Rotational-Quasidifferential Framework

A Geometric Approach to Rotational-XOR Cryptanalysis

Myungkyu Lee[1], Byoungjin Seok[2], Dongjae Lee[3], Deukjo Hong[4], Jaechul Sung[5] and Seokhie Hong[6]

[1] Korea University, Seoul, Republic of Korea
[2] Hansung University, Seoul, Republic of Korea
[3] Kangwon National University, Chuncheon, Republic of Korea
[4] Jeonbuk National University, Jeonju, Republic of Korea
[5] University of Seoul, Seoul, Republic of Korea
[6] SmartM2M, Busan, Republic of Korea

Abstract. Rotational-XOR (RX) cryptanalysis extends rotational cryptanalysis by combining rotational relations with XOR translations, enabling the analysis of symmetric-key primitives even in the presence of symmetry-breaking constants. Existing analyses of RX characteristics, however, typically rely on independence assumptions when estimating characteristic probabilities, which may lead to inaccurate probability evaluations and even incompatible characteristics. In this paper, we introduce the first application of the geometric approach to RX cryptanalysis. Inspired by the quasidifferential framework of Beyne and Rijmen, we define rotational-quasidifferential trails and derive exact expressions for fixed-key RX characteristic probabilities without relying on round-independence assumptions. We also derive explicit rotational-quasidifferential transition matrices for bitwise AND and modular addition. By incorporating the key schedule into the state space, we further obtain an exact expression for the Expected Rotational-XOR Probability (ERXP), the RX analogue of the Expected Differential Probability (EDP). We apply the framework to the ARX cipher SPECK, the ARX permutation Alzette, and the AND-RX ciphers SIMON and SIMECK. For SPECK, we repair an incompatible 12-round characteristic and show that the longest published RX characteristics for SPECK64/128, SPECK96/144, and SPECK128/256 are incompatible. For Alzette, we show that signed nonzero-mask contributions explain the discrepancy between independent-ADD estimates and experimentally observed full-data-path probabilities. For SIMECK, we experimentally verify a fixed-key probability distribution, explain incompatible characteristics, and correct the weak-key class estimates of rotational-XOR differential rectangle attacks. These results extend the geometric approach to both ARX and AND-RX designs and demonstrate its usefulness for exact characteristic-level analysis.

Keywords: RX cryptanalysis · Geometric approach · Fixed-key analysis · SPECK · Alzette · SIMON · SIMECK

1 Introduction

Rotational cryptanalysis was introduced by Khovratovich and Nikolić and later refined in subsequent work [KN10, KNP+15]. The technique exploits rotational properties arising in symmetric-key primitives and has been successfully applied to various ARX primitives. Early studies demonstrated its applicability to designs such as Threefish and Skein, while subsequent works extended the analysis to additional ARX constructions and improved the understanding of probability estimation in rotational distinguishers.

To overcome the limitations of rotational cryptanalysis in the presence of round constants, Ashur and Liu proposed Rotational-XOR (RX) cryptanalysis [AL16], which extends rotational cryptanalysis by incorporating XOR translations into the rotational relation. RX cryptanalysis enabled the analysis of ARX constructions in settings where constant injection disrupts ordinary rotational symmetry and has been applied to primitives such as SPECK [LWRA17] and SipHash [XLSL19]. Subsequent developments further generalized RX cryptanalysis beyond ARX designs to AND-RX constructions, including SIMON and SIMECK, showing that rotational cryptanalytic techniques remain applicable even when modular addition is replaced by the bitwise AND operation [LLA+20, LLA+22]. More recently, longer RX characteristics have been reported for several ARX ciphers [ZZZW25].

More generally, rotational techniques have been combined with other cryptanalytic paradigms. Examples include rotational-XOR differential rectangle attacks [CZX+23], rotational differential-linear cryptanalysis [LSL21, LNS+23], including extensions to arbitrary output masks and unified Walsh-transform formulations [NSLL22, HHN+26], and rotational-linear attacks [XWL21]. These developments demonstrate that rotational relations can serve as useful building blocks in a broader range of cryptanalytic techniques. Consequently, studying rotational cryptanalysis within a unified mathematical framework may also facilitate future investigations of related rotational cryptanalytic methods.

Cryptanalysis plays a central role in evaluating the security of symmetric-key primitives. Over the past decades, a wide variety of attack techniques have been developed, including differential [BS93], linear [Mat94], and integral [KW02] cryptanalysis. These techniques provide different perspectives on the behavior of a primitive and have become standard tools for assessing its security. Consequently, a cipher is generally regarded as secure only if it withstands all known forms of cryptanalysis with an adequate security margin.

Despite their common goal, these attacks are traditionally studied within separate theoretical frameworks. To address this issue, Beyne introduced the geometric approach, a unified framework for symmetric-key cryptanalysis based on linear operators acting on free vector spaces [Bey23]. The central idea is to represent a cryptographic primitive as a linear map on a high-dimensional vector space and to interpret cryptanalytic properties through suitable choices of basis. Within this framework, several cryptanalytic techniques can be viewed as different coordinate representations of the same underlying operator.

The geometric approach has successfully been applied to reinterpret linear [Bey21], differential [BR22], and (ultrametric) integral cryptanalysis [BV23, BV24], providing a unified description of techniques that were previously studied independently. Moreover, it has enabled the analysis of phenomena that are difficult to capture using classical approaches, including fixed-key differential properties [BR22] and divisibility properties [BV24] arising in integral cryptanalysis without relying on assumptions such as the Markov assumption or the hypothesis of stochastic equivalence [LMM91]. More recently, the framework was further extended through mix-basis configurations, allowing different bases to be used at the input and output spaces simultaneously [HZC+25, CHH+25]. Recent work on rotational differential-linear cryptanalysis also identifies the geometric approach as an independence-free, complementary direction [HHN+26], further motivating the study of rotational techniques in this framework.

Most analyses of rotational and RX cryptanalysis rely on assumptions such as the Markov assumption or the hypothesis of stochastic equivalence. In rotational cryptanalysis, Khovratovich *et al.* [KNP+15] revisited the probability estimates of [KN10] and showed that the independence assumption introduces a non-negligible error. To obtain more accurate estimates, they analyzed dependencies arising from chains of modular additions and derived refined probability evaluations.

Similar issues have also been observed in RX cryptanalysis. Lu *et al.* [LLA+20] proposed RX characteristics for AND-RX constructions, while Liu *et al.* [LWRA17] developed RX cryptanalysis of SPECK. Sadeghi *et al.* [SRB21] subsequently applied MILP-based

verification to characteristics of both SIMECK and SPECK and showed that some of them are incompatible. These results indicate that, similarly to differential cryptanalysis, independence assumptions may lead to inaccurate probability estimates and can even result in invalid trails.

At the operation level, Biryukov, Lambin, and Udovenko [BLU25] derived an exact formula for RX-differential probabilities through modular addition. Operation-level probabilities, however, do not by themselves determine the probability of an iterated RX characteristic, which is commonly estimated by multiplying transition probabilities under a round-independence assumption. MILP verification can test whether a prescribed characteristic is consistent, but it does not provide its exact probability when dependencies remain.

While the geometric approach has recently been applied to several cryptanalytic techniques, including differential [BR22], linear [Bey21], and integral cryptanalysis [BV23, BV24], rotational and RX cryptanalysis have not, to the best of our knowledge, been studied from this perspective. This motivates the development of a geometric framework for RX cryptanalysis.

Our Contributions. We introduce the first framework for rotational-XOR (RX) cryptanalysis based on the geometric approach. Inspired by the quasidifferential framework of Beyne and Rijmen [BR22], we define the rotational-quasidifferential basis, transition matrix (RQTM), and trail. The proposed framework inherits several desirable properties of the quasidifferential framework, including compositionality and tensor-product decomposition for boxed constructions. Furthermore, it provides an exact expression for the fixed-key probability of an RX characteristic as a sum of correlations of the rotational-quasidifferential trails, thereby removing the need for round-independence assumptions. In addition, we derive explicit RQTM expressions for both bitwise AND and modular addition.

We further incorporate key schedules into the framework by treating the key as part of the state space, following the approach of Boura, Derbez, and Germon [BDG25]. This naturally leads to the notion of *Expected Rotational-XOR Probability* (ERXP), which serves as the RX analogue of the Expected Differential Probability (EDP) in differential cryptanalysis. We derive an exact formula expressing the ERXP of an RX characteristic as a sum of correlations of the rotational-quasidifferential trails over the joint plaintext-key space.

We apply the proposed framework to the ARX cipher SPECK, the ARX permutation Alzette, and the AND-RX ciphers SIMON and SIMECK, and obtain several new results. For fixed-key validation, we analyze a segment of the 20-round SIMECK32/64 RX characteristic proposed by Lu *et al.* [LLA+20], derive its exact key-dependent probability, and experimentally verify the predicted probability distribution in Appendix A. For four-step Alzette RX characteristics reported in [BLU25], we evaluate the signed RQ sum across the complete data path. The nonzero-mask trails explain deviations of up to 2.40 bits from the product of the four local ADD probabilities, and the resulting estimates closely match the reported experiments. For SIMECK48/96 and SIMECK64/128, we revisit the incompatible RX characteristics identified by Sadeghi *et al.* [SRB21]. Our framework reproduces their incompatibility results. Moreover, for SIMECK48/96, we identify an additional constraint leading to incompatibility that was not reported in the original work, and for SIMECK64/128, we provide an explicit explanation of the incompatibility. For the 11- and 12-round RX characteristics of SPECK32/64 reported by Liu *et al.* [LWRA17], we reproduce the incompatibility results of Sadeghi *et al.* [SRB21] and show that the two characteristics fail for different reasons. We then repair the incompatible part of the 12-round trail and present a compatible 12-round RX characteristic together with an explicit right key and plaintext pair. We further analyze six SPECK RX characteristics

from [ZZZW25]; the RQ framework finds equal-magnitude, opposite-sign joint trails that prove five of them incompatible and localizes the responsible data/key regions. We revisit the rotational-XOR differential rectangle (RXDR) attacks against SIMECK48/96 proposed by Chen *et al.* [CZX+23]. Using our framework, we show that the weak-key class of the 21-round RXDR distinguisher has size 2^{70} rather than the claimed 2^{72}. In addition, we show that the weak-key class associated with the 17-round RX characteristic used in their 20-round RXDR distinguisher has size 2^{62} rather than 2^{64}.

Outline. The rest of the paper is organized as follows. In Section 2, we review the necessary background on RX cryptanalysis, the geometric approach, and the quasidifferential framework. In Section 3, we introduce the rotational-quasidifferential framework, including the rotational-quasidifferential basis, rotational-quasidifferential transition matrix, rotational-quasidifferential trails, and the notion of Expected Rotational-XOR Probability (ERXP). In Section 4, we analyze full-data-path RX probabilities for Alzette, reinterpret known incompatibilities in SIMECK and SPECK, identify further incompatible SPECK characteristics in the joint data-key setting, and re-evaluate RXDR attacks on SIMECK48/96. Finally, Section 5 concludes the paper.

Our complete source code is available at https://anonymous.4open.science/r/rotational-quasidifferential-31E8.

2 Preliminaries

2.1 Notations

For a vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, we write $x^\top$ for its transpose and $\mathrm{wt}(x)$ for its Hamming weight. For $x, y \in \mathbb{F}_2^n$, the expression $x^\top y$ denotes the standard inner product over $\mathbb{F}_2$. For $u, x \in \mathbb{F}_2^n$, we write $\chi_u(x) = (-1)^{u^\top x}$ for the additive character indexed by u. We write $x \preccurlyeq y$ if $x_i \le y_i$ for every i. Finally, $\vee$ and $\wedge$ denote bitwise OR and bitwise AND, respectively.

When a vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ is interpreted as an n-bit word, we use the little-endian coordinate convention: x_1 is the least significant bit and x_n is the most significant bit, so that $[x] = \sum_{i=1}^{n} x_i 2^{i-1}$. For $0 \le \gamma < n$, we denote by R^γ the cyclic left rotation by γ bit positions. More precisely, $R^\gamma(x_1, \ldots, x_n) = (x_{n-\gamma+1}, \ldots, x_n, x_1, \ldots, x_{n-\gamma})$, with R^0 equal to the identity map. Accordingly, $(R^\gamma)^{-1} = R^{n-\gamma}$ is the cyclic right rotation by γ bit positions.

