Related-Key Differential and Boomerang Cryptanalysis in the Fixed-Key Model (Long Paper)

Verify Related-Key Differentials for SKINNY, GIFT, AES, CRAFT, and Boomerangs for SKINNY and GIFT

Chengcheng Chang[1,3,4], Kai Hu[1,3,4], Muzhou Li[1,3,4], Meiqin Wang[2,1,3,4]

[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] Quancheng Laboratory, Jinan 250103, China.
mqwang@sdu.edu.cn
[3] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China.
[4] State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, Qingdao, 266237, China.

Abstract. Differential cryptanalysis, along with its variants such as boomerang attacks, is widely used to evaluate the security of block ciphers. These cryptanalytic techniques often rely on assumptions like the *hypothesis of stochastic equivalence* and *Markov ciphers assumption*. Recently, more attention has been paid to verifying whether differential characteristics (DCs) meet these assumptions, finding both positive and negative results. A part of these efforts includes the automatic search methods for both the value and difference propagation (e.g., Liu et al. CRYPTO 2020, Nageler et al. ToSC 2025/1), structural constraints analysis (e.g., Tan and Peyrin, ToSC 2022/4), and the quasidifferential (Beyne and Rijmen, CRYPTO 2022). Nevertheless, less attention has been paid to the related-key DCs and boomerang distinguishers, where the same assumptions are used. To the best of our knowledge, only some related-tweakey DCs of SKINNY were checked thanks to its linear word-based key-schedule, and no similar work is done for boomerang distinguishers. The verification of related-key DCs and boomerang distinguishers is as important as that of DCs, as they often hold the longest attack records for block ciphers. This paper focuses on investigating the validity of DCs in the related-key setting and boomerang distinguishers in both single- and related-key scenarios. For this purpose, we generalize Beyne and Rijmen's quasidifferential techniques for the related-key DCs and boomerang attacks.

First, to verify related-key DCs, the related-key quasi-DC is proposed. Similar to the relationship between the quasi-DC and DC, the exact probability of a related-key DC is equal to the sum of all corresponding related-key quasi-DCs' correlations. Since the related-key quasi-DCs involve the key information, we can determine the probability of the target related-key DC in different key subspaces. We find both positive and negative results. For example, we verify the 18-round related-key DC used in the best attack on GIFT-64 whose probability is 2^{-58}, finding that this related-key DC has a higher probability for $2^{128} \times (2^{-5} + 2^{-8})$ keys which is around 2^{-50}, but it is impossible for the remaining keys.

Second, we identify proper bases to describe the boomerang distinguishers with the geometric approach. A quasi-BCT is constructed to consider the value influence in the boomerang connectivity table (BCT). For the DC parts, the quasi-biDDT is used. Connecting the quasi-BCT and quasi-biDDT, we can verify the probability of a boomerang distinguisher with quasi-boomerang characteristics. This also allows us to analyze the probability of the boomerang in different key spaces. For a 17-round boomerang distinguisher of SKINNY-64-128 whose probability is 2^{-50}, we find that the probability can be 2^{-44} for half of keys, and impossible for the other half.

Keywords: Quasidifferential, Boomerang, Related-Key

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.

Verification efforts can be roughly categorized into three categories. The first type of methods are 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 a 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]. Their algorithm can also find the probability of a DC under different key spaces.

The third one is the quasidifferential 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] and (ultrametric) integral cryptanlysis [BV23, BV24]. In this method, the differential cryptanalysis is described by a transition matrix under a pair of quasidifferential bases. The exact probability of a DC can be calculated by summing *correlations* of all quasidifferential 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 signs 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.

Until now, most of the targets of the above methods are single-key DCs. For two of the most important variants of the differential cryptanalysis, i.e., the related-key DCs [Bih94] and boomerang distinguishers [Wag99], less attention has been paid. These two attacks are important, as they often keep the longest attack records for many ciphers. Thus, it is equally desirable to have some methods to verify the validity of the related-key DCs and boomerang distinguishers.

As far as we know, SKINNY [BJK+16] is the only example whose related-key DCs have been checked, one is by Peyrin and Tan in [PT22] and the other Nageler et al. in [NGJE25].

No similar verification results for boomerang distinguishers have been reported[1]. Related-key differential cryptanalysis and boomerang attack (including the rectangle attack) often hit the longest attack record for lots of ciphers, thus verifying the validity of these distinguishers is as same important as verifying the DCs. However, tools that are useful to verify DCs are not trivially applicable to related-key DCs and boomerang distinguishers. Peyrin and Tan's tool is highly tailored for SKINNY [BJK+16] and GIFT [BPP+17], thus it seems not easy to apply it to other ciphers. AutoDiVer is much more versatile, as it basically models the propagation of the two values (including the two keys in the related-key setting) following the DCs. Nevertheless, modeling related-key DCs or boomerang distinguishers will increase the number of their variables, especially with respect to the nonlinear and heavy key schedules. The increase in the number of variables might make AutoDiVer very slow, and it may even become unsolvable. In fact, in [NGJE25, Section 5], the authors of AutoDiVer have found that the key schedule will influence the speed. Additionally, both Peyrin-Tan and AutoDiVer methods cannot give an accurate theoretical model to calculate the exact probability of related-key DCs and boomerang distinguishers.

The (generalized) quasidifferential method seems more suitable in verifying the related-key DCs and boomerang distinguishers. First, the current quasidifferential technique in fact already works for verifying related-key DCs. When treating the key-XOR operation as a normal cipher component (like an S-box), the transition matrix for key-XOR is easy to be established. Second, as an application of the geometric approach, the idea of the quasidifferential can be shifted to the boomerang attacks. A recent work shows that we can allow two different bases in geometric approach to producing more flexible transition matrices [HZC+25]. With this idea, it is potential to construct quasi-boomerang characteristics (quasi-BCs) and use these quasi-BCs to verify the boomerang distinguishers. Due to the similarities, techniques established for quasidifferential cryptanalysis in [BR22] can be naturally used in a similar way to verify related-key DCs and boomerangs.

Our contributions. In this paper, we extend the quasidifferential techniques to cover the related-key differential and boomerang attacks inside the geometric framework, as a tool for the verification of existing distinguishers. Our contributions are two-fold as follows.

Verify related-key DCs with quasidifferential techniques. The quasidifferential technique can construct a transition matrix for a cipher component function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Regarding the key-XOR operation in the related-key setting, denoted by $\mathsf{F}_{k,\Delta k}(x, \Delta x) = (x \oplus k, \Delta x \oplus \Delta k)$, as a single function with the secret key k and known Δk, we can construct the transition matrix for $\mathsf{F}_{k,\Delta k}$. The construction of transition matrices for other non-key-XOR components is the same as [BR22]. Finally, we can get a related-key quasi-DC together with the transition matrices of the key-XOR and non-key-XOR operations. Since the key difference is known, only the key value will be variables, but for a key-alternating cipher, it only affects the sign of the correlation and will be reflected in the final correlation of the related-key quasi-DC. Similarly to the quasi-differential cases, the sum of correlations of all corresponding related-key quasi-DCs is the exact probability of the corresponding related-key DC. By searching for the related-key quasi-DCs with big absolute values, we can approximate the exact probability under the *dominant trail assumption.*

We apply this technique to verify related-key DCs for AES, CRAFT, and GIFT, and estimate their probabilities in different key subspaces. We find that some published related-key DCs of AES and CRAFT are indeed reliable, but some GIFT's related-key DCs only work with a fraction of keys. These results are listed in Table 1.

[1] There have been many works that handle the independent assumption between the upper DC and lower DC of a boomerang, but no work has been done for verifying the independent assumptions for all rounds.

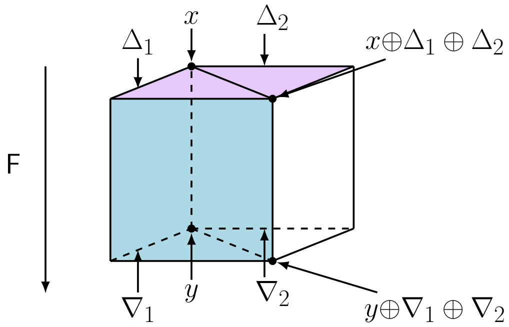

x
Δ_2
Δ_1
$x \oplus \Delta_1 \oplus \Delta_2$
F
∇_1
y
∇_2
$y \oplus \nabla_1 \oplus \nabla_2$

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, Δ_2 is known, and x, Δ_1 can be any value. For both the input and output, the four values in a quartet sum to zero as the four values are $x, x \oplus \Delta_1, x \oplus \Delta_2, x \oplus \Delta_1 \oplus \Delta_2$, to make it a 3rd order space.

Verify boomerang distinguishers with generalized geometric approaches. The current geometric approach has not been applied to describe boomerang attacks. Thus, to verify the boomerang distinguishers with the quasidifferential techniques, we should first extend the geometric approach to cover the boomerang distinguisher. In [HZC+25], the authors introduced a generalized geometric approach framework, where two different bases are allowed to use to make the geometric approach more flexible. According to [HZC+25], the boomerang attack should be described as a 4th-order attack, as it traces a quartet of four values. However, the transition matrix of a 4th order attack will have a size of 4 times of the cipher size (with the known differences, the size can be reduced to 3 times of the cipher size). This is too heavy to search for quasi trails. Instead, we notice that the current boomerang attack has an implicit assumption that the sum of the four values of a quartet in boomerang attacks is always zero. This inspires us to describe the boomerang attack by a 3rd-order attack, i.e., we will trace a quartet like $(x_0, x_1, x_2, x_0 \oplus x_1 \oplus x_2)$ whose dimension is only 3.

Next, we choose suitable bases for the boomerang attack. As shown in Figure 1, for the input of a boomerang, the value x and the second difference Δ_2 can be any value, thus, we use $(-1)^{u_0^\top x}(-1)^{u_2^\top \Delta_2}$ to describe them. When $u_0 = u_2 = 0$, x and Δ_2 can be any value. The first difference Δ_1 is known as a fixed value; therefore, we use $\delta_{u_1}(\Delta_1)$ to describe it, where $\delta_u(\cdot)$ is the Dirac delta function. Thus, the input basis is $(-1)^{u_0^\top x}\delta_{u_1}(\Delta_1)(-1)^{u_2^\top \Delta_2}$.

For the output, the value y and the first difference ∇_1 can be any value, thus, we use a $(-1)^{v_0^\top y}(-1)^{v_1^\top \nabla_1}$ to describe them. When $v_0 = v_1 = 0$, y and ∇_1 can be any value. The second difference ∇_1 is known as a fixed value, so we use $\delta_{v_2}(\nabla_2)$ to describe it. Thus, the output basis is $(-1)^{v_0^\top y}(-1)^{v_1^\top \nabla_1}\delta_{v_2}(\nabla_2)$.

Since the input and output bases are different, this attack falls into the mixed-basis attack [HZC+25, Definition 6]. The statistic used for describing the boomerang attack on a cipher F is then

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

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 $\mathsf{F}(x \oplus \Delta_1 \oplus \Delta_2) = y \oplus \nabla_1 \oplus \nabla_2$. When $u_0 = u_2 = v_0 = v_1 = 0$. This formula describes the boomerang attack[2].

[2] Actually, it describes the rectangle attack. The probability of a boomerang attack should be a 2^n times of that of its corresponding rectangle. However, in this paper, we do not specifically distinguish the two attacks. We will always manually multiply a 2^n to the formula to make it a boomerang probability.

