\mathsf{F}(x\oplus\Delta)) \\ &= 2^{-n} \sum_{\substack{\Delta=u_1 \\ \mathsf{F}(x)\oplus\mathsf{F}(x\oplus u_1)=v_1}} (-1)^{u_0^\top x\oplus v_0^\top \mathsf{F}(x)} \end{aligned} \tag{4}$$

This expression is the one for quasi-differential in [BR22].

2.3 Trails in Geometric Approach and Automatic Search Method

Coordinates of the transition matrix of the whole cipher are usually impossible to compute due to the huge complexity. However, ciphers are built on the small components, whose transition matrices are easy to construct. The transition matrices enjoy the following properties, making it possible to compute or approximate the coordinates for the whole cipher.

Theorem 1 ([BR22], Theorem 3.2)**.** *Let n be a positive integer and $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a function. The transition matrix B has the following properties:*

(1) If $\mathsf{F} = \mathsf{F}_1 || \ldots || \mathsf{F}_m$, then $B^{\mathsf{F}} = \bigotimes_{i=1}^m B^{\mathsf{F}_i}$.

(2) If $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$, then $B^{\mathsf{F}} = \prod_{1\le i\le r} B^{\mathsf{F}_i}$.

According to Theorem 1, for a composite cipher $\mathsf{F} = \mathsf{F}_r \circ \mathsf{F}_{r-2} \circ \cdots \circ \mathsf{F}_1$ we have

$$B^{\mathsf{F}}_{u^{r+1},u^1} = \sum_{u^r,\ldots,u^2} \prod_{i=1}^{r} B^{\mathsf{F}_i}_{u^{i+1},u^i}.$$

$(u^1, u^2, \ldots, u^{r+1})$ is called a trail and $\prod_{i=1}^r B^{\mathsf{F}_i}_{u^{i+1},u^i}$ is its correlation. The whole correlation $B^{\mathsf{F}}_{u^{r+1},u^1}$ is equal to the sum of all corresponding trails' correlations. For a d-th-order attack, u^i is a d-tuple, like $u^i = (u^i_1, u^i_2, \ldots, u^i_d)$. Sometimes we need to put some constraints on u^1 and u^{r+1} to meet an existing attack.

Example 3. Consider the quasi-differential transition matrix coordinate in Example 2. By setting $u_0 = v_0 = 0$, we obtain the probability of a differential (u_1, v_1).

To approximate $A^{\mathsf{F}^{\times 2}}_{(0,v_1),(0,u_1)}$, we need to enumerate all trails (DCs) that connect $(0, v_1)$ and $(0, u_1)$ and sum their correlations (probabilities). The sum of the correlations is the exact differential probability.

Dominate trails assumption. In practice, the number of trails is usually huge, making it is impossible to enumerate all of them. Thus, cryptanalysis relies on the dominant trail assumption. For example, in linear cryptanalysis, we assume that the linear trail that has the maximum absolute correlation would dominate the sum of all trails' correlations (or provide some reasonable bounds). In the quasi-differential framework, sometimes, it is also assumed that a small part of quasi-differential trails with the largest absolute correlations would reflect the whole probability of a DC.

3 Geometric Approach for Boomerang Cryptanalysis

In this section, we generalize the geometric approach to describe boomerang cryptanalysis. To represent the boomerang attack shown in Figure 1, we first choose the order of the attack and define the bases for the input and output spaces, so that boomerang attacks can be described as a 3rd-order mix-basis attack [HZC+25]. After that, the two upper and lower differentials (characteristics) can be connected through a single S-box layer in the middle. Next, we define the concepts of BCs and quasi-BCs, and show how to compute the probability of a boomerang in the fixed-key model. The influence of round keys on the boomerang probability can be analyzed similarly to the quasi-DCs in the quasi-differential framework. Finally, we show that the quasi-boomerang framework also applies to the related-key boomerang attacks.

3.1 Choose the Order for Boomerang Attacks

According to [HZC+25], when extending the geometric approach to new attacks, we should first decide the *order* of the attack. Since the boomerang attack treats four values (a quartet), the orders of the input and output spaces are both 4. In this sense, the boomerang attack can be described by a 4th-order attack. In fact, in [WSW+24], Wang et al. extended the quasi-differential framework to quasi-d-differential cryptanalysis. When $d = 3$, the quasi-3-differential cryptanalysis can be used to describe the boomerang attack. This is also similar to the d-difference of the polytope attacks [Tie16].

However, the quasi-3-differential cryptanalysis has two drawbacks: the number of rows and columns in the transition matrix is four times the size of the S-box, which makes the search process very slow, and the number of quasi-3-differential trails is too huge, resulting in the search being impractical. In fact, the authors in [WSW+24] actually searched for only a part of the quasi-3-differentials that correspond to the two middle rounds of a boomerang distinguisher they aimed to check.

To make the search practical, we notice that the orders of the input and output spaces can be described as 3, which is inspired by an implicit assumption that the four values in a quartet will sum to zero for both the classical boomerang distinguishers and the refined ones with BCT [3]. In this case, i.e., assuming that the inner quartet always sums to zero, the theoretical boomerang probability is indeed an estimate of the actual boomerang probability. Then the boomerang analysis can be simplified by adding a constraint to make sure the sum of the quartet is always zero. When checking the probability of a boomerang distinguisher, the differences of the state and key (following key schedule) can be known, making the transition matrices for boomerangs further reduce to twice the size of the S-box, so the search process becomes easier.

In the following, we will refer to this assumption as the *third-order assumption*. We emphasize that most previous boomerang attacks also work under this assumption.

3.2 Quasi-Boomerang Bases as a 3rd-Order Attack

Consider a 3rd-order space $\mathbb{X} = \{(a, b, c, d) : a \oplus b \oplus c \oplus d = 0,\ a, b, c, d \in \mathbb{F}_2^n\}$, and construct the free vector space $\mathbb{Q}[\mathbb{X}]$. We can induce a linear mapping $T^{\mathsf{F}} : \mathbb{Q}[\mathbb{X}] \to \mathbb{Q}[\mathbb{X}]$ for a cipher F.

As shown in Figure 1, in boomerang attacks, we consider the propagation

$$(x, \Delta_1, \Delta_2) \to (y = \mathsf{F}(x), \nabla_1 = \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta_1), \nabla_2 = \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta_2)).$$

Under the standard basis, the transition matrix of F can be obtained, whose coordinates

[3] $x_0 \oplus x_1 \oplus x_2 \oplus x_3 = 0$ is equivalent to $x_0 \oplus x_1 = x_2 \oplus x_3$ or $x_0 \oplus x_2 = x_1 \oplus x_3$.

are

$$T^{\mathsf{F}}_{(v_0,v_1,v_2),(u_0,u_1,u_2)} = \delta_{v_0}(\mathsf{F}(u_0))\delta_{v_1}(\mathsf{F}(u_0)\oplus\mathsf{F}(u_0\oplus u_1))\delta_{v_2}(\mathsf{F}(u_0)\oplus\mathsf{F}(u_0\oplus u_2))$$

Next, we choose an alternative basis to describe the boomerang attack. For the input space, only Δ_1 is explicitly fixed, so we use the standard basis for it, given by $[\delta_{u_1}(\Delta_1)]_{\Delta_1,u_1}$. Simultaneously, x and Δ_2 can take any value. Similar to the setting for input and output values in the quasi-differential framework, we use a linear basis for x and Δ_2, given by $[(-1)^{u_0^\top x}]_{x,u_0}$ and $[(-1)^{u_2^\top \Delta_2}]_{\Delta_2,u_2}$. Putting these components together, the basis for the input space is

$$\begin{aligned} b_{in} &= [(-1)^{u_0^\top x}]_{x,u_0}\otimes[\delta_{u_1}(\Delta_1)]_{\Delta_1,u_1}\otimes[(-1)^{u_2^\top\Delta_2}]_{\Delta_2,u_2} \\ &= [(-1)^{u_0^\top x}\delta_{u_1}(\Delta_1)(-1)^{u_2^\top\Delta_2}]_{(u_0,u_1,u_2),(x,\Delta_1,\Delta_2)} \end{aligned} \tag{5}$$

In the output space, y and ∇_1 can take any value, but ∇_2 will be fixed and determined. Following the same structure as the input, we choose the output basis as

$$\begin{aligned} b_{out} &= [(-1)^{v_0^\top y}]_{y,v_0}\otimes[(-1)^{v_1^\top\nabla_1}]_{\nabla_1,v_1}\otimes[\delta_{v_2}(\nabla_2)]_{\nabla_2,v_2} \\ &= [(-1)^{v_0^\top y}(-1)^{v_1^\top\nabla_1}\delta_{v_2}(\nabla_2)]_{(y,\nabla_1,\nabla_2),(v_0,v_1,v_2)} \end{aligned} \tag{6}$$

Since the input and output bases are different, the boomerang attack can be described as a mix-basis attack. Following [HZC+25], we divide the target cipher F into three parts, $\mathsf{F}=\mathsf{F}_2\circ\mathsf{F}_1\circ\mathsf{F}_0$, where F_1 is an S-box layer. We then construct the transition matrices for each of the three parts.

For $\mathsf{F}_0:(x,\Delta_1,\Delta_2)\to(y,\nabla_1,\nabla_2)$, the basis b_{in} in Equation 5 is used for the input, output, and intermediate spaces. So we obtain a same-basis attack, where the coordinates of the corresponding transition matrix are

$$\begin{aligned} B^{\mathsf{F}_0}_{(v_0,v_1,v_2),(u_0,u_1,u_2)} &= \frac{1}{2^{2n}}\sum_{x,\Delta_1,\Delta_2}(-1)^{u_0^\top x}\delta_{u_1}(\Delta_1)(-1)^{u_2^\top\Delta_2}(-1)^{v_0^\top y}\delta_{v_1}(\nabla_1)(-1)^{v_2^\top\nabla_2} \\ &= \frac{1}{2^{2n}}\sum_{\substack{x\in\mathbb{F}_2^n,\Delta_2\in\mathbb{F}_2^n\\ \Delta_1=u_1,\nabla_1=v_1}}(-1)^{u_0^\top x\oplus u_2^\top\Delta_2\oplus v_0^\top y\oplus v_2^\top\nabla_2} \end{aligned} \tag{7}$$

under the constraint $\mathsf{F}_0(x\oplus\Delta_1\oplus\Delta_2)=\mathsf{F}_0(x)\oplus\mathsf{F}_0(x\oplus\Delta_1)\oplus\mathsf{F}_0(x\oplus\Delta_2)$, where this constraint is to ensure that the elements are from the 3rd-order space $\mathbb{X}$.

For $\mathsf{F}_2:(x,\Delta_1,\Delta_2)\to(y,\nabla_1,\nabla_2)$, the basis b_{out} in Equation 6 is used for the input, output, and intermediate spaces. Therefore, we also obtain a same-basis attack. The coordinates of the corresponding transition matrix are given by

$$\begin{aligned} B^{\mathsf{F}_2}_{(v_0,v_1,v_2),(u_0,u_1,u_2)} &= \frac{1}{2^{2n}}\sum_{x,\Delta_1,\Delta_2}(-1)^{u_0^\top x}(-1)^{u_1^\top\Delta_1}\delta_{u_2}(\Delta_2)(-1)^{v_0^\top y}(-1)^{v_1^\top\nabla_1}\delta_{v_2}(\nabla_2) \\ &= \frac{1}{2^{2n}}\sum_{\substack{x\in\mathbb{F}_2^n,\,\Delta_1\in\mathbb{F}_2^n\\ \Delta_2=u_2,\,\nabla=v_2}}(-1)^{u_0^\top x\oplus u_1^\top\Delta_1\oplus v_0^\top y\oplus v_1^\top\nabla_1} \end{aligned} \tag{8}$$

under the constraint $\mathsf{F}_2(x\oplus\Delta_1\oplus\Delta_2)=\mathsf{F}_2(x)\oplus\mathsf{F}_2(x\oplus\Delta_1)\oplus\mathsf{F}_2(x\oplus\Delta_2)$, which ensures that the elements belong to the 3rd-order space $\mathbb{X}$.

Definition 4 (Quasi-biDDT)**.** We refer to the transition matrices defined in Equation 7 and Equation 8 as the quasi-biDDT, since they model the propagation of two differences. To distinguish between them, we call the one for F_0 the upper quasi-biDDT, and the one for F_2 the lower quasi-biDDT.

For $\mathsf{F}_1 : (x, \Delta_1, \Delta_2) \to (y, \nabla_1, \nabla_2)$, we use b_{in} as the input basis and b_{out} as the output basis. The corresponding transition matrix is

$$\begin{aligned} B^{\mathsf{F}_1}_{(v_0,v_1,v_2),(u_0,u_1,u_2)} &= \frac{1}{2^{2n}} \sum_{x,\Delta_1,\Delta_2} (-1)^{u_0^\top x} \delta_{u_1}(\Delta_1)(-1)^{u_2^\top \Delta_2}(-1)^{v_0^\top y}(-1)^{v_1^\top \nabla_1}\delta_{v_2}(\nabla_2) \\ &= \frac{1}{2^{2n}} \sum_{\substack{x\in\mathbb{F}_2^n,\, \Delta_2\in\mathbb{F}_2^n \\ \Delta_1=u_1,\, \nabla_2=v_2}} (-1)^{u_0^\top x_0 \oplus u_2^\top \Delta_2 \oplus v_0^\top y \oplus v_1^\top \nabla_1} \end{aligned} \tag{9}$$

Again, we impose the constraint $\mathsf{F}_1(x \oplus \Delta_1 \oplus \Delta_2) = \mathsf{F}_1(x) \oplus \mathsf{F}_1(x \oplus \Delta_1) \oplus \mathsf{F}_1(x \oplus \Delta_2)$ to ensure that the transition respects the structure of the 3rd-order space $\mathbb{X}$.

Definition 5 (Quasi-BCT)**.** The transition matrix defined by Equation 9 models the propagation from the upper difference to the lower difference, similar to the BCT. However, unlike the classical BCT, it also takes the values into account. Thus, we call this matrix quasi-BCT.