Throughout this paper, we view the state space as $(\mathbb{F}_2^w)^m$, where w denotes the word size and m the number of words. For $x = (x_1, \ldots, x_m) \in (\mathbb{F}_2^w)^m$, we let $R^\gamma(x) = \big(R^\gamma(x_1), \ldots, R^\gamma(x_m)\big)$, where $R^\gamma(x_i)$ denotes the cyclic left rotation of the w-bit word x_i by γ bit positions according to the convention above. Unless otherwise specified, we write $R = R^1$, following previous works that consider attacks with rotation offset $\gamma = 1$. Most of the framework developed below applies to an arbitrary nonzero rotation offset $1 \le \gamma < w$.

2.2 Rotational Cryptanalysis and Rotational-XOR (RX) Cryptanalysis

Rotational cryptanalysis was formally introduced by Khovratovich and Nikolić and later refined in subsequent work [KN10, KNP+15]. It is a related-key chosen-plaintext attack that exploits rotational properties arising from the underlying operations. The attacker queries plaintext pairs $(x, R(x))$ under related-key pairs $(k, R(k))$ and observes whether the rotational relation is preserved through the encryption process.

The effectiveness of rotational cryptanalysis relies on the fact that rotation and XOR preserve rotational relations deterministically, while nonlinear operations such as modular addition preserve them only with certain probabilities. Consequently, rotational properties

may propagate through multiple rounds with probability significantly larger than random expectation. Later work showed that such probabilities cannot always be estimated by simply multiplying the probabilities of individual operations, since chained nonlinear operations introduce dependencies that violate the Markov assumption [KNP+15]. To reduce rotational distinguishability, designers commonly inject round-dependent constants to break rotational symmetry.

To analyze constructions in the presence of constants, Ashur and Liu proposed Rotational-XOR (RX) cryptanalysis [AL16]. RX cryptanalysis generalizes rotational cryptanalysis by combining rotational relations with XOR translations. To formalize this relation, RX cryptanalysis introduces the notion of RX-difference.

Definition 1 (RX-difference, [AL16])**.** Let $x' = R^\gamma(x) + a$, where γ denotes the rotational offset and a is the translation value. The RX-difference between x and x' is defined as

$$\Delta_\gamma(x, x') = R^\gamma(x) + x'.$$

Using RX-differences, RX cryptanalysis studies whether, for related keys k, k' satisfying a prescribed RX relation, the probability

$$\Pr_{\mathbf{x}}[E_{k'}(R^\gamma(\mathbf{x}) + a) = R^\gamma(E_k(\mathbf{x})) + b]$$

deviates significantly from the random probability 2^{-n}. This enables statistical distinguishers even when rotational symmetry is partially disrupted by constant injection.

An RX-difference can be viewed as a generalization of a rotational pair, where ordinary rotational cryptanalysis corresponds to the special case with zero translation. By combining rotational relations with XOR translations, RX cryptanalysis enables rotational analysis in the presence of symmetry-breaking constants and generalizes rotational distinguishers beyond ordinary rotational pairs.

Using the definition of RX-difference, we can define RX differentials and RX characteristics as follows.

Definition 2 (RX-differential)**.** Let F and G be two functions over $\mathbb{F}_2^n$. An RX-differential is a pair $(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ such that

$$\Delta_\gamma(x, x') = a$$

at the input and

$$\Delta_\gamma\big(F(x), G(x')\big) = b$$

at the output, where $x' = R^\gamma(x) + a$.

The rotational-XOR probability (RXP) of the RX-differential (a, b) over (F, G) is defined as

$$\begin{aligned}\mathrm{RXP}_{F,G}(a \to b) &= \Pr_{\mathbf{x}}\big[\Delta_\gamma\big(F(\mathbf{x}), G(\mathbf{x}')\big) = b\big] \\ &= \Pr_{\mathbf{x}}[G(R^\gamma(\mathbf{x}) + a) = R^\gamma(F(\mathbf{x})) + b]\,,\end{aligned}$$

where $\mathbf{x}$ is uniformly distributed over $\mathbb{F}_2^n$ and $\mathbf{x}' = R^\gamma(\mathbf{x}) + a$.

Definition 3 (RX characteristic)**.** Let $F = F_r \circ \cdots \circ F_1$ and $G = G_r \circ \cdots \circ G_1$ be an iterated construction composed of r transformations. An RX characteristic over F and G is an $(r+1)$-tuple $Q = (a_1, a_2, \ldots, a_{r+1})$, where each a_i denotes the RX-difference between the corresponding internal states before the application of F_i and G_i.

The probability of the RX characteristic Q is defined as

$$\begin{aligned}\mathrm{RXP}(Q) &= \Pr\left[\bigwedge_{i=1}^{r} \Delta_\gamma\big(F_i(\mathbf{x}_i), G_i(\mathbf{x}_i')\big) = a_{i+1}\right] \\ &= \Pr\left[\bigwedge_{i=1}^{r} G_i(R^\gamma(x_i) + a_i) = R^\gamma\big(F_i(x_i)\big) + a_{i+1}\right]\end{aligned}$$

where $\Delta_\gamma(x_i, x_i') = a_i$ for $i = 1, \ldots, r$, x_1 is uniformly random over $\mathbb{F}_2^n$, and $x_{i+1} = F_i(x_i), x_{i+1}' = G_i(x_i')$ for $i = 1, \ldots, r$.

An RX characteristic fixes every intermediate RX-difference, whereas an RX-differential fixes only its input and output RX-differences. Consequently, the events associated with all characteristics having endpoints $a_1 = a$ and $a_{r+1} = b$ form a partition of the RX-differential event, and

$$\mathrm{RXP}_{F,G}(a \to b) = \sum_{a_2, \ldots, a_r} \mathrm{RXP}(a, a_2, \ldots, a_r, b).$$

The exact trail sums developed below evaluate an individual RX characteristic; evaluating the full RX-differential additionally requires this outer sum over all intermediate RX-differences.

The probability of an RX characteristic is commonly estimated under a Markov assumption, namely that the transitions of different rounds are independent. Under this assumption, the probability of the RX characteristic is approximated by the product of the probabilities of its round transitions. More precisely, one obtains the approximation

$$\Pr\left[\bigwedge_{i=1}^{r} \Delta_\gamma\big(F_i(x_i), G_i(x_i')\big) = a_{i+1}\right] \approx \prod_{i=1}^{r} \Pr\big[\Delta_\gamma\big(F_i(x_i), G_i(x_i')\big) = a_{i+1}\big] .$$

2.3 Geometric Approach

The geometric approach, introduced by Beyne [Bey23], provides a unified framework for symmetric-key cryptanalysis by interpreting cryptographic primitives as linear operators acting on high-dimensional vector spaces. Rather than treating each cryptanalytic technique independently, it studies them within a common linear-algebraic framework and provides deeper insight into the underlying mechanisms of symmetric-key attacks.

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a cryptographic primitive. The free vector space $\mathbb{K}[\mathbb{F}_2^n]$ may be identified with the space of $\mathbb{K}$-valued functions on $\mathbb{F}_2^n$. For each $x \in \mathbb{F}_2^n$, let δ_x denote the indicator function defined by $\delta_x(y) = 1$ if $x = y$ and 0 otherwise. The functions $\{\delta_x \mid x \in \mathbb{F}_2^n\}$ form the standard basis of this space. When $\mathbb{K} = \mathbb{R}$, we equip the space with the inner product $\langle f, g\rangle = \sum_{x \in \mathbb{F}_2^n} f(x)g(x)$, under which the standard basis is orthonormal. A primitive induces a linear operator, called the *pushforward operator*, $T^F : \mathbb{K}[\mathbb{F}_2^n] \to \mathbb{K}[\mathbb{F}_2^m]$, defined by $T^F(\delta_x) = \delta_{F(x)}$. Its matrix representation with respect to chosen bases is called the *transition matrix*.

This construction lifts a nonlinear primitive into a linear setting, where round-wise propagation naturally corresponds to matrix multiplication. The key insight is that different cryptanalytic techniques arise from different basis choices. Cryptanalytic properties can therefore be viewed as coordinate representations of the same underlying linear operator.

The framework was initially developed in the context of linear cryptanalysis [Bey21]. It was subsequently extended to differential [BR22], integral [BV23], and ultrametric integral cryptanalysis [BV24]. More recently, mix-basis configurations further expanded the framework, enabling unified treatment of combined attacks and higher-order properties [HZC+25, CHH+25, CHPW26].

Overall, the geometric approach provides a unified viewpoint in which cryptographic primitives are represented by linear operators, while cryptanalytic techniques correspond to basis choices over free vector spaces.

Differential cryptanalysis studies the evolution of pairs of states rather than individual states. For this reason, the relevant vector space is $\mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$. A natural basis of this space is formed by the indicator functions $\delta_{(a,b)}$, where $\delta_{(a,b)}$ is equal to 1 on the pair (a, b) and 0 elsewhere.

For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, pair propagation is described by $(x, y) \mapsto (F(x), F(y))$. The corresponding linear operator is represented by $T^F \otimes T^F$, whose entries are

$$(T^F \otimes T^F)_{(y_1,y_2),(x_1,x_2)} = \delta_{y_1}(F(x_1))\delta_{y_2}(F(x_2)).$$

2.3.1 Quasidifferential Framework

Although this representation completely describes the propagation of pairs, the standard basis is not always the most convenient choice for cryptanalysis. In particular, translations induced by key additions are not represented in a particularly simple form. To obtain a representation that is better adapted to such operations, Beyne and Rijmen [BR22] introduced the quasidifferential basis.

Definition 4 (Quasidifferential basis, [BR22])**.** Let n be a positive integer. For any $u, a \in \mathbb{F}_2^n$, define the function $\beta_{u,a} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{R}$ by

$$\beta_{u,a}(x, y) = \chi_u(x)\delta_a(x + y).$$

The collection $\{\beta_{u,a} \mid u, a \in \mathbb{F}_2^n\}$ forms an orthogonal basis of $\mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$, called the quasidifferential basis.

A fundamental property of the quasidifferential basis is its behavior under translations. For any $u, a, t \in \mathbb{F}_2^n$, it satisfies

$$\beta_{u,a}(x + t, y + t) = \chi_u(t)\beta_{u,a}(x, y).$$

The change-of-basis operator associated with the quasidifferential basis is

$$\mathscr{Q}_n : \mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n] \to \mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n],$$

defined by

$$(\mathscr{Q}_n f)(u, a) = \langle \beta_{u,a}, f \rangle.$$

Since the quasidifferential basis is orthogonal, the value $(\mathscr{Q}_n f)(u, a)/2^n$ gives the coefficient corresponding to the basis element $\beta_{u,a}$.

Expressing $T^F \otimes T^F$ in the quasidifferential basis yields the quasidifferential transition matrix (QDTM), which is particularly suitable for differential cryptanalysis.

Definition 5 (Quasidifferential transition matrix, [BR22])**.** Let n and m be positive integers, and let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. The quasidifferential transition matrix D^F is the representation of the operator $T^F \otimes T^F$ in the quasidifferential basis. Specifically,

$$D^F = \mathscr{Q}_m(T^F \otimes T^F)\mathscr{Q}_n^{-1}.$$

An explicit expression for the entries of D^F is

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

The quasidifferential transition matrix satisfies several useful structural properties, summarized below.

Theorem 1 ([BR22])**.** *Let n and m be positive integers and let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. The matrix D^F has the following properties:*

(1) If F is a bijection, then D^F is an orthogonal matrix.

(2) If $F = (F_1, \ldots, F_m)$*, then* $D^F = \bigotimes_{i=1}^{m} D^{F_i}$.

(3) If $F = F_2 \circ F_1$*, then* $D^F = D^{F_2} D^{F_1}$.

(4) If $F(x) = x + t$ *for some* $t \in \mathbb{F}_2^n$*, then* $D^F_{(v,b),(u,a)} = \chi_v(t)\delta_v(u)\delta_b(a)$.

(5) If F *is linear, then* $D^F_{(v,b),(u,a)} = \delta_u(F^\top(v))\delta_b(F(a))$.