After covering the boomerang attack by the geometric approach, we define the *boomerang characteristic* (BC) as an approximation to the real boomerang distinguisher. The quasi-boomerang characteristics (quasi-BCs) can also be defined as the quasi-DCs. To do it, following the framework of handling the mix-basis attack in [HZC+25], we divide a cipher F into three parts as $\mathsf{F} = \mathsf{F}_2 \circ \mathsf{F}_1 \circ \mathsf{F}_0$. For F_0 (F_2), a same-basis attack can be derived, whose transition matrix is called an upper (lower) quasi-biDDT. For F_1, a mix-basis attack is obtained; we call its transition matrix the quasi-BCT. The trails connecting these transition matrices are called quasi-BCs. By searching for the quasi-BCs, we can verify if a BC is valid.

Similarly to [BR22], this technique can be used to check the validity of a boomerang characteristic (in both single-key and related-key settings). We apply this method to SKINNY and GIFT, improving the probabilities in certain key spaces or disproving some. The results are shown in Table 1.

All source codes and results of this paper are provided at https://github.com/ccc53021/related-key-quasi.

Outline. In Section 2, we briefly recall the related works of differential, boomerang attacks, and Beyne's geometric approach. Section 3 generalizes the geometric approach to the differential and boomerang distinguishers in the related-key setting. In Section 4 and Section 5, we apply our technique to verify the validity of the differential characteristic and boomerang distinguishers, respectively. Section 6 discusses and compares our technique with Peyrin and Tan's work and AutoDiVer.

2 Preliminaries

In this section, we recall the differential cryptanalysis, the boomerang attacks and their related-key variants, and Beyne's geometric approach. We first introduce the notations used in this paper.

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:

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

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:

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

Table 1: Our results of the verification of DCs and BCs. For a cipher with n-bit key, the size of key space is **#Key** $\times 2^n$ and full denotes the size of key space is 2^n. **#DC/BC** denotes the number of DC/BC. In our results, the probability is zero except for the given key space.

Cipher	**#R**	**#DC/BC**	**Valid?**	**#Key**	**Prob.**	**Reference**
`GIFT-64`	15	DC-1	✗	Full	2^{-48}	[JZZD20, Table 10]
				2^{-1}	$2^{-46.42}$	Section 4.1
	18	DC-2	✗	Full	2^{-58}	[SWW21, Figure 8]
				2^{-8}	$2^{-49.42}$	Section 4.1
				2^{-5}	$2^{-52.42}$	
`AES`	4	DC-3	✓	Full	2^{-81}	[FJP13, Figure 14]
				Full	2^{-81}	Section 4.2
	4	DC-4	✓	Full	2^{-81}	[FJP13, Figure 15]
				Full	2^{-81}	Section 4.2
	5	DC-5	✓	Full	2^{-105}	[FJP13, Figure 16]
				Full	2^{-105}	Section 4.2
	6	DC-6	✓	Full	2^{-130}	[SGL+17, Table 1]
				Full	2^{-130}	Section 4.2
`CRAFT`	30	DC-7	✓	Full	2^{-30}	[SWW22, Figure 3]
				Full	2^{-30}	Section 4.3
`SKINNY-64-128`	$2^{\dagger}$	BC-1	✓	Full	$2^{-8.42}$	[LGS17, Table 12]
				Full	2^{-2}	[CHP+18]
				Full	2^{-2}	Section 5.1
	17	BC-3	✗	Full	2^{-50}	[LGS17, Table 12]
				2^{-1}	2^{-44}	Section 5.1
`SKINNY-64-192`	$2^{\dagger}$	BC-2	✓	Full	$2^{-16.30}$	[LGS17, Table 14]
				Full	$2^{-5.31}$	[CHP+18]
				Full	$2^{-5.29}$	Section 5.1
	22	BC-4	✓	Full	2^{-80}	[LGS17, Table 14]
				Full	2^{-62}	Section 5.1
`GIFT-64`	2	BC-5	✗	Full	1	[CWZ19, Table 5]
				Full	2^{-18}	[JZZD20]
				2^{-1}	2^{-15}	Section 5.2
				2^{-1}	2^{-16}	

† The middle two rounds of the boomerang distinguishers including clustering effect.

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 the boomerang connectivity table (BCT) technique [CHP+18]. 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 T, in which the entry for the (β, γ) position is given by

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

Again, if there is a differential $\alpha \xrightarrow{\mathsf{F}_0} \beta$ with probability p, and $\gamma \xrightarrow{\mathsf{F}_1} \delta$ 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_1, 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 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 the 2^n times of that of the corresponding rectangle distinguisher, with a formal analysis with 3-differential cryptanalysis, where n is the length of the block. Since this paper focuses on verification, we always use the boomerang attack as the example, we do not strictly distinguish the 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.

Differential and 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 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

Let n be positive integers, $\mathbb{Q}$ is the rational number field, the free vector space over $\mathbb{Q}$ (in fact, any field works for the geometric approach) is denoted as $\mathbb{Q}[\mathbb{F}_2^n]$, and every element in $\mathbb{Q}[\mathbb{F}_2^n]$ is represented by $\sum_i k_u\delta_u$, where $k_u \in k, \delta_u \in \mathbb{F}_2^n$. For a block cipher $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$, Beyne shows that F can be regarded as a linear mapping over $\mathbb{Q}[\mathbb{F}_2^n]$ [Bey21]. For $v = \mathsf{F}(u)$, we can get a pushforward operator of F, denoted by $T^{\mathsf{F}} : \mathbb{Q}[\mathbb{F}_2^n] \to \mathbb{Q}[\mathbb{F}_2^n]$ which satisfies $T^{\mathsf{F}}(\delta_u) = \delta_v$. Regarding δ_u as a unit vector with only the u-th element being 1, $\delta_0, \delta_1, \ldots, \delta_{2^n-1}$ form a set of standard basis of $\mathbb{Q}[\mathbb{F}_2^n]$.

We borrow the notation from [HZC+25]. Writing all these 2^n unit vectors in 2^n columns, we will obtain a matrix, denoted by $[\delta_u(x)]_{x,u}$, where the element at the u-th column and x-th row is just $\delta_u(x)$. $\delta_x(y)$ is the Dirac delta function as

$$\delta_x(y) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}$$

Actually, $\delta_u = [\delta_u(x), x = 0, 1, \ldots, 2^n - 1]$, which justify the usage of δ_u as a unit vector and $\delta_u(\cdot)$ a function.

Under this set of basis, the matrix of T^{F} can be obtained, which is a $2^n \times 2^n$ matrix whose element in the u-th column and v-th row is $\delta_v(\mathsf{F}(u))$. Since T^{F} is a linear mapping over a linear space $\mathbb{Q}[\mathbb{F}_2^n]$, the matrix corresponding to T^{F} changes as the basis changes.

To study differential cryptanalysis in a fixed key setting, Beyne and Rijmen studied the pushforward induced by F over $\mathbb{Q}[\mathbb{F}_2^n \otimes \mathbb{F}_2^n]$, where $\mathbb{F}_2^n \otimes \mathbb{F}_2^n = \{x \otimes y : x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^n\}$, which is still denoted by T^{F}, where here "$x \otimes y$" is the tensor product of two vectors. For example, $[a_0, a_1] \otimes [b_0, b_1] = [a_0b_0, a_0b_1, a_1b_0, a_1b_1]$.

Remark (the notation trick). To describe the quasidifferential cryptanalysis easier, we use the *notation trick* in [HZC+25, Section 3.1]. (x_0, x_1) *denotes the input value and input difference of* F*, and* $(\mathsf{F}(x_0), \mathsf{F}(x_1))$ *denote the output value and output difference.*

The $u_0||u_1$-th standard basis for the differential attack is

$$\delta_{u_0||u_1} = [\delta_{u_0}(x_0) \otimes \delta_{u_1}(x_1), x_0||x_1 = 0, 1, \ldots, 2^{2n} - 1].$$

Thus, $T^{\mathsf{F}}(\delta_{u_0||u_1}) = \delta_{\mathsf{F}(u_0)||\mathsf{F}(u_1)}$. Then the matrix of T^{F} under the standard basis is T satisfying

$$T_{v_0||v_1, u_0||u_1} = \delta_{v_0||v_1}(\mathsf{F}(u_0)||\mathsf{F}(u_1)).$$

Beyne and Rijmen chose 2^{2n} linearly-independent vectors as the quasidifferential basis, where the $u_0||u_1$-th basis is

$$\beta_{u_0, u_1} = [(-1)^{u_0^\top x_0} \otimes \delta_{u_1}(x_1), x_0||x_1 = 0, 1, \ldots, 2^{2n} - 1].$$

The basis in the matrix form is then $[(-1)^{u_0^\top x_0} \otimes \delta_{u_1}(x_1)]_{x_0||x_1, u_0||u_1}$.

With the quasidifferential basis, the quasidifferential transition matrix D is calculated as

$$\begin{aligned} D^{\mathsf{F}}_{v_0||v_1, u_0||u_1} &= \frac{1}{2^n} \sum_{x_0||x_1 \in \mathbb{F}_2^n \times \mathbb{F}_2^n} (-1)^{u_0^\top x_0} \delta_{u_1}(x_1) (-1)^{v_0^\top \mathsf{F}(x_0))} \delta_{v_1}(\mathsf{F}(x_1)) \\ &= \frac{1}{2^n} \sum_{\substack{x_0 \in \mathbb{F}_2^n \\ \mathsf{F}(x_0 \oplus u_1) \oplus \mathsf{F}(x_0) = v_1}} (-1)^{u_0^\top x_0 \oplus v_0^\top \mathsf{F}(x_0)}, \end{aligned} \tag{3}$$

where $u_0, u_1, v_0, v_1 \in \mathbb{F}_2^n$. The quasidifferential combines the linear mask and difference propagations, thus following [BR22], we call (u_0, u_1) is the input mask-difference pair, and (v_0, v_1) is the output mask-difference pair.

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 D has the following properties:*

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

(2) If $\mathsf{F} = \mathsf{F}_2 \circ \mathsf{F}_1$, then $D^{\mathsf{F}} = D^{\mathsf{F}_2} D^{\mathsf{F}_1}$.

Definition 2 ([BR22], Definition 4.1)**.** A quasidifferential characteristic (quasi-DC) for a function $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$ is a sequence $\omega_1, \omega_2, \ldots, \omega_{r+1}$ of mask-difference pairs $\omega_i = (u_0^i, u_1^i)$. The correlation of this quasi-DC is defined as $\prod_{i=1}^r D^{\mathsf{F}_i}_{\omega_{i+1}, \omega_i}$.

According to Theorem 2, if $\mathsf{F} = \mathsf{F}_r \circ \mathsf{F}_{r-2} \circ \cdots \circ \mathsf{F}_1$ we have

$$D^{\mathsf{F}}_{0||u_1^{r+1}, 0||u_1^1} = \sum_{\omega_r, \ldots, \omega_2} \prod_{i=1}^r D^{\mathsf{F}_i}_{w_{i+1}, w_i} \text{ with } \omega_0 = 0||u_0^1, \omega_{r+1} = 0||u_1^{r+1}.$$

Note that $D^{\mathsf{F}}_{0||u_1^{r+1},0||u_1^1}$ is exact the differential probability of F with input/output difference u_1^1 and u_1^{r+1}. Given a DC of F, say $(u_1^1, u_1^2, \ldots, u_1^{r+1})$, then the probability of the DC is exactly calculated by

$$\mathrm{Pr}_{DC}[u_1^1, \ldots, u_1^r] = \sum_{u_0^2,\ldots,u_0^r} \prod_{i=1}^{r} D^{\mathsf{F}_i}_{u_0^{i+1}||u_{i+1}^1, u_0^i||u_1^i} \text{ with } u_0^1 = 0, u_0^{r+1} = 0.$$

To sum up, the exact probability of a DC is equal to the summation of correlations of all its corresponding quasi-DCs.

