

An Exact Four-Wise Framework for Boomerang Cryptanalysis

Chengcheng Chang¹, Kai Hu¹, Shuo Peng¹, and Haoyang Wang²

¹ Shandong University, Qingdao, China

kai.hu@sdu.edu.cn, chengcheng.chang@mail.sdu.edu.cn,
pengshuo@mail.sdu.edu.cn

² Shanghai Jiaotong University, Shanghai, China
haoyang.wang@sjtu.edu.cn

Abstract. Boomerang cryptanalysis is inherently a four-point phenomenon, yet its recent geometric formulation relies on a 3-wise representation imposed by a quartet-sum-zero assumption. This simplification makes the transition matrices tractable, but it also removes boomerangs with unequal paired differences and prevents the framework from modeling impossible boomerang distinguishers.

We propose an exact 4-wise geometric framework for boomerang cryptanalysis that is a *strict generalization* of the 3-wise framework: it recovers the 3-wise framework as the equal-difference $a = a'$, $b = b'$ specialization, and at the same computational cost additionally covers the unequal-difference boomerangs and impossible boomerang distinguishers that the 3-wise representation cannot reach. By choosing bases adapted to the two value coordinates and two difference coordinates of a boomerang quartet, our framework removes the 3-wise assumption and gives a unified transition-matrix description for both impossible boomerang distinguishers and fixed-key boomerang probabilities.

The framework has two concrete applications. First, it yields a positive (satisfiability) model for searching for impossible boomerang distinguishers from the difference coordinates in the 4-wise representation. Using this model, we find new impossible boomerang distinguishers for PRESENT, ASCON, SKINNY, and GIFT. Second, it computes fixed-key boomerang probabilities as sums of *quasi-boomerang quartet characteristic* correlations. For the 13- and 17-round boomerang distinguishers of SKINNY-64-128 and SKINNY-64-192, respectively, the resulting probabilities match the experimental results and explain the gap left by the 3-wise framework through contributions from unequal-difference boomerangs.

Keywords: Boomerang · Impossible Boomerang · Geometric Approach · Mix-Basis · Fixed-Key Cryptanalysis

1 Introduction

Differential cryptanalysis [11] is one of the most fundamental techniques in modern symmetric-key cryptanalysis. It seeks high-probability differential characteristics (DCs) whose probability is classically estimated as the product of

one-round differential probabilities. Building on it, Wagner [42] introduced the boomerang attack, which decomposes the target cipher as $F = F_1 \circ F_0$ and combines two short high-probability differentials of F_0 and F_1 into a longer distinguisher; it has since become a cornerstone of block cipher cryptanalysis [9,10].

A complementary line of work studies the *impossible* variants of these attacks, where the adversary exploits zero-probability events to discard wrong key candidates. Lu [37,38] adapted the impossible-differential idea to the boomerang setting and introduced the *impossible boomerang attack* (IBA). Its core ingredient is an *impossible boomerang distinguisher* (IBD): a boomerang transition $(a, a') \rightarrow (b, b')$ that no plaintext quartet can satisfy, obtained by a miss-in-the-middle contradiction between two upper and two lower probability-one differentials. After a decade of slow progress, the IBA has seen a sharp resurgence in the last two years [46,14,30,15,18,31], and it is now an active branch of boomerang cryptanalysis on equal footing with the classical (probability- p) boomerang.

Despite their success, both branches rely on strong independence assumptions. The most notable ones are the *Markov cipher* assumption and the *hypothesis of stochastic equivalence* [36]. These assumptions are convenient but are not always justified. The true probability of a DC may deviate significantly from its theoretical estimate, and in the boomerang setting, the gap can be even more severe due to the additional coupling between the two halves. In the impossible setting, an unjustified independence step is equally dangerous. It can declare a quartet impossible when it is not, as recently witnessed by the disproof of a SKINNY-128-384 IBD in [15]. Whether and when these assumptions hold has therefore been the subject of intensive scrutiny.

Among the various tools developed to address this question, the *geometric approach* introduced by Beyne [4] has emerged as a particularly promising framework. It interprets cryptanalytic techniques as linear operators acting on vector spaces, with transition matrices arising from a change of basis. One concrete success in this direction is the *quasi-differential* framework of Beyne and Rijmen [5], which expresses the exact probability of a DC as the sum of correlations over all quasi-differential trails (quasi-DCs), free of any Markov or independence assumption. The framework has since been extended to integral cryptanalysis [6,7] and higher-order differential-linear cryptanalysis [28], establishing the geometric approach as a unifying language for symmetric-key cryptanalysis.

The mix-basis variant of the geometric approach originates in Beyne’s thesis [4] and was taken up by Hu et al. [29] at CRYPTO 2025, who used different bases for the input and output spaces. Soon after, Chang et al. [17] applied this mix-basis framework to boomerang cryptanalysis, describing a boomerang quartet as a *3-wise* attack under the assumption that $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$. This assumption keeps the transition matrices tractable, but it collapses the boomerang space into a 3-dimensional affine subspace. On the input side it forces $x_1 \oplus x_2 = x_3 \oplus x_4$, and on the output side it forces $x_1 \oplus x_4 = x_2 \oplus x_3$. As we now explain, this single restriction is the common bottleneck behind both the fixed-key probability problem and the IBD search problem.

Bottleneck 1. Fixed-key probability when the two differentials differ.

The 3-wise representation forces $a = a'$ on the input side and $b = b'$ on the output side. It therefore covers only those boomerangs whose upper and lower differentials share endpoints, and is structurally blind to the unequal-difference case $a \neq a'$ or $b \neq b'$, which is unavoidable in related-key cryptanalysis where the key schedule may inject different differences into the two halves. For such boomerangs the 3-wise framework returns no fixed-key probability at all. Wang et al. [44] addressed this case by extending the quasi-differential framework to quasi- d -differential cryptanalysis [41] and treating a boomerang as a quasi-3-differential. The construction is exact but intractable: a boomerang viewed as a 3-differential leaves parts of its input and output free, generating an enormous number of quasi-3-differential trails with tiny correlations, and [44] reports no concrete distinguisher.

Bottleneck 2. Searching for impossible boomerang distinguishers.

The same $a = a'$, $b = b'$ restriction makes the 3-wise representation blind to all IBDs whose contradiction relies on unequal differences in the upper or lower half. The same shortcoming surfaces, in a different language, in the use of the Double Boomerang Connectivity Table (DBCT) [25,45]: Bonnetain and Lallemand [15] showed that the DBCT only certifies impossibility under the equal-difference constraint, and used this to disprove one of the SKINNY-128-384 IBDs claimed by Zhang et al. [46].

After Lu’s original manual constructions [37,38] and Choy and Yap’s extension [19] to generalized Feistel structures, the topic lay dormant for a decade. The recent resurgence has produced several dedicated search tools, each cipher-specific or limited in scope. Bonnetain et al. [14] gave ad-hoc contradiction constructions for SIMON and SKINNYee. Hu et al. [30] developed a framework that interleaves differential-, state-, and table-based propagations, reaching more rounds at the price of an intricate construction with cipher-specific propagation rules. In parallel, the wave of work on IB *key recovery* [18,31] has sharpened the need for a clean and cipher-agnostic IBD-search tool, since the quality of the underlying IBD bounds the reach of any subsequent key recovery.

As a consequence, a simple and unified theoretical tool for boomerang cryptanalysis is still missing, both for impossible boomerang distinguishers and for boomerang cryptanalysis in the fixed-key model. The contrast with impossible differential cryptanalysis, which has long enjoyed clean and cipher-agnostic automated search [26], makes this gap especially conspicuous. The 4-wise framework developed below closes it, putting impossible boomerang search on the same methodological footing as impossible differential search.

Our contributions. We propose an exact *4-wise geometric framework* for boomerang cryptanalysis that is a *strict generalization* of the 3-wise framework of [17]: setting $u_2 = u_3$ and $v_2 = v_3$ together with the quartet-sum-zero constraint recovers their construction, and at the same computational cost our framework additionally covers the unequal-difference and impossibility cases that the 3-wise representation cannot reach, resolving both bottlenecks above.

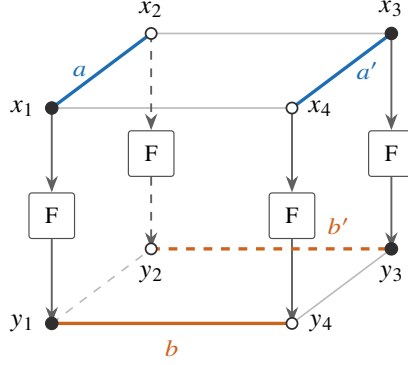


Fig. 1: The 4-wise representation of a boomerang quartet. Filled dots are the base value coordinates (x_1, x_3) and (y_1, y_3) . The input differences a, a' sit on the slanted edges of the top face, the output differences b, b' sit on the horizontal edges of the bottom face, perpendicular to a, a' . This perpendicularity is the geometric signature of a boomerang. Hidden edges are dashed.

The framework works directly on the natural $4n$ -dimensional sample space of a boomerang quartet, putting impossible boomerang and fixed-key boomerang analysis on the same theoretical footing as the quasi-differential framework of [5].

The 4-wise framework (Section 3). A boomerang attack handles a quartet (x_1, x_2, x_3, x_4) , so it is intrinsically a 4-wise attack in the sense of the geometric approach [4, 29]. We parametrize the quartet by two value coordinates (x_1, x_3) and two difference coordinates $(a, a') = (x_1 \oplus x_2, x_3 \oplus x_4)$ on the input side, and symmetrically on the output side, see Figure 1. On the two value coordinates we place a linear (Walsh) basis $(-1)^{u^\top x}$ and on the two difference coordinates a Standard (Dirac) basis $\delta_u(\cdot)$. This mixed choice yields a single closed-form transition matrix that uniformly subsumes the BCT [20], the 3-differential representation [44], and the 3-wise mix-basis matrix of [17] as special cases. Mirroring the DC/quasi-DC hierarchy of [5], we organize the search into *boomerang quartet characteristics* (BQCs) and *quasi-boomerang quartet characteristics* (*quasi-BQCs*), with the exact probability of a distinguisher equal to the sum of correlations of all quasi-BQCs. Formal definitions and the closed-form matrix are deferred to Section 3.

We apply the framework to PRESENT, ASCON, SKINNY, and GIFT; the results are summarized in Table 1.

Application I. A positive SAT model for IBDs (Section 4). The framework yields a clean sufficient condition for impossibility, namely that *no BQC with non-zero correlation exists*. Instead of enumerating all input/output differences and waiting for UNSAT, we turn the search into a *positive* SAT problem that models deterministic differential propagation in F_0 and F_1 and matches

an impossible pattern in F_m . The model finds new RK-IBDs covering 5 rounds of ASCON- p , 8 rounds of PRESENT-80, 12 rounds of GIFT-64, 11/14/18 rounds of SKINNY-64- $\{64, 128, 192\}$, including unequal-difference IBDs that fall outside the reach of [46,14,30].

Application II. Exact fixed-key boomerang probability (Section 5).

Without any assumption, the framework returns the exact fixed-key probability as a sum of all quasi-BQC correlations. For a 13-round SKINNY-64-128 boomerang, it predicts $2^{-4.84}$, and for a 17-round SKINNY-64-192 boomerang, it predicts $2^{-5.35}$; both match the experimental values, whereas the 3-wise estimate of [17] is significantly off as it ignores the unequal-difference contributions.

Outline. Section 2 recalls boomerang attacks and the geometric approach. Section 3 develops the exact 4-wise framework. Section 4 gives the impossible boomerang application. Section 5 gives the fixed-key probability calculation application.

2 Preliminaries

In this section, we recall the boomerang cryptanalysis and its variant, and the geometric approach.

2.1 Boomerang Cryptanalysis and Its Variants

The boomerang attack of Wagner [42] viewed the target cipher F as a composition of two parts $F = F_1 \circ F_0$. Suppose that a differential $\alpha \xrightarrow{F_0} \beta$ with probability p for the upper part F_0 , and a differential $\gamma \xrightarrow{F_1} \delta$ with probability q for the lower part. Under the independence assumption between F_0 and F_1 , the boomerang's return probability is then

$$\Pr[F^{-1}(F(x_1) \oplus \delta) \oplus F^{-1}(F(x_1 \oplus \alpha) \oplus \delta) = \alpha] = p^2 q^2.$$

The boomerang attack is an adaptive chosen plaintext-ciphertext attack. Kelsey et al. [33] proposed the amplified boomerang attack. Later, Biham et al. [9,10] proposed the rectangle attack, turning the boomerang attack into the chosen plaintext scenario.

Soon, several works [39,12,35] studied the independence assumption of the two parts and showed that it is always unreliable, far from the real probability. Dunkelman et al. [24] proposed the *sandwich attack*, which regards the cipher F into three parts $F = F_1 \circ F_m \circ F_0$. The middle part F_m is introduced to study the incompatibility of the upper part F_0 and lower part F_1 . Later, the Boomerang Connectivity Table (BCT) framework [20] assumed the middle part F_m is an S-box layer. The BCT is defined as follows.