To analyze the propagation of pair distributions through an iterated function, Beyne and Rijmen [BR22] introduced quasidifferential trails, which are defined using the quasidifferential transition matrix.

Definition 6 (Quasidifferential trail, [BR22])**.** A quasidifferential trail for a function $F = F_r \circ \cdots \circ F_1$ is a sequence $(u_1, a_1), \ldots, (u_{r+1}, a_{r+1})$ of mask-difference pairs. The correlation of this quasidifferential trail is defined as

$$\prod_{i=1}^{r} D^{F_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}.$$

A differential characteristic can be viewed as a special case of a quasidifferential trail in which all masks are zero. From the definition of D^F, the correlation of such a quasidifferential trail is

$$\prod_{i=1}^{r} D^{F_i}_{(0,a_{i+1}),(0,a_i)} = \prod_{i=1}^{r} \Pr[F_i(\mathbf{x} + a_i) = F_i(\mathbf{x}) + a_{i+1}],$$

where $\mathbf{x}$ is uniformly random over $\mathbb{F}_2^n$. This coincides with the usual estimate of differential characteristic probabilities obtained under the Markov assumption.

The following results provide the main connection between quasidifferential trails and characteristic probabilities.

Theorem 2 ([BR22])**.** *Let* $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *be a function such that* $F = F_r \circ \cdots \circ F_1$*. The probability of a characteristic with differences* $a_1, \ldots, a_{r+1}$ *is equal to the sum of the correlations of all quasidifferential trails with the same intermediate differences:*

$$\Pr\left[\bigwedge_{i=1}^{r} F_i(\mathbf{x}_i + a_i) + F_i(\mathbf{x}_i) = a_{i+1}\right] = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} D^{F_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}$$

with $u_1 = u_{r+1} = 0$*,* $\mathbf{x}_i = F_{i-1}(\mathbf{x}_{i-1})$ *for* $i = 2, \ldots, r$*, and* $\mathbf{x}_1$ *uniformly random on* $\mathbb{F}_2^n$.

Theorem 2 shows that the exact probability of a differential characteristic can be expressed as a sum of correlations of quasidifferential trails sharing the same intermediate differences.

The following result provides a useful criterion for proving that a differential characteristic is incompatible.

Theorem 3 ([BR22])**.** *Let* $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *be a function such that* $F = F_r \circ \cdots \circ F_1$*. Let* $a_1, \ldots, a_{r+1}$ *be a characteristic whose corresponding zero-mask quasidifferential trail has correlation* p*. Then the following properties hold.*

(1) Let $(u_1, a_1), \ldots, (u_{r+1}, a_{r+1})$ *be a quasidifferential trail with correlation* $(-1)^b p$*, where* $b \in \{0, 1\}$*, and let* $(v_1, a_1), \ldots, (v_{r+1}, a_{r+1})$ *be another quasidifferential trail with correlation* c*. Then* $(u_1 + v_1, a_1), \ldots, (u_{r+1} + v_{r+1}, a_{r+1})$ *is a quasidifferential trail with correlation* $(-1)^b c$*. Equivalently,*

$$\prod_{i=1}^{r} D^{F_i}_{(u_{i+1}+v_{i+1},a_{i+1}),(u_i+v_i,a_i)} = (-1)^b \prod_{i=1}^{r} D^{F_i}_{(v_{i+1},a_{i+1}),(v_i,a_i)}.$$

(2) If there exists a collection of quasidifferential trails with differences $a_1, \ldots, a_{r+1}$ and correlation $\pm p$ whose correlations sum to zero, then the probability of the characteristic $(a_1, \ldots, a_{r+1})$ is zero.

2.3.2 Extended Quasidifferential Framework

Boura, Derbez, and Germon extended the quasidifferential framework in two complementary directions [BDG25]. First, they allowed the two executions to use different functions, which provides a direct formulation of related-key propagation. Second, they incorporated the key state into a joint data-key space, enabling expected differential probabilities to be analyzed with the key schedule in both single-key and related-key settings.

Let F and G be two functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. For the first extension, the quasidifferential transition matrix is defined for a pair of functions as follows:

$$D^{F/G}_{(v,b),(u,a)} = \frac{1}{2^n} \sum_{\substack{x \in \mathbb{F}_2^n \\ G(x+a)=F(x)+b}} (-1)^{u^\top x + v^\top F(x)}$$

For instance, if $F(x) = x + t$ and $G(x) = x + t + c$ where $t, c \in \mathbb{F}_2^n$, then

$$D^{F/G}_{(v,b),(u,a)} = \chi_u(t)\delta_u(v)\delta_b(a + c).$$

Using this extension, Theorem 2 admits the following related-key analogue. The identity is exact for the prescribed component functions F_i and G_i and does not require an independence assumption between their transitions.

Theorem 4 ([BDG25])**.** *Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be two functions such that $F = F_r \circ \cdots \circ F_1$ and $G = G_r \circ \cdots \circ G_1$. Then,*

$$\Pr\left[\bigwedge_{i=1}^{r} G_i(x_i + a_i) + F_i(x_i) = a_{i+1}\right] = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} D^{F_i/G_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}$$

with $u_1 = u_{r+1} = 0$, $x_i = F_{i-1}(x_{i-1})$ for $i = 2, \ldots, r$, and x_1 uniformly random on $\mathbb{F}_2^n$.

To account for the key schedule, quasidifferential propagation is next formulated over the joint data-key space. Let ℓ denote the dimension of the key state. More precisely, an operation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ acting on the data path is extended to

$$\begin{aligned} \bar{F} : \mathbb{F}_2^n \times \mathbb{F}_2^\ell &\to \mathbb{F}_2^n \times \mathbb{F}_2^\ell \\ (x, k) &\mapsto (F(x), k). \end{aligned}$$

By Theorem 1, an operation acting solely on the data path can be lifted to the joint data-key space while leaving the key component unchanged. In particular, for $\bar{F}(x, k) = (F(x), k)$, the associated correlation coefficient decomposes as $D^{\bar{F}}_{(v_1|v_2,b_1|b_2),(u_1|u_2,a_1|a_2)} = D^{F}_{(v_1,b_1),(u_1,a_1)}\delta_{v_2}(u_2)\delta_{b_2}(a_2)$. An analogous property holds for operations acting solely on the key path.

For the key-addition operation

$$\begin{aligned} G : \mathbb{F}_2^n \times \mathbb{F}_2^n &\to \mathbb{F}_2^n \times \mathbb{F}_2^n, \\ (x, k) &\mapsto (x + k, k), \end{aligned}$$

the corresponding correlation coefficient is given by Proposition 1.

Proposition 1 ([BDG25])**.** *Let n be a positive integer.*
For any $v_x, v_k, b_x, b_k, u_x, u_k, a_x, a_k \in \mathbb{F}_2^n$, it holds that

$$D^{G}_{(v_x\|v_k,b_x\|b_k),(u_x\|u_k,a_x\|a_k)} = \delta_{b_x}(a_x + a_k)\delta_{b_k}(a_k)\delta_{v_x}(u_x)\delta_{v_k}(u_x + u_k).$$

This expression does not depend on the actual key value. Consequently, fixed-key information disappears at key-addition layers. The extended quasidifferential framework nevertheless provides an exact expression for the EDP of the resulting characteristic:

Theorem 5 ([BDG25])**.** *Let $E = F_r \circ \cdots \circ F_1$ and let $Q = \big((a_x^1, a_k^1), \ldots, (a_x^{r+1}, a_k^{r+1})\big)$ be a related-key differential characteristic over E. The sequences $(a_x^i)_{i=1}^{r+1}$ and $(a_k^i)_{i=1}^{r+1}$ describe the corresponding characteristics on the plaintext and key paths, respectively. If $a_k^1 = \cdots = a_k^{r+1} = 0$, then Q reduces to a single-key characteristic. The EDP of Q is given by*

$$\begin{aligned}\mathrm{EDP}(Q) &= \Pr\left[\bigwedge_{i=1}^{r} F_i\big((x_i, k_i) + (a_x^i, a_k^i)\big) + F_i(x_i, k_i) = (a_x^{i+1}, a_k^{i+1})\right] \\ &= \sum_{\substack{u_x^2,\ldots,u_x^r \\ u_k^2,\ldots,u_k^r}} \prod_{i=1}^{r} D^{F_i}_{((u_x^{i+1},u_k^{i+1}),(a_x^{i+1},a_k^{i+1})),((u_x^i,u_k^i),(a_x^i,a_k^i))}.\end{aligned}$$

where $(u_x^1, u_k^1) = (u_x^{r+1}, u_k^{r+1}) = (0, 0)$ and $(x_i, k_i) = F_{i-1}(x_{i-1}, k_{i-1})$ for $i = 2, \ldots, r$, with (x_1, k_1) sampled uniformly from $\mathbb{F}_2^n \times \mathbb{F}_2^\ell$.

Hence, the EDP of a related-key characteristic is obtained by summing the correlations of all associated quasidifferential trails defined over the joint data-key space.

3 Rotational-Quasidifferential Framework

In this section, we develop a rotational-quasidifferential framework for RX cryptanalysis within the geometric approach. We introduce the rotational-quasidifferential basis and the associated rotational-quasidifferential transition matrix, and use them to define rotational-quasidifferential trails. These trails provide exact expressions for the probabilities of RX characteristics in both fixed-key and average-key settings. In addition, they offer a natural way to analyze incompatible RX characteristics.

3.1 Rotational-Quasidifferential Basis

To analyze RX cryptanalysis within the geometric approach, a basis adapted to rotational relations is required. The following definition introduces the rotational-quasidifferential basis, which plays a role analogous to the quasidifferential basis in differential cryptanalysis.

Definition 7 (Rotational-quasidifferential basis)**.** Let n be a positive integer. For any $u, a \in \mathbb{F}_2^n$, the function $\rho_{u,a} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{R}$ is defined by

$$\rho_{u,a}(x, y) = \chi_u(x)\delta_a(R(x) + y).$$

The set of all functions $\{\rho_{u,a} \mid u, a \in \mathbb{F}_2^n\}$ is called the rotational-quasidifferential (RQ) basis for $\mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$.

The following lemma gives two fundamental properties of the rotational-quasidifferential basis.

Lemma 1. *Let $\rho_{u,a}(x, y) = \chi_u(x)\delta_a(R(x) + y)$. Then the following properties hold:*

(1) $\langle \rho_{u,a}, \rho_{v,b} \rangle = 2^n \delta_v(u)\delta_b(a)$.

(2) $\rho_{u,a}(x + t, y + R(t)) = \chi_u(t)\rho_{u,a}(x, y)$ *for all* $t \in \mathbb{F}_2^n$

Proof. For (1), we compute

$$\begin{aligned}\langle \rho_{u,a}, \rho_{v,b} \rangle &= \sum_{x,y \in \mathbb{F}_2^n} \chi_u(x)\delta_a(R(x)+y)\chi_v(x)\delta_b(R(x)+y) \\ &= \delta_b(a) \sum_{x \in \mathbb{F}_2^n} (-1)^{(u+v)^\top x} \\ &= 2^n \delta_v(u)\delta_b(a)\end{aligned}$$

For (2), it follows directly from the definition of $\rho_{u,a}$ that

$$\begin{aligned}\rho_{u,a}(x+t, y+R(t)) &= \chi_u(x+t)\delta_a\big(R(x+t)+y+R(t)\big) \\ &= \chi_u(t)\chi_u(x)\delta_a\big(R(x)+y\big) \\ &= \chi_u(t)\rho_{u,a}(x,y)\end{aligned}$$

□

Property (1) shows that the rotational-quasidifferential basis is orthogonal. Property (2) shows that the basis elements behave as eigenfunctions under simultaneous translations satisfying the rotational relation. This eigenfunction property is fundamental for the analysis of RX cryptanalysis in the rotational-quasidifferential framework.

We define the change-of-basis operator from the standard basis to the rotational-quasidifferential basis by

$$\mathscr{R}_n : \mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n] \to \mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n],$$

where

$$(\mathscr{R}_n f)(u,a) = \langle \rho_{u,a}, f \rangle.$$

Since $\langle \rho_{u,a}, \rho_{u,a} \rangle = 2^n$, it follows that $(\mathscr{R}_n f)(u,a)/2^n$ is the coefficient of $\rho_{u,a}$ in the expansion of f in the rotational-quasidifferential basis.