Generalization of the geometric approach. In [HZC+25], the authors generalized the geometric approach. An attack has an important information called the *order* which indicates the dimension of its input spaces.

Definition 3 (The order of an attack [HZC+25])**.** The dimension of the input space of an attack is called the order of the attack.

The order of an attack is crucial when we choose bases to describe it with the geometric approach. For

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

if the input and output bases are chosen as the standard basis $[\delta_u(x)]_{x,u}$, the matrix of T^{F} is just $[\delta_u(x)]_{x,u}$. When we choose another pair of bases for the input and output spaces, say $[\alpha_u(x)]_{x,u}$ and $[\beta_u(x)]_{x,u}$, the transition matrix of T^{F} can be calculated by

$$A^{\mathsf{F}}_{v,u} = \sum_{x \in (\mathbb{F}_2^n)^{\otimes d}} \beta^{\star}_{\mathsf{F}(x)}(v) \ \alpha_u(x)$$

according to [HZC+25], where $[\beta^{\star}_u(x)]_{x,u}$ represents the inverse matrix of $[\beta_u(x)]_{x,u}$.

Distinguished by whether we use the same basis for the input and output spaces, attacks can be divided into same-basis and mix-basis attacks.

Definition 4 (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, a mix-basis attack.

With this generalization, the transition matrices are obtained considering the input/output bases. The properties of these transition matrices are as same as those in the original geometric approach [Bey23].

3 Verify Related-Key DC and Boomerang Distinguishers with Geometric Approach

In this section, we show how to extend the geometric approach to the related-key differential and boomerang attacks. In the related-key differential attack, it is assumed that the attacker has known the difference of round keys. Thus, parts of the state difference might be canceled by the round key difference, which can bring longer DC in the related-key setting. From the perspective of the geometric approach, the key-XOR is not special from other components. Thus, the quasidifferential technique can be almost directly applied to the key-XOR operation. In other words, it is natural to apply the geometric approach to verify the related-key DCs. The case for boomerang distinguishers is much more complicated. There are no known applications of the geometric approach to this attack. Thus, we will extend the geometric approach to cover the boomerang attack.

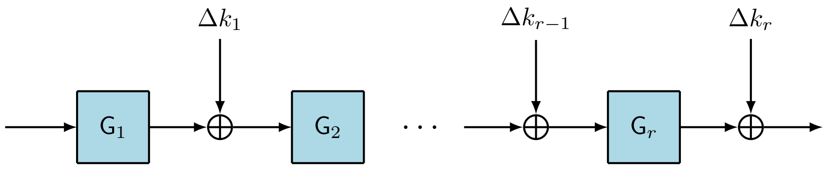


Figure 2: Related-key differential characteristic for a key-alternating composite cipher.

3.1 Transition Matrix of Key-XOR Operation in Related-Key Setting

Following the quasidifferential framework, the key-XOR operation for key-alternating ciphers in the related-key setting can be described as a function

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

Applying Equation (3) to $\mathsf{F}_{k,\Delta k}$, we obtain the transition matrix of $\mathsf{F}_{k,\Delta k}$ whose element is

$$\begin{aligned} D^{\mathsf{F}}_{v_0||v_1,u_0||u_1} &= \frac{1}{2^n} \sum_{x_0||x_1 \in \mathbb{F}_2^n \times \mathbb{F}_2^n} (-1)^{u_0^\top x_0} \delta_{u_1}(x_1)(-1)^{v_0^\top (x_0 \oplus k)} \delta_{v_1}(x_1 \oplus \Delta k) \\ &= \frac{1}{2^n} \sum_{\substack{x_0 \in \mathbb{F}_2^n \\ u_1 \oplus \Delta k = v_1}} (-1)^{u_0^\top x_0 \oplus v_0^\top x_0 \oplus v_0^\top k} \\ &= (-1)^{v_0^\top k} \delta_{v_1}(u_1 \oplus \Delta k) \delta_{v_0}(u_0) \end{aligned} \tag{4}$$

The term $\delta_{v_0}(u_0)$ says that the input and output masks should be unchanged. The $\delta_{v_1}(u_1 \oplus \Delta k)$ term ensures that the difference of the key changes the state difference from u_1 to $u_1 \oplus \Delta k$. The $(-1)^{v_0^\top k}$ term shows that the value of k will influence the sign of the correlation of a quasi-DC in the related-key setting (for the sake of simplicity, we call it related-key quasi-DC).

Consider a composite cipher $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$, where for some i, F_i will be the key-XOR operation $\mathsf{F}_{k,\Delta k}$. For those operations that are not the key-XOR, the transition matrix is built in the same way as the original quasidifferential cryptanalysis. For the key-XOR operations, the difference changes, and the value of the key contributes to a sign. Then, the correlation of a related-key quasi-DC can be defined similar to that of a quasi-DC [BR22].

Definition 5 (Related-key quasi-DC and its correlation)**.** A related-key quasi-DC for a function $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$ is a sequence $\omega_1, \omega_2, \ldots, \omega_{r+1}$ of the related-key mask-difference pairs with a key difference sequence $\Delta k_1, \Delta k_2, \ldots, \Delta k_r$, where $\omega_i = (u_0^i, u_1^i), 1 \le i \le r+1$ and Δk_i is the i-th key difference for $1 \le i \le r$. The correlation of the related-key quasi-DC can be expressed as $\prod_{i=1}^{r} D^{\mathsf{F}_i}_{\omega_{i+1},\omega_i}$.

Compute the probability of differential characteristic in the related-Key setting. For a key-alternating cipher in the related-key setting, the round function can be written as $\mathsf{F}_i(x) = \mathsf{F}_{k_i,\Delta k_i} \circ \mathsf{G}_i(x), 1 \le i \le r$. With the transition matrix of $\mathsf{F}_{k,\Delta k}$, the related-key quasi-DC has properties similar to the quasi-DC. According to [BR22, Section 4], when $u_0^1 = u_0^1 = \cdots = u_0^{r+1} = 0$, the related-key quasi-DC corresponds to the related-key DC. Additionally, the exact probability of the related-key DC can be calculated by summing up all correlations of related-key quasi-DCs related to this related-DC [BR22, Theorem 4.1].

Corollary 1. *Suppose that* $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$ *has a related-key DC denoted by* $(a_1, a_2, \ldots, a_{r+1})$ *with key difference sequence is* $\Delta k_1, \ldots, \Delta k_r$*, where* $\mathsf{F}_i = \mathsf{F}_{k_i,\Delta k_i} \circ \mathsf{G}_i(x)$*. The probability* *of this related-key DC is equal to the sum of the correlation of all quasi-DCs with the same intermediate differences:*

$$\begin{aligned}\mathrm{Pr}_{DC}[a_1, a_2, \dots, a_{r+1}] &= \sum_{u_0^2,\dots,u_0^r} \prod_{i=1}^{r} D^{\mathsf{F}_i}_{u_0^{i+1}||u_1^{i+1},u_0^i||u_1^i} \\ &= \sum_{u_0^2,\dots,u_0^r} \prod_{i=1}^{r} (-1)^{(u_0^{i+1})^{\mathsf{T}} k_i} D^{\mathsf{G}_i}_{u_0^{i+1}||(a_{i+1}\oplus\Delta k_i),u_0^i||a_i}\end{aligned} \tag{5}$$

with $u_0^1 = u_0^{r+1} = 0$.

Proof. Since the key-XOR is regarded as a normal cipher component, whose transition matrix is calculated by Equation (4). According to Theorem 1(2), the proof ends. □

3.2 Geometric Approach for Boomerang Cryptanalysis

In the following, we generalize the geometric approach to describe boomerang cryptanalysis. To describe the boomerang attack shown in Figure 1 by Beyne's geometric theory, we first choose the attack order and define the input and output space bases for the boomerang attack that the two upper and lower DCs can be combined by one Sbox layer as the middle part. Then we give the definition of the quasi-boomerang trail and propose how to calculate the exact probability of a boomerang characteristic.

3.2.1 Choose the Order for Boomerang Attack

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 quasidifferential cryptanalysis 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 3-differential has a disadvantage in that the row and column size of the transition matrix is 4 times of the Sbox size, which makes the search very slow. Actually, both [KT22] and [WSW$^+$24] can only search for (a part of) the 3-differential trails for two middle rounds of a boomerang distinguisher. In [WSW$^+$24], the authors in fact only searched for only a part of the 3-differentials corresponding to the 2-round boomerang distinguisher that they want to verify.

We notice that for both the classical boomerang distinguishers and refined ones with BCT, there is an implicit assumption that the 4 values in a quartet will sum to zero, i.e., the orders of the input and output spaces can be 3. In this case, the theoretical boomerang probability (the sum of the inner quartets is always zero) is actually an approximation of the real boomerang probability.

If we add a constraint to make sure that the sum of the quartet is always zero, then the orders of the input and output spaces become 3, which is easier to handle. Considering that in a verification work, the differences of the states (and differences in the key schedule) are known, the matrices for quasi trails will further reduce to 2 times of the Sbox size, making the search work.

3.2.2 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 as $\mathbb{Q}[\mathbb{X}]$. The pushforward of a cipher F is a linear mapping over

$\mathbb{Q}[\mathbb{X}]$. Next, we choose proper bases to describe the boomerang attack. As shown in Figure 1, for the input space, we need to consider the value of x, the difference Δ_1, and the difference Δ_2. However, only Δ_1 will be explicitly determined, so we choose the standard basis for Δ_1, which is $\delta_{u_1}(\Delta_1)$. x and Δ_2 can be any value, which is like the value in the quasidifferential attack. Thus, we choose the linear basis for x and Δ_2, which is $(-1)^{u_0^\top x}(-1)^{u_2^\top \Delta_2}$. Finally, the basis written in the matrix form for the input space is

$$[(-1)^{u_0^\top x} \otimes \delta_{u_1}(\Delta_1) \otimes (-1)^{u_2^\top \Delta_2}]_{x||\Delta_1||\Delta_2, u_0||u_1||u_2} \tag{6}$$

For the output space, we consider the value of $\mathsf{F}(x)$, the difference $\mathsf{F}(\Delta_1) \overset{\triangle}{=} \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta_1)$ and the difference $\mathsf{F}(\Delta_2) \overset{\triangle}{=} \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta_2)$ (recall the notation trick in Section 2.2). However, for the output, $\mathsf{F}(x)$ and $\mathsf{F}(\Delta_1)$ can be any value, but the $\mathsf{F}(\Delta_2)$ will be determined. Similar to the input basis, we choose the output basis as

$$[(-1)^{u_0^\top \mathsf{F}(x)} \otimes (-1)^{u_1^\top \mathsf{F}(\Delta_1)} \otimes \delta_{u_2}(\mathsf{F}(\Delta_2))]_{\mathsf{F}(x)||\mathsf{F}(\Delta_1)||\mathsf{F}(\Delta_2), u_0||u_1||u_2} \tag{7}$$

The input and output bases are different, so the boomerang attack will be described by a mix-basis attack according to [HZC⁺25].

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 a layer of Sbox, and construct the transition matrices for each of the three parts.