Table 1: Our results of (impossible) boomerang distinguishers. Our contributions are highlighted in gray.

ID and IB distinguishers. SK/RK = Single/Related-(twea)key setting.					
Target cipher	Scenario	Rounds	Number	Method	Reference
ASCON- p	Permutation	5	many	ID	[26]
	Permutation	5	many	IBD	Section 4
PRESENT-80	SK	6	many	ID	[26]
	SK	6	58	IBD	[30]
	SK	6	many	IBD	Section 4
	RK	8	many	IBD	Section 4
SKINNY-64-64	RK	11	many	IBD	Section 4
SKINNY-64-128	RK	14	many	IBD	Section 4
SKINNY-64-192	RK	17	1	ID	[27]
	RK	18	1	IBD	[46]
	RK	18	many	IBD	Section 4
	RK	19	3	IBD	[30]
	RK	19	5	IBD	Appendix A
GIFT-64	SK	6	many	IBD	Section 4
	RK	12	48	ID	[32]
	RK	12	many	IBD	Section 4
	RK	13	48	IBD	[30]
	RK	13	48	IBD	Appendix B
Results of boomerang distinguishers in the fixed-key model.					
Target cipher	Key-Independent	Rounds	Key-Size	Probability	Reference
SKINNY-64-128	✓	13	2^{128}	$2^{-4.84}$	Section 5
SKINNY-64-192	✓	17	2^{192}	$2^{-5.35}$	Section 5

Definition 1 (Boomerang Connectivity Table (BCT) [20]). Let S be an n -bit invertible S -box, and $\beta, \gamma \in \mathbb{F}_2^n$. The BCT of S is a $2^n \times 2^n$ table, in which the probability of the entry for (β, γ) is given by

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

Therefore, a boomerang distinguisher consists of three parts. The upper part is a differential $\alpha \xrightarrow{F_0} \beta$ with probability p , the lower part is a differential $\gamma \xrightarrow{F_1} \delta$ with probability q , and the middle is an S -box switch with probability $r = \text{BCT}(\beta, \gamma)$. The probability of a boomerang distinguisher of F is $p^2 q^2 r$. Following the BCT technique, many works generalized it to multiple rounds [40, 43, 21, 25].

However, the round-independence assumption still exists in the full boomerang distinguisher. Chang et al. [17] described the boomerang as a 3-wise attack in the mix-basis framework, thereby removing the round-independence assumption and computing the fixed-key probability of a boomerang distinguisher, but still

under the assumption $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$. This work removes this 3-wise assumption and verifies the validity of the boomerang distinguishers without any assumption.

Impossible boomerang cryptanalysis. The impossible boomerang attack was introduced by Lu [37] and soon generalized to Feistel structures by Choy and Yap [19]. Lu split the cipher as $F = F_1 \circ F_0$ and combined two probability-1 (truncated) differentials for the upper part and two for the lower part,

$$\alpha \xrightarrow{F_0} \beta, \quad \alpha' \xrightarrow{F_0} \beta', \quad \delta \xrightarrow{F_1^{-1}} \gamma, \quad \delta' \xrightarrow{F_1^{-1}} \gamma',$$

such that the four intermediate differences satisfy $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$. This *miss-in-the-middle* contradiction certifies that no valid boomerang quartet can exist along the chosen difference propagation, yielding an IBD.

Lu’s manual construction lay dormant for over a decade, and the relationship between IBDs and other boomerang incompatibilities, such as BCT contradictions, remained unclear. The recent resurgence has produced three lines of automated search, each with its own limitation. Zhang et al. [46] proposed a MIQCP-based model and used the DBCT to detect two-round contradictions, but the approach turned out to be unsound. Bonnetain and Lallemand [15] showed that the DBCT only certifies impossibilities under the equal-difference constraint, and disproved one of the SKINNY-128-384 IBDs from [46]. Bonnetain et al. [14] gave ad-hoc contradiction constructions for SIMON and SKINNYee. Most recently, Hu et al. [30] developed a framework that interleaves differential-, state-, and table-based propagations; this approach reaches more rounds, but the construction is intricate and the propagation rules are cipher-specific, making the framework heavy to deploy.

The situation contrasts sharply with impossible differential cryptanalysis, which has long enjoyed clean and cipher-agnostic automated search [26]. The 4-wise framework developed in this paper closes this gap, giving impossible boomerang search the same level of clean and uniform methodology.

2.2 Geometric Approach

Beyne [4,3] proposed the geometric approach, a unified tool for various cryptanalysis techniques. It has been applied to linear cryptanalysis [3], differential cryptanalysis [5], and integral cryptanalysis [6,8]. In this framework, cryptanalytic methods are interpreted as linear operators acting on vector spaces of functions, represented in different choices of basis. Cryptanalytic techniques differ in how many cipher values they jointly sample. Linear cryptanalysis acts on one value, differential cryptanalysis on a pair, and boomerang cryptanalysis on a quartet. Hu et al. [29] organize this by the dimension of the input sample space.

Definition 2 (*d*-wise space and attack, adapted from [29]). A subspace $S \subseteq (\mathbb{F}_2^n)^s$ has order d if $\dim_{\mathbb{F}_2}(S) = dn$, equivalently if $S \cong (\mathbb{F}_2^n)^d$ as an

$\mathbb{F}_2$ -vector space. An attack on $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is called a d -wise attack if its samples are taken from an order- d space S , and its transition matrix is the matrix representation of the map induced by $F^{\times s}$ on S , expressed in a chosen pair of input and output bases.

Linear cryptanalysis is a 1-wise attack, differential and differential-linear cryptanalysis are 2-wise attacks. A boomerang quartet has four free values, so boomerang cryptanalysis is intrinsically a 4-wise attack on $(\mathbb{F}_2^n)^4$. However, prior work using the geometric approach treats it as a 3-wise attack on a smaller subspace, as we will see in Example 3 below. Removing this restriction is the focus of the present paper.

Vector spaces and transition matrices. Let $F : X \rightarrow Y$ be a function between two finite sets, and let $\mathbb{K}$ be a field. The geometric approach works with two dual vector spaces attached to X . The first is the *free vector space* on X ,

$$\mathbb{K}[X] = \left\{ \sum_{x \in X} u[x] \delta_x : u[x] \in \mathbb{K} \right\},$$

where $\{\delta_x : x \in X\}$ is the standard basis indexed by X and $u[x] \in \mathbb{K}$ is the coordinate (the coefficient of δ_x) of $u \in \mathbb{K}[X]$. From a cryptanalytic viewpoint, an element of $\mathbb{K}[X]$ assigns a $\mathbb{K}$ -valued weight to each $x \in X$. Its dual is

$$\mathbb{K}^X = \{ f : X \rightarrow \mathbb{K} \},$$

the space of $\mathbb{K}$ -valued functions on X ; every such f extends uniquely to a linear functional on $\mathbb{K}[X]$ by $\delta_x \mapsto f(x)$, so the canonical pairing is $f(u) = \sum_{x \in X} f(x) u[x]$.

The function $F : X \rightarrow Y$ induces the *push-forward* $T^F : \mathbb{K}[X] \rightarrow \mathbb{K}[Y]$, defined on the standard basis by $T^F \delta_x = \delta_{F(x)}$ and extended linearly. Its matrix in chosen bases of $\mathbb{K}[X]$ and $\mathbb{K}[Y]$ is the *transition matrix* of F . Transition matrices behave well under both sequential and parallel composition of functions.

Theorem 1 (Propagation of transition matrices, [3,5]). *The transition matrix T^F satisfies:*

- (1) If $F = F_r \circ \dots \circ F_1$ (sequential composition), then $T^F = T^{F_r} \dots T^{F_1}$.
- (2) If $F = F_1 \parallel \dots \parallel F_m$ (parallel composition), then $T^F = \bigotimes_{i=1}^m T^{F_i}$.

A *cryptanalytic property* of F , in the sense of [4], is a pair (u, v) with $u \in \mathbb{K}[X]$ and $v \in \mathbb{K}^Y$; its value is $v(T^F u)$. Concretely, let $\{\alpha^u\}$ be a basis of $\mathbb{K}^X$ with dual basis $\{\alpha_u\}$ of $\mathbb{K}[X]$, and let $\{\beta^v\}$ be a basis of $\mathbb{K}^Y$ with dual basis $\{\beta_v\}$ of $\mathbb{K}[Y]$. Then the matrix entries of T^F are

$$T_{v,u}^F = \beta^v(T^F \alpha_u) = \sum_{x \in X} \beta^v(F(x)) \alpha_u[x],$$

i.e., $T_{v,u}^F$ is the value of the cryptanalytic property (α_u, β^v) . Specific properties (linear correlation, differential probability, integral parity, ...) are recovered by choosing suitable input and output bases.

Example 1. (linear cryptanalysis, $d = 1$) Take $X = Y = \mathbb{F}_2^n$ and $\mathbb{K} = \mathbb{R}$. Use the same basis on both sides, the *linear basis*

$$\chi^u(x) = (-1)^{u^\top x}, \quad \chi_u[x] = \frac{(-1)^{u^\top x}}{2^n}.$$

In this basis, the transition matrix is the *correlation matrix* C^F with entries

$$C_{v,u}^F = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{u^\top x \oplus v^\top F(x)},$$

which is exactly the linear correlation of the mask pair (u, v) .

Example 2. (differential cryptanalysis, $d = 2$) Take $X = Y = \mathbb{F}_2^n \times \mathbb{F}_2^n$, and let F act componentwise by $F : (x, y) \mapsto (F(x), F(y))$. Using the same basis on both sides, the *quasi-differential basis* [5] is

$$q^{(u,a)}(x, y) = (-1)^{u^\top x} \delta_a(x \oplus y), \quad q_{(u,a)}[(x, y)] = \frac{(-1)^{u^\top x} \delta_a(x \oplus y)}{2^n},$$

where $\delta_a(\cdot)$ is the indicator function ($\delta_a(z) = 1$ iff $z = a$), to be distinguished from the standard basis vector $\delta_x \in \mathbb{K}[X]$. In this basis, the transition matrix is the *quasi-differential transition matrix* D^F with entries

$$D_{(v,b),(u,a)}^F = \frac{1}{2^n} \sum_{\substack{x \in \mathbb{F}_2^n \\ F(x) \oplus F(x \oplus a) = b}} (-1)^{u^\top x \oplus v^\top F(x)}. \quad (1)$$

The mask-zero column $D_{(0,b),(0,a)}^F = \text{DDT}^F(a, b)/2^n$ recovers the (normalized) differential probability, while the other entries carry the Walsh phase as quasi-differential corrections. The exact (fixed-key) probability of a DC is the sum of correlations of all of its quasi-DCs, without any assumption.

The mix-basis framework. In the above examples, the same basis is used on the input and output sides; such attacks are called *same-basis* attacks. Hu et al. [29] generalized the framework by allowing the input basis $\{\alpha_u\}$ of $\mathbb{K}[X]$ and the output basis $\{\beta^v\}$ of $\mathbb{K}^Y$ to be of different styles. The matrix entries are still given by $T_{v,u}^F$. Such attacks are called *mix-basis* attacks.

This flexibility provides a unified description of asymmetric cryptanalytic settings. A typical example, given in [29], is differential-linear cryptanalysis, viewed as a mix-basis attack in which the input side uses the quasi-differential basis and the output side uses the linear basis.

Example 3. (3-wise quasi-boomerang framework, $d = 3$) As an application of the mix-basis framework, Chang et al. [17] described boomerang cryptanalysis as a 3-wise mix-basis attack with $s = 4$ and $d = 3$. Under the quartet-sum-zero assumption $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$, the input quartet is parameterized by $(x, \Delta_1, \Delta_2) \in (\mathbb{F}_2^n)^3$ as

$$(x_1, x_2, x_3, x_4) = (x, x \oplus \Delta_1, x \oplus \Delta_2, x \oplus \Delta_1 \oplus \Delta_2),$$

so that the underlying space is the order-3 subspace

$$X_3 = \{(x_1, x_2, x_3, x_4) \in (\mathbb{F}_2^n)^4 : x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0\} \cong (\mathbb{F}_2^n)^3.$$

The output is parameterized analogously by (y, ∇_1, ∇_2) with $y_i = F(x_i)$. The input basis of $\mathbb{K}^{X_3}$ is

$$b^{(u_0, u_1, u_2)}(x, \Delta_1, \Delta_2) = (-1)^{u_0^\top x} \delta_{u_1}(\Delta_1) (-1)^{u_2^\top \Delta_2},$$

and the output basis is

$$c^{(v_0, v_1, v_2)}(y, \nabla_1, \nabla_2) = (-1)^{v_0^\top y} (-1)^{v_1^\top \nabla_1} \delta_{v_2}(\nabla_2).$$

In these bases, the entries of T^F are the quasi-boomerang correlations, and the fixed-key probability of a boomerang under the 3-wise assumption is the sum of correlations of all quasi-boomerang characteristics (quasi-BCs).