Remark. The value calculated by Equation 9 represents the probability of a rectangle distinguisher. To obtain the boomerang probability, we need to multiply this value by a factor of 2^n. Throughout this paper, we report the probability of the boomerang distinguishers, so we always apply the 2^n factor to the probability obtained from Equation 9.

3.3 Probability Calculation from Quasi-Boomerang Characteristics

To compute the probability of boomerang distinguishers, we build a framework similar to the one used for differentials. A given differential distinguisher may include many quasi-DCs, some of which play a dominant role in determining the overall probability. Following the structure of the framework for basic differential distinguishers, we first define the concept of boomerang characteristics (BCs) and then show that the probability of a boomerang distinguisher can be determined by the probability of its so-called quasi-boomerang characteristics (quasi-BCs).

Consider $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$. By Theorem 1 and Equation 7, Equation 8 and Equation 9, we have

$$B^{\mathsf{F}}_{\omega_{r+1},\omega_1} = \sum_{\omega_2,\ldots,\omega_r} \prod_{i=1}^{r} B^{\mathsf{F}_i}_{\omega_{i+1},\omega_i}, \tag{10}$$

where $w_i = (u_0^i, u_1^i, u_2^i)$ is a 3-tuple. To obtain the exact probability of the boomerang distinguisher (under the 3rd-order assumption) with the input difference of the upper DC being Δ_1 and the output difference of the lower DC being ∇_2, we can set $\omega_1 = (0, \Delta_1, 0)$ and $\omega_{r+1} = (0, 0, \nabla_2)$, search for all trails $(\omega_1, \omega_2, \ldots, \omega_{r+1})$ that connect ω_1 and ω_{r+1}, and sum up their correlations.

However, usually the number of trails is huge, so it is difficult to exhaust all of them. To make the search easier, we mimic the quasi-differential framework by defining the boomerang characteristics (BCs) and quasi-boomerang characteristics (quasi-BCs). In this way, first, we search for BCs. Second, for each BC, we search for quasi-BCs corresponding to this BC.

Definition 6 (Boomerang characteristic (BC))**.** Consider a composite cipher $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_{m+1} \circ \mathsf{F}_m \circ \mathsf{F}_{m-1} \circ \cdots \circ \mathsf{F}_1$, where the subcipher $\mathsf{F}_{m-1} \circ \cdots \circ \mathsf{F}_1$ has a differential characteristic $(a_1, \ldots, a_m)$, and the subcipher $\mathsf{F}_r \circ \cdots \circ \mathsf{F}_{m+1}$ has a differential characteristic $(a_{m+1}, \ldots, a_{r+1})$. Assuming that the BCT connects a_m and a_{m+1}, the full sequence $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$ can serve as an approximation of the boomerang distinguisher, which we refer to as a *boomerang characteristic*, abbreviated as BC.

Under the round-independence assumption, the probability of a boomerang characteristic is approximated as [4]

$$\begin{aligned}\Pr_{\mathrm{BC}}[a_1,\ldots,a_m,a_{m+1},\ldots,a_{r+1}] &\approx \left(\Pr_{\mathrm{DC}}[a_1,\ldots,a_m]\right)^2 \cdot \left(\Pr_{\mathrm{DC}}[a_{m+1},\ldots,a_{r+1}]\right)^2 \cdot \Pr_{\mathrm{BCT}}[a_m,a_{m+1}] \\ &\approx \prod_{i=1}^{m-1} (\Pr_{DC}[a_i,a_{i+1}])^2 \Pr_{BCT}[a_m,a_{m+1}] \prod_{i=m+1}^{r} (\Pr_{DC}[a_i,a_{i+1}])^2\end{aligned} \tag{11}$$

The approximate probability of a BC is natural when we set $u_0 = u_2 = v_0 = v_2 = 0$ in Equation 7, set $u_0 = u_1 = v_0 = v_1 = 0$ in Equation 8, and set $u_0 = u_2 = v_0 = v_1 = 0$ in Equation 9.

An intuitive explanation for this is that these zero values allow any values for intermediate values and some differences, which actually leads to the round-independence assumption.

According to Theorem 1, the probability of a boomerang distinguisher for F, can be calculated by summing all the correlations of the quasi-boomerang characteristics.

Definition 7 (Quasi-boomerang characteristic (quasi-BC))**.** A quasi-boomerang characteristic for a function $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_{m+1} \circ \mathsf{F}_m \circ \cdots \circ \mathsf{F}_1$ is a sequence $\omega_1,\ldots,\omega_m,\omega_{m+1},\ldots,\omega_{r+1}$ of triples, where each $\omega_i = (u_0^i, u_1^i, u_2^i)$ for $1 \le i \le r+1$. We calculate the correlation of the quasi-BC as $\prod_{i=1}^{r} B^{\mathsf{F}_i}_{\omega_{i+1},\omega_i}$. Here, B^{F_i} is the transition matrix associated with the component F_i:

- for $i < m$, B^{F_i} is the upper quasi-biDDT (Equation 7),
- for $i = m$, B^{F_i} is the quasi-BCT (Equation 9),
- for $i > m$, B^{F_i} is the lower quasi-biDDT (Equation 8).

When $\forall i$, $u_0^i = 0$, $\forall i \le m$, $u_2^i = 0$, and $\forall i \ge m+1$, $u_1^i = 0$, the quasi-BC corresponds to a BC. Similar to [BR22, Theorem 4.1], we can use the quasi-BC to compute the exact probability of a BC, as stated in the following proposition. Note that Equation 11 gives the approximate probability of a BC under the round-independence assumption, but the following is without the assumption.

Proposition 1. *Consider $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_{m+1} \circ \mathsf{F}_m \circ \cdots \circ \mathsf{F}_1$. The exact probability of a BC $(a_1,\ldots,a_m,a_{m+1},\ldots,a_{r+1})$ is equal to the sum of the correlations of all quasi-BCs that share the same intermediate differences (we use t to represent 1 or 2. For example, u_t can be u_1 or u_2, according to the round number):*

$$\Pr_{\mathrm{BC}}[a_1,a_2,\ldots,a_{r+1}] = \Pr_{BC}\left[\bigwedge_{i=1}^{r} a_i \xrightarrow{\mathsf{F}_i} a_{i+1}\right] = \sum_{u_0^2,\ldots,u_0^r} \sum_{u_t^1,\ldots,u_t^r} \prod_{i=1}^{r} B^{\mathsf{F}_i}_{\omega_{i+1},\omega_i}, \tag{12}$$

where $\omega_i = (u_0^i, a_i, u_2^i)$ for $1 \le i \le m$, and $\omega_i = (u_0^i, u_1^i, a_i)$ for $m+1 \le i \le r+1$, with $u_0^1 = u_0^{r+1} = 0$, $u_1^{r+1} = 0$, and $u_2^1 = 0$.

Proof. The proof is analogous to that of [BR22, Theorem 4.1]. After substituting quasi-biDDTs and quasi-BCT into the right side of Equation 12, we get

$$\prod_{i=1}^{r} B^{\mathsf{F}_i}_{\omega_{i+1},\omega_i} = \frac{1}{2^{2nr}} \sum_{\substack{x_1,\ldots,x_r \\ \Delta_t^1,\ldots,\Delta_t^r \\ a_i \to a_{i+1}}} \prod_{i=1}^{r} (-1)^{(u_0^i)^\top x_i \oplus (v_0^i)^\top \mathsf{F}_i(x_i)} (-1)^{(u_t^i)^\top \Delta_t^i \oplus (v_t^i)^\top (\mathsf{F}_i(x_i) \oplus \mathsf{F}_i(x_i \oplus \Delta_t^i))}$$

[4] The BC takes the same position as the DC in the quasi-differential framework. However, the probability of a BC is usually far smaller than the real probability of a boomerang distinguisher, as the independence assumption and dominant trail assumption barely hold for boomerang attacks, which is very different from the DC cases. Hence, the probability of a BC is not used for computing/approximating the probability of the boomerang distinguisher in this paper. BCs are used as a bridging step for searching for quasi-BCs.

Summing over $(u_0^2, u_t^2), (u_0^2, u_t^2), \ldots, (u_0^r, u_t^r)$ results in

$$\begin{aligned}
&\sum_{(u_0^1,u_t^1),\ldots,(u_0^r,u_t^r)} \prod_{i=1}^{r} B^{\mathsf{F}_i}_{\omega_{i+1},\omega_i} \\
&= \sum_{\substack{x_1,\ldots,x_r \\ \Delta_t^1,\ldots,\Delta_t^r \\ a_i \to a_{i+1}}} \prod_{i=1}^{r} \left(2^{-n} \sum_{u_0^i} (-1)^{(u_0^i)^\top (x_{i+1} \oplus \mathsf{F}(x_i))}\right) \left(2^{-n} \sum_{u_0^i} (-1)^{(u_t^i)^\top (\Delta_t^{i+1} \oplus \mathsf{F}^\Delta(\Delta_t^i))}\right) \\
&= \frac{1}{2^{2n}} \sum_{\substack{x_1,\ldots,x_r \\ \Delta_t^1,\ldots,\Delta_t^r \\ a_i \to a_{i+1}}} \prod_{i=1}^{r} \delta_{x_{i+1}}\left(\mathsf{F}(x_i)\right) \delta_{\Delta_t^{i+1}}(\mathsf{F}_i^\Delta(\Delta_t^i)).
\end{aligned}$$

$\mathsf{F}_i^\Delta(\Delta_t^i)$ means the value Δ_t^i becomes after F, which can be the output difference of the upper-biDDT, the lower-biDDT, or the quasi-BCT according to the round number. Writing the last part of the above equation into the probability leads to the result.

□

To end this section, we give the proposition about the quasi-BC whose absolute correlation is equal to the BC's probability (Equation 11). This proposition is analogous to [BR22, Theorem 4.2]. Similarly to the quasi-differential framework, such quasi-BCs are of specific interest, as they are useful to split the key space, which will be used in our applications.

Proposition 2. *For $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_{m+1} \circ \mathsf{F}_m \circ \cdots \circ \mathsf{F}_1$ and a BC $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$ with probability p, it holds that:*

(1) If $(u_0^1, a_1, u_2^1), \ldots, (u_0^m, a_m, u_2^m), (u_0^{m+1}, u_1^{m+1}, a_{m+1}), \ldots, (u_0^{r+1}, u_1^{r+1}, a_{r+1})$ is a quasi-BC with correlation $(-1)^b p$, where $b \in \{0, 1\}$, then for any quasi-BC $(v_0^1, a_1, v_2^1), \ldots, (v_0^m, a_m, v_2^m), (v_0^{m+1}, v_1^{m+1}, a_{m+1}), \ldots, (v_0^{r+1}, v_1^{r+1}, a_{r+1})$ with correlation c, the correlation of the quasi-BC $(u_0^1 + v_0^1, a_1, u_2^1 + v_2^1), \ldots, (u_0^m + v_0^m, a_m, u_2^m + v_2^m), (u_0^{m+1} + v_0^{m+1}, u_1^{m+1} + v_1^{m+1}, a_{m+1}), \ldots, (u_0^{r+1} + v_0^{r+1}, u_1^{r+1} + v_1^{r+1}, a_{r+1})$ is $(-1)^b c$.

(2) If the correlations of any number of quasi-BCs with differences $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$ of the BC and correlation $\pm p$ sum to zero, then the probability of the BC $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$ is zero.

Proof. For the first property, if the quasi-BC $(u_0^1, a_1, u_2^1), \ldots, (u_0^m, a_m, u_2^m), (u_0^{m+1}, u_1^{m+1}, a_{m+1}), \ldots, (u_0^{r+1}, u_1^{r+1}, a_{r+1})$ with correlation $(-1)^b p, b \in \{0, 1\}$, then $B^{\mathsf{F}_i}_{\omega_{i+1},\omega_i}$ is equal to $(-1)^{b_i} p_i$ for $1 \le i \le r$, where

$$p_i = \begin{cases} B^{\mathsf{F}_i}_{(0,a_{i+1},0)(0,a_i,0)}, & 1 \le i \le m-1, \\ B^{\mathsf{F}_i}_{(0,0,a_{i+1}),(0,a_i,0)}, & i = m \\ B^{\mathsf{F}_i}_{(0,0,a_{i+1}),(0,0,a_i)}, & m+1 \le i \le r \end{cases}$$

That is, the expressions of the power of (-1) for all x and Δ_1/Δ_2 satisfying the constraint $\mathsf{F}(x \oplus \Delta_1 \oplus \Delta_2) = \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta_1 \oplus \Delta_2)$ in the Equation 7, Equation 8 and Equation 9 have the same sign $(-1)^{b_i}$. Thus, the correlation of the i-th transition matrix B^{F_i} of the quasi-BC $(u_0^1 + v_0^1, a_1, u_2^1 + v_2^1), \ldots, (u_0^m + v_0^m, a_m, u_2^m + v_2^m), (u_0^{m+1} + v_0^{m+1}, u_1^{m+1} + v_1^{m+1}, a_{m+1}), \ldots, (u_0^{r+1} + v_0^{r+1}, u_1^{r+1} + v_1^{r+1}, a_{r+1})$ is multiplied by $(-1)^{b_i}$.

The first property implies that all quasi-BCs with absolute correlation p have a total power of two and can be divided into subsets according to those quasi-BCs with correlation $-p$, i.e., the probability of the BC is zero if there exists a quasi-BC with correlation $-p$. □

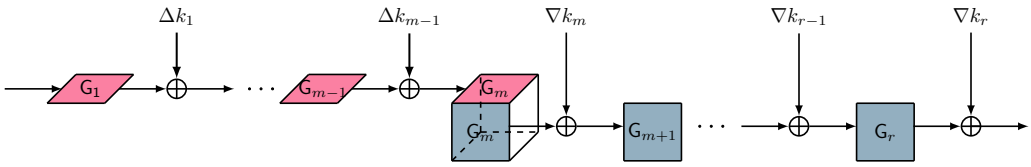

Figure 2: The BC in the related-key setting for a composite key-alternating cipher $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_{m+1} \circ \mathsf{F}_m \circ \cdots \circ \mathsf{F}_1$.