For F_0, the basis in Equation (6) is used for the input, output, and intermediate spaces. So we obtain a same-basis attack, where the element of the corresponding transition matrix is

$$\begin{aligned} B^{\mathsf{F}_0}_{v_0||v_1||v_2, u_0||u_1||u_2} &= \frac{1}{2^{2n}} \sum_{x_0, \Delta_1, \Delta_2} (-1)^{u_0^\top x_0} \delta_{u_1}(\Delta_1)(-1)^{u_2^\top \Delta_2}(-1)^{u_0^\top \mathsf{F}(x_0)} \delta_{v_1}(\mathsf{F}(\Delta_1))(-1)^{u_2^\top \Delta_2} \\ &= \frac{1}{2^{2n}} \sum_{\substack{x_0 \in \mathbb{F}_2^n, \Delta_2 \in \mathbb{F}_2^n \\ \Delta_1 = u_1, \mathsf{F}(\Delta_1) = v_1}} (-1)^{u_0^\top x_0 \oplus u_2^\top \Delta_2 \oplus v_0^\top \mathsf{F}(x_0) \oplus v_2^\top \mathsf{F}(\Delta_2)} \end{aligned} \tag{8}$$

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

For F_2, the basis in Equation (7) is used for the input, output and intermediate spaces. Therefore we obtain a same-basis attack too. The element of the corresponding transition matrix is

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

under the constraint $\mathsf{F}_0(x \oplus \Delta_1 \oplus \Delta_2) = \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta_1 \oplus \Delta_2)$

Definition 6 (Quasi-biDDT)**.** The transition matrices defined by Equations (8) and (9) model the propagation of two differences, thus we call them quasi-biDDT. To distinguish the two quasi-biDDT, the one for F_0 is called the upper quasi-biDDT, and the one for F_2 lower quasi-biDDT.

For F_1, Equation (6) is used for the input basis and Equation (7) is used for the output basis. The transition matrix is

$$\begin{aligned} B^{\mathsf{F}_1}_{v_0||v_1||v_2,u_0||u_1||u_2} &= \frac{1}{2^{2n}} \sum_{x_0,\Delta_1,\Delta_2} (-1)^{u_0^\top x_0} \delta_{u_1}(\Delta_1)(-1)^{u_2^\top \Delta_2}(-1)^{u_0^\top \mathsf{F}(x_0)}(-1)^{v_1^\top \mathsf{F}(\Delta_1)}\delta_{u_2}(\mathsf{F}(\Delta_2)) \\ &= \frac{1}{2^{2n}} \sum_{\substack{x_0\in\mathbb{F}_2^n,\Delta_2\in\mathbb{F}_2^n \\ \Delta_1=u_1,\mathsf{F}(\Delta_2)=v_2}} (-1)^{u_0^\top x_0 \oplus u_2^\top \Delta_2 \oplus v_0^\top \mathsf{F}(x_0) \oplus v_1^\top \mathsf{F}(\Delta_1)} \end{aligned} \tag{10}$$

under the constraint $\mathsf{F}_0(x \oplus \Delta_1 \oplus \Delta_2) = \mathsf{F}(x) \oplus \mathsf{F}(x \oplus \Delta_1 \oplus \Delta_2)$.

Definition 7 (Quasi-BCT)**.** The transition matrix defined by Equation (10) models the propagation from the upper difference to the lower difference, which is like the BCT considering the values. Thus, we call this matrix quasi-BCT.

Remark. The value calculated by Equation (10) is actually the probability of a rectangle distinguisher, while the probability should be multiplied with a 2^n term. In this paper, we will always consider the boomerang distinguisher, so we multiply 2^n with the probability calculated from Equation (10).

3.2.3 Use Quasi-Boomerang Characteristic to Approximate Boomerang Distinguisher

Like that a differential can contain lots of DCs, and some of these DCs will play a dominant role in deciding the probability of the differential. The probability of a boomerang distinguisher can be approximated by a so-called boomerang characteristic.

Definition 8 (Boomerang characteristic)**.** Suppose a composite cipher $\mathsf{E} = \mathsf{E}_r \circ \cdots \circ \mathsf{E}_{m+1} \circ \mathsf{E}_m \circ \mathsf{E}_{m-1} \circ \cdots \circ \mathsf{E}_1$, where $\mathsf{E}_{m-1} \circ \cdots \circ \mathsf{E}_0$ has a DC $(a_1, \ldots, a_m)$ and $\mathsf{E}_r \circ \cdots \circ \mathsf{E}_{m+1}$ has a DC $(a_{m+1}, \ldots, a_{r+1})$. Using the BCT connecting a_m and a_{m+1}, $(a_1, \ldots, a_m, a_{m+1}, \ldots, a_{r+1})$ can represent a boomerang distinguisher, which is called a boomerang distinguisher (BC), whose probability is

$$\Pr_{BC}[a_0, \ldots, a_m, a_{m+1}, \ldots, a_{r+1}] = \Pr^2_{DC}[a_1, \ldots a_m]\Pr^2_{DC}[a_{m+1}, \ldots a_{r+1}]\Pr_{BCT}[a_m, a_{m+1}].$$

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

Definition 9 (Quasi-boomerang characteristic)**.** A quasi-boomerang characteristic for a function $\mathsf{E} = \mathsf{E}_r \circ \cdots \mathsf{E}_{m+1} \circ \mathsf{E}_m \circ \cdots \circ \mathsf{E}_1$ is a sequence $\omega_1, \omega_2, \ldots, \omega_m, \omega_{m+1}, \ldots, \omega_{r+1}$ of the triples, where $\omega_i = (u_0^i, u_1^i, u_2^i)$ for $1 \leq i \leq r+1$. The correlation of the quasi-BC can be calculated as $\prod_{i=1}^r B^{\mathsf{E}_i}_{\omega_{i+1},\omega_i}$. B^{E_i} is the transition matrix of E_i:

- for $i < m$, B^{E_i} is the upper quasi-biDDT (Equation (8)),
- for $i = m$, B^{E_i} is the quasi-BCT (Equation (10)),
- for $i > m$, B^{E_i} is the lower quasi-biDDT (Equation (9)).

When $\forall i, u_0^i = 0$, $\forall i \leq m, u_2^i = 0$ and $\forall i \geq m+1, u_1^i = 0$, the quasi-BC corresponds to a BC. Their correlation is equal to the product of the one-round probabilities of the BC $(a_1, ..., a_{r+1})$, i.e.,

$$\begin{aligned} \Pr_{BC}[a_1, a_2, \ldots, a_{r+1}] &= \left(\prod_{i=1}^{m-1} B^{\mathsf{E}_i}_{0||a_{i+1}||0,0||a_i||0}\right)^2 B^{\mathsf{E}_m}_{0||0||a_{m+1},0||a_m||0} \left(\prod_{i=m+1}^{r} B^{\mathsf{E}_i}_{0||0||a_{i+1},0||0||a_i}\right)^2 \\ &= \Pr^2_{DC}[a_1, \ldots a_m]\Pr^2_{DC}[a_1, \ldots a_m]\Pr_{BCT}[a_m, a_{m+1}] \end{aligned}$$

Similarly to [BR22, Theorem 4.1], we can also use the quasi-BC to compute the exact probability of a BC as shown in the following Theorem.

Corollary 2. *For $\mathsf{E} = \mathsf{E}_r \circ \cdots \mathsf{E}_{m+1} \circ \mathsf{E}_m \circ \cdots \circ \mathsf{E}_1$, the probability of a boomerang characteristic $(\alpha_1, \alpha_2, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_r)$ is equal to the sum of the correlations of all quasi-boomerang trails with the same intermediate differences:*

$$\mathsf{Pr}_{BC}[a_1, a_2, \ldots, a_{r+1}] = \sum_{u_0^2,\ldots,u_0^r} \sum_{u_1^{m+1},\ldots,u_1^r} \sum_{u_2^2,\ldots,u_2^m} B^{\mathsf{E}_m}_{\omega_{m+1},\omega_m} \prod_{i=1}^{m} B^{\mathsf{E}_i}_{\omega_{i+1},\omega_i} \prod_{i=m+1}^{r} B^{\mathsf{E}_i}_{\omega_{i+1},\omega_i},$$

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

Proof. The proof directly follows Theorem (1) and Equations (8), (9) and (10). □

3.2.4 Quasi-BC for Key-Alternating Ciphers in the Related-Key Setting

Similar to the related-key quasi-DC case, the key-XOR operation for key-alternating ciphers in the related-key boomerang attack can be described as a function

$$\mathsf{F}_{k,\Delta k,\nabla k} : (x_0, \Delta_1, \Delta_2) \to (x_0 \oplus k, \Delta_1 \oplus \Delta k, \Delta_2 \oplus \nabla k)$$

The upper quasi-biDDT for $\mathsf{F}_{k,\Delta k,\nabla k}$ can be calculated according to Equation (8) as

$$\begin{aligned} B^{\mathsf{F}_{k,\Delta k,\nabla k}}_{v_0||v_1||v_2,u_0||u_1||u_2} &= \frac{1}{2^{2n}} \sum_{\substack{x_0\in\mathbb{F}_2^n,\Delta_2\in\mathbb{F}_2^n,\Delta_1=u_1\\ u_1\oplus\Delta_k=v_1}} (-1)^{u_0^\top x_0 \oplus u_2^\top \Delta_2 \oplus v_0^\top (x_0\oplus k)\oplus v_2^\top(\Delta_2\oplus\nabla k)} \\ &= (-1)^{v_0^\top k \oplus v_2^\top \nabla k} \delta_{v_1}(u_1 \oplus \Delta k)\delta_{v_0}(u_0)\delta_{v_2}(u_2) \end{aligned} \tag{11}$$

Similarly, the lower quasi-biDDT for $\mathsf{F}_{k,\Delta k,\nabla k}$ can be calculated according to Equation (9) as

$$B^{\mathsf{F}_{k,\Delta k,\nabla k}}_{v_0||v_1||v_2,u_0||u_1||u_2} = (-1)^{v_0^\top k \oplus v_1^\top \Delta k} \delta_{v_2}(u_2 \oplus \nabla k)\delta_{v_0}(u_0)\delta_{v_1}(u_1) \tag{12}$$

Consider a key-alternating cipher $\mathsf{E} = \mathsf{E}_r \circ \cdots \circ \mathsf{E}_{m+1} \circ \mathsf{E}_m \circ \cdots \circ \mathsf{E}_1$ in the related-key setting. Assume that for $1 \leq i < m$, $\mathsf{E}_i = \mathsf{F}_{k_i,\Delta k_i,\nabla k_i} \circ \mathsf{G}_i$; for $m+1 \leq i \leq r$, $\mathsf{E} = \mathsf{G}_i \circ \mathsf{F}_{k,\Delta k,\nabla k}$ the round function satisfies that $\mathsf{E}_i(x) = \mathsf{F}_{k_i,\Delta k_i,\nabla k_i} \circ \mathsf{G}_i(x)$; as illustrated in Figure 3.

Therefore, the probability of a BC $(\alpha_1, \alpha_2, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_r)$ is that

$$\begin{aligned} &\mathrm{Pr}_{BC}[\alpha_1, \ldots, \alpha_{m-1}, \alpha_m, \ldots, \alpha_{r+1}] \\ &= \sum_{u_0^2,\ldots,u_0^r} \sum_{u_1^{m+2},\ldots,u_1^r} \sum_{u_2^2,\ldots,u_2^{m+1}} \prod_{i=1}^{r-1}(-1)^{(u_0^{i+1})^\top k_i} \prod_{i=1}^{m-1}(-1)^{(u_2^{i+1})^\top \nabla k_i} \prod_{i=m}^{r}(-1)^{(u_1^{i+1})^\top \Delta k_i} \\ &\qquad B^{\mathsf{G}_m}_{u_0^{m+1}||u_1^{m+1}||\alpha_{m+1},u_0^m||\alpha_m||u_2^m} \prod_{i=1}^{m-1} B^{\mathsf{G}_i}_{\omega_{i+1},\omega_i} \prod_{i=m+1}^{r} B^{\mathsf{G}_i}_{(\omega_{i+1},\omega_i)}, \end{aligned}$$

where $\omega_i = (u_0^i, \alpha_i, u_2^i)$ for $1 \leq i \leq m$, $\omega_i = (u_0^i, u_1^i, \alpha_i)$ for $m+1 \leq i \leq r$, and with $u_0^1 = u_0^{r+1} = 0, u_1^{r+1} = 0, u_2^0 = 0, x_i = \mathsf{F}_{i-1}(x_{i-1}) = \mathsf{G}_{i-1}(x_{i-1}) \oplus k_i, 2 \leq i \leq r$.