3.2 Rotational-Quasidifferential Transition Matrix

Since RX cryptanalysis is formulated in the related-key setting, the related-key extension of the quasidifferential framework introduced in [BDG25] serves as a natural starting point for our construction.

Let F and G be two functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. We consider the transition matrix $T^F \otimes T^G$.

Definition 8 (Rotational-quasidifferential transition matrix)**.** Let n and m be positive integers, and let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be functions. The rotational-quasidifferential transition matrix $A^{F/G}$ is defined as the matrix representation of $T^F \otimes T^G$ with respect to the rotational-quasidifferential basis. Specifically, $A^{F/G} = \mathscr{R}_m(T^F \otimes T^G)\mathscr{R}_n^{-1}$. When $F = G$, we simply write A^F instead of $A^{F/F}$.

We refer to $A^{F/G}$ as the RQTM of the pair (F, G), or simply as the RQTM of F when $F = G$. The coordinates of $A^{F/G}$ can be derived as follows. Here, $\mathscr{R}_n^{-1} = \mathscr{R}_n^T/2^n$ holds due to the orthogonality of the RQ basis.

$$\begin{aligned}A^{F/G}_{(v,b),(u,a)} &= 2^{-n}\langle \rho_{v,b}, (T^F \otimes T^G)\rho_{u,a} \rangle \\ &= 2^{-n} \sum_{x,y \in \mathbb{F}_2^n} \chi_v(F(x))\delta_b(R(F(x))+G(y))\chi_u(x)\delta_a(R(x)+y) \\ &= 2^{-n} \sum_{\substack{x \in \mathbb{F}_2^n \\ G(R(x)+a)=R(F(x))+b}} (-1)^{u^\top x + v^\top F(x)}\end{aligned} \tag{1}$$

The right-hand side can be interpreted as the correlation of the linear approximation with masks (u, v) restricted to the set of inputs satisfying the RX relation $G(R(x) + a) = R(F(x)) + b$.

When the rotation offset satisfies $\gamma = 0$, the rotation operator reduces to the identity map. In this case, the rotational-quasidifferential basis coincides with the quasidifferential basis, and the rotational-quasidifferential transition matrix reduces to the quasidifferential transition matrix.

Relation to the QDTM. The relation can be made explicit at the level of individual matrix entries. Let R_n and R_m denote the rotations on the input and output spaces, respectively, and define the conjugated second branch

$$\widetilde{G} = R_m^{-1} \circ G \circ R_n.$$

Applying R_m^{-1} to the constraint in (1) gives

$$G(R_n(x) + a) = R_m(F(x)) + b \quad \Longleftrightarrow \quad \widetilde{G}(x + R_n^{-1}(a)) = F(x) + R_m^{-1}(b).$$

Comparison with the extended QDTM in Section 2 therefore yields

$$A^{F/G}_{(v,b),(u,a)} = D^{F/\widetilde{G}}_{(v,R_m^{-1}(b)),(u,R_n^{-1}(a))}.$$

Since R_n and R_m are bijections, the two reindexing maps

$$(u, a) \longmapsto (u, R_n^{-1}(a)), \qquad (v, b) \longmapsto (v, R_m^{-1}(b))$$

are bijections. In particular, when a layer commutes with the rotation and $F = G$, as for a bitwise AND layer, $\widetilde{G} = F$, so its RQTM entries are precisely ordinary QDTM entries with the input and output differences rotated as above.

The advantage of the RQ representation is that it keeps the original cipher layers unchanged and propagates RX-differences directly in their native coordinates. This distinction is particularly useful for modular addition: word rotation does not commute with addition, so the conjugated map is no longer a standard modular addition and existing modular-addition QDTM formulas cannot be applied to it directly. The RQTM instead provides native transition matrices that compose without rewriting the data path, constant additions, or key schedule. Appendix C.1 gives a detailed consistency check with the AND-QDTM when $\gamma = 0$, while Appendix C.2 relates the zero-mask ADD-RQTM coefficient to the exact RX-differential probability formula for modular addition derived by Biryukov, Lambin, and Udovenko [BLU25].

The rotational-quasidifferential transition matrix satisfies the following properties.

Theorem 6. *Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be functions. The matrix $A^{F/G}$ satisfies the following properties:*

(1) If $F = (F_1, \ldots, F_m)$ and $G = (G_1, \ldots, G_m)$, then $A^{F/G} = \bigotimes_{i=1}^{m} A^{F_i/G_i}$.

(2) If $F = F_2 \circ F_1$ and $G = G_2 \circ G_1$, then $A^{F/G} = A^{F_2/G_2} A^{F_1/G_1}$.

(3) If $F(x) = x + t$ and $G(x) = x + R(t) + c$ for some $t, c \in \mathbb{F}_2^n$, then $A^{F/G}_{(v,b),(u,a)} = \chi_v(t)\delta_v(u)\delta_b(a + c)$.

(4) If F, G are linear and $G \circ R = R \circ F$, then $A^{F/G}_{(v,b),(u,a)} = \delta_u(F^\top(v))\delta_b(G(a))$.

(5) If $F(x) = G(x) = x + t$ for some $t \in \mathbb{F}_2^n$, then $A^{F}_{(v,b),(u,a)} = \chi_v(t)\delta_v(u)\delta_b(a + t + R(t))$.

Proof. Property (1) follows from the separability of the RX basis and the mixed-product property of the Kronecker product. Property (2) follows from $(T^{F_2 \circ F_1} \otimes T^{G_2 \circ G_1}) = (T^{F_2} \otimes T^{G_2})(T^{F_1} \otimes T^{G_1})$.

For (3), substituting $F(x) = x + t$ and $G(x) = x + R(t) + c$ into (1), the constraint becomes $R(x) + a + R(t) + c = R(x + t) + b$, or equivalently $b = a + c$. Hence

$$A^{F/G}_{(v,b),(u,a)} = \chi_v(t)\delta_b(a + c)2^{-n} \sum_x (-1)^{(u+v)^\top x},$$

and the claim follows from the orthogonality of characters.

For (4), since F and G are linear and satisfy $G \circ R = R \circ F$, the constraint in (1) reduces to $RF(x) + G(a) = RF(x) + b$, i.e., $b = G(a)$. Therefore

$$A^{F/G}_{(v,b),(u,a)} = \delta_b(G(a))2^{-n} \sum_x (-1)^{(u+F^\top(v))^\top x},$$

and the result again follows from the orthogonality of characters.

Finally, (5) is obtained from (3) by setting $c = t + R(t)$. □

Properties (1) and (2) are direct analogues of the corresponding properties of the quasidifferential transition matrix. The key difference is that the rotational-quasidifferential transition matrix diagonalizes related-key additions satisfying the rotational relation, rather than single-key additions. In particular, Property (3) shows that round-key additions become diagonal in the rotational-quasidifferential basis whenever the related keys satisfy the prescribed RX relation.

Unlike the quasidifferential transition matrix, the constraint $G(R(x)+a) = R(F(x))+b$ generally does not simplify when F and G are linear. Consequently, a closed-form expression for the entries of the rotational-quasidifferential transition matrix is not available for arbitrary linear functions. Property (4) therefore requires the additional condition $G \circ R = R \circ F$.

Property (5) is particularly useful for analyzing round-constant additions. Unlike round-key additions, the constant value is known, so the induced RX-difference is completely determined by the term $\delta_b(a + t + R(t))$, while $\chi_v(t)$ records its exact contribution to the sign. In the applications of Section 4, Property (5) accounts for the fixed XOR constants used in the SIMON and SIMECK key schedules, the SPECK round-key expansion, and the Alzette data path.

Property (4) of Theorem 6 immediately yields the following corollary, which describes the rotational-quasidifferential transition matrices of bit rotations, copy operations, and bitwise XOR.

Corollary 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. The matrix A^F satisfies the following properties:*

(1) If $F = R^\gamma$, then $A^F_{(v,b),(u,a)} = \delta_u(F^\top(v))\delta_b(F(a))$.

(2) If $F = \mathrm{COPY}$, i.e., $F(x) = (x, x)$, then $A^F_{(v_1\|v_2,b_1\|b_2),(u,a)} = \delta_u(v_1 + v_2)\delta_{b_1}(a)\delta_{b_2}(a)$.

(3) If $F = \mathrm{XOR}$, i.e., $F(x, y) = x + y$, then $A^F_{(v,b),(u_1\|u_2,a_1\|a_2)} = \delta_{u_1}(v)\delta_{u_2}(v)\delta_b(a_1 + a_2)$.

Theorem 6 and Corollary 1 provide explicit RQTM expressions for the linear and affine operations used by the ciphers analyzed in Section 4. We next derive explicit RQTM expressions for two nonlinear operations of particular interest: bitwise AND and modular addition.

Bitwise AND We now turn to the analysis of the bitwise AND operation, which is the main nonlinear component of AND-RX ciphers. The analysis of the AND operation relies on the following lemma.

Lemma 2. *For $p, q, r, u, v, w \in \mathbb{F}_2^n$, let*

$$S_n(p,q,r;u,v,w) = \sum_{\substack{x,y\in\mathbb{F}_2^n \\ p\wedge x+q\wedge y=r}} (-1)^{u^\top x+v^\top y+w^\top(x\wedge y)}.$$

Then $S_n(p,q,r;u,v,w) \neq 0$ if and only if

$$q\wedge u + p\wedge v + w\wedge r = w\wedge p\wedge q$$

and

$$\bar{p}\wedge\bar{q}\wedge(r\vee u\vee v) \preccurlyeq w.$$

In this case, $S_n(p,q,r;u,v,w) = 2^{n+\mathrm{wt}(\bar{p}\wedge\bar{q}\wedge\bar{w})}(-1)^{\mathrm{wt}((\bar{q}\wedge r\wedge u)\vee(u\wedge v\wedge w)\vee(q\wedge r\wedge v))}$.

Proof. Observe that the constraint $p\wedge x+q\wedge y = r$ is coordinate-wise, namely $p_ix_i+q_iy_i = r_i$ for every $1 \le i \le n$. Moreover,

$$u^\top x + v^\top y + w^\top(x\wedge y) = \sum_{i=1}^{n}\big(u_ix_i + v_iy_i + w_ix_iy_i\big),$$

and therefore

$$(-1)^{u^\top x+v^\top y+w^\top(x\wedge y)} = \prod_{i=1}^{n}(-1)^{u_ix_i+v_iy_i+w_ix_iy_i}.$$

It follows that

$$S_n(p,q,r;u,v,w) = \prod_{i=1}^{n}\left(\sum_{\substack{a,b\in\mathbb{F}_2 \\ p_ia+q_ib=r_i}}(-1)^{u_ia+v_ib+w_iab}\right) = \prod_{i=1}^{n} S_1(p_i,q_i,r_i;u_i,v_i,w_i).$$

Hence S_n factorizes into a product of one-bit contributions. Therefore, it suffices to compute the case $n = 1$, and the stated formula follows by taking the product over coordinates.

For $n = 1$, we distinguish four cases according to the values of (p_i, q_i).