3.4 Quasi-BC for Key-Alternating Ciphers

In this subsection, we consider the quasi-boomerang framework for the key-alternating ciphers. As a convention, we assume that the round keys are independent variables, as illustrated in Figure 2.

Single-key model. Let $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_{m+1} \circ \mathsf{F}_m \circ \mathsf{F}_{m-1} \circ \cdots \circ \mathsf{F}_1$ be a key-alternating cipher. In the single-key model, $\mathsf{F}_i = \mathsf{F}_{k_i} \circ \mathsf{G}_i$, where $\mathsf{F}_k(x) = x \oplus k$. From Equation 10 and Theorem 1(2), we can get

$$B^{\mathsf{F}}_{\omega_{r+1},\omega_1} = \sum_{\omega_2,\ldots,\omega_r} \prod_{i=1}^{r} (-1)^{(u_0^i)^\top k_i} B^{\mathsf{G}_i}_{\omega_{i+1},\omega_i}, \tag{13}$$

where $\omega_i = (u_0^i, u_1^i, u_2^i)$ for $1 \le i < r$. Analogous to the quasi-differential, the round key values only affect the sign of a quasi-BC's correlation for key-alternating ciphers. In terms of the BC's probability, a corollary of Proposition 1 is obtained.

Corollary 1. *Consider a key-alternating cipher* $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_m \circ \cdots \circ \mathsf{F}_1$*, where* $\mathsf{F}_i = \mathsf{F}_{k_i} \circ \mathsf{G}_i$ *and let* F_m *be the middle subcipher. The probability of a BC* $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$ *is*

$$\Pr_{\mathrm{BC}}[a_1, a_2, \ldots, a_{r+1}] = \sum_{\substack{u_0^2,\ldots,u_0^r \\ u_2^2,\ldots,u_2^m,u_1^{m+1}\ldots,u_1^r}} \prod_{i=1}^{r} (-1)^{(u_0^i)^\top k_i} B^{\mathsf{F}_m}_{\omega_{m+1},\omega_m} \prod_{i=1}^{r} B^{\mathsf{G}_i}_{\omega_{i+1},\omega_i} \tag{14}$$

where $\omega_i = (u_0^i, a_i, u_2^i)$ *for* $1 \le i \le m$*, and* $\omega_i = (u_0^i, u_1^i, a_i)$ *for* $m+1 \le i \le r+1$*, with* $u_0^1 = u_0^{r+1} = 0$*,* $u_1^{r+1} = 0$*, and* $u_2^1 = 0$*.*

Related-key setting. As illustrated in Figure 2, in related-key boomerang attacks, $\mathsf{F}_i = \mathsf{F}_{k_i,\Delta k_i,\nabla k_i} \circ \mathsf{G}_i$, where

$$\mathsf{F}_{k,\Delta k,\nabla k} : (x, \Delta_1, \Delta_2) \to (x \oplus k, \Delta_1 \oplus \Delta k, \Delta_2 \oplus \nabla k).$$

The upper quasi-biDDT for $\mathsf{F}_{k,\Delta_1 k,\Delta_2 k}$ can be calculated according to Equation 7 as

$$\begin{aligned} B^{\mathsf{F}_{k,\Delta k,\nabla k}}_{(v_0,v_1,v_2),(u_0,u_1,u_2)} &= \frac{1}{2^{2n}} \sum_{\substack{x\in\mathbb{F}_2^n,\nabla k\in\mathbb{F}_2^n,\Delta_1=u_1 \\ u_1\oplus\Delta k=v_1}} (-1)^{u_0^\top x \oplus u_2^\top \Delta_2 \oplus v_0^\top (x\oplus k) \oplus v_2^\top (\Delta_2 \oplus \nabla k)} \\ &= (-1)^{v_0^\top k \oplus v_2^\top \nabla k} \delta_{v_1}(u_1 \oplus \Delta k)\delta_{v_0}(u_0)\delta_{v_2}(u_2). \end{aligned} \tag{15}$$

Similarly, the lower quasi-biDDT for $\mathsf{F}_{k,\Delta k,\nabla k}$ can be calculated according to Equation 8 as

$$B^{\mathsf{F}_{k,\Delta k,\nabla k}}_{(v_0,v_1,v_2),(u_0,u_1,u_2)} = (-1)^{v_0^\top k \oplus v_1^\top \Delta k} \delta_{v_2}(u_2 \oplus \nabla k)\delta_{v_0}(u_0)\delta_{v_1}(u_1) \tag{16}$$

Let F_m be the middle subcipher. In the related-key setting, Equation 13 becomes to

$$B^{\mathsf{F}}_{\omega_{r+1},\omega_1} = \sum_{\omega_2,\ldots,\omega_r} \left(\prod_{i=1}^{m-1} (-1)^{(u_0^i)^\top k_i \oplus (u_2^i)^\top \nabla k_i} \prod_{i=m}^{r} (-1)^{(u_0^i)^\top k_i \oplus (u_1^i)^\top \Delta k_i} \right) \prod_{i=1}^{r} B^{\mathsf{G}_i}_{\omega_{i+1},\omega_i}, \tag{17}$$

where $\omega_i = (u_0^i, u_1^i, u_2^i)$. The round key values and round key differences only affect the sign of a quasi-BC's correlation.

Suppose that we have known the differences of round keys as $((\Delta k_1, \nabla k_1), \ldots, (\Delta k_r, \nabla k_r))$, the probability of a related-key BC $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$ under the key differences also equals the sum of correlations of quasi-BCs.

Corollary 2. *Consider a key-alternating cipher* $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_m \circ \cdots \circ \mathsf{F}_1$*, where* $\mathsf{F}_i = \mathsf{F}_{k_i,} \circ \mathsf{G}_i$ *and let* F_m *be the middle subcipher. The probability of a related-key BC* $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$ *under the round key differences* $((\Delta k_1, \nabla k_1), \ldots, (\Delta k_r, \nabla k_r))$ *is*

$$\begin{aligned} &\Pr_{\mathrm{BC}}[a_1, a_2, \ldots, a_{r+1}] \\ &= \sum_{\substack{u_0^2,\ldots,u_0^r \\ u_2^2,\ldots,u_2^m,u_1^{m+1}\ldots,u_1^r}} \left(\prod_{i=1}^{m-1} (-1)^{(u_0^i)^\top k_i \oplus (u_2^i)^\top \nabla k_i} \prod_{i=m}^{r} (-1)^{(u_0^i)^\top k_i \oplus (u_1^i)^\top \Delta k_i} \right) \prod_{i=1}^{r} B^{\mathsf{G}_i}_{\omega_{i+1},\omega_i}, \end{aligned} \tag{18}$$

where $\omega_i = (u_0^i, a_i, u_2^i)$ *for* $1 \le i \le m$*, and* $\omega_i = (u_0^i, u_1^i, a_i)$ *for* $m+1 \le i \le r+1$*, with* $u_0^1 = u_0^{r+1} = 0$*,* $u_1^{r+1} = 0$*, and* $u_2^1 = 0$*.*

Revisiting the quasi-differential case [BDG25]. In [BDG25], Boura, Derbez, and Germon extended the quasi-differential framework to the related-key setting. Instead of applying the change-of-basis operation for $T^{\mathsf{F}} \otimes T^{\mathsf{F}}$, they consider $T^{\mathsf{F}} \otimes T^{\mathsf{G}}$ by defining a new function G that reflects the difference in the round keys (or in the key schedule functions). Their method works well for the related-key differential. However, we argue that such a method might not be the best way to extend the quasi-differential to the related-key setting. For example, to study the related-key quasi-d-differential, we need to define d new functions.

In the following, we revisit the transition matrix of the key-XOR operation in the related-key setting when assuming the round keys are independent. Instead of defining a new function G, we regard the key-XOR function $\mathsf{F}_{k,\Delta k}$ as

$$\mathsf{F}_{k,\Delta k} : (x, \Delta) \to (x \oplus k, \Delta \oplus \Delta k).$$

Thus, applying the quasi-differential transition matrix (Equation 4) to $\mathsf{F}_{k,\Delta k}$, we get

$$\begin{aligned} D^{\mathsf{F}_{k,\Delta k}}_{(v_0,v_1),(u_0,u_1)} &= 2^{-n} \sum_{x \in \mathbb{F}_2^n, x \oplus k \oplus x \oplus u_1 \oplus k \oplus \Delta k = v_1} (-1)^{u_0^\top x \oplus v_0^\top (x \oplus k)} \\ &= (-1)^{v_0^\top k} \delta_{v_1}(u_1 \oplus \Delta k) 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{(u_0^\top \oplus v_0^\top) x} \\ &= (-1)^{v_0^\top k} \delta_{v_1}(u_1 \oplus \Delta k) \delta_{v_0}(u_0). \end{aligned}$$

The same expression was obtained in [BDG25].

Difference between Boura's and our perspectives. The underlying ideas are the same. However, the authors of [BDG25] defined a new function G to make an asymmetric pair of functions (F, G), and apply the quasi-differential framework to (F, G). Our viewpoint is that G is naturally derived from F when regarding the differential attack as a second-order

attack. Formally, there is an operator that generates a second-order F from the original F as

$$\mathsf{F} \to \mathsf{F}^{\times 2} \quad \text{where} \quad \mathsf{F}^{\times 2}(x, \Delta) = (\mathsf{F}(x), \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta)).$$

Then we apply the geometric approach to $\mathsf{F}^{\times 2}$.

Let $D_\Delta \mathsf{F}(x) := \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta)$ be the derivative of F in direction Δ evaluated on x. When studying the d-differential attack, we can generate a $(d+1)$-th order F as

$$\mathsf{F} \to \mathsf{F}^{\times (d+1)} \quad \text{where} \quad \mathsf{F}^{\times (d+1)}(x, \Delta_1, \ldots, \Delta_d) = (\mathsf{F}(x), D_{\Delta_1}\mathsf{F}(x), \ldots, D_{\Delta_d}\mathsf{F}(x)).$$

Then the quasi-differential framework as well as the related-key theorems can be extended to the d-differential case, by applying the quasi-d-differential basis [WSW+24] to $\mathsf{F}^{\times (d+1)}$.

4 Applications to Boomerang Distinguishers

Automatic Search Model. According to Definition 6 and Definition 7, for $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_{m+1} \circ \mathsf{F}_m \circ \cdots \circ \mathsf{F}_1$, a BC is a sequence of differences like

$$(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1}),$$

while a quasi-BC is a sequence of triples like

$$(\omega_1, \ldots, \omega_m, \omega_{m+1}, \ldots, \omega_{r+1}),$$

where $\omega_i = (u_0^i, u_1^i, u_2^i)$, for $1 \le i \le r+1$ and $u_0^1 = u_2^1 = u_0^{r+1} = u_1^{r+1} = 0$. Replacing the corresponding differences of the quasi-BC from the given BC, we can search for the sequence of the remaining two masks in each triple, which is like

$$((0, a_1, 0), \ldots, (u_0^m, a_m, u_2^m), (u_0^{m+1}, u_1^{m+1}, a_{m+1}), \ldots, (0, 0, a_{r+1})).$$

According to Proposition 1, the sum of all correlations of such quasi-BCs is exactly the probability of the above BC. The `SMT` solver `Boolector` [5] is used for searching for the quasi-BCs.

A real boomerang distinguisher, like one differential including multiple DCs, usually contains multiple BCs with the fixed input (resp. output) difference a_1 (resp. a_{r+1}). In the related-key setting, these BCs work under the fixed difference of the key. Thus, the searching process for a boomerang distinguisher can be in two phases (*BC's search* and *quasi-BC's search*):

BC's search: Set $u_0^i = u_2^i = 0$ (resp. $u_0^i = u_1^i = 0$) for $1 \le i \le m$ (resp. $m+1 \le i \le r+1$), we can search for all BCs. Each BC is a difference sequence $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$. In this case, the probability of a BC following the round-independence assumption can be calculated by (note a_1 and a_{r+1} are fixed differences)

$$B_{(0,a_m,0),(0,0,a_{m+1})} \prod_{i=1}^{m} B_{(0,a_i,0),(0,a_{i+1},0)} \prod_{i=m+1}^{r+1} B_{(0,0,a_i),(0,0,a)},$$

indeed equals to Equation 11.

Quasi-BC's search: We divide the quasi-BC's searching phase into two steps to make the search easier.

[5] https://boolector.github.io

1. Key dependencies detection: For each given BC, set the mask of round-keys as all-zero values, i.e., $u_0^i = 0$ for $1 \le i \le r+1$. If there is no other solution for the model, the BC is key-independent, i.e., all key masks must be zero. Otherwise, the BC is key-dependent, and we detect key dependencies. The boomerang distinguisher is key-independent when all BCs are key-independent.

2. Quasi-BC's search: For each given BC, if the BC is key-independent, we set $u_0^i = 0$ for $1 \le i \le r+1$ to search for all quasi-BCs. Otherwise, we search for all quasi-BCs for each solution of $(u_0^1, \ldots, u_0^{r+1})$ by step 1.

After the above two phases, we obtain all quasi-BCs, which can be used to compute the probability of a boomerang distinguisher and to derive the key conditions.

Derive key dependencies. From all quasi-BCs we searched corresponding to all BCs of a boomerang distinguisher, we can derive the key conditions and analyze the impact of the keys. Suppose the key difference sequence of the related-key boomerang distinguisher is $(\Delta k_1, \ldots, \Delta k_{m-1}, \nabla k_m, \ldots, \nabla k_r)$. According to Equation 15 and Equation 16, each quasi-BC can suggest one bit key condition. For example, from the ℓ-th quasi-BC, we can get a bit of the key condition:

$$\mathcal{K}_\ell = \bigoplus_{i=1}^{r-1} (u_{i+1}^{(\ell)})^\top k_i \oplus \bigoplus_{i=1}^{m-1} (v_{i+1}^{(\ell)})^\top \nabla k_i \oplus \bigoplus_{i=m}^{r-1} (w_{i+1}^{(\ell)})^\top \Delta k_i. \tag{19}$$

Note that multiple BCs belonging to a boomerang distinguisher may be incompatible in a fixed-key space, just like the case of multiple DCs in a differential pointed out by Beyne and Rijmen in [BR22]. Following [BR22], we study the derivation of the key's subspaces and the compatibility among these BCs in a fixed-key subspace.