4 Applications to Verify the Differential Characteristic

In this section, we combine the quasidifferential framework and the related-key quasi-DCs to verify the given related-key DCs.

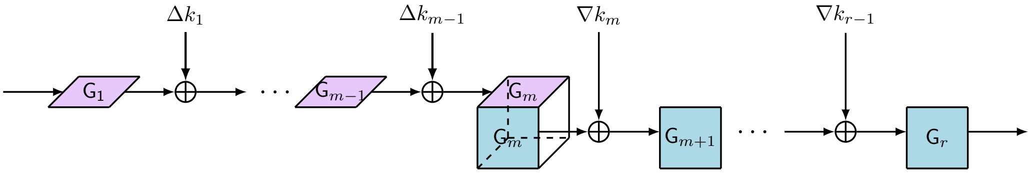


Figure 3: The BC in the related-key setting for a composite key-alternating cipher $\mathsf{E} = \mathsf{E}_r \circ \cdots \circ \mathsf{E}_{m+1} \circ \mathsf{E}_m \circ \cdots \circ \mathsf{E}_1$.

Automatic search model for related-key quasi-DCs of a given related-key DC. Any cipher can be regarded as a composition of small components. For each component including the key-XOR, the transition matrix of the quasidifferential differential is first built. The transition matrix of a component function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a $2^{2m} \times 2^{2n}$ matrix. However, since the input and output differences are known according to the given DC, the related-key quasi-DC in fact follows a $2^m \times 2^n$ submatrix. We utilize the `SMT` solver `Boolector`[3] to search for related-key quasi-DCs that follow these submatrices and set the input mask and output mask of the quasi-DC be zero. Every solution returned by the solver is a valid related-key quasi-DC that corresponds to the given DC.

Derive the key conditions. Consider $\mathsf{E} = \mathsf{E}_r \circ \cdots \circ \mathsf{E}_1$ where $\mathsf{E}_i = \mathsf{F}_{k_i,\Delta k_i} \circ \mathsf{G}_i(x)$. Suppose a related-key DC with the key difference sequence $\Delta k_1, \ldots, \Delta k_r$ of E, denoted by $(\alpha_0, \ldots, \alpha_{r+1})$, has m quasi-DCs. According to Corollary 5, the correlation of the ℓ-th $(1 \le \ell \le m)$ quasi-DC, say $(0, u_1^{(\ell)}, \ldots, u_r^{(\ell)}, 0)$, can be calculated by

$$\mathscr{C}_l = \prod_{i=1}^{r} (-1)^{(u_{i+1}^{(\ell)})^\top k_i} \prod_{i=1}^{r} D^{\mathsf{G}_i}_{u_{i+1}^{(\ell)}||\alpha_{i+1}\oplus\Delta_{k_i}, u_i^{(\ell)}||\alpha_i} = (-1)^{\sum_{i=1}^{r}(u_{i+1}^{(\ell)})^\top k_i} C^{(\ell)},$$

where $u_0^{(\ell)} = u_{r+1}^{(\ell)} = 0$, and $C^{(\ell)} = \prod_{i=1}^{r} D^{\mathsf{G}_i}_{u_{i+1}^{(\ell)}||\alpha_{i+1}\oplus\Delta_{k_i}, u_i^{(\ell)}||\alpha_i}$ is the correlation of non-key-XOR components.

Therefore, we can control $\prod_{i=1}^{r}(-1)^{(u_{i+1}^{(\ell)})^\top k_i}$ by imposing conditions on keys to determine the sign of the correlation of the ℓ-th quasi-DC. Suppose that the rank of all non-all-zero-mask conditions (there must be an all-zero mask quasi-DC, which is just the DC) from the m quasi-DCs is m'. Thus, there are $2^{m'}$ possibilities to assign values to these conditions, which also divide the whole key space into $2^{m'}$ subspaces.

According to [BR22, Theorem 4.2], the quasi-DCs whose correlation has the same absolute value with their corresponding DC are specifically interesting. If the sum of their correlations is zero, then the sum of all quasi-DCs is always zero. We call these quasi-DCs *maximum-correlation* quasi-DCs. In terms of the related-key quasi-DC, this theorem naturally applies. Therefore, we can divide the $2^{m'}$ conditions into two categories. In the first category, the key conditions make the sum of correlations of all related-key maximum-correlation quasi-DCs be zero. Thus, the target related-key DC is also zero. In the second category, the key conditions make the sum of maximum-correlation quasi-DCs non-zero, thus the related-key DC may work in this key subspace. We will try to search for all related-key quasi-DCs and sum their correlations to approximate the probability of the target DC. However, it is actually very difficult to exhaust all related-key quasi-DCs, so we will search for related-key quasi-DCs with large absolute correlations. These related-key quasi-DCs are called the dominant related-key quasi-DCs. The sum of these dominant related-key quasi-DCs' correlation is used to approximate the probability of the DC. Note that this is the same strategy with that in [BR22]. In Section 6.1, we will discuss the plausibility of this approximation in our applications.

[3] `https://boolector.github.io`

We apply these techniques to related-key DCs of AES, CRAFT, and GIFT, respectively, searching for quasi-DCs corresponding to the related-key DCs, deriving the key conditions from the dominant quasi-DCs, and estimating the probability in the different key spaces. For GIFT, the round key constraints can be transformed to the mask key constraints as the linear key schedule.

4.1 Applications to 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).

Verification of a 15-round related-key DC of GIFT-64 (DC-1). In [JZZD20, Table 10], Ji et al. proposed a 15-round related-key DC for GIFT-64 whose probability is 2^{-48}. We search and find 2 maximum-correlation quasi-DCs with correlation values being (positive) 2^{-48}. The first one has the related-key quasi-DC with all zero masks, thus the key values have no influence on its sign. The second one provides a 1-bit key condition as $RK_6^{14} \oplus RK_6^{30}$, interestingly, the round key bits involved in this condition are actually two master key bits, thanks to the simple linear key schedule of GIFT. Finally, we obtain a condition of 2 master key bits, which is $k_2^3 \oplus k_2^{11}$.

On the one hand, when $k_2^3 \oplus k_2^{11} = 1$, the correlations of the two related-key quasi-DCs will sum to zero. According to [BR22, Theorem 4.2], the summation of all related-key quasi-DCs' correlations is zero under this condition.

In the other hand, when $k_2^3 \oplus k_2^{11} = 0$, the correlations of the two related-key quasi-DCs will sum to 2^{-47}. To get a better approximation to the real probability of DC-1, we continue to search for all related-key quasi-DCs with absolute correlations from 2^{-48} to 2^{-63}. The sum of all these correlations is $2^{-46.42}$.

Therefore, for half of the keys, this 15-round related-key DC is invalid. For the other half of the keys, the probability is about $2^{-46.42}$.

Verification of a 18-round related-key DC of GIFT-64 (DC-2). In [SWW21, Figure 8], Sun et al. presented a first 26-round differential attack on GIFT-64 in the related-key scenario, utilizing an 18-round related-key DC with probability 2^{-58}. We search for quasi-DCs with absolute correlation 2^{-58} and find 128 maximum-correlation quasi-DCs with correlation 2^{-58}, and 128 maximum-correlation quasi-DCs with correlation -2^{-58}. Among the 256 maximum-correlation quasi-DCs, there is one with all zero masks. The remaining 255 provide 255 key conditions, but the rank of them is only 8. Thus, we have 256 possibilities for the key spaces. These key bits is as follows,

$$\begin{aligned} &k_0^4 + k_0^6 + k_2^8 + k_2^{15} + k_5^7 + k_5^9 + k_7^3 + k_7^{11} = z_0 && k_0^5 + k_0^6 + k_2^8 + k_5^7 + k_5^9 + k_7^{11} = z_1 \\ &k_2^0 + k_2^8 = z_2 && k_2^7 + k_2^{15} = z_3 \\ &k_3^3 = z_4 && k_3^{11} = z_5 \\ &k_6^1 = z_6 && k_6^6 + k_6^{14} = z_7. \end{aligned}$$

When $(z_0, \ldots, z_7) = (0, 1, 0, 1, 1, 1, 1, 0)$, the sum of the maximum-correlation related-key quasi-DCs' (including the zero-mask quasi-DC) correlation is 2^{-50}. We continue to search for all quasi-DCs with absolute correlations from 2^{-49} to 2^{-64}. The sum of correlations is $2^{-49.42}$.

For 8 subspaces, i.e.,

$$(z_0,\dots,z_7) \in \left\{\begin{matrix}(1,0,0,0,1,1,1,0),(0,1,0,0,1,1,1,0),(0,0,1,0,1,1,1,0),(1,1,1,0,1,1,1,0)\\(0,0,0,1,1,1,1,0),(1,1,0,1,1,1,1,0),(1,0,1,1,1,1,1,0),(0,1,1,1,1,1,1,0)\end{matrix}\right\},$$

the sum of the maximum-correlation related-key quasi-DCs' (including the zero-mask quasi-DC) correlation is 2^{-53}. Thus, we continue to search for all quasi-DCs with absolute correlations from 2^{-49} to 2^{-64}. The sum of correlations is $2^{-52.42}$.

For the remaining 247 subspaces, the sum of the maximum-correlation related-key quasi-DCs' (including the zero-mask quasi-DC) correlation is zero. Therefore, the probability of the related-key DC is always zero.

Therefore, for $\frac{1}{256}$ keys, the probability of this 18-round related-key DC is about $2^{-49.52}$. For $\frac{1}{256} \times 8 = \frac{1}{32}$ keys, the probability is about $2^{-52.42}$. For the remaining keys, the probability is zero.

4.2 Applications to AES-128

Specification of AES. The Advanced Encryption Standard (AES) [DR20] is a symmetric key encryption algorithm widely used for information security. Established by the National Institute of Standards and Technology (NIST) in 2001, AES operates on 128-bit block sizes and supports key lengths of 128, 192, and 256 bits. The encryption algorithm includes three versions: rounds 10 for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys, respectively, with each round. The round function consists of SubBytes (8-bit S-box), ShiftRows, MixColumns, and AddRoundKey. Note that the final round omits the MixColumns operation.

Verification of a 6-round related-key DC of AES-128 (DC-3). In [SGL+17, Table 1], Sun et al. proposed the (currently) optimal 6-round related-key DC of AES-128 with probability 2^{-131} that the probabilities of state DC (denoted as p_s) and key DC (denoted as p_k) are 2^{-92} and 2^{-39}, respectively.

To verify this related-key DC, we first check the DC of the states assuming that the round keys are all independent. We search for quasi-DCs whose absolute correlation is from 2^{-92} to 2^{-142}, and only one quasi-DC with all-zero masks is found, whose correlation is 2^{-92}. That means the round keys will not influence the validity of the state DC.

Since the key schedule of AES-128 is also non-linear, we still need to ensure that the difference propagation in the key schedule is also valid. Thus, we search for quasi-DCs whose absolute correlations from 2^{-39} to 2^{-89} corresponding to the key schedule DC, also, only one quasi-DC with all-zero masks is found whose correlation is 2^{-39}.