If $p_i = q_i = 1$, then $a + b = r_i$, and $u_ia + v_ib + w_iab = (u_i + v_i + w_i + w_ir_i)a + v_ir_i$. Hence,

$$S_1(p_i,q_i,r_i;u_i,v_i,w_i) = 2(-1)^{v_ir_i}\delta_{u_i+v_i+w_i+w_ir_i=0}.$$

If $p_i = 1$ and $q_i = 0$, then $a = r_i$, and $u_ia + v_ib + w_iab = u_ir_i + (v_i + w_ir_i)b$. Hence,

$$S_1(p_i,q_i,r_i;u_i,v_i,w_i) = 2(-1)^{u_ir_i}\delta_{v_i+w_ir_i=0}.$$

Similarly, if $p_i = 0$ and $q_i = 1$, then $b = r_i$, and

$$S_1(p_i,q_i,r_i;u_i,v_i,w_i) = 2(-1)^{v_ir_i}\delta_{u_i+w_ir_i=0}.$$

If $p_i = q_i = 0$, then $r_i = 0$, and

$$\begin{aligned} S_1(p_i,q_i,r_i;u_i,v_i,w_i) &= \sum_{a,b\in\mathbb{F}_2}(-1)^{u_ia+v_ib+w_iab} \\ &= 1 + (-1)^{u_i} + (-1)^{v_i} + (-1)^{u_i+v_i+w_i} \\ &= 2^{2-w_i}(-1)^{u_iv_i}\delta_{u_i\vee v_i\le w_i} \end{aligned}$$

Combining the four cases, $S_1(p_i, q_i, r_i; u_i, v_i, w_i) \neq 0$ if and only if

$$q_i u_i + p_i v_i + w_i r_i = w_i p_i q_i$$

and

$$\bar{p}_i \bar{q}_i (r_i \vee u_i \vee v_i) \leq w_i.$$

In this case,

$$S_1(p_i, q_i, r_i; u_i, v_i, w_i) = 2^{1+\bar{p}_i \wedge \bar{q}_i \wedge \bar{w}_i} (-1)^{p_i q_i v_i r_i + p_i \bar{q}_i u_i r_i + \bar{p}_i q_i v_i r_i + \bar{p}_i \bar{q}_i u_i v_i}.$$

The exponent can be simplified to $\bar{q}_i r_i u_i \vee u_i v_i w_i \vee q_i r_i v_i$. Taking the product over all coordinates yields the stated expression for S_n, which completes the proof. □

Although Theorem 7 could also be obtained from the general RQTM–QDTM correspondence and the known AND-QDTM, we derive it directly in the RQ basis because the coordinate-wise character sum in Lemma 2 is also used later in the derivation of the modular-addition RQTM. Using this lemma, the rotational-quasidifferential transition matrix of the bitwise AND operation can be derived explicitly.

Theorem 7 (RQTM of bitwise AND)**.** *Let $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ be defined by $F(x, y) = x \wedge y$. Then $A^F_{(w,c),(u\|v,a\|b)} \neq 0$ if and only if*

$$q \wedge u + p \wedge v + w \wedge r = w \wedge p \wedge q$$

and

$$\bar{p} \wedge \bar{q} \wedge (r \vee u \vee v) \preccurlyeq w$$

where $p = R^{-1}(b), q = R^{-1}(a), r = R^{-1}(c + a \wedge b)$. Moreover, whenever these conditions hold,

$$A^F_{(w,c),(u\|v,a\|b)} = 2^{-n+\mathrm{wt}(\bar{p}\wedge\bar{q}\wedge\bar{w})} (-1)^{\mathrm{wt}((\bar{q}\wedge r\wedge u)\vee(u\wedge v\wedge w)\vee(q\wedge r\wedge v))}.$$

Proof.

$$\begin{aligned}
A^F_{(w,c),(u\|v,a\|b)} &= 2^{-2n} \sum_{\substack{x,y\in\mathbb{F}_2^n \\ ((R(x)+a)\wedge(R(y)+b))=R(x\wedge y)+c}} (-1)^{u^\top x + v^\top y + w^\top (x\wedge y)} \\
&= 2^{-2n} \sum_{\substack{x,y\in\mathbb{F}_2^n \\ b\wedge R(x)+a\wedge R(y)=c+a\wedge b}} (-1)^{u^\top x + v^\top y + w^\top (x\wedge y)} \\
&= 2^{-2n} \sum_{\substack{x,y\in\mathbb{F}_2^n \\ R^{-1}(b)\wedge x+R^{-1}(a)\wedge y=R^{-1}(c+a\wedge b)}} (-1)^{u^\top x + v^\top y + w^\top (x\wedge y)} \\
&= 2^{-2n} S_n(p, q, r; u, v, w),
\end{aligned}$$

where

$$p = R^{-1}(b), \qquad q = R^{-1}(a), \qquad r = R^{-1}(c + a \wedge b).$$

The result now follows immediately from Lemma 2. □

As a consistency check, Appendix C.1 compares this expression with the AND-QDTM of Beyne and Rijmen [BR22]. It shows that, when $\gamma = 0$, the two formulas have identical support, absolute values, and signs, as expected from the reduction of the rotational-quasidifferential basis to the ordinary quasidifferential basis.

Modular addition We next consider modular addition. For two n-bit words $x, y \in \mathbb{F}_2^n$, we denote their addition modulo 2^n by $x \boxplus y$. Throughout this paragraph, we fix a nonzero rotation offset $1 \le \gamma < n$ and let $R = R^\gamma$.

Our analysis is based on the CCZ representation of modular addition due to Schulte-Geers [SG13], which was also used by Beyne and Rijmen in their quasidifferential analysis of modular addition [BR22, Appendix A.4]. Define the linear map $M : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

$$M(x)_1 = 0, \qquad M(x)_i = \sum_{j=1}^{i-1} x_j, \quad 2 \le i \le n.$$

Thus, $M(x_1, \dots, x_n) = (0, x_1, x_1 + x_2, \dots, x_1 + \cdots + x_{n-1})$.

We also write e_i for the i-th unit vector of $\mathbb{F}_2^n$. For a vector y satisfying $y_1 = 0$, define

$$(M^\dagger y)_i = y_i + y_{i+1}, \quad 1 \le i < n, \qquad (M^\dagger y)_n = 0.$$

Then $M(M^\dagger y) = y$ and $\ker M = \operatorname{span}\{e_n\}$.

The following lemma transfers an RQTM entry of modular addition to the quadratic function $(x, y) \mapsto M(x \wedge y)$.

Lemma 3. *Let $F(x, y) = x \boxplus y$ and $F_M(x, y) = M(x \wedge y)$. For $a, b, c, u, v, w \in \mathbb{F}_2^n$, define*

$$a' = b + c, \quad b' = a + c, \quad c' = a + b + c,$$
$$u' = u + w, \quad v' = v + w, \quad w' = u + v + w.$$

Then

$$A^F_{(w,c),(u\|v,a\|b)} = A^{F_M}_{(w',c'),(u'\|v',a'\|b')}.$$

Proof. Let $T(x, y, z) = (x + z, y + z, x + y + z)$. By the CCZ-equivalence established by Schulte-Geers [SG13], T sends the graph of $F_M(x, y) = M(x \wedge y)$ onto the graph of $F(x, y) = x \boxplus y$.

Since T consists only of coordinate-wise additions, it commutes with the rotation applied simultaneously to its three components: $T\big(R(x), R(y), R(z)\big) = R\big(T(x, y, z)\big)$.

Moreover, $T^{-1}(x, y, z) = (y + z, x + z, x + y + z)$, and the matrix representing T is symmetric. Consequently, $T^{-1}(a, b, c) = (b + c, a + c, a + b + c)$ for the RX-differences, whereas $T^\top(u, v, w) = (u + w, v + w, u + v + w)$ for the masks. Substituting these transformations into the definition of the RQTM gives the result. □

To analyze the RQTM of M, we first characterize its failure to commute with the rotation. Let $j = n - \gamma$ and define

$$U = (\underbrace{1, \dots, 1}_{j}, \underbrace{0, \dots, 0}_{\gamma}), \quad V = (\underbrace{0, \dots, 0}_{j}, \underbrace{1, \dots, 1}_{\gamma}),$$
$$P = (\underbrace{1, \dots, 1}_{\gamma}, \underbrace{0, \dots, 0}_{j}), \quad Q = (\underbrace{0, \dots, 0}_{\gamma}, \underbrace{1, \dots, 1}_{j}).$$

Lemma 4. *For $L = MR + RM$, it holds that $L(x) = (U^\top x)P + (V^\top x)Q$ for every $x \in \mathbb{F}_2^n$. Consequently,*

$$\operatorname{rank}(L) = 2, \qquad \operatorname{Im}(L) = \langle P, Q \rangle, \qquad \operatorname{Im}(L^\top) = \langle U, V \rangle.$$

Proof. Write $x = (x_1, \dots, x_j, x_{j+1}, \dots, x_n)$. Since $R(x) = (x_{j+1}, \dots, x_n, x_1, \dots, x_j)$, by the definition of M, a direct coordinate-wise computation gives

$$(MR(x) + RM(x))_i = \begin{cases} \displaystyle\sum_{\ell=1}^{j} x_\ell, & 1 \le i \le \gamma, \\ \displaystyle\sum_{\ell=j+1}^{n} x_\ell, & \gamma + 1 \le i \le n. \end{cases}$$

Hence $L(x) = (U^\top x)P + (V^\top x)Q$. Since $(PU^\top)x = (U^\top x)P$ and $(QV^\top)x = (V^\top x)Q$, this is equivalently written as $L = PU^\top + QV^\top$. The vectors P and Q are nonzero and have disjoint supports, and are therefore linearly independent. Thus, $\mathrm{rank}(L) = 2$ and $\mathrm{Im}(L) = \langle P, Q\rangle$.

Taking the transpose gives $L^\top = UP^\top + VQ^\top$, and hence $\mathrm{Im}(L^\top) \subseteq \langle U, V\rangle$. Since $\mathrm{rank}(L^\top) = \mathrm{rank}(L) = 2$, while U and V are also nonzero and have disjoint supports, $\dim\langle U, V\rangle = 2$. Therefore, $\mathrm{Im}(L^\top) = \langle U, V\rangle$, which proves the last claim. □

The rank-two structure in Lemma 4 gives a simple expression for the RQTM of M.

Lemma 5. *Let $s, d, w, c \in \mathbb{F}_2^n$. Then $A^M_{(w,c),(s,d)} \neq 0$ if and only if there exist unique $\kappa, \eta, \lambda, \mu \in \mathbb{F}_2$ such that*

$$c + M(d) = \kappa P + \eta Q \qquad \text{and} \qquad s + M^\top(w) = \lambda U + \mu V.$$

Whenever these conditions hold,

$$A^M_{(w,c),(s,d)} = \frac{1}{4}(-1)^{\lambda\kappa+\mu\eta}.$$

Proof. Set $t = c + M(d)$ and $h = s + M^\top(w)$. By the definition of the RQTM and the linearity of M,

$$A^M_{(w,c),(s,d)} = 2^{-n} \sum_{\substack{x\in\mathbb{F}_2^n \\ L(x)=t}} (-1)^{h^\top x},$$

where $L = MR + RM$.

The equation $L(x) = t$ has a solution exactly when $t \in \mathrm{Im}(L)$. By Lemma 4, this is equivalent to $t = \kappa P + \eta Q$ for some $\kappa, \eta \in \mathbb{F}_2$.

Assume that this condition holds and let x_0 be a particular solution. Then every solution is of the form $x_0 + z$ with $z \in \ker L$, so

$$A^M_{(w,c),(s,d)} = 2^{-n}(-1)^{h^\top x_0} \sum_{z\in\ker L} (-1)^{h^\top z}.$$

By the orthogonality of characters on the subspace $\ker L$, the last sum is nonzero exactly when $h \in (\ker L)^\perp = \mathrm{Im}(L^\top)$. Again by Lemma 4, this is equivalent to $h = \lambda U + \mu V$ for some $\lambda, \mu \in \mathbb{F}_2$.

Since $\mathrm{rank}(L) = 2$, we have $|\ker L| = 2^{n-2}$. Moreover, $x_0 = \kappa e_1 + \eta e_{j+1}$ is a particular solution, because $L(e_1) = P$ and $L(e_{j+1}) = Q$. For $h = \lambda U + \mu V$, this gives $h^\top x_0 = \lambda\kappa + \mu\eta$. Since $h \in (\ker L)^\perp$, the value of $h^\top x_0$ does not depend on the choice of the particular solution. Therefore,

$$A^M_{(w,c),(s,d)} = \frac{1}{4}(-1)^{\lambda\kappa+\mu\eta},$$

which proves the result. □

We now combine Lemma 5 with the RQTM of bitwise AND to derive the RQTM of modular addition. Since $F_M = M \circ \mathrm{AND}$, Property (2) of Theorem 6 gives

$$A^{F_M}_{(w',c'),(u'\|v',a'\|b')} = \sum_{s,d\in\mathbb{F}_2^n} A^M_{(w',c'),(s,d)} A^{\mathrm{AND}}_{(s,d),(u'\|v',a'\|b')}.$$

Only the pairs (s, d) for which the first coefficient is nonzero can contribute to this sum.