Suppose we have n quasi-BCs and the rank of these key conditions (excluding the all-zero mask quasi-BC) is n', then the key space can be divided into $2^{n'}$ subspaces. For each subspace, we can compute the probability of the target BCs of a boomerang by summing the correlations of all its quasi-BCs in this fixed-key subspace.

We apply these techniques to boomerang distinguishers of `SKINNY`-64 and `GIFT`-64 to search for quasi-BCs, derive the key dependencies, and compute the probability in the fixed-key model. In Subsection 4.1, we provide four examples of `SKINNY`-64. Following the sandwich framework, in Subsection 4.2, we propose a divide-and-conquer approach for boomerangs whose probabilities are too small to experiment and analyze. In this framework, a boomerang distinguisher can be divided into three parts: $\mathsf{F}_0, \mathsf{F}_1$, and F_2, for each part, we can apply the same techniques. We provide 2/1 examples of `SKINNY`-64/`GIFT`-64.

4.1 Applications to Full Boomerang Distinguishers

This subsection provides four examples of `SKINNY`-64, including two probability-1 and two probability-2^{-4} boomerang distinguishers, which are generated by the method of Hadipour, Bagheri, and Song's paper [HBS21]. For each boomerang distinguisher, we conduct the two search phases to obtain all quasi-BCs. After that, from these quasi-BCs, we derive the key conditions and compute the probability in the fixed-key model. The probabilities computed from the quasi-boomerang framework meet the experimental probabilities well, which shows the correctness of our theory.

Specification of `SKINNY`. `SKINNY` is a tweakable block cipher proposed by Beierle et al. [BJK+16], and has two versions by the block size $n = 64, 128$. Let t denote the tweakey size and c denote the cell size, the `SKINNY` family, denoted as `SKINNY`-n-t, has six main versions: for each $n \in \{64, 128\}$, the tweakey size has three versions $t = n, t = 2n$, and $t = 3n$. The round function contains five operations: `SubCell`, `AddConstants`, `AddRoundTweakey`,

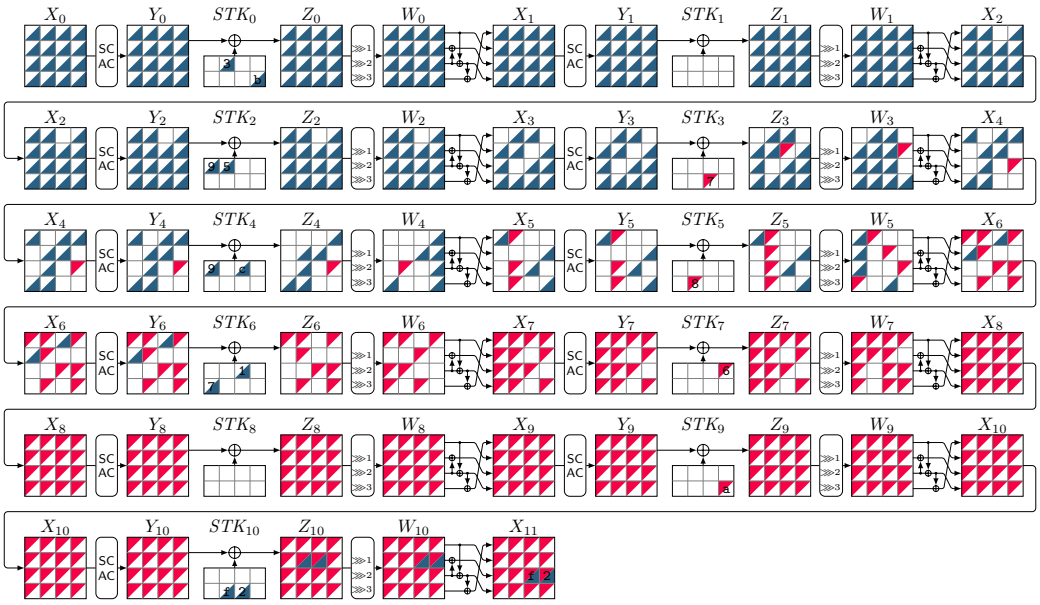

Figure 3: 11-round boomerang distinguisher for SKINNY-64-128 from the tool in [HBS21].

ShiftRows, and MixColumns. The tweakey schedule is linear, containing cell shuffle and two linear feedback shift registers. Let $TKm[i]$ denotes the i-th bit of TKm, $m \in \{1, 2, 3\}$.

4.1.1 Probability-1 11-Round Boomerang Distinguisher of SKINNY-64-128

At FSE 2023, Hadipour et al. [HNE22] presented a deterministic boomerang distinguisher for 11 rounds of SKINNY-64-128 (see Figure 3). This distinguisher was deliberately constructed using two differential trails that should be impossible according to the verification tool in [PT22], due to the dependency issue within the individual underlying differential trails. The goal was to demonstrate that the tool in [PT22] is limited to ordinary differential trails and cannot be used to verify boomerang distinguishers. However, the proposed boomerang distinguisher by Hadipour et al. was only verified experimentally for a limited number of random keys, and the authors posed the development of an analytical method for verifying boomerang distinguishers as an open question. Here, we address this question using our quasi-boomerang framework.

Figure 3 illustrates this 11-round boomerang distinguisher for SKINNY-64-128. The squares marked by ◪ and ◪ indicate active cells within deterministic difference propagation in the forward (upper) and backward (lower) trails, respectively. As shown in Figure 3, there is no overlap between the upper and lower deterministic trails through the S-box layers. Therefore, the probability of the boomerang distinguisher in Figure 3 is one, due to the cell-wise switch (ladder switch). However, one differential characteristic inside this boomerang has no right pairs according to the tools in [PT22].

To apply Proposition 1 to compute its probability, we select the S-box layer at the 6th round (i.e., the transformation $X_5 \rightarrow Y_5$ in Figure 3) as the middle subcipher F_1. This allows the boomerang distinguisher to combine a 5-round upper differential with a 6-round lower differential, resulting in fewer active S-boxes.

Quasi-BC's search. In the first phase, we search for BCs using the fixed input difference 0x0000000000000000, output difference 0x00002f0000000000, and the key differences of

the upper and lower differential

$$\begin{aligned}\Delta TK &= \Delta TK1||\Delta TK2 = \texttt{0x00000d0000000000}||\texttt{0x0000060000000000},\\ \nabla TK &= \nabla TK1||\nabla TK2 = \texttt{0x00000000e00000a0}||\texttt{0x0000000050000090},\end{aligned} \tag{20}$$

and find 384 BCs. Among these, there are 128 BCs with probability 2^{-16} and 256 BCs with probability 2^{-18}.

In the second phase, for step 1, we find that all the 384 BCs are key-independent. After step 2, the quasi-BCs we found are as follows: each of the 128 BCs with probability 2^{-16} has 256 quasi-BCs with correlation 2^{-16}; each of the 256 BCs with probability 2^{-18} has 512 quasi-BCs with correlation 2^{-18}.

Key derivation and probability calculation. According to Equation 19, we derive the conditions of the key difference from all 163840 quasi-BCs and get 8-bit conditions of key difference are as follows

$$\begin{cases} \nabla TK1[44] \oplus \nabla TK2[44] \oplus \nabla TK2[45] = C_1, & \nabla TK1[60] \oplus \nabla TK2[60] \oplus \nabla TK2[61] = C_5,\\ \nabla TK1[45] \oplus \nabla TK2[45] \oplus \nabla TK2[46] = C_2, & \nabla TK1[61] \oplus \nabla TK2[61] \oplus \nabla TK2[62] = C_6,\\ \nabla TK1[46] \oplus \nabla TK2[46] \oplus \nabla TK2[47] = C_3, & \nabla TK1[62] \oplus \nabla TK2[62] \oplus \nabla TK2[63] = C_7,\\ \nabla TK1[47] \oplus \nabla TK2[44] = C_4, & \nabla TK1[63] \oplus \nabla TK2[60] = C_8. \end{cases} \tag{21}$$

The conditions of the key difference should always be satisfied by the boomerang distinguisher, i.e., $(C_1, \ldots, C_8)$ can be computed by the fixed key difference of the upper and lower differential, i.e., ΔTK and ∇TK in Equation 20. Hence,

$$(C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8) = (0, 0, 0, 0, 0, 0, 0, 0). \tag{22}$$

Thus, the probability of the 11-round boomerang distinguisher in the condition (Equation 22) is 1 ($128 \times 256 \times 2^{-16} + 256 \times 512 \times 2^{-18} = 1$), according to Proposition 1 and Corollary 2. The experimental probability is indeed 1 among all keys we tried.

4.1.2 Probability-2^{-4} 12-Round Boomerang Distinguisher of SKINNY-64-128

The 12-round boomerang distinguisher of SKINNY-64-128 in Figure 4 has a probability of 2^{-4}. This probability can be derived either theoretically, using the BCT framework, or empirically. To estimate it theoretically based on the sandwich and BCT frameworks, we decompose the distinguisher as $\mathsf{F}_2 \circ \mathsf{F}_1 \circ \mathsf{F}_0$, where F_0 corresponds to the initial rounds, F_1 covers the remaining 11 rounds, and F_2 is the identity function. The probability of the differential transition over F_0 is $p = \texttt{DDT}[\texttt{0x4}][\texttt{0x2}]/2^4 = 2^{-2}$. The boomerang switch probability over F_1 is $r = 1$, since there is no overlap between the two differential trails. The differential probability over F_2 is also 1, as F_2 is the identity function, i.e., $q = 1$. Therefore, the overall probability is given by $p^2q^2r = 2^{-4}$. Note that this probability assumes a uniform random key rather than a fixed key.

Now we compute the fixed-key probability using the quasi-boomerang framework. We select the Sbox layer at the 7th round (i.e., the transformation $X_6 \to Y_6$ in Figure 4) as the middle subcipher F_1, so that the 12-round boomerang distinguisher is combined with a 6-round upper differential and a 6-round lower differential.

Quasi-BC's search. In the first phase, we search for BCs using the fixed input difference 0x0000000000000800, output difference 0x000000b000000000, and key differences of the upper and lower differentials are

$$\begin{aligned}\Delta TK &= \Delta TK1||\Delta TK2 = \texttt{0x000000000000000c}||\texttt{0x000000000000000e},\\ \nabla TK &= \nabla TK1||\nabla TK2 = \texttt{0x0000009000000000}||\texttt{0x000000c000000000}.\end{aligned} \tag{23}$$

We find 48 BCs, including 16 BCs with probability 2^{-14} and 32 BCs with probability 2^{-16}.

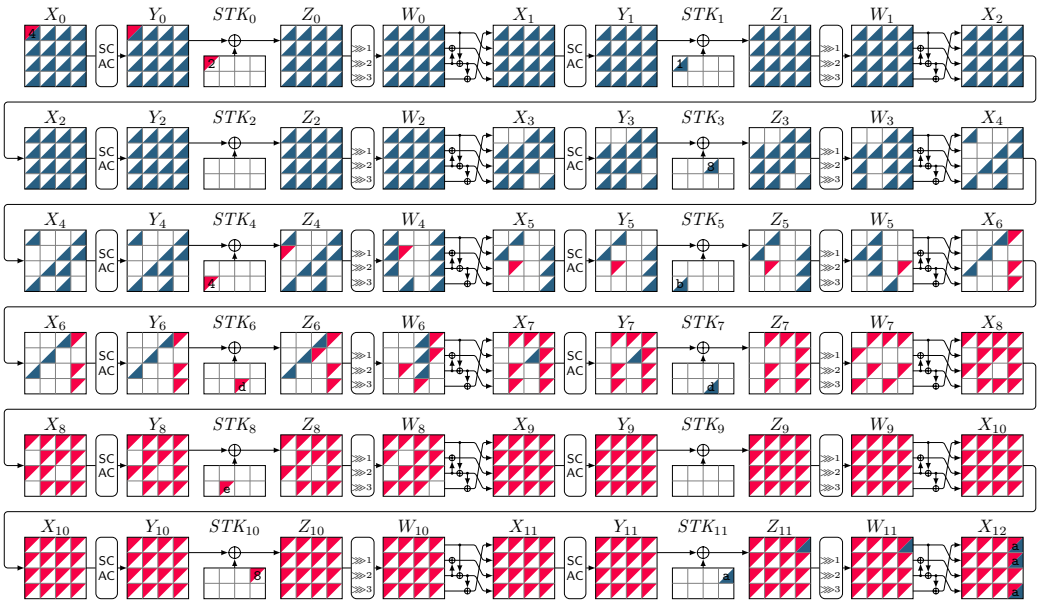

Figure 4: 12-Round boomerang distinguisher for SKINNY-64-128 from the tool in [HBS21].

In the second phase, we find that the 48 BCs are all key-independent in step 1. The quasi-BCs we found in step 2 are as follows: each of the 16 BCs with probability 2^{-14} has 32 quasi-BCs with correlation 2^{-14}; each of the 32 BCs with probability 2^{-16} has 64 quasi-BCs with correlation 2^{-16}.

Key derivation and probability calculation. The 4-bit conditions of the key difference derived from all 2560 quasi-BCs are:

$$\begin{cases} \nabla TK1[28] \oplus \nabla TK2[28] \oplus \nabla TK2[29] = C_1, & \nabla TK1[30] \oplus \nabla TK2[30] \oplus \nabla TK2[31] = C_3, \\ \nabla TK1[29] \oplus \nabla TK2[29] \oplus \nabla TK2[30] = C_2, & \nabla TK1[31] \oplus \nabla TK2[28] = C_4. \end{cases} \tag{24}$$

By Equation 23, we get $(C_1, C_2, C_3, C_4) = (0, 0, 0, 0)$. Thus, in this fixed condition, the probability of the 12-round boomerang distinguisher of SKINNY-64-128 is 2^{-4} ($16 \times 32 \times 2^{-14} + 32 \times 64 \times 2^{-16} = 2^{-4}$), which is consistent with the experimental probability.