Therefore, we fully verify that this 6-round related-key DC of AES-128 is reliable, and it is independent of keys.

Verification of a 5-round related-key DC of AES-128 (DC-4). The best 5-round related-key DC of AES-128 is proposed in [FJP13, Figure 16]. The probability is 2^{-105} ($p_s = 2^{-66}$ and $p_k = 2^{-39}$).

Similar to the 6-round case, only one quasi-DC with all-zero masks is found corresponding to the state DC when searching for the absolute correlation from 2^{-66} to 2^{-116} and only one quasi-DC with all-zero masks is found of the key DC when searching for the absolute correlation from 2^{-39} to 2^{-89}.

Therefore, we fully verify this 5-round related-key DC of AES-128, and it is independent of keys.

Verification of the first 4-round DC of AES-128 (DC-5). For the 4-round best related-key DC of AES-128 [FJP13, Figure 14] with probability 2^{-81} ($p_s = 2^{-48}$ and

$p_k = 2^{-33}$), we find that only one quasi-DC with all-zero masks when searching for the absolute correlation from 2^{-48} to 2^{-98} corresponding to the state DC and only one quasi-DC with all-zero masks is found corresponding to the key DC when searching for the absolute correlation from 2^{-33} to 2^{-83}, which means this 4-round related-key DC of AES-128 is independent of keys and reliable.

Verification of the second 4-round DC of AES-128 (DC-6). For another 4-round best related-key DC of AES-128 [FJP13, Figure 15] with probability 2^{-81} ($p_s = 2^{-48}$ and $p_k = 2^{-33}$), only one quasi-DC with all-zero masks is found corresponding to the state DC when searching for the absolute correlation from 2^{-48} to 2^{-98}. When searching for the absolute correlation from 2^{-33} to 2^{-83} of quasi-DC corresponding to the key DC, we find only one quasi-DC. Then this 4-round related-key DC of AES-128 is also reliable and independent of the keys.

4.3 Applications to CRAFT

Specification of CRAFT. CRAFT [BLMR19] is a lightweight symmetric encryption algorithm designed for constrained environments, focusing on efficiency and security. It operates on 64-bit block sizes, supports key sizes of 128 bits, and tweak size of 80 bits. The algorithm employs an SPN structure and the internal state can be viewed as a 4 × 4 square. During encryption, the plaintext through a combination of the round function and the subkey is derived from the main key. The round function includes five operations: MixColumn, AddConstants, AddTweakey, PermuteNibbles, and SubBox (4-bit S-box).

Verification of a 30-round DC of CRAFT (DC-7). In [SWW22, Figure 3], Sun et al. presented a practical key-recovery attack on the full-round CRAFT in the related-key setting that only uses one DC with probability 2^{-30}. We search for all quasi-DCs with absolute correlation being 2^{-30} to 2^{-80} in the related-key setting corresponding to this DC. There is only one quasi-DC with all-zero masks, making this 30-round DC and the practical full-round attack reliable.

5 Applications to Verify the Boomerang Distinguishers

Automatic Search Model. According to Definitions 8 and 9, for $\mathsf{E} = \mathsf{E}_r \circ \cdots \circ \mathsf{E}_{m+1} \circ \mathsf{E}_m \circ \cdots \circ \mathsf{E}_1$, a BC is a sequence of differences like

$$(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_{r+1}),$$

while a quasi-BC is a sequence of triples like

$$((u_1, v_1, w_1), \ldots, (u_{m-1}, v_{m-1}, w_{m-1}), (u_m, v_m, w_m), \ldots, (u_{r+1}, v_{r+1}, w_{r+1}))$$

with $u_1 = w_1 = u_{r+1} = v_{r+1} = 0$. Replacing the corresponding differences of the quasi-BC with the differences from the given BC, we can search for the sequence of the remaining two masks in each triple, which is like

$$((0, \alpha_1, 0), \ldots, (u_{m-1}, \alpha_{m-1}, w_{m-1}), (u_m, v_m, \alpha_m), \ldots, (0, 0, \alpha_{r+1}))$$

According to Theorem 2, the sum of all correlations of such quasi-BCs is exactly the probability of the above BC. The SMT solver Boolector is also used for searching for the quasi-BCs.

Derive key conditions. Suppose the key difference sequence of a related-key BC is $(\Delta k_1, \ldots, \Delta k_{m-1}, \nabla k_m, \ldots, \nabla k_{r-1})$, we can get a bit of key conditions according to

Equations (11) and (12) for each quasi-BC, which is similar to the related-key DC case. Suppose we have m quasi-BCs, and the ℓ-th quasi-BC suggests a key condition as

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

Suppose the rank of these key conditions (excluding the all-zero mask quasi-BC) is m', then the key space can be divided into $2^{m'}$ subspaces. For each subspace, we can search for all quasi-BCs to compute the probability of the target BC.

We apply these techniques to SKINNY-64 and GIFT, respectively, searching for the quasi-BCs corresponding to the tested related-key BCs. We derive the key constraints and estimate the probability in different key subspaces. Note that our techniques naturally apply to single-key case, too.

5.1 Applications to SKINNY-64

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, 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, $m \in \{1, 2, 3\}$.

Verification of a 2-round BC (including clustering effect) of SKINNY-64-128 (BC-1). In [LGS17, Table 12], Liu et al. proposed a 17-round related-tweakey 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}, thus the probability of the 17-round distinguisher is 2^{-64} following Equation (2). Cid et al. [CHP+18] proposed the BCT to analyze the dependent Sboxes. They first applied the BCT to analyze the above results under the assumption that the DDT and BCT in consecutive two rounds can be evaluated independently, then the probability is 2^{-4} including the clustering effect. They also made careful analysis including dependency of consecutive Sbox applications that list the possible paired values before and after the Sbox by the DDT and BCT, with the randomness based on the XOR subtweakey values and the MixColumns, then they reported that the probability should be 2^{-2}.

We apply our quasi-BC model to the middle two rounds of the boomerang distinguishers of SKINNY-64-128, automatically search for the quasi-BCs with absolute correlation from 2^0 to 2^{-100}, and consider the clustering effect of BCs, i.e., we consider all BCs with the given input and output differences. We find 4096 quasi-BCs corresponding to all 64 BCs, each of which has 64 quasi-BCs with correlation 2^{-14}. By deriving the key conditions from all quasi-BCs, we get 3-bit key conditions. The fixed related-TK2 conditions are as follows by satisfying the deterministic key difference.

$$\Delta TK1[4] + \Delta TK2[4] = 0, \Delta TK1[6] + \Delta TK2[6] = 0, \Delta TK1[7] + \Delta TK2[7] = 0. \quad (13)$$

By checking the related-tweakey sequence in [LGS17, Table 12], we find

$$\Delta TK1[4] = \Delta TK2[4] = \Delta TK1[6] = \Delta TK2[6] = \Delta TK1[7] = \Delta TK1[7] = \Delta TK2[7] = 0$$

Thus, Condition (13) is already satisfied. Thus, this related-key BC is reliable. The sum of all correlations is 2^{-2}. We also implement the experiment to verify the middle two rounds including the clustering effect and the probability is about 2^{-2}. The results are listed in Table 2.

Table 2: Comparison of the middle two round 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 probability by quasi-BCs	2^{-2}	$2^{-5.29}$	2^{-15}
Our experimental probability	2^{-2}	$2^{-5.2}$	2^{-13}

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

Verification of a 2-round BC (including clustering effect) of SKINNY-64-192 (BC-2). Liu et al. proposed a 22-round related-tweakey 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], then the probability of the 22-round BC is 2^{-80} following Equation (2). In [LGS17], Liu et al. proposed that the probability of the middle two rounds including the clustering effect is $2^{-16.30}$, while their experimental verification probability is $2^{-7.53}$.

Similarly to the analysis of the middle two rounds of SKINNY-64-128, Cid et al. [CHP+18] gave the probability of the middle two rounds of SKINNY-64-192 including the clustering effect is $2^{-5.31}$ by combining BCT and dependency of consecutive Sbox.

We automatically search for the quasi-BCs considering the clustering effect and find 6144 quasi-BCs corresponding to all 32 BCs, including 512 quasi-BCs with correlation 2^{-16}, 768 quasi-BCs with correlation 2^{-17}, 1792 quasi-BCs with correlation 2^{-18}, 2304 quasi-BCs with correlation 2^{-19} and 768 quasi-BCs with correlation 2^{-20}. By deriving the key conditions from all quasi-BCs, we get the 3-bit conditions, the fixed related-TK3 conditions are as follows by satisfying the deterministic key difference.

$$\begin{cases} \Delta TK1[4] + \Delta TK2[4] + \Delta TK3[4] = 0, \\ \Delta TK1[6] + \Delta TK2[6] + \Delta TK3[6] = 0, \\ \Delta TK1[7] + \Delta TK2[7] + \Delta TK3[7] = 0. \end{cases} \tag{14}$$

by checking [LGS17, Table 14], we found that Condition (14) are already valid. The probability of the 2-round boomerang distinguisher including clustering effect is $2^{-5.29}$ by summing up all correlations of all quasi-BCs. In addition, we implement the experiment and obtain the experimental probability is about $2^{-5.2}$. The results are listed in Table 2.

Verification of a 17-round BC of SKINNY-64-128 (BC-3). Furthermore, we apply the approach to search for the quasi-BCs of the complete 17-round BC of SKINNY-64-128. We find the maximum absolute correlation of quasi-BCs is 2^{-62}. The number of quasi-BCs is too numerous to enumerate, we find 4542 maximum-correlation quasi-BCs so far.

To verify the validity of this BC, we divide the 17-round BC into three parts. The first part is the first 7 rounds of the upper DC, whose probability is 2^{-12} in [LGS17, Table 12]. The second part is the middle two rounds (including the clustering effect), i.e., the 8-th round of the upper DC and the 9-th round of the lower DC. In Table 2, the probability of the second part is $2^{-8.42}$ estimated by Liu et al. [LGS17], 2^{-2} by Cid et al. [CHP+18], and 2^{-2} by our. The third part is the last 8 rounds of the lower DC, whose probability is 2^{-36}. Then we apply our quasi-BC's automatic model to these three parts, respectively. When deriving the key conditions, we combine the quasi-BCs of three parts as a whole. This search method assumes that the three parts are independent. The 17-round BC is depicted in Figure 4.

For the first and the third part, we automatically search for the quasi-BCs with absolute correlation from 2^0 to 2^{-100}. We find only one quasi-BC with correlation 2^{-12} corresponding to the first part with all-zero masks and 4 quasi-BCs with correlation 2^{-32} corresponding to the third part. For the second part, we utilize the above results of the middle two rounds including the clustering effect, i.e., 4096 quasi-BCs with correlation 2^{-14} corresponding to all 64 BCs. By deriving the key conditions from all quasi-BCs, we get 5-bit key conditions. The fixed related-TK2 conditions are as follows by satisfying the deterministic key difference. A 1-bit condition of the key value is derived from the quasi-BCs of the third part.

$$\begin{cases} TK1[42] + TK2[40] + TK2[42] + TK2[43] = 0, \\ \Delta TK1[56] + \Delta TK2[56] + \Delta TK2[58] + \Delta TK2[59] = 0, \\ \Delta TK1[58] + \Delta TK2[57] + \Delta TK2[58] = 0, \\ \Delta TK1[59] + \Delta TK2[58] + \Delta TK2[59] = 0, \\ \nabla TK1[42] + \nabla TK2[40] + \nabla TK2[42] + \nabla TK2[43] = 0. \end{cases} \tag{15}$$

By checking [LGS17, Table 12], the last four related-Tk2 conditions in Condition (15) are already valid. Analyzing the first conditions of key value in Condition (23), the probability of the 17-round BC is 2^{-44} for $\frac{1}{2}$ keys (i.e., $TK1[42]+TK2[40]+TK2[42]+TK2[43] = 0$), and invalid for the other $\frac{1}{2}$ keys. The result shows that the probability of boomerang distinguishers is key-dependent, i.e., it may be impossible to cluster the upper DCs and lower DCs independently.