By Lemma 5, this requires

$$c' + M(d) = \kappa P + \eta Q \qquad \text{and} \qquad s + M^\top(w') = \lambda U + \mu V$$

for some $\kappa, \eta, \lambda, \mu \in \mathbb{F}_2$. Since $(M(d))_1 = 0$, $P_1 = 1$, and $Q_1 = 0$, the first condition necessarily gives $\kappa = c'_1$; hence, κ is fixed rather than a free variable.

The remaining solutions can be parametrized by

$$d = M^{\dagger}(c' + \kappa P + \eta Q) + \tau e_n, \qquad s = M^{\top}(w') + \lambda U + \mu V,$$

where $\tau \in \mathbb{F}_2$ accounts for $\ker M = \mathrm{span}\{e_n\}$. Since $M^{\dagger}(Q) = e_\gamma$, it is convenient to set $d_0 = M^{\dagger}(c' + \kappa P)$ and $s_0 = M^{\top}(w')$, so that

$$d = d_0 + \eta e_\gamma + \tau e_n, \qquad s = s_0 + \lambda U + \mu V.$$

Consequently, only 16 pairs (s, d), indexed by $\lambda, \mu, \eta, \tau \in \mathbb{F}_2$, need to be considered.

For each of these pairs, the corresponding AND coefficient is given by Theorem 7. In its notation, set $p = R^{-1}(b')$ and $q = R^{-1}(a')$, and define $r_0 = R^{-1}(d_0 + a' \wedge b')$. Then

$$\begin{aligned} r &= R^{-1}(d + a' \wedge b') \\ &= r_0 + \eta e_n + \tau e_j, \end{aligned}$$

where $j = n - \gamma$. Thus, the RQTM entry of modular addition is obtained as the sum of the 16 AND-RQTM contributions corresponding to $\lambda, \mu, \eta, \tau \in \mathbb{F}_2$.

For $1 \le i \le n$ and $s, r \in \mathbb{F}_2$, define the normalized one-bit coefficient

$$\phi_i(s, r) = \frac{1}{4} \sum_{\substack{x,y \in \mathbb{F}_2 \\ p_i x + q_i y = r}} (-1)^{u'_i x + v'_i y + sxy}.$$

By Lemma 2, $\phi_i(s, r)$ is nonzero if and only if $q_i u'_i + p_i v'_i + sr = s p_i q_i$ and $\bar{p}_i \bar{q}_i (r \vee u'_i \vee v'_i) \le s$. When these conditions hold,

$$\phi_i(s, r) = 2^{-1 + \bar{p}_i \bar{q}_i \bar{s}} (-1)^{(\bar{q}_i r u'_i) \vee (u'_i v'_i s) \vee (q_i r v'_i)}.$$

Recall that $j = n - \gamma$. We split the n coordinates into the two blocks $\{1, \dots, j\}$ and $\{j+1, \dots, n\}$, and define

$$\begin{aligned} F_0(\lambda, \tau) &= \left(\prod_{i=1}^{j-1} \phi_i((s_0)_i + \lambda, (r_0)_i) \right) \phi_j((s_0)_j + \lambda, (r_0)_j + \tau), \\ F_1(\mu, \eta) &= \left(\prod_{i=j+1}^{n-1} \phi_i((s_0)_i + \mu, (r_0)_i) \right) \phi_n((s_0)_n + \mu, (r_0)_n + \eta), \end{aligned}$$

where an empty product is equal to 1. For later use, set

$$G_0(\lambda) = \sum_{\tau \in \mathbb{F}_2} F_0(\lambda, \tau), \qquad G_1(\mu) = \sum_{\eta \in \mathbb{F}_2} (-1)^{\mu\eta} F_1(\mu, \eta).$$

Theorem 8 (RQTM of modular addition)**.** *Let $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ be defined by $F(x, y) = x \boxplus y$. For $a, b, c, u, v, w \in \mathbb{F}_2^n$, let κ, G_0, and G_1 be defined by the preceding modular-addition construction with respect to the rotation $R = R^\gamma$, where $1 \le \gamma < n$. Then*

$$A^F_{(w,c),(u \| v, a \| b)} = \frac{1}{4} \big(G_0(0) + (-1)^{\kappa} G_0(1) \big) \big(G_1(0) + G_1(1) \big).$$

In particular, the entry is nonzero if and only if both factors on the right-hand side are nonzero.

Proof. By Lemma 3, $A^{F}_{(w,c),(u\|v,a\|b)} = A^{F_M}_{(w',c'),(u'\|v',a'\|b')}$. From the preceding discussion and Lemma 5, the latter reduces to

$$A^{F}_{(w,c),(u\|v,a\|b)} = \frac{1}{4} \sum_{\lambda,\mu,\eta,\tau\in\mathbb{F}_2} (-1)^{\lambda\kappa+\mu\eta} A^{\mathrm{AND}}_{(s_0+\lambda U+\mu V,\, d_0+\eta e_\gamma+\tau e_n),(u'\|v',a'\|b')}.$$

For the AND coefficient, the vector r in Theorem 7 is

$$R^{-1}(d_0 + \eta e_\gamma + \tau e_n + a' \wedge b') = r_0 + \eta e_n + \tau e_j,$$

where we used $R^{-1}(e_\gamma) = e_n$ and $R^{-1}(e_n) = e_j$.

The dependence of the mask $s_0 + \lambda U + \mu V$ on λ and μ is confined to the first block $\{1, \ldots, j\}$ and the second block $\{j+1, \ldots, n\}$, respectively. Likewise, the dependence of $r_0 + \eta e_n + \tau e_j$ on τ and η is confined to the first and second blocks, respectively. Since the RQTM of bitwise AND factorizes coordinate-wise, it follows that

$$A^{\mathrm{AND}}_{(s_0+\lambda U+\mu V,\, d_0+\eta e_\gamma+\tau e_n),(u'\|v',a'\|b')} = F_0(\lambda,\tau)F_1(\mu,\eta).$$

Therefore, the four summation variables separate into two independent pairs:

$$\begin{aligned} A^{F}_{(w,c),(u\|v,a\|b)} &= \frac{1}{4} \left(\sum_{\lambda,\tau\in\mathbb{F}_2} (-1)^{\lambda\kappa} F_0(\lambda,\tau) \right) \left(\sum_{\mu,\eta\in\mathbb{F}_2} (-1)^{\mu\eta} F_1(\mu,\eta) \right) \\ &= \frac{1}{4} \big(G_0(0) + (-1)^{\kappa} G_0(1)\big)\big(G_1(0) + G_1(1)\big), \end{aligned}$$

as claimed. □

Theorem 8 also gives a simple description of the possible values of an RQTM entry of modular addition.

Corollary 2. *For every $\lambda, \mu \in \mathbb{F}_2$, the values $G_0(\lambda)$ and $G_1(\mu)$ are either zero or signed powers of two. Consequently, every nonzero RQTM entry of modular addition can be written as*

$$A^{F}_{(w,c),(u\|v,a\|b)} = \sigma\, 2^{-W} f_0 f_1, \qquad f_i \in \{1,\, 2^{d_i} - 1,\, 2^{d_i} + 1\},$$

where $\sigma \in \{-1, 1\}$, W is an integer, and each d_i is a positive integer whenever the corresponding factor is not 1.

Equivalently, every nonzero entry admits a representation $A^{F}_{(w,c),(u\|v,a\|b)} = N/2^{n+2}$ for some integer N, and the odd part of $|N|$ is the product of at most two factors of the form $2^d - 1$ or $2^d + 1$.

Proof. For fixed λ, the two terms $F_0(\lambda, 0)$ and $F_0(\lambda, 1)$ differ only in the second argument of the boundary coefficient ϕ_j. Whenever both are nonzero, these two coefficients have the same absolute value. Hence $G_0(\lambda)$ is either zero or a signed power of two. The same argument applies to $G_1(\mu)$, where only the second argument of ϕ_n varies and the factor $(-1)^{\mu\eta}$ changes only the relative sign.

Each of the two factors in Theorem 8 is therefore a sum of at most two signed powers of two. If their exponents coincide, the sum is either zero or another signed power of two. Otherwise, for $r < s$, a sum of the form $\pm 2^{-r} \pm 2^{-s}$ equals $\pm 2^{-s}(2^{s-r} \pm 1)$. This proves the first statement.

Finally, before the two-block factorization, the RQTM entry is a sum of terms consisting of a factor $1/4$ from Lemma 5 and an AND-RQTM coefficient whose denominator divides 2^n. Hence the complete entry can be written as $N/2^{n+2}$ for some integer N. The claimed structure of the odd part of $|N|$ then follows from the factorized form above. □

Appendix C.2 shows that the zero-mask specialization of Theorem 8, including its validity criterion, agrees exactly with the RX-differential probability formula of Biryukov, Lambin, and Udovenko [BLU25]. For constraint-based trail searches, an equivalent support-sign-weight representation of the two factors is given in Appendix D.

3.3 Rotational-Quasidifferential Trails

Motivated by the notion of a quasidifferential trail, we introduce the concept of a rotational-quasidifferential trail, which describes the propagation of RX relations through an iterated construction.

Definition 9 (Rotational-quasidifferential trail)**.** Let $F = F_r \circ \cdots \circ F_1$ and $G = G_r \circ \cdots \circ G_1$ be iterated functions. A rotational-quasidifferential trail, or simply an RQ trail, for F and G is a sequence $(u_1, a_1), \ldots, (u_{r+1}, a_{r+1})$ of RX mask-difference pairs. The correlation of this rotational-quasidifferential trail is defined as

$$\prod_{i=1}^{r} A^{F_i/G_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}.$$

The entrywise RQTM–QDTM correspondence established in Section 3.2 extends directly to trails. Consider a sequence of layer pairs (F_i, G_i), where $F_i, G_i : \mathbb{F}_2^{n_i} \to \mathbb{F}_2^{n_{i+1}}$ for $i = 1, \ldots, r$, and let R_i denote the rotation on $\mathbb{F}_2^{n_i}$. For each layer, define $\widetilde{G}_i = R_{i+1}^{-1} \circ G_i \circ R_i$, and for each state index $i = 1, \ldots, r+1$, define $\Phi_i(u_i, a_i) = (u_i, R_i^{-1}(a_i))$. The maps Φ_i give a one-to-one correspondence between RQ trails for $(F_i, G_i)_{i=1}^r$ and quasidifferential trails for $(F_i, \widetilde{G}_i)_{i=1}^r$, and corresponding trails have exactly the same correlation.

A rotational-quasidifferential trail whose masks are all zero corresponds directly to an RX characteristic. Moreover, by (1),

$$A^{F_i/G_i}_{(0,a_{i+1}),(0,a_i)} = \Pr_{\mathbf{x}_i}[G_i(R(\mathbf{x}_i) + a_i) = R(F_i(\mathbf{x}_i)) + a_{i+1}]\,.$$

Therefore, the correlation of the zero-mask rotational-quasidifferential trail can be computed as $\prod_{i=1}^r A^{F_i/G_i}_{(0,a_{i+1}),(0,a_i)}$, which coincides with the probability estimate of an RX characteristic under the round-independence assumption described in Section 2.2.

The following theorem provides an exact expression for the probability of an RX characteristic.

Theorem 9. *Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be functions such that $F = F_r \circ \cdots \circ F_1$ and $G = G_r \circ \cdots \circ G_1$. The probability of an RX characteristic with intermediate RX-differences $a_1, \ldots, a_{r+1}$ is equal to the sum of the correlations of all rotational-quasidifferential trails with the same intermediate differences:*

$$\Pr\left[\bigwedge_{i=1}^{r} G_i(R(\mathbf{x}_i) + a_i) = R(F_i(\mathbf{x}_i)) + a_{i+1}\right] = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} A^{F_i/G_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}$$

with $u_1 = u_{r+1} = 0$, $\mathbf{x}_i = F_{i-1}(\mathbf{x}_{i-1})$ for $i = 2, \ldots, r$, and $\mathbf{x}_1$ uniformly random on $\mathbb{F}_2^n$.

This theorem concerns only the state-update function and does not incorporate the key schedule. It shows that the exact fixed-key probability of an RX characteristic can be obtained by summing the correlations of all rotational-quasidifferential trails sharing the same sequence of intermediate RX-differences.