4.1.3 Probability-1 15-Round Boomerang Distinguisher of SKINNY-64-192

For the 15-round boomerang distinguisher of SKINNY-64-192 in Figure 5, which has a probability of 1 as the upper and lower differential trails have no overlaps, we select the S-box layer at the 8th round (i.e., the transformation $X_7 \rightarrow Y_7$ in Figure 5) as the middle subcipher F_1. Then this distinguisher with a 7-round upper differential and an 8-round lower differential.

Quasi-BC's search. In the first phase, we search for BCs using the fixed input difference 0x0000000000000000, output difference 0x0001000000010001, and the key differences of the upper and lower differentials are

$$\begin{aligned} \Delta TK &= \Delta TK1 || \Delta TK2 || \Delta TK3 \\ &= \texttt{0x0100000000000000} || \texttt{0x0700000000000000} || \texttt{0x0c00000000000000}, \\ \nabla TK &= \nabla TK1 || \nabla TK2 || \nabla TK3 \\ &= \texttt{0x0000000000000500} || \texttt{0x0000000000000800} || \texttt{0x0000000000000700}. \end{aligned} \tag{25}$$

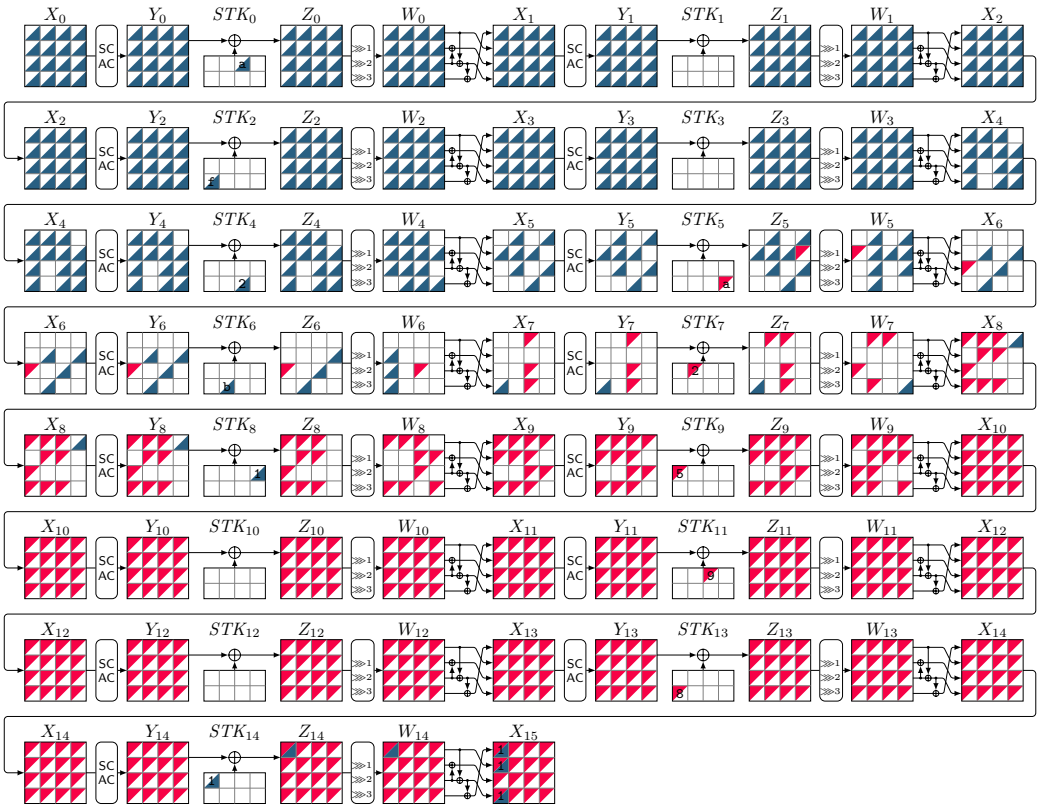

Figure 5: 15-Round boomerang distinguisher for SKINNY-64-192 from the tool in [HBS21].

We find 36 BCs, including 4 BCs with probability 2^{-8}, 16 BCs with probability 2^{-10}, and 16 BCs with probability 2^{-12}.

In the second phase, for step 1, we find that all 36 BCs are independent of round-keys. After step 2, the quasi-BCs we found are: each of the 4 BCs with probability 2^{-8} has 16 quasi-BCs with correlation 2^{-8}; each of the 16 BCs with probability 2^{-10} has 32 quasi-BCs with correlation 2^{-10}; each of the 16 BCs with probability 2^{-12} has 64 quasi-BCs with correlation 2^{-12}.

Key derivation and probability calculation. We get 4-bit conditions of the key difference derived from all 1600 quasi-BCs:

$$\begin{cases} \nabla TK1[40] \oplus \nabla TK2[40] \oplus \nabla TK2[42] \oplus \nabla TK2[43] \oplus \nabla TK3[40] \oplus \nabla TK3[43] = C_1, \\ \nabla TK1[41] \oplus \nabla TK2[40] \oplus \nabla TK2[41] \oplus \nabla TK3[40] \oplus \nabla TK3[41] \oplus \nabla TK3[43] = C_2, \\ \nabla TK1[42] \oplus \nabla TK2[41] \oplus \nabla TK2[42] \oplus \nabla TK3[40] \oplus \nabla TK3[41] \oplus \nabla TK3[42] \oplus \nabla TK3[43] = C_3, \\ \nabla TK1[43] \oplus \nabla TK2[42] \oplus \nabla TK2[43] \oplus \nabla TK3[40] \oplus \nabla TK3[41] \oplus \nabla TK3[42] = C_4. \end{cases} \tag{26}$$

By Equation 25, we get that $(C_1, C_2, C_3, C_4) = (0, 0, 0, 0)$. Thus, the probability of the 15-round boomerang distinguisher of SKINNY-64-192 is 1 ($4 \times 16 \times 2^{-8} + 16 \times 32 \times 2^{-10} + 16 \times 64 \times 2^{-12} = 1$) in the fixed condition. The experimental probability is indeed 1 among all keys we tried.

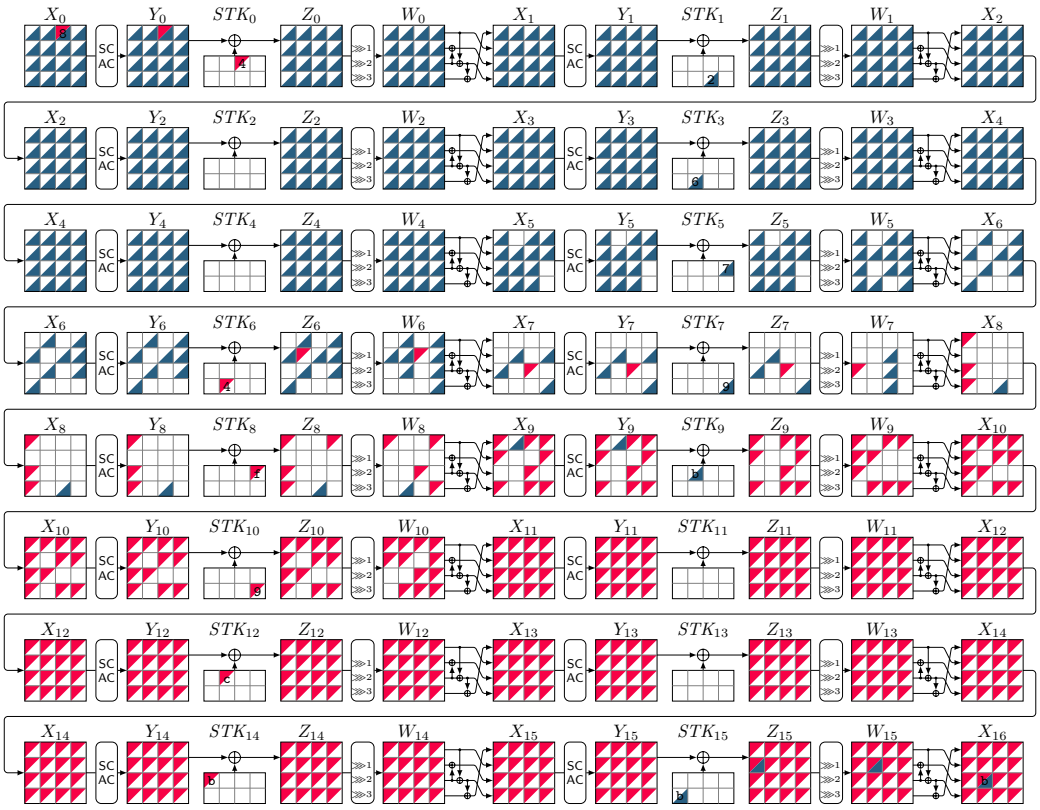

Figure 6: 16-Round boomerang distinguisher for SKINNY-64-192 from the tool in [HBS21].

4.1.4 Probability-2^{-4} 16-Round Boomerang Distinguisher of SKINNY-64-192

The 16-round boomerang distinguisher of SKINNY-64-192 in Figure 6 has a probability of 2^{-4}. This probability can be derived either theoretically, using the BCT framework, or empirically. To estimate it theoretically with the BCT framework, we decompose the distinguisher as $\mathsf{F}_2 \circ \mathsf{F}_1 \circ \mathsf{F}_0$, where F_0 corresponds to the initial rounds, F_1 (the boomerang switch) includes the remaining 15 rounds, and F_2 is the identity function. The probability of the differential transition over F_0 is $p = \mathtt{DDT}[\mathtt{0x8}][\mathtt{0x2}]/2^4 = 2^{-2}$. The boomerang switch probability over F_1 is $r = 1$, as there is no overlap between the two differential trails. The differential probability over F_2 is also $q = 1$, since F_2 is the identity function. Therefore, the overall probability, based on the sandwich and BCT frameworks, is given by $p^2q^2r = 2^{-4}$ by assuming the random key is uniform rather than fixed.

Now, to compute the probability in the fixed key with quasi-boomerang framework, we select the S-box layer at the 9th round (i.e., the transformation $X_8 \rightarrow Y_8$ in Figure 6) as the middle subcipher F_1, so that the 16-round boomerang is combined with an 8-round upper differential and an 8-round lower differential.

Quasi-BC's search. In the first phase, we search for BCs using the fixed input difference 0x0000000000000800, output difference 0x000000b000000000, and the key differences of

the upper and lower differentials

$$\begin{aligned}\Delta TK &= \Delta TK1||\Delta TK2||\Delta TK3\\ &= \texttt{0x0000000000000700}||\texttt{0x0000000000000600}||\texttt{0x0000000000000500},\\ \nabla TK &= \nabla TK1||\nabla TK2||\nabla TK3\\ &= \texttt{0x0004000000000000}||\texttt{0x000a000000000000}||\texttt{0x0006000000000000}.\end{aligned} \tag{27}$$

We find 36 BCs, including 4 BCs with probability 2^{-12}, 16 BCs with probability 2^{-14}, and 16 BCs with probability 2^{-16}.

In the second phase, we find that the 36 BCs are all key-independent in step 1. The quasi-BCs we found in step 2 are as follows: each of the 4 BCs with probability 2^{-12} has 16 quasi-BCs with correlation 2^{-12}; each of the 16 BCs with probability 2^{-14} has 32 quasi-BCs with correlation 2^{-14}; each of the 16 BCs with probability 2^{-16} has 64 quasi-BCs with correlation 2^{-16}.

Key derivation and probability calculation. The 4-bit conditions of the key difference derived from all 1600 quasi-BCs are that

$$\begin{cases}\nabla TK1[24] \oplus \nabla TK2[24] \oplus \nabla TK2[26] \oplus \nabla TK2[27] \oplus \nabla TK3[24] \oplus \nabla TK3[27] = C_1,\\ \nabla TK1[25] \oplus \nabla TK2[24] \oplus \nabla TK2[25] \oplus \nabla TK3[24] \oplus \nabla TK3[25] \oplus \nabla TK3[27] = C_2,\\ \nabla TK1[26] \oplus \nabla TK2[25] \oplus \nabla TK2[26] \oplus \nabla TK3[24] \oplus \nabla TK3[25] \oplus \nabla TK3[26] \oplus \nabla TK3[27] = C_3,\\ \nabla TK1[27] \oplus \nabla TK2[26] \oplus \nabla TK2[27] \oplus \nabla TK3[24] \oplus \nabla TK3[25] \oplus \nabla TK3[26] = C_4.\end{cases} \tag{28}$$

By Equation 27, we get $(C_1, C_2, C_3, C_4) = (0, 0, 0, 0)$. Thus, according to the Proposition 1 and Corollary 2, the probability of the 16-round boomerang distinguisher of SKINNY-64-192 is 2^{-4} $(4 \times 16 \times 2^{-12} + 16 \times 32 \times 2^{-14} + 16 \times 64 \times 2^{-16} = 2^{-4})$ in above fixed condition, which is consistent with the experimental probability among all keys we tried.

4.2 Applications to Joint Boomerang Distinguishers

If the boomerang (or more generally, sandwich) distinguisher is short enough or its probability is sufficiently large, we can verify it either experimentally or analytically using the mix-basis geometric approach proposed in Section 3, which also derives the conditions on the sub-keys required for the distinguisher to hold.

However, this verification may become computationally difficult when the overall probability is too small to be handled within our computational limits, especially when the distinguisher spans many rounds. This is often the case for the best attacks in terms of round count. To address this, we propose a divide-and-conquer heuristic approach to analyze such sandwich distinguishers and derive supporting key conditions.

As shown in Figure 7, assume that, following the sandwich framework, we split the block cipher into three parts: F_0 (r_0-round), F_1 (r_1-round), and F_1 (r_2-round), such that $\Pr(\Delta_i \overset{\mathsf{F}_0}{\rightleftharpoons} \Delta_m) = p$, $\Pr(\Delta_m \overset{\mathsf{F}_1}{\rightleftharpoons} \nabla_m) = r$, and $\Pr(\nabla_m \overset{\mathsf{F}_2}{\rightleftharpoons} \nabla_o) = q$, with the total probability given by $p_t = pqr$. While verifying the entire distinguisher analytically or experimentally may be computationally challenging, verifying and deriving key conditions for the individual components F_0, F_1, and F_2 can be significantly easier, for example, when p_t is small, but its components p, r, and q are large enough.