Limitations of the 3-wise framework and our 4-wise setting. The quartet-sum-zero assumption forces $\Delta_1 = a = a'$ on the input side and $\nabla_2 = b = b'$ on the output side. As discussed in the introduction, this restriction has two unavoidable consequences. First, the fixed-key probability returned by [17] is only an approximation whenever the upper and lower differentials carry distinct differences, a setting that arises naturally in related-key cryptanalysis. Second, the 3-wise representation is structurally blind to impossible boomerang distinguishers whose contradiction relies on $a \neq a'$ or $b \neq b'$.

To resolve both, we discard the quartet-sum-zero restriction and work directly on the full space

$$X = (\mathbb{F}_2^n)^4,$$

of dimension $4n$ over $\mathbb{F}_2$. Boomerang cryptanalysis is then a 4-wise attack in the sense of Definition 2, with $s = d = 4$. The corresponding 4-wise framework, comprising the basis choice, the resulting closed-form transition matrix B^F , and the BQC/quasi-BQC trail hierarchy, is developed in Section 3.

3 Exact 4-wise Mix-Basis Framework for Boomerang

A boomerang quartet (x_1, x_2, x_3, x_4) has four independent values, so by the geometric-approach principle of [29] it is naturally a 4-wise attack with a transition matrix of size $(2^n)^4 \times (2^n)^4$. The 3-wise framework of Chang et al. [17]

avoids this matrix by quotienting the $4n$ -dimensional space to its $3n$ -dimensional sum-zero subspace, shrinking the matrix to $(2^n)^3 \times (2^n)^3$ at the price of the two structural limitations discussed in Section 2.

We keep the full $4n$ -dimensional quartet space and recover tractability through a careful basis choice. The two *differences* (a, a') and the two *base values* (x_1, x_3) play different roles in a boomerang and should be expanded in different bases. On the differences, we use the standard basis $\delta_u(\cdot)$, which pins each difference coordinate to a single value and makes the corresponding factor of the transition matrix sparse. On the values, we use the linear basis $(-1)^{u^\top x}$, which diagonalizes the action of key-XOR and lets the key-dependence factor cleanly, exactly as in the quasi-differential framework [5]. Although the resulting matrix conceptually has size $(2^n)^4 \times (2^n)^4$, in this mixed basis its entries $B_{\mathbf{v}, \mathbf{u}}^F$ admit the closed form (4), in which the four difference coordinates fix the pair structure and reduce the entry to a single sum over the two value coordinates x_1, x_3 . The 4-wise framework is therefore no costlier to evaluate than the 3-wise framework of [17]; it simply covers cases the 3-wise framework cannot reach.

3.1 New 4-wise Mix-Basis Framework

Quartet parameterization. Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a cipher and (x_1, x_2, x_3, x_4) be a boomerang quartet with outputs $y_i = F(x_i)$, as depicted in Figure 1. We parameterize the input space $X = (\mathbb{F}_2^n)^4$ by the two base values and the two input differences,

$$(x_1, x_3, a, a'), \quad a = x_1 \oplus x_2, \quad a' = x_3 \oplus x_4,$$

and the output space $Y = (\mathbb{F}_2^n)^4$ by the two base values and the two output (crossed) differences,

$$(y_1, y_3, b, b'), \quad b = y_1 \oplus y_4, \quad b' = y_2 \oplus y_3.$$

Both parameterizations are invertible $\mathbb{F}_2$ -linear changes of variable on $(\mathbb{F}_2^n)^4$, and no quartet constraint is imposed. The quartet space remains $4n$ -dimensional.

Mix-basis on the quartet space. Following the conventions of Section 2, we work with bases of $\mathbb{K}^X$ and $\mathbb{K}^Y$ that mix the linear basis on the two value coordinates and the standard (indicator) basis on the two difference coordinates. The input basis is

$$b^{(u_0, u_1, u_2, u_3)}(x_1, x_3, a, a') = (-1)^{u_0^\top x_1} (-1)^{u_1^\top x_3} \delta_{u_2}(a) \delta_{u_3}(a'), \quad (2)$$

and the output basis is

$$c^{(v_0, v_1, v_2, v_3)}(y_1, y_3, b, b') = (-1)^{v_0^\top y_1} (-1)^{v_1^\top y_3} \delta_{v_2}(b) \delta_{v_3}(b'), \quad (3)$$

where $u_0, u_1, u_2, u_3, v_0, v_1, v_2, v_3 \in \mathbb{F}_2^n$ and $\delta_a(\cdot)$ is the indicator function. The dual bases on $\mathbb{K}[X]$ and $\mathbb{K}[Y]$ are obtained as in Section 2, with each linear

factor carrying the $1/2^n$ normalization. We write $\mathbf{u} = (u_0, u_1, u_2, u_3)$ and $\mathbf{v} = (v_0, v_1, v_2, v_3)$ for the input and output coordinate tuples.

For any function $H : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ acting on the parameterized quartet by $(x_1, x_3, a, a') \xrightarrow{H} (H(x_1), H(x_3), b, b')$, a direct change of basis from the standard basis to (2) and (3) yields the closed-form transition matrix

$$B_{\mathbf{v}, \mathbf{u}}^H = \frac{1}{2^{2n}} \sum_{\substack{x_1, x_3 \in \mathbb{F}_2^n \\ a=u_2, a'=u_3, b=v_2, b'=v_3}} (-1)^{u_0^\top x_1 \oplus u_1^\top x_3 \oplus v_0^\top H(x_1) \oplus v_1^\top H(x_3)}. \quad (4)$$

Parallel with the (quasi-)differential framework. Comparing (4) with the quasi-differential transition matrix (1) of Example 2 in Section 2, the 4-wise entry has the same shape. Both are a normalized sum over value coordinates, restricted by input and output difference constraints, and weighted by a Walsh phase on the value coordinates and their images. The boomerang quartet simply uses two value coordinates (x_1, x_3) , two input-difference constraints (a, a') , two output-difference constraints (b, b') , and four Walsh masks (u_0, u_1, v_0, v_1) , where the quasi-differential entry uses one of each.

The implications carry over verbatim. Setting $u_0 = u_1 = v_0 = v_1 = 0$ removes the Walsh phase and reduces $B_{(0,0,v_2,v_3),(0,0,u_2,u_3)}^F$ to a normalized count of pairs (x_1, x_3) realizing the prescribed differences (a, a', b, b') . This counting entry is the (rectangle-style) boomerang probability, the boomerang analogue of $\text{DDT}^F(a, b)/2^n$. The remaining entries carry the Walsh phase as quasi-differential-style corrections, and summing the counting entry with all corrections sharing the same difference coordinates yields the exact fixed-key probability, just as in [5].

For impossible boomerangs, if the input difference pair (a, a') cannot propagate to the output difference pair (b, b') across the cipher, meaning the counting entry $B_{(0,0,v_2,v_3),(0,0,u_2,u_3)}^F$ vanishes for every admissible chain of intermediate differences, then no valid quartet exists and $(a, a') \rightarrow (b, b')$ is an IBD. This is the basis of our IBD search in Section 4, which certifies the vanishing-entry condition exactly as the impossible-differential search of [26] certifies a vanishing DDT entry.

Relation to the 3-wise framework. Specializing $u_2 = u_3$ and $v_2 = v_3$, and imposing the quartet-sum-zero constraint $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$, recovers the 3-wise basis of Chang et al. [17]. Our framework is therefore a strict generalization that also handles the unequal-difference case.

3.2 Transition Matrices of Components

The mix-basis chosen in Section 3.1 differs between the input and output sides of F . The input uses the upper-style pair structure $\{(x_1, x_2), (x_3, x_4)\}$ encoded by the differences (a, a') , and the output uses the lower-style pair structure

$\{(y_1, y_4), (y_2, y_3)\}$ encoded by (b, b') . Round by round, this global mix-basis decomposes naturally into three parts. The upper rounds see the upper-style pairing on both their input and output sides and are therefore *same-basis* transitions in that pair structure. The lower rounds see the lower-style pairing on both sides and are likewise *same-basis*. Between the two, a single *mix-basis* round carries an upper-style input pair into a lower-style output pair.

We accordingly decompose the cipher as $F = F_1 \circ F_m \circ F_0$, where F_0 is the upper sub-cipher, F_1 is the lower sub-cipher, and F_m is the middle switch, taken to be a single S-box layer like [20]. By Theorem 1,

$$B^F = B^{F_1} B^{F_m} B^{F_0}.$$

The middle factor B^{F_m} is exactly (4) applied to the single S-box layer F_m . As written, $B_{\mathbf{v}, \mathbf{u}}^{F_m}$ computes a rectangle entry, and we multiply by 2^n throughout the paper to convert it to a boomerang entry [34]. The remainder of this subsection derives the upper and lower factors B^{F_0} and B^{F_1} .

The upper and lower sub-ciphers are products of round transition matrices. A typical round function further decomposes as $F_i = F_k \circ F_l \circ F_s$, where F_s is the S-box layer, F_l the invertible linear layer, and F_k the round key-XOR, so by Theorem 1

$$B^{F_i} = B^{F_k} B^{F_l} B^{F_s}.$$

The S-box matrix B^{F_s} instantiates (4) according to the pair structure of the part it sits in. The linear-layer and key-XOR matrices admit simpler closed forms, derived below.

S-box layer. An S-box layer F_s in F_0 or F_1 acts component-wise on each of the four values, with the input and output pair structures matched to its position (upper-style $(x_1, x_2), (x_3, x_4)$ in F_0 , lower-style $(x_1, x_4), (x_3, x_2)$ in F_1). Substituting the corresponding difference pairs into (4) gives

$$B_{\mathbf{v}, \mathbf{u}}^{F_s} = \frac{1}{2^{2n}} \begin{cases} \sum_{\substack{x_1, x_3 \in \mathbb{F}_2^n \\ x_1 \oplus x_2 = u_2, x_3 \oplus x_4 = u_3 \\ F_s(x_1) \oplus F_s(x_2) = v_2 \\ F_s(x_3) \oplus F_s(x_4) = v_3}} (-1)^{u_0^\top x_1 \oplus u_1^\top x_3 \oplus v_0^\top F_s(x_1) \oplus v_1^\top F_s(x_3)} & (\text{in } F_0), \\ \sum_{\substack{x_1, x_3 \in \mathbb{F}_2^n \\ x_1 \oplus x_4 = u_2, x_3 \oplus x_2 = u_3 \\ F_s(x_1) \oplus F_s(x_4) = v_2 \\ F_s(x_3) \oplus F_s(x_2) = v_3}} (-1)^{u_0^\top x_1 \oplus u_1^\top x_3 \oplus v_0^\top F_s(x_1) \oplus v_1^\top F_s(x_3)} & (\text{in } F_1). \end{cases} \quad (5)$$

Linear layer. For a linear function F_l in F_0 or F_1 , instantiating (4) gives a formula of the same shape as (5) with F_s replaced by F_l . By linearity, the difference constraints collapse to $F_l(u_2) = v_2$ and $F_l(u_3) = v_3$, and the Walsh phase factors through $F_l^\top$, so the two cases reduce to the single closed form

$$B_{\mathbf{v}, \mathbf{u}}^{F_l} = \delta_{u_0}(F_l^\top(v_0)) \delta_{u_1}(F_l^\top(v_1)) \delta_{v_2}(F_l(u_2)) \delta_{v_3}(F_l(u_3)). \quad (6)$$

Key-XOR. For the key-XOR $F_k : x \mapsto x \oplus k$ with a key quartet (k_1, k_2, k_3, k_4) in the related-key setting, write $(\Delta_k, \Delta'_k) = (k_1 \oplus k_2, k_3 \oplus k_4)$ for the key differences in F_0 and $(\nabla_k, \nabla'_k) = (k_1 \oplus k_4, k_2 \oplus k_3)$ for those in F_1 . The transition matrix is

$$B_{\mathbf{v}, \mathbf{u}}^{F_k} = \begin{cases} (-1)^{v_0^\top k_1 \oplus v_1^\top k_3} \delta_{v_0}(u_0) \delta_{v_1}(u_1) \delta_{v_2}(u_2 \oplus \Delta_k) \delta_{v_3}(u_3 \oplus \Delta'_k) & (\text{in } F_0), \\ (-1)^{v_0^\top k_1 \oplus v_1^\top k_3} \delta_{v_0}(u_0) \delta_{v_1}(u_1) \delta_{v_2}(u_2 \oplus \nabla_k) \delta_{v_3}(u_3 \oplus \nabla'_k) & (\text{in } F_1). \end{cases} \quad (7)$$

The single-key setting is recovered by $k_1 = k_2 = k_3 = k_4$.

3.3 Multi-Round Composition via the BQC / Quasi-BQC Hierarchy

For an r -round cipher $F = F_r \circ \dots \circ F_1$, the transition matrix factors by Theorem 1 as

$$B^F = B^{F_r} B^{F_{r-1}} \dots B^{F_1}.$$

We organize the resulting trail enumeration in two levels, mirroring the DC / quasi-DC hierarchy of the quasi-differential framework [5].

BQC and quasi-BQC. A *boomerang quartet characteristic* (BQC) captures only the chain of intermediate difference pairs across rounds, while a *quasi-boomerang quartet characteristic* (quasi-BQC) refines a BQC by also tracking the Walsh masks on the value coordinates round by round.