The following theorem is the rotational analogue of Theorem 3 and provides a useful criterion for proving that an RX characteristic is incompatible.

Theorem 10. *Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be functions such that $F = F_r \circ \cdots \circ F_1$ and $G = G_r \circ \cdots \circ G_1$. Let $a_1, \ldots, a_{r+1}$ be an RX characteristic, and let p denote the correlation of the zero-mask rotational-quasidifferential trail $(0, a_1), \ldots, (0, a_{r+1})$ associated with the characteristic.*

(1) Let $(u_1, a_1), \ldots, (u_{r+1}, a_{r+1})$ *be a rotational-quasidifferential trail with correlation* $(-1)^b p$*, where* $b \in \{0, 1\}$*, and let* $(v_1, a_1), \ldots, (v_{r+1}, a_{r+1})$ *be another rotational-quasidifferential trail with correlation* c*. Then* $(u_1 + v_1, a_1), \ldots, (u_{r+1} + v_{r+1}, a_{r+1})$ *has correlation* $(-1)^b c$*. Equivalently,*

$$\prod_{i=1}^{r} A^{F_i/G_i}_{(u_{i+1}+v_{i+1}, a_{i+1}),(u_i+v_i, a_i)} = (-1)^b \prod_{i=1}^{r} A^{F_i/G_i}_{(v_{i+1}, a_{i+1}),(v_i, a_i)}.$$

(2) If there exists a collection of rotational-quasidifferential trails with differences $a_1, \ldots, a_{r+1}$ *and correlations* $\pm p$ *whose correlations sum to zero, then the probability of the RX characteristic* $(a_1, \ldots, a_{r+1})$ *is zero.*

3.3.1 Incorporating the Key Schedule

The previous results concern only the state-update function. Since RX cryptanalysis tracks RX-differences in both the data path and the key path, the key schedule must also be taken into account.

As in the extended quasidifferential framework [BDG25], we treat the key as part of the state. This enables the exact evaluation of RX characteristic probabilities averaged over uniformly sampled plaintexts and master keys; all round keys are then determined by the key schedule. The corresponding quantity is formalized by the notion of Expected Rotational-XOR Probability (ERXP), defined below.

Definition 10 (Expected rotational-XOR probability (ERXP))**.** Let E be a block cipher with plaintext space $\mathcal{X} = \mathbb{F}_2^n$ and master-key space $\mathcal{K} = \mathbb{F}_2^\ell$, where each instance E_k is a permutation on $\mathcal{X}$ indexed by $k \in \mathcal{K}$. Given an input RX-difference a, an output RX-difference b, and a master-key RX-difference c, the Expected Rotational-XOR Probability (ERXP) of (a, b) under c is defined as

$$\mathrm{ERXP}_E(a \to b; c) = \Pr_{\mathbf{x},\mathbf{k}}[E_{\mathbf{k}'}(R^\gamma(\mathbf{x}) + a) = R^\gamma(E_{\mathbf{k}}(\mathbf{x})) + b],$$

where $\mathbf{x}$ and $\mathbf{k}$ are sampled independently and uniformly from $\mathcal{X}$ and $\mathcal{K}$, respectively, $\mathbf{x}' = R^\gamma(\mathbf{x}) + a$, and $\mathbf{k}' = R^\gamma(\mathbf{k}) + c$.

To account for RX-differences in the round keys, we extend the state space by including the key schedule. This allows us to compute the average RX probability over both plaintexts and keys, rather than for a fixed key. As in the extended quasidifferential framework [BDG25], the ERXP of an RX characteristic is obtained by summing the correlations of all associated rotational-quasidifferential trails defined over the joint plaintext-key space.

Theorem 11. *Let* $F = F_r \circ \cdots \circ F_1$ *act on the joint plaintext–key state* $\mathbb{F}_2^n \times \mathbb{F}_2^\ell$*, and let* $Q = \big((a_x^1, a_k^1), \ldots, (a_x^{r+1}, a_k^{r+1})\big)$ *be an RX characteristic over* F*. The sequences* $(a_x^1, \ldots, a_x^{r+1})$ *and* $(a_k^1, \ldots, a_k^{r+1})$ *describe the RX characteristics on the plaintext and key paths, respectively. Then,*

$$\mathrm{ERXP}(Q) := \Pr\left[\bigwedge_{i=1}^{r} F_i\big(R(x_i, k_i) + (a_x^i, a_k^i)\big) = R(F_i(x_i, k_i)) + (a_x^{i+1}, a_k^{i+1})\right]$$

$$= \sum_{\substack{u_x^2, \ldots, u_x^r \\ u_k^2, \ldots, u_k^r}} \prod_{i=1}^{r} A^{F_i}_{((u_x^{i+1}, u_k^{i+1}),(a_x^{i+1}, a_k^{i+1})),((u_x^i, u_k^i),(a_x^i, a_k^i))}.$$

where $(u_x^1, u_k^1) = (u_x^{r+1}, u_k^{r+1}) = (0, 0)$*,* $(x_i, k_i) = F_{i-1}(x_{i-1}, k_{i-1})$ *for* $i = 2, \ldots, r$*, and* (x_1, k_1) *is sampled uniformly from* $\mathbb{F}_2^n \times \mathbb{F}_2^\ell$*. The initial key-path difference* a_k^1 *is the prescribed master-key RX-difference* c*.*

4 Applications

We apply the proposed framework to the ARX cipher SPECK, the ARX permutation Alzette, and the AND-RX ciphers SIMON and SIMECK. The examples cover three complementary settings. Appendix A gives a fixed-key validation for SIMECK32/64, together with a correction to reported SIMON48/72 characteristics. Section 4.1 uses Alzette, which has no key schedule, to isolate dependencies across a complete ARX data path. The remaining SIMECK and SPECK analyses use the joint data-key model to study average-key behavior over the entire key space. The RX characteristics from previous work that are used in this section are reproduced in Appendix B.

Implementation. We implemented the RQ trail searches in Python using PyBoolector and incremental bit-vector solving. For modular addition, the implementation models the support, sign, and weight of each local RQTM coefficient using the constraints summarized in Appendix D. Given the cipher parameters and the data- and key-path RX characteristics, it first evaluates every zero-mask local coefficient. If the zero-mask product is nonzero, it searches for a nonzero RQ trail with the same absolute correlation and the opposite global sign; otherwise, it reports the zero local coefficients that already prove incompatibility. The implementation stores the input characteristics and the corresponding textual search results together with the search scripts.

4.1 Full-Data-Path RXP Analysis of Alzette

Biryukov, Lambin, and Udovenko [BLU25] searched for four-step RX characteristics of the 64-bit ARX permutation Alzette and evaluated each characteristic by multiplying the exact RX probabilities of its four modular additions. Their accompanying experiments show that this independent-ADD estimate can differ from the probability observed over the complete data path. We use the RQ framework to explain this discrepancy for the three characteristics considered here.

Write one Alzette step as

$$z_i = x_i + \mathrm{ROR}_{a_i}(y_i), \qquad y_{i+1} = y_i \oplus \mathrm{ROR}_{b_i}(z_i), \qquad x_{i+1} = z_i \oplus c,$$

where

$$(a_i, b_i) \in \{(31, 24), (17, 17), (0, 31), (24, 16)\}$$

and c is the fixed public Alzette constant. We write $c_0 = \texttt{b7e15162}$ and $c_7 = \texttt{c2b3293d}$ for the two constants used below. For RQ masks (X_i, Y_i) and (X_{i+1}, Y_{i+1}) at two consecutive state boundaries, transposing the linear layer gives the masks

$$u_i = X_i, \qquad v_i = \mathrm{ROR}_{a_i}(Y_i \oplus Y_{i+1}), \qquad w_i = X_{i+1} \oplus \mathrm{ROL}_{b_i}(Y_{i+1})$$

at the corresponding modular addition. The constant XOR contributes the sign $(-1)^{\langle X_{i+1}, c\rangle}$. Since Alzette has no key schedule, the resulting signed sum is a full-data-path RXP rather than an expectation over a key space.

With zero internal masks, the RQ correlation equals the product of the four ADD probabilities used in [BLU25]; nonzero-mask trails capture dependencies between the additions that this product omits. Table 1 compares the resulting estimates with the reported experiments.

The strongest effect occurs for c_7 and $\gamma = 12$. The signed RQ sum is approximately 0.19 times the zero-mask value, increasing the weight by 2.40 bits, while the reported experiment differs from the independent estimate by 2.49 bits. The c_0, $\gamma = 1$ case similarly changes by 1.55 bits and closely matches the experimental weight. The c_7, $\gamma = 2$ case serves as a smaller-deviation control.

Table 1: Independent-ADD and full-data-path RQ estimates for four-step Alzette RX characteristics. Here γ is the rotation offset, Independent is the product of the four ADD probabilities, Cutoff is the maximum RQ trail weight included in the signed sum, # Trails counts the included nonzero-mask trails, RQ sum is the resulting truncated signed sum, and Experiment is the value reported in [BLU25]. All probability and cutoff entries are given as negative base-two logarithms; the zero-mask trail is excluded from # Trails.

Constant	γ	Independent	Cutoff	# Trails	RQ sum	Experiment
c_7	12	33.00	45	751	35.40	35.49
c_0	1	33.66	41	133	35.21	35.26
c_7	2	32.45	40	215	32.87	32.79

The RQ expression itself is exact, but the numerical RQ values in Table 1 are truncated sums over all nonzero-mask trails up to the stated cutoff and are not formal bounds on the omitted tail. For c_7 and $\gamma = 12$, increasing the cutoff through 39, 41, 43, and 45 gives weights 34.91, 35.27, 35.41, and 35.40, respectively. This stabilization, together with the agreement in all three experiments, shows that the signed nonzero-mask contributions account for the observed departure from the independent-ADD estimate.

4.2 Revisiting the Results of [SRB21]

In [SRB21], Sadeghi *et al.* showed that the RX characteristics proposed in [LLA+20] for 27 and 35 rounds of SIMECK48/96 and SIMECK64/128, respectively, are incompatible.

In Section 3.3.1, we showed how the ERXP of an RX characteristic can be computed within the geometric framework while taking the key schedule into account. This provides a new perspective on the incompatibility results of [SRB21]. In this section, we reinterpret the incompatibility of the RX characteristics through rotational-quasidifferential trails and identify the corresponding incompatibility constraints. Furthermore, we derive an additional incompatibility constraint for SIMECK48/96 and explain the incompatibility of the SIMECK64/128 characteristic, which remained unexplained in [SRB21]. We then revisit the incompatible 11- and 12-round SPECK32/64 characteristics, show that they fail for different reasons, and repair the incompatible part of the 12-round characteristic.

4.2.1 SIMECK48/96

We first revisit the RX characteristic for SIMECK48/96 analyzed in [SRB21]. Using rotational-quasidifferential trails, we recover the incompatibility condition identified in the previous work and derive an additional incompatibility constraint.

Table 2 shows the first 10 rounds of three rotational-quasidifferential trails with absolute correlation 2^{-94}, excluding the trail with all-zero masks. For all these trails, the masks in the data path are all zero. Therefore, only the masks in the key path are shown. Table 2 lists the masks for the bitwise AND operations in the key path for the first 10 rounds; all masks in the key path for the remaining rounds are zero.

Let $g(x) = x \wedge (x \lll 5)$ denote the nonlinear AND term in the SIMECK round function, and let $\Delta_1\alpha$ and $\Delta_1\beta$ denote the input and output RX-differences of g, respectively. In [SRB21], Sadeghi *et al.* showed the incompatibility by using the observations that

$$(x_{j+1} \wedge x_{j+6}) + ((x_{j+6} + \Delta_1\alpha_{j+5}) \wedge (x_{j+1} + \Delta_1\alpha_{j+1})) = \Delta_1\beta_j$$

and

$$k^6_{18} = (k^3_{23} \wedge k^3_{18}) + k^3_{19} + k^2_{18} + c^3_{18} \tag{2}$$

Table 2: Masks of rotational-quasidifferential trails for SIMECK48/96 in [LLA+20].