Therefore, our idea is to analyze each component of the sandwich distinguisher separately, derive the constraints on the sub-keys individually, and then combine these constraints to obtain necessary conditions on the keys for the entire distinguisher to hold. To achieve this, we trade a bit of accuracy for higher efficiency by treating each component independently. In the quasi-boomerang framework, the independence is achieved by setting $u_0^{r_0+1} = u_2^{r_0+1} = u_0^{r_0+r_1+1} = u_1^{r_0+r_1+1} = 0$. Note that although we handle the components

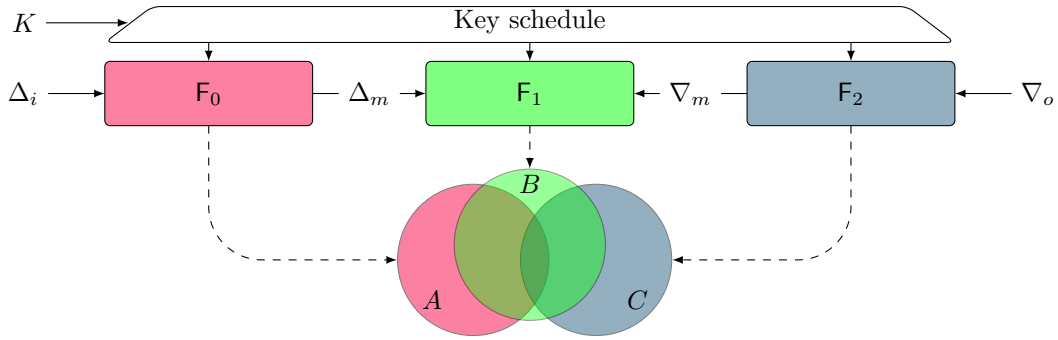

Figure 7: Satisfying keys for three differential transitions in a sandwich distinguisher.

independently, we take into account all dependencies within each component, as well as the dependencies between the two trails inside each part. Additionally, we consider the key schedule when merging the constraints on the sub-keys from different components, in order to translate them into conditions on the master key.

We begin with an overview of our approach, followed by several examples. Given a boomerang distinguisher discovered by previous tools, such as the one in [HBS21], we fix only the differences at the junction points of the three components, namely Δ_i, Δ_m, ∇_m, and ∇_o (see Figure 7), and allow all intermediate differences to take arbitrary possible values in order to capture the clustering effect.

Next, for each component, we compute all quasi-BCs with input difference Δ_i (resp. Δ_m, ∇_m) and output difference Δ_m (resp. ∇_m, ∇_o) of part F_0 (resp. $\mathsf{F}_1, \mathsf{F}_2$), and extract the constraints on the sub-keys induced by the boomerang transitions through F_0 (resp. $\mathsf{F}_1, \mathsf{F}_2$). As illustrated in Figure 7, let A, B and C denote the sets of keys that satisfy the boomerang transitions over $\mathsf{F}_0, \mathsf{F}_1$ and F_2, respectively.

Finally, we merge the constraints from each component to derive the overall key conditions required for the full distinguisher to hold. As illustrated in Figure 7, the intersection $A \cap B \cap C$ represents the set of keys that satisfy the entire distinguisher.

We provide three examples of `SKINNY`-64 and `GIFT`-64 following this sandwich framework in this subsection. Each example is divided into three parts: F_0 (r_0-round), F_1 (r_1-round), and F_2 (r_2-round). A BC is a difference sequence of F_0 (resp. $\mathsf{F}_1, \mathsf{F}_2$) like

$$(a_1, \ldots, a_{r_0+1})(resp.\ (a_{r_0+1}, \ldots, a_m, a_{m+1}, \ldots, a_{r_0+r_1+1}),\ (a_{r_0+r_1+1}, \ldots, a_{r_0+r_1+r_2+1})),$$

while quasi-BCs corresponding to the given BC sequence of parts $\mathsf{F}_0, \mathsf{F}_1$, and F_2 are triple-sequences as follows, respectively:

$$\begin{aligned}
&((0, a_1, 0), (u_0^2, a_2, u_2^2), \ldots, (u_0^{r_0}, a_{r_0}, u_2^{r_0}), (0, a_{r_0+1}, 0)),\\
&((0, a_{r_0+1}, 0), \ldots, (u_0^m, a_m, u_2^m), (u_0^{m+1}, u_1^{m+1}, a_{m+1}), (0, 0, a_{r_0+r_1+1})),\\
&((0, 0, a_{r_0+r_1+1}), (u_0^{r_0+r_1+2}, u_1^{r_0+r_1+2}, a_{r_0+r_1+2}), \ldots, (0, 0, a_{r_0+r_1+r_2+1})).
\end{aligned}$$

For each part, we search for quasi-BCs in two phases and derive the sub-key conditions, using the method at the beginning of Section 4. Next, from all quasi-BCs, we can get the interaction between the conditions of the three parts by the key schedule and compute the probability of the joint boomerang distinguisher in the fixed-key model. We also implement the experiments for each example. The results of the analysis and experiment are listed in Table 3.

Table 3: Results of the joint boomerang distinguishers of SKINNY-64 and GIFT-64. $p/r/q$ and $p_e/r_e/q_e$ denote the calculated probability and the experimental probability of $\mathsf{F}_0/\mathsf{F}_1/\mathsf{F}_2$, respectively.

Algorithm	Part	Rounds	$\Delta_i \to \Delta_m$ / $\Delta_m \to \nabla_m$ / $\nabla_m \to \nabla_o$	$p/r/q$	#Key	$p_e/r_e/q_e$
SKINNY-64-128 [LGS17, Table 12]	F_0	7	0x1000000000000000 → 0x0010001000000010	$2^{-10.42}$	2^{128}	$2^{-10.43}$
	F_1	2	0x0010001000000010 → 0x0300000003000000	2^{-2}	2^{128}	$2^{-2.00}$
				0	2^{126}	0
	F_2	8	0x0300000003000000 → 0xd00600000068006	2^{-31}	2^{126}	$2^{-30.79}$
				2^{-33}	2^{127}	$2^{-32.98}$
SKINNY-64-192 [LGS17, Table 14]	F_0	10	0x0100100000010020 → 0x0040004000000040	$2^{-26.67}$	2^{192}	$2^{-26.78}$
	F_1	2	0x0040004000000040 → 0x00b0000000000000	$2^{-5.09}$	2^{192}	$2^{-5.10}$
	F_2	10	0x00b0000000000000 → 0x2020250000202022	$2^{-22.03}$	2^{192}	$2^{-22.00}$
GIFT-64 [CWZ19, Table 5]	F_0	9	0x000000a000006000 → 0x0100000001020200	2^{-28}	2^{128}	$2^{-28.02}$
	F_1	2	0x0100000001020200 → 0x0a00000000000000	$2^{-4.19}$	2^{128}	$2^{-3.43}$
	F_2	8	0x0a00000000000000 → 0x0800000000000010†	2^{-22}	2^{128}	$2^{-21.94}$

† The output difference in [CWZ19] was written as 0x0800000000000000. However, we find it should be 0x0800000000000010. It should be a typo in [CWZ19].

4.2.1 17-Round Boomerang Distinguisher of SKINNY-64-128

In [LGS17, Table 12], Liu et al. proposed a 17-round boomerang distinguisher for SKINNY-64-128, combining an 8-round upper DC with probability 2^{-12} and a 9-round lower DC with probability 2^{-20}. We regenerated this distinguisher within the sandwich framework using the tool from [HBS21], with the 17 rounds decomposed as $7+2+8$ (see Figure 8). In Figure 8, the cells marked by ◪ and ◪ indicate the active cells in the propagation of differences forward (upper trail) and backward (lower trail) through $\mathsf{F}_0, \mathsf{F}_1$ and F_2. The input/output difference and result for each part are listed in Table 3. The key differences of the upper and the lower are:

$$\begin{aligned} \Delta TK &= \Delta TK1||\Delta TK2 = \texttt{0x0000000600000000}||\texttt{0x0000000900000000}, \\ \nabla TK &= \nabla TK1||\nabla TK2 = \texttt{0xe00000000000c000}||\texttt{0x6000000000000a000}. \end{aligned} \tag{29}$$

Search for quasi-BCs. In the BC's search phase, we find 3 BCs with probability 2^{-12} of F_0, 4 BCs with probability 2^{-36} of F_2, and 64 BCs with probability 2^{-14} of F_1. For part F_1, the Sbox layer at the 2nd round (the 9th round in the 17-round) is selected as the connection point.

In the quasi-BC's search phase, for step 1, we find 3 (resp. 64) BCs of F_0 (resp. F_1) are all key-independent, and detect key dependencies for 4 BCs of F_2 (2/2 of 4 BCs have 4/2 solutions of $(u_0^{r_0+r_1+1}, \ldots, u_0^{r_0+r_1+r_2+1})$, respectively). After step 2, the quasi-BCs we found are: each of the 3 (resp. 64) BCs of F_0 (resp. F_1) has 1 (resp. 64) quasi-BC(s) with correlation 2^{-12} (resp. 2^{-14}); each of the 2 (resp. 2) of the 4 BCs of F_2 has 8 (resp. 4) quasi-BCs with correlation 2^{-36} and 8 (resp. 4) quasi-BCs with correlation -2^{-36}. That is, the numbers of the quasi-BCs for $\mathsf{F}_0, \mathsf{F}_1$ and F_2 are 3, 4096, and 40, respectively.

Derive key conditions. From all quasi-BCs for each part, we get 3-bit conditions of F_1:

$$\begin{cases} \Delta TK1[56] \oplus \Delta TK2[56] \oplus \Delta TK2[58] \oplus \Delta TK2[59] = C_1, \\ \Delta TK1[58] \oplus \Delta TK2[57] \oplus \Delta TK2[58] = C_2,\ \Delta TK1[59] \oplus \Delta TK2[58] \oplus \Delta TK2[59] = C_3. \end{cases} \tag{30}$$

and 4-bit conditions of F_2:

$$\begin{cases} TK1[16] \oplus TK2[17] \oplus TK2[19] = C_4, & \nabla TK1[16] \oplus \nabla TK2[17] \oplus \nabla TK2[19] = C_6, \\ TK1[18] \oplus TK2[16] \oplus TK2[17] = C_5, & \nabla TK1[18] \oplus \nabla TK2[16] \oplus \nabla TK2[17] = C_7. \end{cases} \tag{31}$$

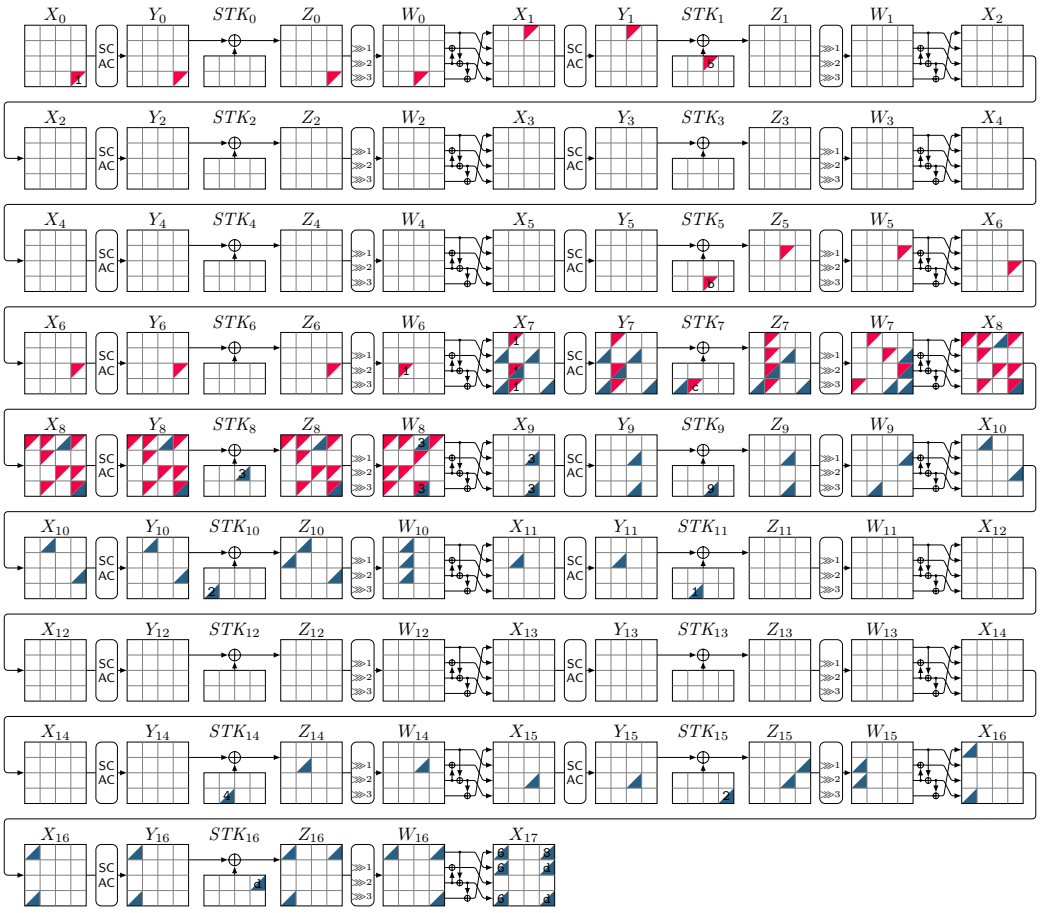

Figure 8: 17-round boomerang distinguisher for SKINNY-64-128 from [LGS17], regenerated by the tool from [HBS21].

By Equation 29, $(C_1, C_2, C_6, C_7) = (0, 0, 0, 0)$. In this fixed condition, the probability of F_0 (resp. F_1) is $2^{-10.42}$, i.e., 3×2^{-12} (resp. 2^{-2}, i.e., $64 \times 64 \times 2^{-14}$). According to Proposition 2, the probability of F_2 is $0/2^{-31}/2^{-33}/2^{-33}$ when $(C_4, C_5) = (0, 0)/(1, 0)/(0, 1)/(1, 1)$, respectively.