Experimental verification. We further verify the middle four rounds of the 17-round BC of SKINNY-64-128 with probability 2^{-32}. We search for the quasi-BCs with the absolute correlation from 2^0 and find that the maximum absolute correlation is 2^{-30}, which includes 4096 quasi-BCs with correlation 2^{-30}. By deriving the key conditions, we get 5-bit key conditions, the fixed related-Tk2 conditions are as follows by satisfying the deterministic key difference.

$$\begin{cases} \Delta TK1[60] + \Delta TK2[62] + \Delta TK2[63] = 0, \\ \Delta TK1[62] + \Delta TK2[61] = 0, \\ \nabla TK1[0] + \nabla TK1[1] + \nabla TK2[0] + \nabla TK2[2] + \nabla TK2[3] = 0, \\ \nabla TK1[2] + \nabla TK2[1] = 0, \\ \nabla TK1[3] + \nabla TK2[2] = 0. \end{cases} \tag{16}$$

These conditions are already valid by checking that the probability of the 4-round BC is 2^{-18} by summing up all correlations of 4096 quasi-BCs.

We also implement the experiment for these middle four rounds, the probability of the experiment is about 2^{-17}.

Verification of a 22-round BC of SKINNY-64-192 (BC-4). For the 22-round BC of SKINNY-64-192 with probability 2^{-80}, we automatically search for the quasi-BCs with absolute correlation from 2^0 and find the maximum absolute correlation is 2^{-69}. By searching for the quasi-BCs with absolute correlation from 2^{-69} to 2^{-74}, we find 128 quasi-BCs with correlation 2^{-69}, 256 quasi-BCs with correlation 2^{-70}, 384 quasi-BCs with correlation 2^{-72}, 1536 quasi-BCs with correlation 2^{-73}, and 768 quasi-BCs with correlation -2^{-73}. By deriving the key conditions from all quasi-BCs, we get 8-bit key conditions, the fixed related-TK3 conditions are as follows by satisfying the deterministic key difference.

$$\begin{cases}\Delta TK1[4]+\Delta TK2[5]+\Delta TK2[7]+\Delta TK3[4]+\Delta TK3[5]+\Delta TK3[7]=1,\\ \Delta TK1[5]+\Delta TK2[4]+\Delta TK2[6]+\Delta TK2[7]+\Delta TK3[4]+\Delta TK3[5]+\Delta TK3[6]+\Delta TK3[7]=0,\\ \Delta TK1[6]+\Delta TK2[4]+\Delta TK2[5]+\Delta TK3[4]+\Delta TK3[5]+\Delta TK3[6]=0,\\ \Delta TK1[7]+\Delta TK2[5]+\Delta TK2[6]+\Delta TK3[5]+\Delta TK3[6]+\Delta TK3[7]=1,\\ \Delta TK1[16]+\Delta TK2[17]+\Delta TK2[19]+\Delta TK3[16]+\Delta TK3[17]+\Delta TK3[19]=0,\\ \Delta TK1[18]+\Delta TK2[16]+\Delta TK2[17]+\Delta TK3[16]+\Delta TK3[17]+\Delta TK3[18]=0,\\ \nabla TK1[40]+\nabla TK1[43]+\nabla TK2[41]+\nabla TK2[42]+\nabla TK3[41]+\nabla TK3[43]=1,\\ \nabla TK1[42]+\nabla TK2[40]+\nabla TK2[42]+\nabla TK2[43]+\nabla TK3[41]+\nabla TK3[42]+\nabla TK3[43]=1.\end{cases} \tag{17}$$

By checking [LGS17, Table 14], the Condition (17) are already valid. Thus, the probability of the 22-round BC is 2^{-62} by summing up all correlations of all quasi-BCs.

5.2 Applications to GIFT-64

Verification of 2-round BC of GIFT-64 (BC-5). Chen et al. presented a 23-round attack on GIFT-64 in [CWZ19] utilizing a 19-round related-key boomerang distinguisher [CWZ19, Table 5]. The probability of the middle part (round 10 to 11) is 1 according to the BCT.

In [JZZD20], Ji et al. pointed out that the probability of the middle two rounds is only 2^{-18} calculated by BDT proposed in [WP19], which means the 23-round attack proposed in [CWZ19] is invalid.

From the perspective of 3-differential, Wang et al. [WSW+24] searched for quasi-3-DCs corresponding to partial (optimal) 3-DCs 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 the middle two rounds when comparing the result 2^{-18} proposed in [JZZD20].

We apply our quasi-BC model to the middle two rounds of the BC of GIFT-64, automatically search for the quasi-BCs with the absolute correlation from 2^0 to 2^{-100}, and find 512 quasi-BCs with correlation 2^{-25} and 1024 quasi-BCs with correlation 2^{-26}. The fixed related-key conditions are as follows by satisfying the deterministic key difference. In addition, we get a 1-bit condition of the key value.

$$\begin{aligned}&k_0^9=0,\\ &\Delta k_0^1=0,\Delta k_0^8+\Delta k_1^{12}=0,\Delta k_0^9=0,\Delta k_0^{11}=0,\Delta k_1^5=0,\Delta k_1^{13}=0,\Delta k_1^{15}=0\end{aligned} \tag{18}$$

By checking [CWZ19, Table 6], the last 7 related-key conditions in Condition (18) are already valid. By analyzing the first condition k_0^9 of the key value, we obtain the probability of the 2-round BC is 2^{-16} for $\frac{1}{2}$ keys (i.e., $k_0^9=0$), and 2^{-16} for the other $\frac{1}{2}$ keys.

6 Discussion and Comparison

6.1 Comparison with Peyrin-Tan Method and AutoDiVer

Peyrin and Tan [PT22] focused on verifying DCs of SKINNY and GIFT by structural analysis. The advantage of their work is that they can identify the impossibility or compute the probability distribution in different key spaces for DCs of SKINNY and GIFT by detecting constraints on the internal value. However, for other ciphers, their algorithm does not seem general. In addition, for SKINNY-128 with an 8-bit Sbox, the probability distribution in different key spaces in their work is infeasible for a theoretical computation, so they had to estimate it by experiments. Thus, we expect their method is not easy to generalize for verifying more kinds of ciphers in related-key settings and for verifying boomerang distinguishers.

The advantage of the tool AutoDiVer presented by Nageler et al. [NGJE25] is adaptive and practical for more kinds of block ciphers by modeling the propagation of input values, output values, and (optional) key schedules. Their work also can deduce the key conditions and estimate the set of valid keys. While for some ciphers such as SKINNY, estimating the probability distribution in different key spaces seems not easy by their tool. The author also pointed out that the limitation of AutoDiVer is the effectiveness, which will be influenced by the key schedule. For related-key DCs and boomerang distinguishers, AutoDiVer should set more variables, which will further slow down their speed.

Advantage and limitation of our framework. The quasidifferential/geometric approach framework, including our extension for related-key DC and boomerang, is general and applicable to various block ciphers. It also brings a rigorous theory on probability computation, i.e., in theory, we can compute the exact probability of a DC or BC.

However, the quasi-DCs/BCs with lower absolute correlation are too numerous to enumerate, the key dependencies having to be analyzed by the so-called dominant quasi-DCs. In [NGJE25], Nageler et al. pointed out that obtaining key dependencies for quasi-DCs with lower absolute correlation is not always easy, although the correlations of these quasi-DCs may affect the probability of DC. We do not know whether the quasi-DCs/BCs without being considered will finally affect our analysis.

To partially mitigate the concern, we draw figures about the probability computed from enumerating quasi-DCs in Figure 5. In cases of DC-1, DC-2, DC-8, DC-9, the probabilities of the DCs increase or keep stable as we enumerate more quasi-DCs with smaller absolute correlations, which shows the dominant quasi-DC assumptions work well. However, there are also two exceptions for DC-10, as the enumeration, the DC probability first increases but reduces again. In DC-11, the probability first stays stable but then goes down. However, it seems the probabilities will stay stable in new values. These figures remind us the dominant quasi-DCs assumptions might fail sometimes. But it also shows in more cases, it works well.

6.2 A Detailed Comparison on Related-Key DCs for SKINNY

As mentioned in Section 1, SKINNY is the only cipher whose related-key DCs have been verified by Peyrin and Tan [PT22] and the AutoDiVer. For a better comparison, we also apply our framework to SKINNY, to obtain a direct contrast with the two tools. Through these comparisons, one can find that our framework is more consistent in different cases.

Verification of a 10-round related-key DC of SKINNY-64-64 (DC-8). The best 10-round related-TK1 DC of SKINNY-64-64 was presented in [DDH+21, Table 7], the probability of which is 2^{-46}. In [PT22], Peyrin and Tan found that this 10-round DC is impossible by structural analysis.

To check it with our method, we search for quasi-DCs with absolute correlation 2^{-46}, i.e., the maximum-correlation quasi-DCs, and find 16 quasi-DCs with correlation 2^{-46}, 16 quasi-DCs with -2^{-46}. Then we derive the values of the TK1 by these 32 maximum-correlation quasi-DCs and get 2-bit keys: TK1[13] and TK1[15]. We further compute the probability distribution by summing the correlations of these 32 maximum-correlation quasi-DCs in different key spaces (i.e., the different values of TK1[13] and TK1[15]). We find that no matter what TK1[13] and TK1[15] are, the sum of these 32 quasi-DCs is zero. Thus, it is invalid.

Verification of a 13-round DC of SKINNY-64-128 (DC-9). For the best 13-round TK2 DC of SKINNY-64-128 ([DDH+21], Table 8) with probability 2^{-55}, Peyrin and Tan

[PT22] found that the probability is 2^{-51} for 2^{-4} of keys, and zero for other keys.

We search for quasi-DCs of the 13-round DC and find 8 maximum-correlation quasi-DCs with correlation 2^{-55}. By deriving the key (TK1 and TK2) conditions, We find that for the following 2^{-4} of keys, the probability is 2^{-51} and zero for other keys, which is consistent with the result of Peyrin and Tan.

$$\begin{cases} TK1[25] + TK2[25] + TK2[26] + TK[27] = 0, \\ TK1[26] + TK1[27] + TK2[24] + TK2[25] + TK2[26] + TK2[27] = 0, \\ TK1[36] + TK2[38] + TK[39] = 1, \\ TK1[38] + TK2[37] = 0. \end{cases} \tag{19}$$

We further search for the quasi-DCs with the absolute correlation from 2^{-56} to 2^{-75}, and the sum of the correlations is 2^{-51}. Therefore, for 2^{-4} of keys, the probability of this 13-round DC is about 2^{-51}, and zero for the remaining keys.

Verification of a 15-round DC of SKINNY-64-192 (DC-10). For the best 15-round TK3 DC of SKINNY-64-192 ([DDH+21], Table 9) with probability 2^{-54}, Peyrin and Tan [PT22] found that the probability is about 2^{-48} to 2^{-47} for $2^{-6.19}$ of keys, Nageler et al. [NGJE25] estimated that the number of linear constraints is 5 and the key size is about $2^{-6.48}$ to $2^{-6.11}$ but not predict the probability in the different key spaces.