Definition 3 (Boomerang quartet characteristic (BQC)). A *boomerang quartet characteristic* for an r -round function $F = F_r \circ \dots \circ F_1$ is a difference sequence

$$((a_1, a'_1), (a_2, a'_2), \dots, (a_{r+1}, a'_{r+1})),$$

where (a_i, a'_i) is the difference pair entering round i .

Definition 4 (Quasi-boomerang quartet characteristic (quasi-BQC)). A *quasi-boomerang quartet characteristic* refining a BQC $((a_1, a'_1), \dots, (a_{r+1}, a'_{r+1}))$ is a sequence

$$\Omega = (\Omega_1, \dots, \Omega_{r+1}), \quad \Omega_i = (u_0^{(i)}, u_1^{(i)}, a_i, a'_i),$$

where $(u_0^{(i)}, u_1^{(i)})$ are the per-round Walsh masks on the two value coordinates and $u_0^{(1)} = u_1^{(1)} = u_0^{(r+1)} = u_1^{(r+1)} = 0$. Its correlation is

$$\text{cor}(\Omega) = \prod_{i=1}^r B_{\Omega_{i+1}, \Omega_i}^{F_i}.$$

Each BQC is therefore covered by a family of quasi-BQCs sharing its difference coordinates (a_i, a'_i) , and the round-independence approximation corresponds to the unique quasi-BQC whose intermediate Walsh masks are all zero.

Exact and approximate boomerang probability. The exact probability of an r -round boomerang distinguisher with input difference pair (a_1, a'_1) and output difference pair (a_{r+1}, a'_{r+1}) is the sum of correlations over all quasi-BQCs joining them,

$$B_{\Omega_{r+1}, \Omega_1}^F = \sum_{\Omega_2, \dots, \Omega_r} \prod_{i=1}^r B_{\Omega_{i+1}, \Omega_i}^{F_i}, \quad (8)$$

with $\Omega_1 = (0, 0, a_1, a'_1)$ and $\Omega_{r+1} = (0, 0, a_{r+1}, a'_{r+1})$. Direct enumeration over all quasi-BQCs is infeasible because the search space has size 2^{4nr} , so we use the two-level hierarchy.

Fixing all intermediate value masks to zero, $u_0^{(i)} = u_1^{(i)} = 0$ for $i = 2, \dots, r$, picks out a single quasi-BQC per BQC and gives the round-independence approximation

$$\Pr_{\text{BQC}}[(a_1, a'_1), \dots, (a_{r+1}, a'_{r+1})] \approx \prod_{i=1}^r B_{(0,0,a_{i+1},a'_{i+1}), (0,0,a_i,a'_i)}^{F_i}. \quad (9)$$

Removing this assumption recovers the exact probability of a BQC.

Proposition 1. *For an r -round cipher $F = F_r \circ \dots \circ F_1$, the exact (fixed-key) probability of a BQC $((a_1, a'_1), \dots, (a_{r+1}, a'_{r+1}))$ is*

$$\Pr_{\text{BQC}}[(a_1, a'_1), \dots, (a_{r+1}, a'_{r+1})] = \sum_{u_0^{(2)}, \dots, u_0^{(r)}} \sum_{u_1^{(2)}, \dots, u_1^{(r)}} \prod_{i=1}^r B_{\Omega_{i+1}, \Omega_i}^{F_i},$$

where $\Omega_i = (u_0^{(i)}, u_1^{(i)}, a_i, a'_i)$ with $u_0^{(1)} = u_1^{(1)} = u_0^{(r+1)} = u_1^{(r+1)} = 0$.

Proof. Substitute the closed form (4) into each factor of $\prod_{i=1}^r B_{\Omega_{i+1}, \Omega_i}^{F_i}$ and reorder the Walsh phases. Each intermediate mask $u_0^{(i)}$ (for $i = 2, \dots, r$) appears as $(u_0^{(i)})^\top [x_1^{(i)} \oplus F_{i-1}(x_1^{(i-1)})]$, and similarly for $u_1^{(i)}$. Summing these masks out via $\frac{1}{2^n} \sum_u (-1)^{u^\top z} = \delta_0(z)$ forces $x_1^{(i)} = F_{i-1}(x_1^{(i-1)})$ and $x_3^{(i)} = F_{i-1}(x_3^{(i-1)})$ at every round interface. The remaining sum is a normalized count of pairs $(x_1^{(1)}, x_3^{(1)})$ whose orbits under $F_1, \dots, F_r$ realize the prescribed difference chain, which is the BQC probability. $\square$

Proposition 1 motivates a two-step search. We first enumerate BQCs (a difference-only object of size 2^{2nr} across the round-interface difference pairs), and then for each candidate BQC compute its exact probability by enumerating its $2^{2n(r-1)}$ refining quasi-BQCs. The combined complexity $2^{2n(2r-1)}$ is far below the 2^{4nr} of direct quasi-BQC enumeration. The following structural property further reduces the per-BQC enumeration.

Proposition 2. *Let $F = F_r \circ \dots \circ F_1$ and fix a BQC $((a_1, a'_1), \dots, (a_{r+1}, a'_{r+1}))$.*

- (1) If some quasi-BQC refining this BQC with masks $(u_0^{(i)}, u_1^{(i)})$ has correlation $(-1)^b p$ for some $b \in \{0, 1\}$, then for any other quasi-BQC with masks $(v_0^{(i)}, v_1^{(i)})$ and correlation c , the quasi-BQC with masks $(u_0^{(i)} \oplus v_0^{(i)}, u_1^{(i)} \oplus v_1^{(i)})$ has correlation $(-1)^b c$.
- (2) If, among the quasi-BQCs refining this BQC, the correlations $\pm p$ sum to zero, the BQC probability is zero.

Proof. A quasi-BQC has correlation $(-1)^b p$ iff for every round i , all (x_1, x_3) contributing to $B_{\Omega_{i+1}, \Omega_i}^{F_i}$ share a single sign $(-1)^{b_i}$ with $\sum_i b_i \equiv b \pmod{2}$. Adding offsets $(v_0^{(i)}, v_1^{(i)})$ multiplies each round factor by $(-1)^{b_i}$ and hence the total correlation by $(-1)^b$. Part (2) is immediate by partitioning the quasi-BQC space into $\pm p$ cosets. $\square$

3.4 Specialization to Key-Alternating Ciphers

Most modern ciphers have the key-alternating form $F = F_r \circ \dots \circ F_m \circ \dots \circ F_1$ with $F_i = F_k^{(i)} \circ G_i$, where $F_k^{(i)}$ is the round key-XOR and G_i the keyless part of the round. By (7), key-XOR contributes only a sign to the correlation of a quasi-BQC, so

$$\text{cor}(\Omega) = \prod_{i=1}^r (-1)^{(u_0^{(i+1)})^\top k_1^{(i)} \oplus (u_1^{(i+1)})^\top k_3^{(i)}} B_{\omega_{i+1}, \omega_i}^{G_i}, \quad (10)$$

where in the related-key setting

$$\omega_{i+1} = \begin{cases} (u_0^{(i+1)}, u_1^{(i+1)}, a_{i+1} \oplus \Delta_{k^{(i)}}, a'_{i+1} \oplus \Delta'_{k^{(i)}}) & i = 1, \dots, m-1, \\ (u_0^{(i+1)}, u_1^{(i+1)}, a_{i+1} \oplus \nabla_{k^{(i)}}, a'_{i+1} \oplus \nabla'_{k^{(i)}}) & i = m, \dots, r, \end{cases}$$

with $u_0^{(1)} = u_1^{(1)} = u_0^{(r+1)} = u_1^{(r+1)} = 0$. The single-key setting is the case $\Delta_{k^{(i)}} = \Delta'_{k^{(i)}} = \nabla_{k^{(i)}} = \nabla'_{k^{(i)}} = 0$. Substituting (10) into the expression of Proposition 1 gives the exact BQC probability for key-alternating ciphers,

$$\text{Pr}_{\text{BQC}}[(a_1, a'_1), \dots, (a_{r+1}, a'_{r+1})] = \sum_{u_0^{(2)}, \dots, u_0^{(r)}} \sum_{u_1^{(2)}, \dots, u_1^{(r)}} \text{cor}(\Omega).$$

4 Applications to Impossible Boomerang Distinguishers

Section 3 established an exact and unified 4-wise theoretical framework for boomerang cryptanalysis. In this section, we apply this framework to the search for IBDs. Our emphasis is on how the framework naturally yields a difference-level criterion for *direct impossibility* [27, 26, 16, 22], and how this criterion can be turned into an efficient *positive* automated model.

4.1 From the 4-Wise Framework to Direct Impossibility

Let $F = F_r \circ \dots \circ F_1$ be an r -round function. By the exact composition formula (8) in Section 3, the probability of the boomerang distinguisher with input difference pair (a_1, a'_1) and output difference pair (a_{r+1}, a'_{r+1}) is

$$B_{\Omega_{r+1}, \Omega_1}^F = \sum_{\Omega_2, \dots, \Omega_r} \prod_{i=1}^r B_{\Omega_{i+1}, \Omega_i}^{F_i}, \quad \Omega_1 = (0, 0, a_1, a'_1), \quad \Omega_{r+1} = (0, 0, a_{r+1}, a'_{r+1}).$$

Thus, an IBD is an input-output difference-pair transition

$$(a_1, a'_1) \rightsquigarrow (a_{r+1}, a'_{r+1}),$$

such that $B_{(0,0,a_{r+1},a'_{r+1}), (0,0,a_1,a'_1)}^F$ is zero.

At the 4-wise level, this zero can arise in two ways:

- (1) **Direct impossibility:** no BQC connects (a_1, a'_1) to (a_{r+1}, a'_{r+1}) with non-zero correlation.
- (2) **Cancellation impossibility:** non-zero quasi-BQCs do exist, but their correlations cancel in the sum, i.e., $B_{(0,0,a_{r+1},a'_{r+1}), (0,0,a_1,a'_1)}^F = 0$.

This section first focuses on the former case; the complementary cancellation case will be revisited in Section 4.4. In the case of the direct impossibility, one immediately obtains a natural verification strategy: fix candidate input/output difference pairs and check whether any valid propagation exists between them. Equivalently, one may search for a difference sequence

$$((a_1, a'_1), (a_2, a'_2), \dots, (a_{r+1}, a'_{r+1}))$$

such that $\prod_{i=1}^r B_{(0,0,a_{i+1},a'_{i+1}), (0,0,a_i,a'_i)}^{F_i} \neq 0$. If no such sequence exists, then no BQC connects (a_1, a'_1) to (a_{r+1}, a'_{r+1}) , and the boomerang is impossible.

This is the most immediate consequence of the 4-wise framework. It is also the boomerang analogue of the classical *validation* approach in impossible differential (ID) cryptanalysis: one fixes the input and output differences and proves that no valid DC exists between them.

However, although this view of fixed-key input/output infeasibility is conceptually natural, it is not the most efficient way to search for impossible distinguishers. In ID cryptanalysis, several recent works [27,26,16,22] have moved from a negative model (fix a candidate and prove UNSAT) to a *positive* one (find satisfiability) that directly generates structures likely to yield impossible transitions, showing in practice that such a model is useful for finding optimal attacks that combine impossible distinguishers with key recovery. In particular, Hadipour et al. [27,26] proposed a unified satisfiability-based model for finding IDs, which leads to an optimal key-recovery attack.

The main advantage is that the solver no longer spends its effort rejecting many input/output candidates one by one. Instead, it directly constructs deterministic propagations that are predisposed to contradiction. We adopt the

same perspective here. More precisely, we transfer the modeling idea used for IDs to the boomerang setting under our 4-wise framework. The outcome is a positive model for *direct impossible boomerangs*: rather than fixing (a_1, a'_1) and (a_{r+1}, a'_{r+1}) in advance, we ask the solver to build deterministic upper and lower propagations that necessarily meet an impossible middle transition.

4.2 A Positive Model for Direct IBDs

We consider an r -round function

$$F = F_r \circ \dots \circ F_{m+1} \circ F_m \circ F_{m-1} \circ \dots \circ F_1,$$

where F_m is the middle S-box layer in the sandwich framework. The idea is simple: if the upper part propagates deterministically from the input, the lower part propagates deterministically backward from the output, and these two deterministic propagations force an impossible transition through the middle layer, then the whole boomerang is directly impossible.

Impossible transitions in the middle layer. For the middle S-box layer F_m , define

$$\mathcal{I}_s := \{(a, a', b, b') : B_{(0,0,b,b'),(0,0,a,a')}^{F_m} = 0\}.$$

Thus, every element of $\mathcal{I}_s$ is a concrete impossible boomerang transition through the middle S-box layer. Suppose now that a candidate boomerang propagates deterministically through rounds $1, \dots, m-1$ in the upper part and backward through rounds $m+1, \dots, r$ in the lower part, while the induced middle input/output difference pair belongs to $\mathcal{I}_s$. Then the middle layer rejects every compatible BQC, and the end-to-end boomerang is a direct IBD.

This directly suggests a positive search model. Instead of enumerating candidate endpoints and checking infeasibility, we search for deterministic upper and lower propagations that meet a middle pattern from $\mathcal{I}_s$, see Figure 2.