Experimental verification. Following the sandwich framework, we get the probabilities p, q and r are $2^{-10.42}, 2^{-2}$, and 0(for $\frac{1}{4}$ keys)$/2^{-31}$(for $\frac{1}{4}$ keys)$/2^{-33}$(for $\frac{1}{2}$ keys), respectively. Thus, the probability pqr of the 17-round boomerang distinguisher of SKINNY-64-128 is zero for $\frac{1}{4}$ keys, $2^{-43.42}$ for $\frac{1}{4}$ keys, and $2^{-45.42}$ for $\frac{1}{2}$ keys. We implement the experiments to verify the probability of the three parts using the same master-key, the results are listed in Table 3.

We also provide a comparison of the F_1 part in Table 4. The probability of the F_1 part is $2^{-8.42}$ estimated by Liu et al. [LGS17], 2^{-2} by Cid et al. [CHP+18], and 2^{-2} by us.

4.2.2 22-Round Boomerang Distinguisher of SKINNY-64-192

Liu et al. proposed a 22-round boomerang distinguisher of SKINNY-64-192, combining an 11-round upper DC with probability 2^{-20} and an 11-round lower DC with probability 2^{-20} in [LGS17, Table 14]. We divide this 22-round boomerang distinguisher into F_0 (10-round),

Table 4: Comparison of the F_1 (middle two round) part of boomerang distinguishers of SKINNY-64 and GIFT-64.

Probabilities	SKINNY-64-128	SKINNY-64-192	GIFT-64
$(pq)^2$ including clustering effect	$2^{-8.42}$ [LGS17]	$2^{-16.30}$ [LGS17]	-
Probability obtained by BCT	2^{-4} [CHP+18]	$2^{-5\dagger}$	1 [CWZ19]
Probability obtained by BCT and values	2^{-2} [CHP+18]	$2^{-5.31}$ [CHP+18]	-
Probability obtained by BDT	-	-	2^{-18} [JZZD20]
Our calculated probability	2^{-2}	$2^{-5.09}$	$2^{-4.19}$
Our experimental probability	$2^{-2.00}$	$2^{-5.10}$	$2^{-3.43}$

† The probability is calculated following [CHP+18].

F_1 (2-round), and F_2 (10-round), respectively. The input/output difference and results for each part are listed in Table 3. The key differences of the upper and the lower are:

$$\begin{aligned}\Delta TK &= \Delta TK1||\Delta TK2||\Delta TK3\\ &= \texttt{0x00000000000000a0}||\texttt{0x0000000000000020}||\texttt{0x00000000000000d0},\\ \nabla TK &= \nabla TK1||\nabla TK2||\nabla TK3\\ &= \texttt{0x00000a0000000000}||\texttt{0x0000070000000000}||\texttt{0x00000e0000000000}.\end{aligned} \tag{32}$$

Search for quasi-BCs. In the BC's search phase, we find that 10 BCs (1/5/4 with probability $2^{-28}/2^{-30}/2^{-32}$, respectively) of F_0, 36 BCs (4/6/10/12/4 with probability $2^{-16}/2^{-17}/2^{-18}/2^{-19}/2^{-20}$, respectively) of F_1, and 16 BCs (2/6/6/2 with probability $2^{-24}/2^{-26}/2^{-28}/2^{-30}$, respectively) of F_2. The F_1 part selects the Sbox layer at the 2nd round (the 12th round in the 22-round) as the connection point.

In the quasi-BC's search phase, we find 10 (resp. 36, 16) BCs of F_0 (resp. $\mathsf{F}_1, \mathsf{F}_2$) are all key-independent in step 1. After step 2, we find that each of the 10 (resp. 16) BCs of F_0 (resp. F_2) only has one quasi-BC with all-zero masks and 7680 quasi-BCs (512/768/2304/3072 with correlation $2^{-16}/2^{-17}/2^{-18}/2^{-19}/2^{-20}$, respectively) corresponding to the 36 BCs of F_1.

Derive key conditions. From all quasi-BCs for each part, we get 3-bit conditions of the key difference of F_1:

$$\begin{cases}\Delta TK1[16] \oplus \Delta TK2[17] \oplus \Delta TK2[19] \oplus \Delta TK3[16] \oplus \Delta TK3[17] \oplus \Delta TK3[19] = C_1,\\ \Delta TK1[18] \oplus \Delta TK2[16] \oplus \Delta TK2[17] \oplus \Delta TK3[16] \oplus \Delta TK3[17] \oplus \Delta TK3[18] = C_2,\\ \Delta TK1[19] \oplus \Delta TK2[17] \oplus \Delta TK2[18] \oplus \Delta TK3[17] \oplus \Delta TK3[8] \oplus \Delta TK3[19] = C_3.\end{cases} \tag{33}$$

By Equation 32, $(C_1, C_2, C_3) = (0, 0, 0)$. Thus, the probability of F_0 (resp. $\mathsf{F}_1, \mathsf{F}_2$) is $2^{-26.67}$ (resp. $2^{-5.09}, 2^{-22.03}$) in this fixed condition.

Experimental verification. Following the sandwich framework, we get the probabilities p, q and r are $2^{-26.67}, 2^{-5.09}$, and $2^{-22.03}$, respectively. Thus, the probability pqr of the 22-round boomerang distinguisher of SKINNY-64-192 is $2^{-53.79}$. In addition, the experiments are conducted to verify the probability of the three parts using the same master-key, and the results are listed in Table 3. The comparison of results of F_1 is listed in Table 4.

4.2.3 19-Round Boomerang Distinguisher of GIFT-64

Specification of GIFT. The block cipher GIFT, proposed by Banik et al. [BPP+17] at CHES 2017, includes two variants: GIFT-64 and GIFT-128, both utilizing an SPN structure

with a 128-bit key. The GIFT-64 processes 64-bit inputs while the GIFT-128 processes 128-bit inputs, corresponding to 28 and 40 rounds, respectively. Each round function contains four operations: SubCells (4-bit S-box), PermBits, AddRoundConstants, and AddRoundKey. Additionally, the key schedule initializes a 128-bit master key divided into 16-bit segments, extracting round keys differently for each version. Let k_i^j denotes the j-th bit of the i-th segment ($0 \leq i \leq 7, 0 \leq j \leq 15$) of the master key and RK_r^i denotes the i-th bit of the r-th round key ($0 \leq i \leq 31$ for GIFT-64 and $0 \leq i \leq 63$ for GIFT-128).

Chen et al. presented a 23-round attack on GIFT-64 in [CWZ19] utilizing a 19-round boomerang distinguisher [CWZ19, Table 5]. The probability of the middle two rounds (round 10 to 11) is one according to the BCT. Zhao et al. [ZDM+20] proposed a 24-round attack using the same 19-round distinguisher. In [JZZD20], Ji et al. pointed out that the probability of the middle two rounds of the 19-round boomerang is only 2^{-18} calculated by BDT [WP19], and considered the 23-round attack in [CWZ19] and the 24-round attack in [ZDM+20] are invalid.

To re-estimate the probability, we divide this 19-round boomerang distinguisher into F_0 (9-round), F_1 (2-round), and F_2 (8-round), respectively. The input/output differences and results are listed in Table 3. The key differences of the upper and lower are:

$$\begin{aligned} \Delta k &= \texttt{0x00000000000000002000000001004000}, \\ \nabla k &= \texttt{0x00000008000000020000010000000000}. \end{aligned} \tag{34}$$

Search for quasi-BCs. In the BC's search phase, we find 1 BC with probability 2^{-28} of F_0, 1 BC with probability 2^{-22} of F_2. We find 576 BCs of F_1 by selecting the Sbox layer at the 2nd round (the 11th round in the 19-round) as the connection point, including 32 BCs with probability 2^{-20}, 128 BCs with probability 2^{-22}, 32 BCs with probability 2^{-23}, 128 BCs with probability 2^{-24}, 128 BCs with probability 2^{-25}, and 128 BCs with probability 2^{-27}.

In the quasi-BC's search phase, we find that these BCs are all key-independent in step 1. In step 2, each of the BCs of F_0 and F_2 only has one quasi-BC with all-zero masks, 576 BCs of F_1 have 819200 quasi-BCs.

Derive key conditions. The 8-bit conditions of the key difference obtained from all quasi-BCs of F_1 are:

$$\Delta k_2^0 = C_1, \Delta k_2^1 = C_2, \Delta k_2^3 = C_3, \Delta k_2^9 = C_4, \Delta k_3^0 = C_5, \Delta k_3^1 = C_6, \Delta k_3^3 = C_7, \Delta k_3^9 = C_8. \tag{35}$$

By Equation 34, we get

$$(C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8) = (0, 0, 0, 0, 0, 0, 0, 0). \tag{36}$$

Thus, the probability of F_0 (resp. $\mathsf{F}_1, \mathsf{F}_2$) is 2^{-28} (resp. $2^{-4.19}, 2^{-22}$) in this fixed condition.

Experimental verification. The probabilities p, q and r are $2^{-28}, 2^{-4.19}$, and 2^{-22}, respectively, according to the sandwich framework. Thus, the probability pqr of the 19-round boomerang distinguisher of GIFT-64 is $2^{-54.19} < 2^{-64}$, which is indeed valid. The experimental results of the three parts using the same master-key are listed in Table 3.

The comparison of results of F_1 is listed in Table 4. In addition, from the perspective of 3-differential, Wang et al. [WSW+24] searched for quasi-3-DCs corresponding to partial (optimal) 3-DCs of F_1 and claimed all optimal 3-DCs are impossible. Indeed, the sum of the probabilities of all optimal 3-DCs is about $2^{-25.83}$, which has little impact on the probability of F_1.

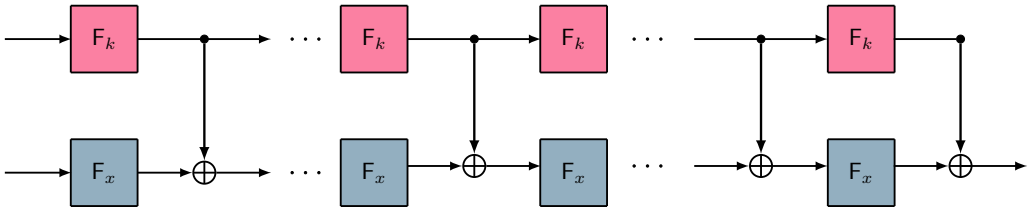

Figure 9: The key-alternating cipher.

5 Quasi-Boomerang Framework Considering Keyschedule

In Subsection 3.4, we studied the quasi-boomerang framework for key-alternating ciphers, assuming that all round keys are independent variables. However, the quasi-boomerang framework also works when taking the keyschedule into consideration. In this section, we describe the theories of it. In addition, we revisit Boura, Derbez, and Germon's recent paper [BDG25] that extended the quasi-differential to the related-key differential attacks. Interestingly, when applying similar ideas to the quasi-differential framework, some formulas in [BDG25] can be obtained in an easier way.

5.1 Quasi-Boomerang Case

A key-alternating cipher consists of two kinds of operations; one is the public component, including functions in the encryption and key schedule, and the other is the key-XOR, as shown in Figure 9. In the following, we take the related-key setting as an instance; the single-key setting case can be deduced by forcing the difference in the key schedule to be zero. The public component is a function consisting of two parallel functions F_x and F_k, i.e., $\mathsf{F} = \mathsf{F}_x||\mathsf{F}_k$.

Suppose the quasi-boomerang transition matrices of F_x and F_k are B^{F_x} and B^{F_k}, respectively. According to Theorem 1(1), the quasi-boomerang transition matrix of F is then

$$B^{\mathsf{F}} = B^{\mathsf{F}_x} \otimes B^{\mathsf{F}_k}.$$

The coordinate of B^{F} is

$$B^{\mathsf{F}}_{(v_0^x||v_0^k,v_1^x||v_1^k,v_2^x||v_2^k),(u_0^x||u_0^k,u_1^x||u_1^k,u_2^x||u_2^k)} = B^{\mathsf{F}_x}_{(v_0^x,v_1^x,v_2^x),(u_0^x,u_1^x,u_2^x)} B^{\mathsf{F}_k}_{(v_0^k,v_1^k,v_2^k),(u_0^k,u_1^k,u_2^k)}.$$

Hence, the upper and lower quasi-biDDTs and quasi-BCT of F can be constructed upon those of F_x and F_k.

Suppose the size of the key schedule is also n (for other sizes, similar theories can be obtained). The key-XOR component is a function $\mathsf{F} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ as

$$\mathsf{F} : (x||k, \Delta_1^x||\Delta_1^k, \Delta_2^x||\Delta_2^k) \to (x \oplus k||k, \Delta_1^x \oplus \Delta_1^k||\Delta_1^k, \Delta_2^x \oplus \Delta_2^k||\Delta_2^k).$$

Applying Equation 7 to this F, we get the upper quasi-biDDT of the key-XOR as

$$
\begin{aligned}
&B^{\mathsf{F}}_{(v_0^x||v_0^k,v_1^x||v_1^k,v_2^x||v_2^k),(u_0^x||u_0^k,u_1^x||u_1^k,u_2^x||u_2^k)} \\
&= \frac{1}{2^{4n}} \sum_{\substack{x||k\in\mathbb{F}_2^{2n},\Delta_2^x||\Delta_2^k\in\mathbb{F}_2^{2n} \\ \Delta_1^x||\Delta_1^k=u_1^x||u_1^k \\ \Delta_1^x\oplus\Delta_1^k||\Delta_1^k=v_1^x||v_1^k}} (-1)^{(u_0^x||u_0^k)^\top(x||k)\oplus(u_2^x||u_2^k)^\top(\Delta_2^x||\Delta_2^k)\oplus(v_0^x||v_0^k)^\top(x\oplus k||k)\oplus(v_2^x||v_2^k)^\top(\Delta_2^x\oplus\Delta_2^k||\Delta_2^k)} \\
&= \delta_{v_1^x}(u_1^x\oplus u_1^k)\delta_{v_1^k}(u_1^k)\left(\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{(u_0^x\oplus v_0^x)^\top x}\right)\left(\frac{1}{2^n}\sum_{k\in\mathbb{F}_2^n}(-1)^{(u_0^k\oplus v_0^x\oplus v_0^k)^\top k}\right)\cdots \\
&= \delta_{v_1^x}(u_1^x\oplus u_1^k)\delta_{v_1^k}(u_1^k)\delta_{v_0^x}(u_0^x)\delta_{u_0^k}(v_0^x\oplus v_0^k)\delta_{v_2^x}(u_2^x)\delta_{u_2^k}(v_0^x\oplus v_0^k).
\end{aligned} \tag{37}
$$

In a similar way, we can get the lower quasi-biDDT expression for key-XOR, which is omitted here.