We search for and find 16 maximum-correlation quasi-DCs with correlation 2^{-54}, 16 maximum-correlation quasi-DCs with correlation -2^{-54}. By deriving the key (TK1, TK2, and TK3) conditions, We get 5-bit key conditions and find that for the following 2^{-5} of keys, the probability is 2^{-49} and zero for other keys.

$$\begin{cases} TK1[36] + TK1[37] + TK1[38] + TK2[36] + TK2[39] + TK3[37] + TK3[39] = 1, \\ TK1[39] + TK2[36] + TK3[36] + TK3[37] + TK3[38] + TK3[39] = 0, \\ TK1[40] + TK2[40] + TK2[43] + TK3[40] + TK3[42] + TK3[43] = 1, \\ TK1[41] + TK1[43] + TK2[42] + TK2[43] + TK3[40] + TK3[41] + TK3[42] + TK3[43] = 0, \\ TK1[42] + TK2[40] + TK2[41] + TK2[42] + TK2[43] + TK3[41] + TK3[42] = 0 \end{cases} \tag{20}$$

We continue to search for the quasi-DCs with the absolute correlation from 2^{-54} to 2^{-70}. The sum of these correlations is 2^{-48}. Therefore the probability is about 2^{-48} for 2^{-5} of keys and zero for others.

The key size we obtained is smaller than Peyrin and Tan's [PT22], while the estimated probability in the different key spaces is consistent with them. This result implies that although maximum-correlation quasi-DCs may leave out some key bits, also make a major contribution to the probability.

Verification of a 17-round DC of SKINNY-128-384 (DC-11). For the best 17-round related-TK3 DC of SKINNY-128-384 ([DDH+21], Table 12) with probability 2^{-110}, Nageler et al. [NGJE25] estimated that the number of linear constraints is 6 and the key size is about $2^{-7.98}$ to $2^{-7.39}$, but not predict the probability in the different key spaces.

We search for and find 128 maximum-correlation quasi-DCs with correlation 2^{-110}. We get 6-bit key (TK1, TK2, and TK3) conditions and find that for the following 2^{-6} of keys, the probability is 2^{-103} and zero for other keys.

$$\begin{cases} TK1[16] + TK2[16] + TK3[16] = 0, \\ TK1[27] + TK2[29] + TK2[31] + TK3[31] = 0, \\ TK1[35] + TK2[37] + TK2[39] + TK3[39] = 0, \\ TK1[89] + TK2[92] + TK2[94] + TK3[92] = 0, \\ TK1[123] + TK2[120] + TK3[126] = 0, \\ TK1[127] + TK2[126] + TK3[120] + TK3[126] = 1 \end{cases} \tag{21}$$

By further searching for the quasi-DCs with absolute correlation from 2^{-111} to 2^{-117}, we get the probability is about $2^{-104.4}$ for 2^{-6} of keys and zero for other keys. The key size that we find is smaller than Nageler et al., which means those quasi-DCs with lower correlation may introduce 1-bit or more key information.

References

[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, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I*, volume 13090 of *Lecture Notes in Computer Science*, pages 36–66. Springer, 2021.

[Bey23] Tim Beyne. A geometric approach to symmetric-key cryptanalysis. 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 Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BLMR19] Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks. *IACR Trans. Symmetric Cryptol.*, 2019(1):5–45, 2019.

[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 Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, 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 Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, 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, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, 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.

[BV24] Tim Beyne and Michiel Verbauwhede. Ultrametric integral cryptanalysis. *IACR Cryptol. ePrint Arch.*, page 722, 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, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, 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.

[DDH⁺21] Stéphanie Delaune, Patrick Derbez, Paul Huynh, Marine Minier, Victor Mollimard, and Charles Prud'homme. Efficient methods to search for best differential characteristics on SKINNY. In Kazue Sako and Nils Ole Tippenhauer, editors, *Applied Cryptography and Network Security - 19th International Conference, ACNS 2021, Kamakura, Japan, June 21-24, 2021, Proceedings, Part II*, volume 12727 of *Lecture Notes in Computer Science*, pages 184–207. Springer, 2021.

[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, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 393–410. Springer, 2010.

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

[FJP13] Pierre-Alain Fouque, Jérémy Jean, and Thomas Peyrin. Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 183–203. Springer, 2013.

[HZC⁺25] Kai Hu, Chi Zhang, Chengcheng Chang, Jiashu Zhang, Meiqin Wang, and Thomas Peyrin. Periodic Table of Cryptanalysis-Geomertic Approach with Different Bases. *to appear in ePrint*, 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, *Selected Areas in Cryptography - SAC 2020 - 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers*, 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, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, 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, *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, 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, *Information Security and Privacy - 29th Australasian Conference, ACISP 2024, Sydney, NSW, Australia, July 15-17, 2024, Proceedings, Part I*, 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.

[SGL$^+$17] Siwei Sun, David Gérault, Pascal Lafourcade, Qianqian Yang, Yosuke Todo, Kexin Qiao, and Lei Hu. Analysis of aes, skinny, and others with constraint programming. *IACR Trans. Symmetric Cryptol.*, 2017(1):281–306, 2017.

[SWW21] Ling Sun, Wei Wang, and Meiqin Wang. Accelerating the search of differential and linear characteristics with the SAT method. *IACR Trans. Symmetric Cryptol.*, 2021(1):269–315, 2021.

[SWW22] Ling Sun, Wei Wang, and Meiqin Wang. Key-recovery attacks on CRAFT and WARP. In Benjamin Smith and Huapeng Wu, editors, *Selected Areas in Cryptography - 29th International Conference, SAC 2022, Windsor, ON, Canada, August 24-26, 2022, Revised Selected Papers*, volume 13742 of *Lecture Notes in Computer Science*, pages 77–95. Springer, 2022.

[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.

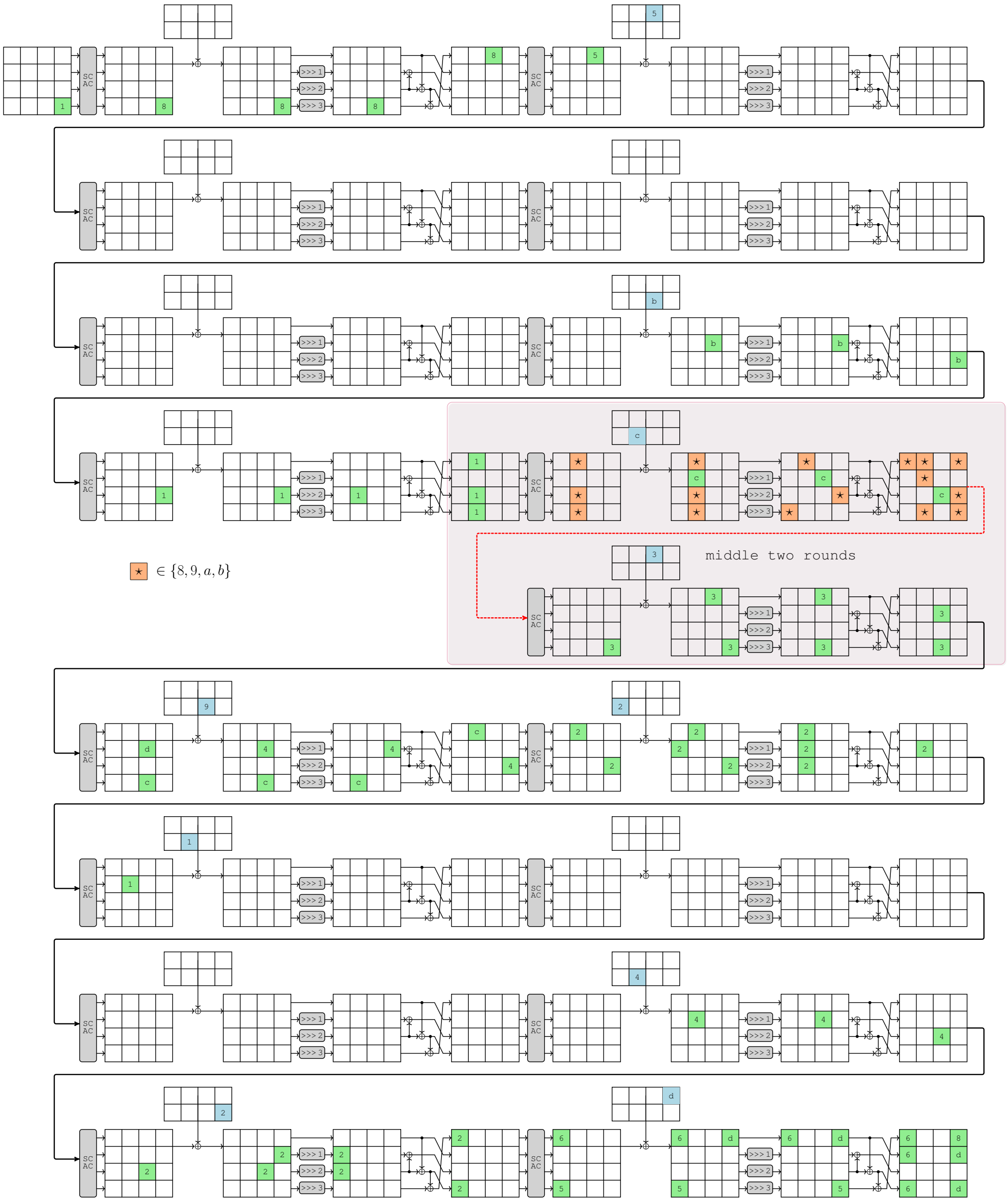
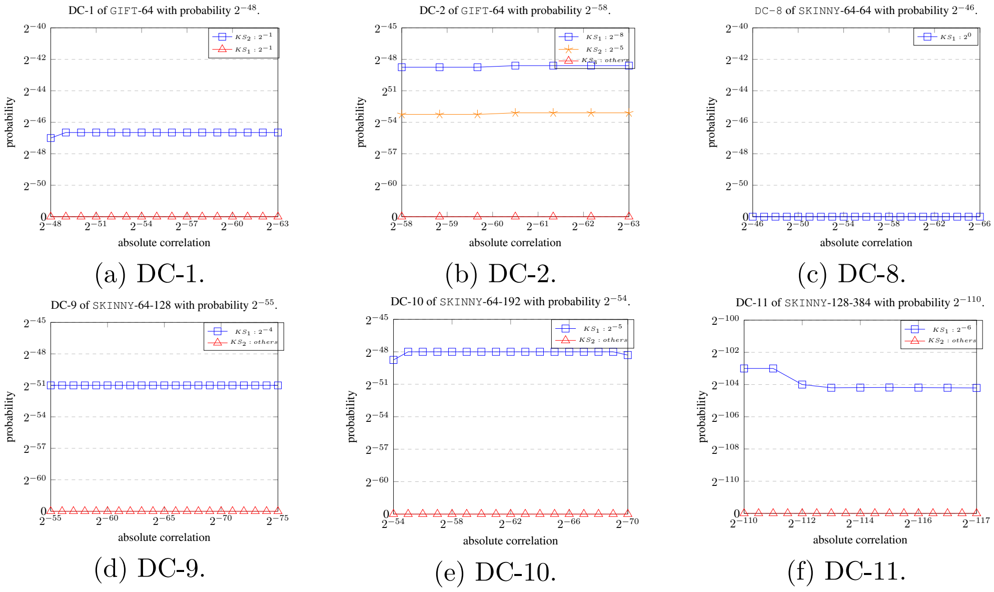


Figure 4: The 17-round BC of SKINNY-64-128.



(a) DC-1.

(b) DC-2.

(c) DC-8.

(d) DC-9.

(e) DC-10.

(f) DC-11.

Figure 5: The relationship between the absolute correlation and probability of DCs.