Pattern representation. As in ID search, we represent differences by ternary patterns in $\{0, 1, *\}^n$, where $*$ denotes a free bit. A pattern compactly describes a set of concrete differences. For a tuple

$$(p_{in}, p'_{in}, p_{out}, p'_{out}).$$

The first two and last two items denote a set of input/output difference pairs, respectively. This representation allows us to precompute local S-box propagation information and then connect round-wise constraints globally through the linear and key-XOR layers.

Deterministic and impossible pattern sets. For each S-box layer, we precompute three sets:

- (1) *Upper deterministic set* $\mathcal{U}_s$. It contains all patterns $(p_{in}, p'_{in}, p_{out}, p'_{out})$ such that every concrete input pair covered by (p_{in}, p'_{in}) propagates through the upper S-box function in (5) to an output pair covered by (p_{out}, p'_{out}) .

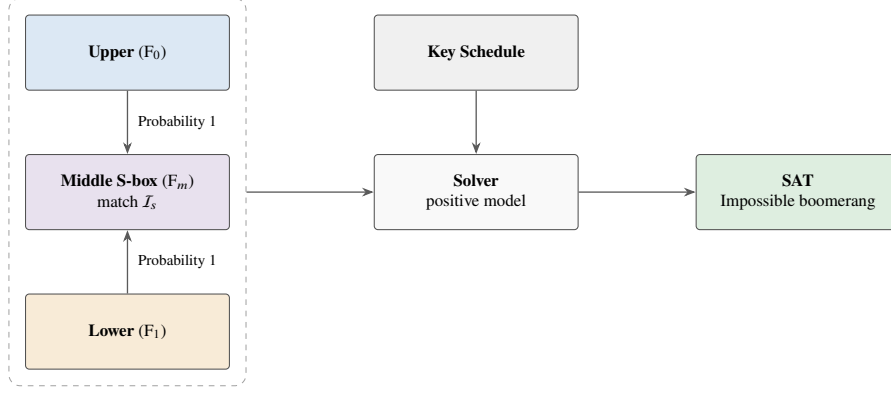


Fig. 2: Positive model for searching direct IBDs.

- (2) *Lower deterministic set* $\mathcal{L}_s$. Similarly, but for the lower S-box function in (5).
- (3) *Maximal impossible set* $\mathcal{I}_p^{max}$. Starting from the concrete impossible set $\mathcal{I}_s$, we derive the pattern set $\mathcal{I}_p$ consisting of all impossible patterns, and then keep only its maximal elements under pattern inclusion. The resulting $\mathcal{I}_p^{max}$ is much smaller while still preserving full coverage of impossible middle transitions.

The numbers of the patterns in $\mathcal{U}_s$ and $\mathcal{L}_s$ are both 3^{2n} .

Remark. A key point is that $\mathcal{I}_s$ is defined on the full 4-wise difference spaces (a, a', b, b') , rather than the restricted equal-difference case (a, a, b, b) . This is one of the practical advantages of the exact 4-wise framework: unequal-difference pairs can be handled natively. Table 2 presents the comparison for several common S-boxes. (a, a, b, b) and (a, a', b, b') represent the equal-difference case and general case, respectively. Both $\mathcal{I}_p$ and $\mathcal{I}_p^{max}$ correspond to the general case.

Table 2: Comparison of the sizes of impossible (pattern) sets for S-boxes.

S-box instance	Bit n	$\#\mathcal{I}_s(a, a, b, b)$	$\#\mathcal{I}_s(a, a', b, b')$	$\#\mathcal{I}_p$	$\#\mathcal{I}_p^{max}$
ASCON	5	445	510613	17936578	681130
PRESENT	4	107	28931	276568	34942
GIFT	4	102	29348	356705	29296
CRAFT	4	107	28931	355013	30748
SKINNY-64	4	103	28875	474437	25038

Propagation through linear and key-XOR layers. Pattern propagation through the remaining layers is standard. For a linear layer, an output bit is fixed if all involved input bits are fixed; otherwise, it becomes *. For a key-XOR layer in the related-key setting, the same rule applies by XORing the

state-difference pattern with the round-key difference pattern. In the single-key setting, the key-XOR layer leaves the state difference unchanged.

Construct positive model. We treat the input/output difference pair as free variables and asks the solver to find any solution satisfying: the upper and lower parts propagate deterministically through rounds $1, \dots, m-1$ and $m+1, \dots, r$ via $\mathcal{U}_s$ and $\mathcal{L}_s$, respectively; the middle input/output pattern belongs to $\mathcal{I}_p^{max}$; and linear propagation is used to connect the pattern variables between adjacent round. Thus, each solution yields an IBD. The positive model is in Figure 2.

4.3 Applications

We apply the above model using the SMT solver Boolector³, to several ciphers. In each case, the IBD is obtained directly from a satisfiability solution.

Application to PRESENT. For PRESENT-80 [13], we consider both single-key and related-key settings.

In the single-key setting, our model finds 6-round IBDs. Compared with the previous search that restricted the active cell of the first S-box [30], our model naturally explores a larger search space and finds many additional 6-round IBDs. One example is listed as IBD 1 in Table 3.

In the related-key setting, we leave the upper key-difference pair free and set the lower key-difference pair to zero. For the non-linear key schedule, the S-box is modeled by the same deterministic pattern rules as the state S-box. We find 8-round related-key IBDs (RK-IBDs) by adding a key-XOR before the first round, see IBD 2 in Table 3.

Application to ASCON. For ASCON- p [23], with the last linear layer omitted, our model finds 5-round IBDs. An example of the 5-round IBD is in Table 3, IBD 3.

Application to GIFT-64. For GIFT-64 [1], we consider both single-key and related-key settings. In the single-key setting, we obtain 6-round IBDs, see IBD 4 in Table 3. In the related-key setting, both upper and lower key-difference pairs are left free. We obtain 12-round IBDs by adding a key-XOR before the first round, see IBD 5 in Table 3.

Application to SKINNY-64. For SKINNY-64 [2], we consider the related-(twea)key settings without the first SC operation. By leaving the upper and lower key-difference pairs free, we obtain 11-, 14-, and 18-round IBDs for SKINNY-64-64, SKINNY-64-128, SKINNY-64-192, respectively, see IBDs 6, 7, and 8 in Table 3.

4.4 Cancellation Impossibility and Further Results

Section 4.1 explained the direct-impossibility case at the difference level: if no BQC exists between the input and output difference pairs, then the corresponding boomerang is impossible. The exact 4-wise framework also naturally covers the complementary case, in which valid BQCs do exist, but the boomerang is still

³ <https://boolector.github.io>

Table 3: Example IBDs for several ciphers. (a_1, a'_1) and (a_{r+1}, a'_{r+1}) denote the input and output difference pairs of the IBD, respectively. (Δ_k, Δ'_k) and (∇_k, ∇'_k) denote the master-key(tweakey) difference pair of the upper and lower part, respectively. The leftmost bit represents the most significant bit.

IBD 1: 6-round SK-IBD of PRESENT-80.			
a_1	a'_1	a_{r+1}	a'_{r+1}
0000000000001000	0008000000000000	0000000000000500	0000000000000400
IBD 2: 8-round RK-IBD of PRESENT-80.			
a_1	a'_1	a_{r+1}	a'_{r+1}
0000000000000040	0000000000000040	0000050000000000	0000050000000000
Δ_k	Δ'_k	∇_k	∇'_k
0000000000000400000	00000000000000400000	000000000000000000	000000000000000000
IBD 3: 5-round IBD of ASCON- p .			
a_1	a'_1	a_{r+1}	a'_{r+1}
0000000000000000	0000000000000000	0000000000000000	0000000000000000
0000000000000000	2000000000000000	0000000000000000	0000000000000000
0000000000200000	2000000000000000	0000000000000000	0000000000000000
0000000000000000	2000000000000000	0000000000000000	0000000000000000
0000000000000000	2000000000000000	0000000000000010	0000000000000010
IBD 4: 6-round SK-IBD of GIFT-64.			
a_1	a'_1	a_{r+1}	a'_{r+1}
0000c000c000c000	0000000e0000000e	0400014001200420	0020040000400160
IBD 5: 12-round RK-IBD of GIFT-64.			
a_1	a'_1	a_{r+1}	a'_{r+1}
0003000000000000	0001000000000000	0000000003000000	0000000000100000
Δ_k	Δ'_k	∇_k	∇'_k
0000000000000000	0000000000000000	0000000000000000	0000000000000000
0000000010001000	0000000000001000	0080000010001000	0080000000001000
IBD 6: 11-round RK-IBD of SKINNY-64-64.			
a_1	a'_1	a_{r+1}	a'_{r+1}
0000000000000800	0000000000000100	0000000100000000	0000000800000000
Δ_k	Δ'_k	∇_k	∇'_k
0000000000000800	0000000000000100	0000000000000100	0000000000000800
IBD 7: 14-round RK-IBD of SKINNY-64-128.			
a_1	a'_1	a_{r+1}	a'_{r+1}
0000000030000000	0000000030000000	00000d0000000000	00000d0000000000
Δ_k	Δ'_k	∇_k	∇'_k
00000000c0000000	00000000c0000000	0000c0000c000400	0000c0000c000400
00000000f0000000	00000000f0000000	0000400002000600	0000400002000600
IBD 8: 18-round RK-IBD of SKINNY-64-192.			
a_1	a'_1	a_{r+1}	a'_{r+1}
0000000000000200	0000000000000200	000000c000000000	000000c000000000
Δ_k	Δ'_k	∇_k	∇'_k
1000000000000400	1000000000000400	0000080000400000	0000080000400000
d000000000000a00	d000000000000a00	0000050000700000	0000050000700000
7000000000000c00	7000000000000c00	00000d0000700000	00000d0000700000

impossible at the value level. We refer to this case as *cancellation impossibility*, in accordance with the discussion in Section 4.1.

Quartet-level modeling in the 4-wise framework. To study this second case, the difference-level positive model is no longer sufficient. Indeed, the impossibility is no longer explained by the absence of valid difference propagation, but by the fact that no compatible quartet exists for the fixed input/output candidates. Therefore, we refine the search from difference pairs to quartet variables and model the boomerang directly at the value level.

In our 4-wise language, such a quartet can be represented by two differences together with two values, namely (x_1, x_3, a, a') , which is essentially equivalent to the state-based modeling used by Hu et al. [30]. Thus, rather than explicitly enumerating quasi-BQCs and checking the cancellation of their correlations, we formulate an UNSAT-based search model on quartets: if no quartet satisfies the propagation constraints under the fixed input/output candidates for all keys, then the corresponding boomerang distinguisher is impossible.

This viewpoint is fully consistent with the exact 4-wise framework. It provides a quartet-level realization of the same boomerang event and naturally complements the difference-level positive model developed in the previous subsections.

Results for GIFT-64 and SKINNY-64-192. We applied this quartet-level model to the longer distinguishers reported by Hu et al. [30], in particular for GIFT-64 and SKINNY-64-192. As in their work, the modeling exploits the linear key schedule in the related-key setting. The key schedule is used to enforce several rounds of all-zero propagation in the upper and lower parts, so that only a small number of middle rounds contain non-zero differences. These middle rounds form the *core* of the distinguisher, where the round-key differences introduce only one active cell at the input and output of the core, respectively.

Based on this structure, we build the quartet constraints for the core rounds and connect them with the deterministic zero-difference propagation induced by the linear key schedule. In this way, the search remains focused on the quartet-level feasibility of the core, while still describing the full distinguisher within a unified 4-wise formulation.

We implemented the above quartet-level model and compared the results with those of Hu et al. [30]. The comparison shows that our framework not only recovers their distinguishers, but also finds additional ones in the same setting. For SKINNY-64-192, Hu et al. reported 3 19-round IBDs, whereas our model finds 5 in total. All of these 5 IBDs are given in Appendix A. For GIFT-64, we find 48 13-round IBDs, as Hu et al.’s result. All of these 48 IBDs are given in Appendix B. Therefore, even when restricted to the same quartet-level search setting, the exact 4-wise framework leads to a larger set of valid IBDs for the cipher instances.

These results further illustrate the practical strength of the 4-wise framework. On the one hand, the positive model of Section 4.2 efficiently captures direct impossibility at the difference level. On the other hand, the quartet-level model developed here handles longer distinguishers that rely on value-level infeasibility, as in [30].

5 Applications to Boomerang Distinguishers

As a direct application of the exact 4-wise framework developed in Section 3, the fixed-key probability of a boomerang distinguisher is obtained by summing the correlations of all compatible quasi-BQCs. In this section, we use this result to compute the exact fixed-key probabilities and to verify concrete boomerang distinguishers.

In Subsection 5.1, we describe the search procedure for BQCs and quasi-BQCs and derive the corresponding key dependencies. In Subsection 5.2, we first use a 3-round toy example to illustrate the computation. Then we study two boomerang distinguishers of SKINNY-64-128 and SKINNY-64-192. In both cases, the unequal-difference BQCs and their corresponding quasi-BQCs make non-negligible contributions to the fixed-key probability, whereas the 3-wise framework [17] only captures the equal-difference case and therefore underestimates the probability.