Remark. Intuitively, Equation 37 states that the masks (resp. differences) change following the propagation rules of masks (resp. differences) for BRANCH and XOR operations.

5.2 Revisit Quasi-Differential Case

We have revisited the quasi-differential framework for key-alternating ciphers when assuming the round keys are independent [BDG25] in Subsection 3.4. In the following, we revisit [BDG25] to discuss the quasi-differential framework for key-alternating ciphers considering the key schedule. Again, we use our perspective to do it, which provides an alternative method to derive the theorems in [BDG25]. We take [BDG25, Proposition 1] as an instance to show our idea.

Proposition 3 (Proposition 1 in [BDG25])**.** *Consider the key-XOR function*

$$\mathsf{G}:\mathbb{F}_2^n\times\mathbb{F}_2^m\to\mathbb{F}_2^n\times\mathbb{F}_2^m,\quad (x||k)\to(x\oplus k||k).$$

The quasi-differential transition matrix of G *has the coordinates*

$$D^{\mathsf{G}}_{(v_0^x||v_0^k,v_1^x||v_1^k),(u_0^x||u_0^k,u_1^x||u_1^k)} = \delta_{v_1^x}(u_1^x\oplus u_1^k)\delta_{v_1^k}(u_1^k)\delta_{v_0^x}(u_0^x)\delta_{v_0^k}(u_0^x\oplus u_0^k).$$

Proof. (Alternative) The quasi-differential matrix of a function F is given in Equation 4. Differential cryptanalysis is a 2nd-order attack, so G actually does the following thing

$$\mathsf{G}:(x||k,\Delta x||\Delta k)\to(x\oplus k||k,\Delta x\oplus\Delta k||\Delta k)$$

Let $\mathsf{F}=\mathsf{G}$, $v_0=v_0^x||v_0^k, v_1=v_1^x||v_1^k, u_0=u_0^x||u_0^k, u_1=u_1^x||u_1^k$, and working it out, we get

$$
\begin{aligned}
&D^{\mathsf{G}}_{(v_0^x||v_0^k,v_1^x||v_1^k),(u_0^x||u_0^k,u_1^x||u_1^k)} \\
&= \frac{1}{2^{n+m}} \sum_{\substack{x||k\in\mathbb{F}_2^{n+m} \\ ((x\oplus k)||k)\oplus((x\oplus u_1^x\oplus k\oplus u_1^k)||(k\oplus u_1^k))=v_1^x||v_1^k}} (-1)^{(u_0^x||u_0^k)^\top(x||k)\oplus(v_0^x||v_0^k)^\top(x\oplus k||k)} \\
&= \delta_{v_1^x}(u_1^x\oplus u_1^k)\delta_{v_1^k}(u_1^k)\left(\frac{1}{2^n}(-1)^{(u_0^x\oplus v_0^x)^\top x}\right)\left(\frac{1}{2^m}\sum_{k\in\mathbb{F}_2^m}(-1)^{(u_0^k\oplus v_0^x\oplus v_0^k)^\top k}\right) \\
&= \delta_{v_1^x}(u_1^x\oplus u_1^k)\delta_{v_1^k}(u_1^k)\delta_{v_0^x}(u_0^x)\delta_{u_0^k}(v_0^x\oplus v_0^k)
\end{aligned}
$$

□

6 Conclusion

In this paper, we proposed the quasi-boomerang framework, an extension of the quasi-differential framework [BR22] to the boomerang distinguisher in both single-key and related-key scenarios by the geometric approach. Following Hu et al.'s work [HZC+25], by choosing a suitable pair of bases for the input and output spaces, the boomerang attack can be described as a 3rd-order attack. Then the probability of the boomerang distinguisher can be calculated by the sum of quasi-boomerang characteristics' correlations. The analysis of the influence of the keys is similar to the quasi-differential framework, which allows us to investigate the probability of the boomerang in the fixed-key model more practically. After applying to `SKINNY`-64 and `GIFT`-64, we found several boomerang distinguishers obtained by the tools proposed in [HBS21] having high probabilities and are key-independent. We also proposed a divide-and-conquer approach following the sandwich framework and utilized it to check three existing boomerang distinguishers and recalculated their probabilities. In addition, as an independent interest, we revisited Boura et al.'s work [BDG25] in an easier way by regarding the key-XOR operation as a normal cipher component.

Acknowledgments. We sincerely thank the anonymous reviewers for providing valuable comments to help us improve the overall quality of the paper. This research is supported by the National Key R&D Program of China (Grant No. 2024YFA1013000, 2023YFA1009500), the National Natural Science Foundation of China (Grant No. 62032014, U2336207), the National Cryptologic Science Fund of China (2025NCSF01013), Department of Science & Technology of Shandong Province (No. SYS202201). Hosein Hadipour was supported by the European Research Council (ERC) project SYMTRUST (grant agreement No. 101097056). Kai Hu is supported by the National Cryptologic Science Fund of China (2025NCSF02007), the National Natural Science Foundation of China (62402283), the Natural Science Foundation of Shandong Province (2025HWYQ-025), the Natural Science Foundation of Jiangsu Province (BK20240420) and Program of Qilu Young Scholars of Shandong University.

References

[BDG25] Christina Boura, Patrick Derbez, and Baptiste Germon. Extending the quasidifferential framework: From fixed-key to expected differential probability. *IACR Trans. Symmetric Cryptol.*, 2025(1):515–541, 2025.

[BDK01] Eli Biham, Orr Dunkelman, and Nathan Keller. The Rectangle Attack - Rectangling the Serpent. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 340–357. Springer, 2001.

[BDK02] Eli Biham, Orr Dunkelman, and Nathan Keller. New Results on Boomerang and Rectangle Attacks. In Joan Daemen and Vincent Rijmen, editors, *Fast Software Encryption - FSE 2002*, volume 2365 of *LNCS*, pages 1–16. Springer, 2002.

[Bey21] Tim Beyne. A geometric approach to linear cryptanalysis. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021*, volume 13090 of *Lecture Notes in Computer Science*, pages 36–66. Springer, 2021.

[Bey23] Tim Beyne. A geometric approach to symmetric-key cryptanalysis. PhD thesis, 2023.

[Bih94] Eli Biham. New Types of Cryptanalytic Attacks Using Related Keys. *J. Cryptol.*, 7(4):229–246, 1994.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In *CRYPTO 2016*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A small present - towards reaching the limit of lightweight encryption. In *CHES 2017*, volume 10529 of *Lecture Notes in Computer Science*, pages 321–345. Springer, 2017.

[BR22] Tim Beyne and Vincent Rijmen. Differential cryptanalysis in the fixed-key model. In *CRYPTO 2022*, volume 13509 of *Lecture Notes in Computer Science*, pages 687–716. Springer, 2022.

[BS90] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

[BS91] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *J. Cryptol.*, 4(1):3–72, 1991.

[BV23] Tim Beyne and Michiel Verbauwhede. Integral cryptanalysis using algebraic transition matrices. *IACR Trans. Symmetric Cryptol.*, 2023(4):244–269, 2023.

[BV24a] Tim Beyne and Michiel Verbauwhede. Ultrametric integral cryptanalysis. *IACR Cryptol. ePrint Arch.*, page 722, 2024.

[BV24b] Tim Beyne and Michiel Verbauwhede. Ultrametric integral cryptanalysis. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024*, volume 15490 of *Lecture Notes in Computer Science*, pages 392–423. Springer, 2024.

[CHP+18] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018*, volume 10821 of *Lecture Notes in Computer Science*, pages 683–714. Springer, 2018.

[CWZ19] Lele Chen, Gaoli Wang, and Guoyan Zhang. Milp-based related-key rectangle attack and its application to gift, khudra, MIBS. *Comput. J.*, 62(12):1805–1821, 2019.

[DDV20] Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. Catching the fastest boomerangs application to SKINNY. *IACR Trans. Symmetric Cryptol.*, 2020(4):104–129, 2020.

[DEFN22] Patrick Derbez, Marie Euler, Pierre-Alain Fouque, and Phuong Hoa Nguyen. Revisiting related-key boomerang attacks on AES using computer-aided tool. In *ASIACRYPT 2022*, volume 13793 of *Lecture Notes in Computer Science*, pages 68–88. Springer, 2022.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3g telephony. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 393–410. Springer, 2010.

[DQSW22] Xiaoyang Dong, Lingyue Qin, Siwei Sun, and Xiaoyun Wang. Key guessing strategies for linear key-schedule algorithms in rectangle attacks. In *EUROCRYPT 2022*, volume 13277 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2022.

[DR20] Joan Daemen and Vincent Rijmen. *The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition.* Information Security and Cryptography. Springer, 2020.

[HBS21] Hosein Hadipour, Nasour Bagheri, and Ling Song. Improved rectangle attacks on SKINNY and CRAFT. *IACR Trans. Symmetric Cryptol.*, 2021(2):140–198, 2021.

[HNE22] Hosein Hadipour, Marcel Nageler, and Maria Eichlseder. Throwing boomerangs into feistel structures application to CLEFIA, WARP, LBlock, LBlock-s and TWINE. *IACR Trans. Symmetric Cryptol.*, 2022(3):271–302, 2022.

[HZC+25] Kai Hu, Chi Zhang, Chengcheng Chang, Jiashu Zhang, Meiqin Wang, and Thomas Peyrin. Periodic table of cryptanalysis: Geometric approach with different bases. Cryptology ePrint Archive, Paper 2025/403, 2025.

[JZZD20] Fulei Ji, Wentao Zhang, Chunning Zhou, and Tianyou Ding. Improved (related-key) differential cryptanalysis on GIFT. In Orr Dunkelman, Michael J. Jacobson Jr., and Colin O'Flynn, editors, *SAC 2020*, volume 12804 of *Lecture Notes in Computer Science*, pages 198–228. Springer, 2020.

[KKS00] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and serpent. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *Lecture Notes in Computer Science*, pages 75–93. Springer, 2000.

[KT22] Andreas B. Kidmose and Tyge Tiessen. A formal analysis of boomerang probabilities. *IACR Trans. Symmetric Cryptol.*, 2022(1):88–109, 2022.

[LGS17] Guozhen Liu, Mohona Ghosh, and Ling Song. Security analysis of SKINNY under related-tweakey settings (long paper). *IACR Trans. Symmetric Cryptol.*, 2017(3):37–72, 2017.

[LIMY20] Fukang Liu, Takanori Isobe, Willi Meier, and Zhonghao Yang. Algebraic Attacks on Round-Reduced Keccak/Xoodoo. *IACR Cryptol. ePrint Arch.*, page 346, 2020.

[LMM91] Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In Donald W. Davies, editor, *EUROCRYPT 1991*, volume 547 of *Lecture Notes in Computer Science*, pages 17–38. Springer, 1991.

[LZH+24] Huina Li, Haochen Zhang, Kai Hu, Guozhen Liu, and Weidong Qiu. Algsat - A SAT method for verification of differential trails from an algebraic perspective. In Tianqing Zhu and Yannan Li, editors, *ACISP 2024*, volume 14895 of *Lecture Notes in Computer Science*, pages 450–471. Springer, 2024.

[Mur11] Sean Murphy. The return of the cryptographic boomerang. *IEEE Trans. Inf. Theory*, 57(4):2517–2521, 2011.

[NGJE25] Marcel Nageler, Shibam Ghosh, Marlene Jüttler, and Maria Eichlseder. Autodiver: Automatically verifying differential characteristics and learning key conditions. *IACR Cryptol. ePrint Arch.*, page 185, 2025.

[PT22] Thomas Peyrin and Quan Quan Tan. Mind your path: On (key) dependencies in differential characteristics. *IACR Trans. Symmetric Cryptol.*, 2022(4):179–207, 2022.

[PTZZ25] Thomas Peyrin, Quan Quan Tan, Hongyi Zhang, and Chunning Zhou. Trail-estimator: An automated verifier for differential trails in block ciphers. Cryptology ePrint Archive, Paper 2025/396, 2025.

[SQH19] Ling Song, Xianrui Qin, and Lei Hu. Boomerang connectivity table revisited. application to SKINNY and AES. *IACR Trans. Symmetric Cryptol.*, 2019(1):118–141, 2019.

[SYC+24] Ling Song, Qianqian Yang, Yincen Chen, Lei Hu, and Jian Weng. Probabilistic extensions: A one-step framework for finding rectangle attacks and beyond. In *EUROCRYPT 2024*, volume 14651 of *Lecture Notes in Computer Science*, pages 339–367. Springer, 2024.

[Tie16] Tyge Tiessen. Polytopic Cryptanalysis. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016*, volume 9665 of *LNCS*, pages 214–239. Springer, 2016.

[Wag99] David A. Wagner. The boomerang attack. In Lars R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.

[WP19] Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. application to AES variants and deoxys. *IACR Trans. Symmetric Cryptol.*, 2019(1):142–169, 2019.

[WSW+24] Libo Wang, Ling Song, Baofeng Wu, Mostafizar Rahman, and Takanori Isobe. Revisiting the boomerang attack from a perspective of 3-differential. *IEEE Trans. Inf. Theory*, 70(7):5343–5357, 2024.

[YSZ+24] Qianqian Yang, Ling Song, Nana Zhang, Danping Shi, Libo Wang, Jiahao Zhao, Lei Hu, and Jian Weng. Optimizing rectangle and boomerang attacks: A unified and generic framework for key recovery. *J. Cryptol.*, 37(2):19, 2024.

[ZDM+20] Boxin Zhao, Xiaoyang Dong, Willi Meier, Keting Jia, and Gaoli Wang. Generalized related-key rectangle attacks on block ciphers with linear key schedule: applications to SKINNY and GIFT. *Des. Codes Cryptogr.*, 88(6):1103–1126, 2020.