5.1 Probability Calculation in the Fixed-Key Model

Section 3 gives the definitions of BQC and quasi-BQC. Proposition 1 gives the exact probability of a BQC and motivates a two-step search procedure.

- (1) For an r -round cipher $F = F_r \circ \dots \circ F_m \circ \dots \circ F_1$, a BQC is a sequence of difference pairs

$$((a_1, a'_1), \dots, (a_{r+1}, a'_{r+1})).$$

Under the round-independence assumption $u_0^{(i)} = u_1^{(i)} = 0$ for $i = 1, \dots, r+1$, the probability of a BQC is given by (9). After fixing (a_1, a'_1) and (a_{r+1}, a'_{r+1}) , we first enumerate all BQCs.

- (2) For each BQC, a corresponding quasi-BQC is a sequence of the form

$$((0, 0, a_1, a'_1), (u_0^{(2)}, u_1^{(2)}, a_2, a'_2), \dots, (u_0^{(r)}, u_1^{(r)}, a_r, a'_r), (0, 0, a_{r+1}, a'_{r+1})). \quad (11)$$

By Definition 4, the correlation of such a quasi-BQC is

$$B_{(u_0^{(2)}, u_1^{(2)}, a_2, a'_2), (0, 0, a_1, a'_1)}^{F_0} \prod_{i=2}^{r-1} B_{\Omega_{i+1}, \Omega_i} B_{(0, 0, a_{r+1}, a'_{r+1}), (u_0^{(r)}, u_1^{(r)}, a_r, a'_r)}^{F_r}, \quad (12)$$

where $\Omega_i = (u_0^{(i)}, u_1^{(i)}, a_i, a'_i)$. We then enumerate all quasi-BQCs corresponding to each BQC and sum their correlations.

For a key-alternating cipher with round function $F_i = F_k^{(i)} \circ G_i$, each quasi-BQC yields one-bit of linear key expression by (10):

$$\bigoplus_{i=1}^r (u_0^{(i+1)})^\top k_1^{(i)} \oplus (u_1^{(i+1)})^\top k_3^{(i)}. \quad (13)$$

Suppose the total number of quasi-BQCs is l . Then we obtain l linear key conditions. If their rank is l' after Gaussian elimination, then the key space is divided into $2^{l'}$ subspaces, and the exact probability is computed in each key subspace by summing the correlations of all quasi-BQCs.

5.2 Applications to Boomerang Distinguishers

In this subsection, we first use a 3-round toy example of **SKINNY**-64 to explain the two-step search for BQCs and quasi-BQCs, the derivation of key conditions, and the computation of the exact probability. We then analyze two boomerang distinguishers for **SKINNY**-64.

Example 1. Consider the 3-round toy boomerang characteristic of **SKINNY**-64 in the single-key setting (see Figure 3), proposed in [21, Figure 3]. This

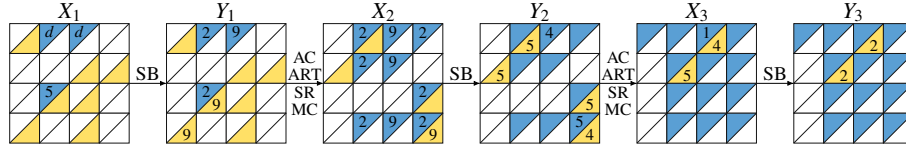


Fig. 3: A 3-round example boomerang distinguisher of **SKINNY**-64.

3-round example acts on a 64-bit state, with one 4-bit **SKINNY** S-box per cell (SB), followed by the linear layer (AC, SR, and MC) and the round-(tweak)key XOR (ART). In Figure 3, $\blacktriangle$ and $\blacktriangleleft$ denote the deterministically active cells in the upper and lower parts, respectively, and the hexadecimal values indicate the difference values.

Following Section 3, we decompose the 3-round function as $F = F_1 \circ F_m \circ F_0$, where F_m is the middle S-box layer corresponding to the transition $X_2 \rightarrow Y_2$. F_1 and F_0 are the upper/lower parts, corresponding to $X_1 \rightarrow X_2$ and $Y_2 \rightarrow Y_3$, respectively. Using the prescribed differences in Figure 3, we search for BQCs and quasi-BQCs using the SMT solver **Boolector**.

BQC enumeration. By setting all value coordinates to zero ($u_0^{(i)} = u_1^{(i)} = 0$), we enumerate all BQCs compatible with the given difference values, and obtain one BQC with correlation 2^{-21} .

Quasi-BQC enumeration. For this BQC, we fix the difference coordinates and enumerate all corresponding quasi-BQCs according to (12). We obtain 64 quasi-BQCs with correlation 2^{-21} , 64 quasi-BQCs with correlation -2^{-21} , 128 quasi-BQCs with correlation 2^{-22} , and 128 quasi-BQCs with correlation -2^{-22} .

Key dependencies. In total, we obtain 384 quasi-BQCs, yielding 384 key conditions (including the all-zero mask). After Gaussian elimination, the rank of these conditions is $l' = 1$. The resulting master-key condition is $k_{63} = 1$. Therefore, the key space is divided into two subspaces of size 2^{63} . The fixed-key probability is

$$\begin{cases} 128 \times 2^{-21} + 256 \times 2^{-22} = 2^{-13}, & k_{63} = 1 \\ 0, & k_{63} = 0 \end{cases}$$

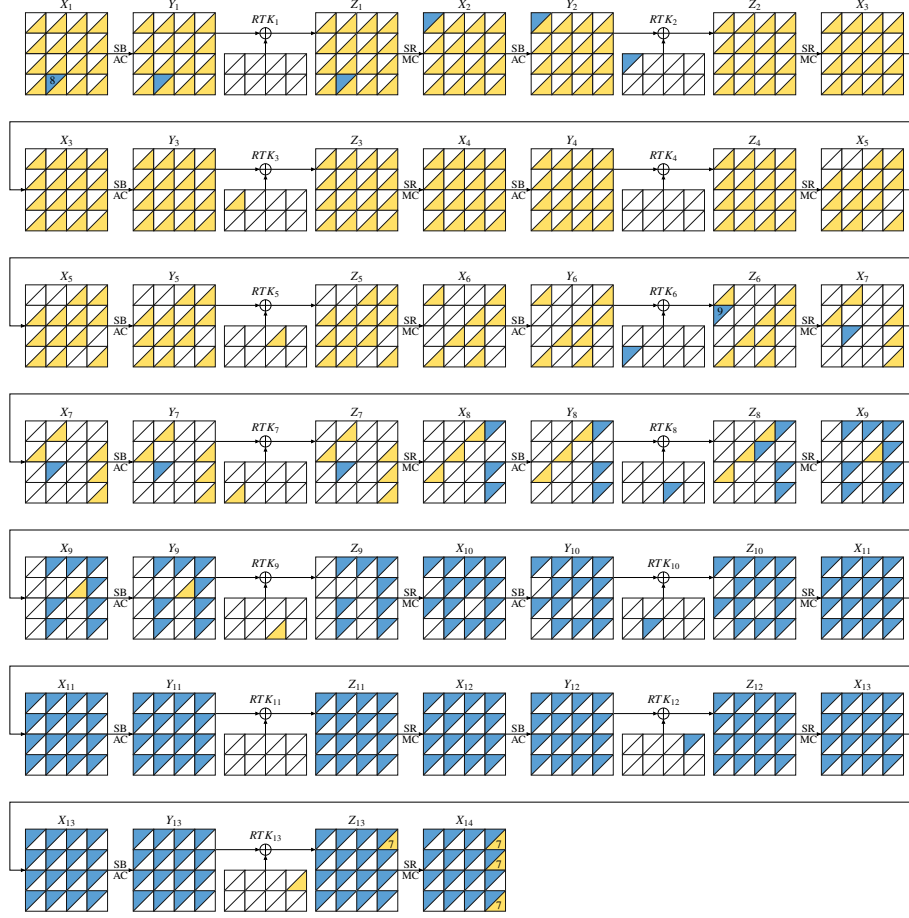


Fig. 4: The 13-round boomerang distinguisher of SKINNY-64-128.

The experiment probability is approximately 2^{-13} for $k_{63} = 1$ and 0 otherwise, whereas the state probability reported in [21] is 2^{-16} .

Application to 13-round SKINNY-64-128. We next consider the 13-round boomerang distinguisher of SKINNY-64-128 (see Figure 4), generated by the tool of Hadipour et al. [25]. Its theoretical probability under the BCT framework is estimated as $2^{-4.84}$. We decompose it as $F = F_1 \circ F_m \circ F_0$, where F_m is the middle S-box layer in the 7th round, i.e., the transition $X_7 \rightarrow Y_7$. The upper and lower parts F_0 and F_1 , cover 6 rounds each. The input quartet is fixed as

$$\Omega_1 = (0, 0, 0x0080000000000000, 0x0080000000000000),$$

and the output quartet is fixed as

$$\Omega_{14} = (0, 0, 0x7000000070007000, 0x7000000070007000).$$

The upper and lower master-(tweak)key differences are

$$\begin{aligned}\Delta_{k(1)} &= 0x000000c000000000||0x000000f000000000, \\ \Delta'_{k(1)} &= 0x000000c000000000||0x000000f000000000, \\ \nabla_{k(1)} &= 0x00000000000000d0||0x0000000000000020, \\ \nabla'_{k(1)} &= 0x00000000000000d0||0x0000000000000020.\end{aligned}$$

After enumerating all BQCs and quasi-BQCs and deriving the key conditions, we find that this boomerang distinguisher is key-independent. Its exact probability is $2^{-4.83}$, which is consistent with our experimental result. The detailed enumeration results are given in Table 4.

Comparison with the 3-wise framework [17]. The 3-wise framework [17] only covers the equal-difference case and misses the unequal-difference case. Restricting the search to boomerang characteristics (BCs) and quasi-BCs, as in the 3-wise framework, yields a probability of $2^{-6.68}$, whereas our exact probability is $2^{-4.83}$. The gap is entirely due to the unequal-difference contributions.

Table 4: Comparison between our 4-wise framework and the 3-wise framework [17] for the 13-round SKINNY-64-128 boomerang distinguisher.

correlation	2^{-16}	2^{-17}	2^{-18}	2^{-19}	2^{-20}	2^{-21}	2^{-22}
#BC	8	-	40	-	64	-	32
#BQC	16	32	80	128	128	128	64
#Quasi-BC	8×16	-	32×32 + 8×16	-	32×64 + 32×32	-	32×64
#Quasi-BQC	16×16	32×16	16×16 + 64×32	128×32	64×32 + 64×64	128×64	64×64

Application to 17-round SKINNY-64-192. We next consider the 17-round SKINNY-64-192 boomerang distinguisher (see Figure 5), generated by the tool [25], whose theoretical probability under the BCT framework is $2^{-5.35}$. We decompose it as $F = F_1 \circ F_m \circ F_0$, where F_m is the middle S-box layer in the 9th round, i.e., the transition $X_9 \rightarrow Y_9$. The upper and lower parts, F_0 and F_1 , cover 8 rounds each. The input and output quartets are fixed as

$$\begin{aligned}\Omega_1 &= (0, 0, 0x0400000000000000, 0x0400000000000000), \\ \Omega_{18} &= (0, 0, 0x0000000800000000, 0x0000000800000000).\end{aligned}$$

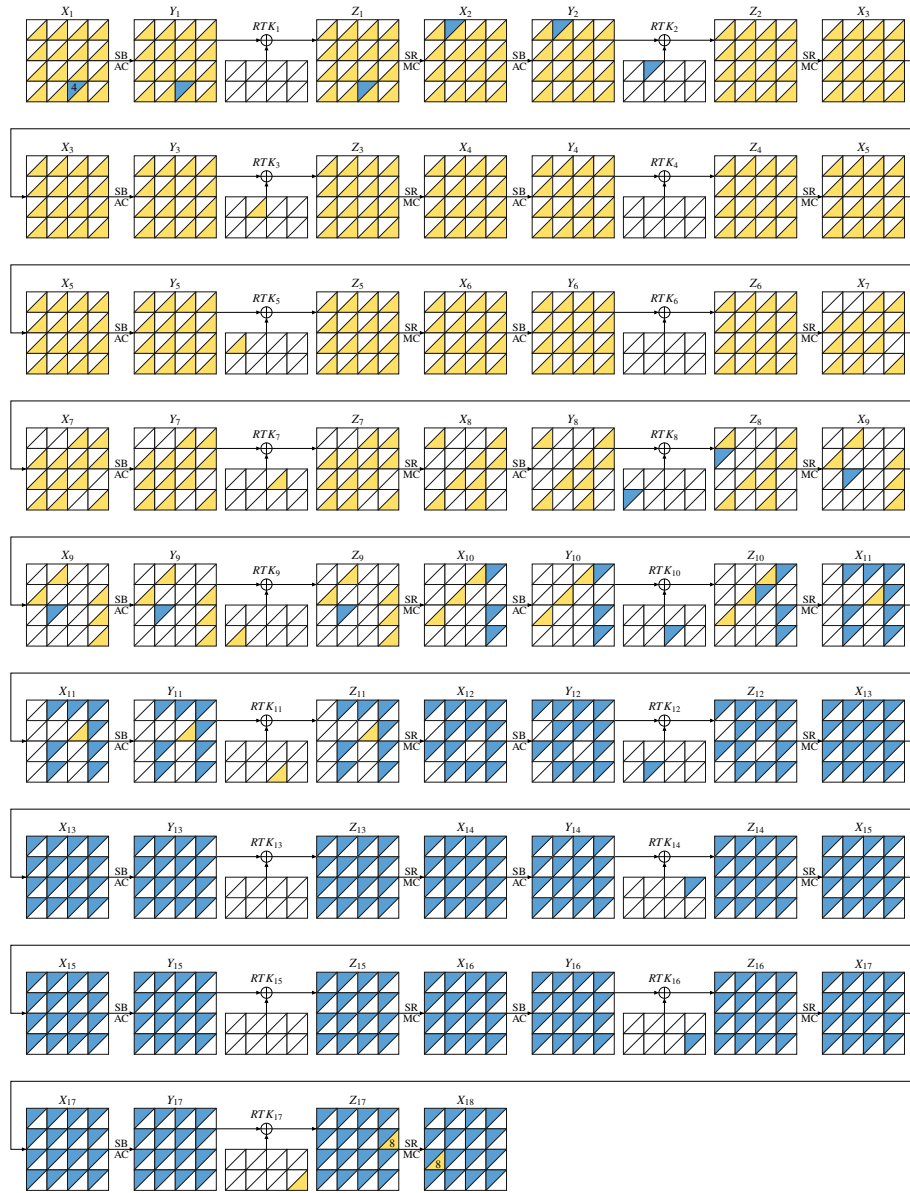


Fig. 5: The 17-round boomerang distinguisher of SKINNY-64-192.

The upper and lower master-(tweak)key differences are

$$\begin{aligned}
 \Delta_k^{(1)} &= 0xe000000000000000||0xd000000000000000||0xf000000000000000, \\
 \Delta_k'^{(1)} &= 0xe000000000000000||0xd000000000000000||0xf000000000000000, \\
 \nabla_k^{(1)} &= 0x00000000a0000000||0x00000000e0000000||0x0000000070000000, \\
 \nabla_k'^{(1)} &= 0x00000000a0000000||0x00000000e0000000||0x0000000070000000.
 \end{aligned}$$

After enumerating all BQCs and quasi-BQCs and deriving the key conditions, we find that this boomerang distinguisher is key-independent. Its exact probability is $2^{-5.35}$, which is consistent with our experimental result. The detailed results are given in Table 5.

Comparison with the 3-wise framework [17]. Restricting the computation to BCs and quasi-BCs, as in the 3-wise framework (see Table 5), gives a probability of $2^{-6.91}$, whereas our exact probability is $2^{-5.35}$. Again, the gap is due to the unequal-difference contributions.

Table 5: Comparison between our 4-wise framework and the 3-wise framework [17] for the 17-round SKINNY-64-192 boomerang distinguisher.

correlation	2^{-18}	2^{-20}	2^{-22}	2^{-24}
#BC	32	64	32	64
#BQC	64	256	320	128
#Quasi-BC	32×32	64×64	32×32	64×64
#Quasi-BQC	64×32	$128 \times 64 + 128 \times 32$	$64 \times 32 + 256 \times 64$	128×64

6 Acknowledgments.

We sincerely thank the anonymous reviewers for providing valuable comments to help us improve the overall quality of the paper.

References

1. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A small present - towards reaching the limit of lightweight encryption. In: Fischer, W., Homma, N. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. pp. 321-345. Lecture Notes in Computer Science, Springer (2017). https://doi.org/10.1007/978-3-319-66787-4_16, https://doi.org/10.1007/978-3-319-66787-4_16
2. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. pp. 123-153. Lecture Notes in Computer Science, Springer (2016). https://doi.org/10.1007/978-3-662-53008-5_5, https://doi.org/10.1007/978-3-662-53008-5_5
3. Beyne, T.: A geometric approach to linear cryptanalysis. In: Tibouchi, M., Wang, H. (eds.) 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. pp. 36-66. Lecture Notes in Com-

- puter Science, Springer (2021). https://doi.org/10.1007/978-3-030-92062-3_2, https://doi.org/10.1007/978-3-030-92062-3_2
4. Beyne, T.: A geometric approach to symmetric-key cryptanalysis. PhD thesis, KU Leuven (2021)
5. Beyne, T., Rijmen, V.: Differential cryptanalysis in the fixed-key model. In: Dodis, Y., Shrimpton, T. (eds.) *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022*, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III. pp. 687–716. *Lecture Notes in Computer Science*, Springer (2022). https://doi.org/10.1007/978-3-031-15982-4_23, https://doi.org/10.1007/978-3-031-15982-4_23
6. Beyne, T., Verbaauwhede, M.: Integral cryptanalysis using algebraic transition matrices. *IACR Trans. Symmetric Cryptol.* **2023**(4), 244–269 (2023). <https://doi.org/10.46586/TOSC.V2023.I4.244-269>, <https://doi.org/10.46586/tosc.v2023.i4.244-269>
7. Beyne, T., Verbaauwhede, M.: Ultrametric integral cryptanalysis. *IACR Cryptol. ePrint Arch.* **2024**, 722 (2024), <https://eprint.iacr.org/2024/722>
8. Beyne, T., Verbaauwhede, M.: Ultrametric integral cryptanalysis. In: Chung, K., Sasaki, Y. (eds.) *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security*, Kolkata, India, December 9-13, 2024, Proceedings, Part VII. pp. 392–423. *Lecture Notes in Computer Science*, Springer (2024). https://doi.org/10.1007/978-981-96-0941-3_13, https://doi.org/10.1007/978-981-96-0941-3_13
9. Biham, E., Dunkelman, O., Keller, N.: The rectangle attack - rectangling the serpent. In: Pfitzmann, B. (ed.) *Advances in Cryptology - EUROCRYPT 2001*, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding. pp. 340–357. *Lecture Notes in Computer Science*, Springer (2001). https://doi.org/10.1007/3-540-44987-6_21, https://doi.org/10.1007/3-540-44987-6_21
10. Biham, E., Dunkelman, O., Keller, N.: New results on boomerang and rectangle attacks. In: Daemen, J., Rijmen, V. (eds.) *Fast Software Encryption, 9th International Workshop, FSE 2002*, Leuven, Belgium, February 4-6, 2002, Revised Papers. pp. 1–16. *Lecture Notes in Computer Science*, Springer (2002). https://doi.org/10.1007/3-540-45661-9_1, https://doi.org/10.1007/3-540-45661-9_1
11. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. *J. Cryptol.* **4**(1), 3–72 (1991). <https://doi.org/10.1007/BF00630563>, <https://doi.org/10.1007/BF00630563>
12. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) *Advances in Cryptology - ASIACRYPT 2009*, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings. pp. 1–18. *Lecture Notes in Computer Science*, Springer (2009). https://doi.org/10.1007/978-3-642-10366-7_1, https://doi.org/10.1007/978-3-642-10366-7_1
13. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbaauwhede, I. (eds.) *Cryptographic Hardware and Embedded Systems - CHES 2007*, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings. pp. 450–466. *Lecture Notes in Computer Science*, Springer (2007). https://doi.org/10.1007/978-3-540-74735-2_31, https://doi.org/10.1007/978-3-540-74735-2_31

14. Bonnetain, X., Cordero, M., Lallemand, V., Minier, M., Naya-Plasencia, M.: On impossible boomerang attacks application to simon and skinny. *IACR Trans. Symmetric Cryptol.* **2024**(2), 222–253 (2024). <https://doi.org/10.46586/TOSC.V2024.I2.222-253>, <https://doi.org/10.46586/tosc.v2024.i2.222-253>
15. Bonnetain, X., Lallemand, V.: A note on the use of the double boomerang connectivity table (DBCT) for spotting impossibilities. *IACR Cryptol. ePrint Arch.* **2024**, 1218 (2024), <https://eprint.iacr.org/2024/1218>
16. Chakraborty, D., Hadipour, H., Nguyen, P.H., Eichlseder, M.: Finding complete impossible differential attacks on andrx ciphers and efficient distinguishers for ARX designs. *IACR Trans. Symmetric Cryptol.* **2024**(3), 84–176 (2024). <https://doi.org/10.46586/TOSC.V2024.I3.84-176>, <https://doi.org/10.46586/tosc.v2024.i3.84-176>
17. Chang, C., Hadipour, H., Hu, K., Li, M., Wang, M.: Mix-basis geometric approach to boomerang distinguishers. *IACR Trans. Symmetric Cryptol.* **2025**(3), 693–728 (2025). <https://doi.org/10.46586/TOSC.V2025.I3.693-728>, <https://doi.org/10.46586/tosc.v2025.i3.693-728>
18. Chen, Y., Fu, Q., Zhao, N., Zhao, J., Song, L., Yang, Q.: A holistic framework for impossible boomerang attacks. *IACR Commun. Cryptol.* **2**(2), 18 (2025). <https://doi.org/10.62056/ABHEE0ZN4>, <https://doi.org/10.62056/abhee0zn4>
19. Choy, J., Yap, H.: Impossible boomerang attack for block cipher structures. In: Takagi, T., Mambo, M. (eds.) *Advances in Information and Computer Security, 4th International Workshop on Security, IWSEC 2009, Toyama, Japan, October 28–30, 2009, Proceedings*. pp. 22–37. *Lecture Notes in Computer Science*, Springer (2009). https://doi.org/10.1007/978-3-642-04846-3_3, https://doi.org/10.1007/978-3-642-04846-3_3
20. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: A new cryptanalysis tool. In: Nielsen, J.B., Rijmen, V. (eds.) *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*. pp. 683–714. *Lecture Notes in Computer Science*, Springer (2018). https://doi.org/10.1007/978-3-319-78375-8_22, https://doi.org/10.1007/978-3-319-78375-8_22
21. Delaune, S., Derbez, P., Vavrille, M.: Catching the fastest boomerangs application to SKINNY. *IACR Trans. Symmetric Cryptol.* **2020**(4), 104–129 (2020). <https://doi.org/10.46586/TOSC.V2020.I4.104-129>, <https://doi.org/10.46586/tosc.v2020.i4.104-129>
22. Derbez, P., Euler, M.: Minimalist model for impossible differentials. In: Boura, C., Mashatan, A., Miri, A. (eds.) *Selected Areas in Cryptography - SAC 2025 - 32nd International Conference, Toronto, ON, Canada, August 13–15, 2025, Revised Selected Papers*. pp. 113–143. *Lecture Notes in Computer Science*, Springer (2025). https://doi.org/10.1007/978-3-032-10536-3_5, https://doi.org/10.1007/978-3-032-10536-3_5
23. Dobraunig, C., Eichlseder, M., Mendel, F., Schl  ffer, M.: Ascon v1.2: Lightweight authenticated encryption and hashing. *J. Cryptol.* **34**(3), 33 (2021). <https://doi.org/10.1007/S00145-021-09398-9>, <https://doi.org/10.1007/s00145-021-09398-9>
24. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3g telephony. In: Rabin, T. (ed.) *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15–19, 2010. Proceedings*. pp. 393–410. *Lec-*

- ture Notes in Computer Science, Springer (2010). https://doi.org/10.1007/978-3-642-14623-7_21, https://doi.org/10.1007/978-3-642-14623-7_21
25. Hadipour, H., Bagheri, N., Song, L.: Improved rectangle attacks on SKINNY and CRAFT. *IACR Trans. Symmetric Cryptol.* **2021**(2), 140–198 (2021). <https://doi.org/10.46586/TOSC.V2021.I2.140-198>, <https://doi.org/10.46586/tosc.v2021.i2.140-198>
 26. Hadipour, H., Gerhalter, S., Sadeghi, S., Eichlseder, M.: Improved search for integral, impossible differential and zero-correlation attacks application to ascon, fork-skinny, skinny, mantis, PRESENT and qarmav2. *IACR Trans. Symmetric Cryptol.* **2024**(1), 234–325 (2024). <https://doi.org/10.46586/TOSC.V2024.I1.234-325>, <https://doi.org/10.46586/tosc.v2024.i1.234-325>
 27. Hadipour, H., Sadeghi, S., Eichlseder, M.: Finding the impossible: Automated search for full impossible-differential, zero-correlation, and integral attacks. In: Hazay, C., Stam, M. (eds.) *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Lyon, France, April 23-27, 2023, Proceedings, Part IV. pp. 128–157. *Lecture Notes in Computer Science*, Springer (2023). https://doi.org/10.1007/978-3-031-30634-1_5, https://doi.org/10.1007/978-3-031-30634-1_5
 28. Hu, K., Niu, Z., Wang, M.: Round-based approximation of (higher-order) differential-linear correlation. *IACR Cryptol. ePrint Arch.* **2026**, 358 (2026), <https://eprint.iacr.org/2026/358>
 29. Hu, K., Zhang, C., Chang, C., Zhang, J., Wang, M., Peyrin, T.: Unlocking mix-basis potential: Geometric approach for combined attacks. In: Kalai, Y.T., Kamara, S.F. (eds.) *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part V. pp. 293–334. *Lecture Notes in Computer Science*, Springer (2025). https://doi.org/10.1007/978-3-032-01901-1_10, https://doi.org/10.1007/978-3-032-01901-1_10
 30. Hu, X., Feng, D., Jiao, L., Hao, Y., Gong, X., Li, Y.: A deep study of the impossible boomerang distinguishers: New construction theory and automatic search methods. *IACR Cryptol. ePrint Arch.* **2024**, 1008 (2024), <https://eprint.iacr.org/2024/1008>
 31. Hu, X., Jiao, L.: Partial-guess, pre-sieve, greedy-search - new unified key recovery framework of impossible boomerang attacks: Full-round attack on ARADI. *IACR Cryptol. ePrint Arch.* **2025**, 56 (2025), <https://eprint.iacr.org/2025/056>
 32. Hu, X., Li, Y., Jiao, L., Tian, S., Wang, M.: Mind the propagation of states - new automatic search tool for impossible differentials and impossible polytopic transitions. In: Moriai, S., Wang, H. (eds.) *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security*, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I. pp. 415–445. *Lecture Notes in Computer Science*, Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_14, https://doi.org/10.1007/978-3-030-64837-4_14
 33. Kelsey, J., Kohno, T., Schneier, B.: Amplified boomerang attacks against reduced-round MARS and serpent. In: Schneier, B. (ed.) *Fast Software Encryption, 7th International Workshop, FSE 2000*, New York, NY, USA, April 10-12, 2000, Proceedings. pp. 75–93. *Lecture Notes in Computer Science*, Springer (2000). https://doi.org/10.1007/3-540-44706-7_6, https://doi.org/10.1007/3-540-44706-7_6

34. Kidmose, A.B., Tiessen, T.: A formal analysis of boomerang probabilities. *IACR Trans. Symmetric Cryptol.* **2022**(1), 88–109 (2022). <https://doi.org/10.46586/TOSC.V2022.I1.88-109>, <https://doi.org/10.46586/tosc.v2022.i1.88-109>
35. Kircanski, A.: Analysis of boomerang differential trails via a sat-based constraint solver URSA. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) *Applied Cryptography and Network Security - 13th International Conference, ACNS 2015, New York, NY, USA, June 2-5, 2015, Revised Selected Papers*. pp. 331–349. *Lecture Notes in Computer Science*, Springer (2015). https://doi.org/10.1007/978-3-319-28166-7_16, https://doi.org/10.1007/978-3-319-28166-7_16
36. Lai, X., Massey, J.L., Murphy, S.: Markov ciphers and differential cryptanalysis. In: Davies, D.W. (ed.) *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of Cryptographic Techniques*, Brighton, UK, April 8-11, 1991, *Proceedings*. pp. 17–38. *Lecture Notes in Computer Science*, Springer (1991). https://doi.org/10.1007/3-540-46416-6_2, https://doi.org/10.1007/3-540-46416-6_2
37. Lu, J.: *Cryptanalysis of block ciphers*. PhD thesis, University of London (2008)
38. Lu, J.: The (related-key) impossible boomerang attack and its application to the AES block cipher. *Des. Codes Cryptogr.* **60**(2), 123–143 (2011). <https://doi.org/10.1007/S10623-010-9421-9>, <https://doi.org/10.1007/s10623-010-9421-9>
39. Murphy, S.: The return of the cryptographic boomerang. *IEEE Trans. Inf. Theory* **57**(4), 2517–2521 (2011). <https://doi.org/10.1109/TIT.2011.2111091>, <https://doi.org/10.1109/TIT.2011.2111091>
40. Song, L., Qin, X., Hu, L.: Boomerang connectivity table revisited. application to SKINNY and AES. *IACR Trans. Symmetric Cryptol.* **2019**(1), 118–141 (2019). <https://doi.org/10.13154/TOSC.V2019.I1.118-141>, <https://doi.org/10.13154/tosc.v2019.i1.118-141>
41. Tiessen, T.: Polytopic cryptanalysis. In: Fischlin, M., Coron, J. (eds.) *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Vienna, Austria, May 8-12, 2016, *Proceedings, Part I*. pp. 214–239. *Lecture Notes in Computer Science*, Springer (2016). https://doi.org/10.1007/978-3-662-49890-3_9, https://doi.org/10.1007/978-3-662-49890-3_9
42. Wagner, D.A.: The boomerang attack. In: Knudsen, L.R. (ed.) *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*. pp. 156–170. *Lecture Notes in Computer Science*, Springer (1999). https://doi.org/10.1007/3-540-48519-8_12, https://doi.org/10.1007/3-540-48519-8_12
43. Wang, H., Peyrin, T.: Boomerang switch in multiple rounds. application to AES variants and deoxys. *IACR Trans. Symmetric Cryptol.* **2019**(1), 142–169 (2019). <https://doi.org/10.13154/TOSC.V2019.I1.142-169>, <https://doi.org/10.13154/tosc.v2019.i1.142-169>
44. Wang, L., Song, L., Wu, B., Rahman, M., Isobe, T.: Revisiting the boomerang attack from a perspective of 3-differential. *IEEE Trans. Inf. Theory* **70**(7), 5343–5357 (2024). <https://doi.org/10.1109/TIT.2023.3324738>, <https://doi.org/10.1109/TIT.2023.3324738>
45. Yang, Q., Song, L., Sun, S., Shi, D., Hu, L.: New properties of double boomerang connectivity table. *IACR Cryptol. ePrint Arch.* **2022**, 1579 (2022), <https://eprint.iacr.org/2022/1579>

46. Zhang, J., Wang, H., Tang, D.: Impossible boomerang attacks revisited: Applications to deoxys-bc, joltik-bc and SKINNY. IACR Cryptol. ePrint Arch. **2024**, 1230 (2024), <https://eprint.iacr.org/2024/1230>

A 19-Round IBDs of SKINNY-64-192

List of 5 19-round IBDs of SKINNY-64-192.

1. $(0000000000000002, 0000000000000002) \not\rightarrow (0000000000900000, 0000000000900000)$
 $(\Delta_{tk1}, \Delta'_{tk1}, \nabla_{tk1}, \nabla'_{tk1}):$
 $(0000000000000004, 0000000000000004, 0000000003000000, 0000000003000000)$
 $(\Delta_{tk2}, \Delta'_{tk2}, \nabla_{tk2}, \nabla'_{tk2}):$
 $(000000000000000a, 000000000000000a, 000000000e000000, 000000000e000000)$
 $(\Delta_{tk3}, \Delta'_{tk3}, \nabla_{tk3}, \nabla'_{tk3}):$
 $(000000000000000c, 000000000000000c, 000000000e000000, 000000000e000000)$

2. $(000000000000000a, 000000000000000a) \not\rightarrow (0000000000b00000, 0000000000b00000)$
 $(\Delta_{tk1}, \Delta'_{tk1}, \nabla_{tk1}, \nabla'_{tk1}):$
 $(0000000000000005, 0000000000000005, 0000000007000000, 0000000007000000)$
 $(\Delta_{tk2}, \Delta'_{tk2}, \nabla_{tk2}, \nabla'_{tk2}):$
 $(000000000000000c, 000000000000000c, 0000000009000000, 0000000009000000)$
 $(\Delta_{tk3}, \Delta'_{tk3}, \nabla_{tk3}, \nabla'_{tk3}):$
 $(0000000000000003, 0000000000000003, 0000000009000000, 0000000009000000)$

3. $(000000000000000d, 000000000000000d) \not\rightarrow (0000000000600000, 0000000000600000)$
 $(\Delta_{tk1}, \Delta'_{tk1}, \nabla_{tk1}, \nabla'_{tk1}):$
 $(000000000000000a, 000000000000000a, 000000000d000000, 000000000d000000)$
 $(\Delta_{tk2}, \Delta'_{tk2}, \nabla_{tk2}, \nabla'_{tk2}):$
 $(000000000000000e, 000000000000000e, 0000000008000000, 0000000008000000)$
 $(\Delta_{tk3}, \Delta'_{tk3}, \nabla_{tk3}, \nabla'_{tk3}):$
 $(0000000000000009, 0000000000000009, 0000000008000000, 0000000008000000)$

4. $(000000000000000d, 000000000000000d) \not\rightarrow (0000000000900000, 0000000000900000)$
 $(\Delta_{tk1}, \Delta'_{tk1}, \nabla_{tk1}, \nabla'_{tk1}):$
 $(000000000000000a, 000000000000000a, 0000000003000000, 0000000003000000)$
 $(\Delta_{tk2}, \Delta'_{tk2}, \nabla_{tk2}, \nabla'_{tk2}):$
 $(000000000000000e, 000000000000000e, 000000000e000000, 000000000e000000)$
 $(\Delta_{tk3}, \Delta'_{tk3}, \nabla_{tk3}, \nabla'_{tk3}):$
 $(0000000000000009, 0000000000000009, 000000000e000000, 000000000e000000)$

5. $(000000000000000d, 000000000000000d) \not\rightarrow (0000000000e00000, 0000000000e00000)$
 $(\Delta_{tk1}, \Delta'_{tk1}, \nabla_{tk1}, \nabla'_{tk1}):$
 $(000000000000000a, 000000000000000a, 000000000c000000, 000000000c000000)$
 $(\Delta_{tk2}, \Delta'_{tk2}, \nabla_{tk2}, \nabla'_{tk2}):$
 $(000000000000000e, 000000000000000e, 000000000d000000, 000000000d000000)$
 $(\Delta_{tk3}, \Delta'_{tk3}, \nabla_{tk3}, \nabla'_{tk3}):$
 $(0000000000000009, 0000000000000009, 000000000d000000, 000000000d000000)$

B 13-Round IBDs of GIFT-64

[illegible]

List of 64 13-round IBDs of GIFT-64 (Cont.)

-
- $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
 14. $(0200000000000000, 0200000000000000) \nrightarrow (0000000000002000, 0000000000002000)$
 $(\Delta_k, \Delta'_k): (00000000000000000000000040000000, 00000000000000000000000040000000)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
15. $(0200000100000000, 0200000100000000) \nrightarrow (0000000000002000, 0000000000002000)$
 $(\Delta_k, \Delta'_k): (00000000000000000000000040000100, 00000000000000000000000040000100)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
16. $(0000001000000000, 0000001000000000) \nrightarrow (2000000000000000, 2000000000000000)$
 $(\Delta_k, \Delta'_k): (000000000000000000000000000200, 000000000000000000000000000200)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
17. $(2000000000000000, 2000000000000000) \nrightarrow (2000000000000000, 2000000000000000)$
 $(\Delta_k, \Delta'_k): (00000000000000000000000080000000, 00000000000000000000000080000000)$
 $(\nabla_k, \nabla'_k): (00000000000000000000000080000000, 00000000000000000000000080000000)$
-
18. $(2000001000000000, 2000001000000000) \nrightarrow (2000000000000000, 2000000000000000)$
 $(\Delta_k, \Delta'_k): (00000000000000000000000080000200, 00000000000000000000000080000200)$
 $(\nabla_k, \nabla'_k): (00000000000000000000000080000000, 00000000000000000000000080000000)$
-
19. $(0000010000000000, 0000010000000000) \nrightarrow (0000200000000000, 0000200000000000)$
 $(\Delta_k, \Delta'_k): (000000000000000000000000000400, 000000000000000000000000000400)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
20. $(0000000000000002, 0000000000000002) \nrightarrow (0000200000000000, 0000200000000000)$
 $(\Delta_k, \Delta'_k): (00000000000000000000000000010000, 00000000000000000000000000010000)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
21. $(0000010000000002, 0000010000000002) \nrightarrow (0000200000000000, 0000200000000000)$
 $(\Delta_k, \Delta'_k): (00000000000000000000000000010400, 00000000000000000000000000010400)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
22. $(0000100000000000, 0000100000000000) \nrightarrow (0000000020000000, 0000000020000000)$
 $(\Delta_k, \Delta'_k): (0000000000000000000000000000800, 0000000000000000000000000000800)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
23. $(0000000000000020, 0000000000000020) \nrightarrow (0000000020000000, 0000000020000000)$
 $(\Delta_k, \Delta'_k): (00000000000000000000000000020000, 00000000000000000000000000020000)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
24. $(0000100000000020, 0000100000000020) \nrightarrow (0000000020000000, 0000000020000000)$
 $(\Delta_k, \Delta'_k): (00000000000000000000000000020800, 00000000000000000000000000020800)$
 $(\nabla_k, \nabla'_k): (000000000000000020000000000000, 000000000000000020000000000000)$
-
25. $(0100000000000000, 0100000000000000) \nrightarrow (0002000000000000, 0002000000000000)$
 $(\Delta_k, \Delta'_k): (0000000000000000000000000004000, 0000000000000000000000000004000)$
 $(\nabla_k, \nabla'_k): (000000000000000040000000000000, 000000000000000040000000000000)$
-
26. $(0000000000020000, 0000000000020000) \nrightarrow (0002000000000000, 0002000000000000)$
-

List of 64 13-round IBDs of GIFT-64 (Cont.)

[illegible]

List of 64 13-round IBDs of GIFT-64 (Cont.)

- [illegible]