	Trail 1			Trail 2			Trail 3		
Round	**in1**	**in2**	**out**	**in1**	**in2**	**out**	**in1**	**in2**	**out**
1	000000	000000	000000	000000	000000	000000	000000	000000	000000
2	000020	000000	000000	000000	000000	000000	000020	000000	000000
3	000010	000000	000020	000000	000000	000000	000010	000000	000020
4	000000	000000	000000	000000	000000	000000	000000	000000	000000
5	000000	000000	000000	000000	000000	000000	000000	000000	000000
6	000020	000000	000000	000020	000000	000000	000000	000000	000000
7	000000	000000	000000	000010	000000	000020	000010	000000	000020
8	000000	000000	000000	000000	000000	000000	000000	000000	000000
9	000000	000000	000000	000000	000000	000000	000000	000000	000000
10	000000	000000	000000	000020	000000	000000	000020	000000	000000
Corr.		-2^{-94}			-2^{-94}			2^{-94}	

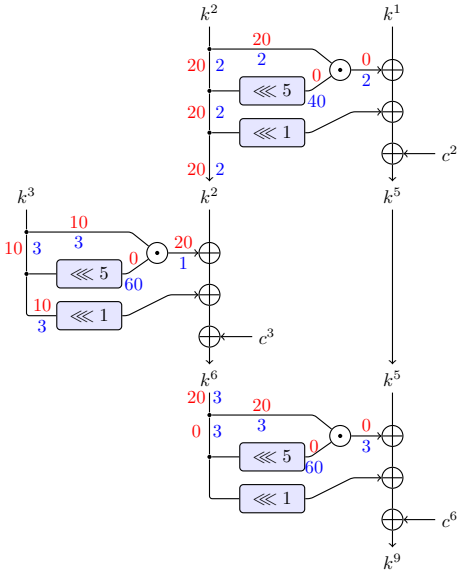

Figure 1: Part of rotational-quasidifferential Trail 1 in Table 2 (rounds 2, 3, and 6). Red denotes masks, blue denotes RX-differences, and values are represented in hexadecimal.

where k^i is the i-th round key and c^i is the word-sized round constant used in the corresponding key-schedule update. Using the first equation, they derived $k^2_{18} = k^3_{18} = k^3_{19} = k^6_{18} = 0$. Substituting these values into Equation 2 gives $0 = c^3_{18} = 1$, a contradiction.

Each nonzero trail corresponds to a specific key constraint. We now show how these constraints recover the incompatibility identified in [SRB21]. The same incompatibility can be interpreted directly from Trail 1 in Table 2. The masks in round 2 are $(0x20, 0x0, 0x0) = (32, 0, 0)$, and we have $A^{\mathrm{AND}}_{(0,0),(0||0,2||64)} = A^{\mathrm{AND}}_{(0,0),(32||0,2||64)} = 2^{-2}$, which implies the constraint $k^2_{18} = 0$. Applying the same argument to round 6 yields $k^6_{18} = 0$. Similarly, round 3 imposes $(in1)_{19} + (out)_{18} = 0$, where $in1 = k^3$ and $out = k^3 \wedge (k^3 \lll 5)$; equivalently, $k^3_{19} + k^3_{18}k^3_{23} = 0$. Finally, for $f_c(x) = x + c^3$, $A^{f_c}_{(32,3),(32,5)} = -1$, which corresponds to Equation 2. The correlation -1 indicates that the induced key condition contradicts the relation imposed by the round-constant addition, proving incompatibility.

Trail 2 yields an additional constraint through rounds 6, 7, and 10. Applying the same analysis yields the constraints $k^6_{18} = 0$, $k^{10}_{18} = 0$, and $k^7_{19} + k^7_{18}k^7_{23} = 0$, which again leads to a contradiction. This additional incompatibility constraint was not identified in [SRB21].

Trail 3 does not introduce any new constraint. Indeed, it can be obtained as the XOR of Trails 1 and 2, which follows directly from Theorem 10.

Table 3: Part of the rotational-quasidifferential trails for SIMECK64/128.

Trail	Round	in1	in2	out
Trail 1	5	00000020	00000000	00000000
	6	00000010	00000000	00000020
	9	00000020	00000000	00000000
	Corr.	-2^{-126}		
Trail 2	21	00000020	00000000	00000000
	22	00000010	00000000	00000020
	25	00000020	00000000	00000000
	Corr.	-2^{-126}		
Trail 3	24	00000020	00000000	00000000
	25	00000010	00000000	00000020
	28	00000020	00000000	00000000
	Corr.	-2^{-126}		

4.2.2 SIMECK64/128

In [SRB21], Sadeghi *et al.* used an MILP-based method to reveal incompatible RX characteristics for SIMECK48/96 and SIMECK64/128, and provided an explanation for the incompatibility observed in SIMECK48/96. However, no corresponding explanation was given for SIMECK64/128. In this work, we identify the underlying reason for this incompatibility by using our framework.

Table 3 shows three rotational-quasidifferential trails corresponding to the RX characteristic of SIMECK64/128. Only the nonzero masks in the key path are listed, since all masks in the data path and the remaining key-path masks are zero.

In total, there are eight rotational-quasidifferential trails corresponding to this RX characteristic, all of which can be generated by linear combinations of the three trails shown in Table 3. The three trails exhibit the same structure as Trails 1 and 2 of the SIMECK48/96 characteristic, but at different round positions. Consequently, the same rotational-quasidifferential analysis yields the following constraints.

Proposition 2. *The RX characteristic of SIMECK64/128 reported in [LLA+20] is incompatible.*

Proof. For each $i \in \{5, 21, 24\}$, the corresponding RQ trails impose

$$k_{18}^{i} = 0, \qquad k_{18}^{i+4} = 0, \qquad k_{19}^{i+1} + k_{18}^{i+1} \wedge k_{23}^{i+1} = 0$$

on the key values. On the other hand, the key schedule gives

$$k_{18}^{i+4} = (k_{23}^{i+1} \wedge k_{18}^{i+1}) + k_{19}^{i+1} + k_{18}^{i} + c_{18}^{i+1}$$

with $c_{18}^{i+1} = 1$. Substituting the three RQ constraints into this relation gives $0 = 1$, a contradiction. □

4.2.3 SPECK32/64

Sadeghi *et al.* [SRB21] showed that both SPECK32/64 RX characteristics in Table 2 of [LWRA17], covering 11 and 12 rounds, are incompatible. Applying the joint data-key RQ model of Section 3.3.1, we reproduce both results. The RQ trails also show that the two characteristics are incompatible for different reasons.

The 11-round characteristic. Let $p > 0$ be the correlation of the all-zero-mask joint RQ trail for the 11-round SPECK32/64 characteristic. Its weight is 67.47, including both the data path and the SPECK key schedule. We find a second joint RQ trail with correlation $-p$. All its data-path masks are zero. In the key path, the nonzero masks appear at the fifth and eighth key-schedule modular additions; these are the only two additions with nonzero masks, as shown in Table 4.

Table 4: Nonzero masks at the key-schedule modular additions of the cancelling RQ trail for the 11-round SPECK32/64 characteristic.

Key ADD	(u, v, w)	Zero-mask correlation	Cancelling-trail correlation
5	$(0000, 0000, 8001)$	2^{-6}	2^{-6}
8	$(0300, 0000, 0000)$	$3 \cdot 2^{-8}$	$-3 \cdot 2^{-8}$

All remaining RQTM correlations have the same value as in the zero-mask trail. Hence the second trail has the same absolute correlation and the opposite sign. The positive correlation at the fifth addition requires the two key bits selected by its output mask to have equal parity. After propagation through the intervening key-schedule updates, these are precisely the two bits selected by the input mask at the eighth addition, whose negative correlation requires opposite parity. Thus, no key state can satisfy both conditions. By Theorem 10, this nonzero-mask RQ trail induces a sign-reversing pairing of all joint RQ trails, so the ERXP is zero. This gives an RQ interpretation of the contradiction between Equations (9) and (12) in [SRB21].

The published 12-round characteristic. The failure occurs earlier than in the 11-round case. The joint RQ trail with all-zero masks already contains two zero coefficients. More precisely, the fifth and sixth key-schedule modular additions have zero-mask RX-difference triples

$$(a, b, c) = (0208, 0001, 0008) \qquad \text{and} \qquad (a, b, c) = (0800, 0000, 000e),$$

respectively, and $A^{\mathrm{ADD}}_{(0,c),(0\|0,a\|b)} = 0$ for both transitions. Thus, these local RX transitions have no right pairs, so the zero-mask product is already zero; an opposite-sign RQ trail is neither needed nor defined relative to a nonzero value p. These two transitions depend only on later differences derived from the published round-key differences. Consequently, choosing different RX-differences for the three omitted master-key words cannot repair the characteristic.

A compatible 12-round characteristic. The RQ analysis localizes the obstruction to the key-schedule segment above. Changing the round-2 key RX-difference from 0001 to 0000, and propagating this change to round 11 and the output, gives the characteristic in Table 5.

Table 5: A compatible 12-round RX characteristic for SPECK32/64.

Round	Key RX-difference	Data RX-difference
0	0000	(0050||2000)
1	0100	(8000||0000)
2	**0000**	(0000||0000)
3	0000	(0000||0000)
4	0001	(0000||0000)
5	0000	(0000||0000)
6	0001	(0000||0000)
7	0200	(0000||0000)
8	0206	(0200||0200)
9	0800	(0000||0800)
10	2001	(0000||2000)
11	**ac0e**	(0000||8000)
12	–	**(2c0e||2c0c)**

The data-path zero-mask weights of this characteristic and the published incompatible trail both round to 25.57; more precisely, the former data correlation is larger by the factor 32769/32767. All key-schedule zero-mask coefficients are now nonzero. The key and joint

zero-mask weights are 59.08 and 84.64, respectively. To the best of our knowledge, Table 5 is the first compatible 12-round RX characteristic for SPECK32/64. Its compatibility is confirmed by an explicit right key and plaintext pair. [1]

This example illustrates why the RQ framework is useful beyond probability evaluation. In this case, we do not need to search for a new RX trail from scratch. It is sufficient to identify the incompatible segment and replace it with a compatible one while preserving the remainder of the trail. The RQ framework plays a central role in this process because it identifies the local transition and the propagated mask responsible for the global contradiction.

The same RQ consistency analysis identifies a likely typographical error in the published 13-round SPECK96/144 characteristic of [LWRA17]. With the printed round-7 key RX-difference `000000000010`, the round-7 data addition and the round-6 and round-7 key additions have RX-difference triples

$$(\texttt{000000000000}, \texttt{000000000000}, \texttt{000000000013}),$$
$$(\texttt{000000000000}, \texttt{000000000001}, \texttt{000000000012}),$$
$$(\texttt{010000000000}, \texttt{000000000010}, \texttt{070000000097}),$$

respectively. For each transition, the all-zero-mask ADD-RQTM correlation is zero, so the transition admits no right pair. In particular, the printed characteristic also fails the local modular-addition validity constraints used by the original search, rather than exposing an additional dependency absent from that model. As in the 12-round SPECK32/64 case, we therefore attribute the discrepancy to a likely transcription or output-reporting error, while noting that its exact origin cannot be established without the original solver output. Correcting the printed value to `000000000002` restores the reported data- and key-path probabilities and yields a compatible characteristic. The corrected characteristic, the RQ-based diagnosis, and an explicit right key and plaintext pair are given in Appendix B.1.

4.3 Analysis of SPECK RX Characteristics from [ZZZW25]

Improved RX characteristics for several SPECK variants were reported in [ZZZW25]. We applied the joint data-key RQ model to the six characteristics listed below. These are the 15-round SPECK48/96, 17-round SPECK64/128, 16- and 17-round SPECK96/144, and 23- and 24-round SPECK128/256 characteristics. The 16-round SPECK96/144 and 23-round SPECK128/256 characteristics are exact prefixes of the displayed 17- and 24-round characteristics, respectively. For the initial key-register differences omitted from the published tables, the exact maximum-probability completion is unique in every case.

Table 6 summarizes the result. The exact zero-mask weights reproduce the values reported in [ZZZW25]. For five of the six characteristics, however, we find a nonzero-mask joint RQ trail having exactly the same absolute correlation as the zero-mask trail and the opposite sign. By Theorem 10, each such trail induces a sign-reversing pairing of all joint RQ trails, and hence proves that the corresponding ERXP is zero.

The 17-round SPECK64/128 characteristic gives a compact representative example. Let p be its zero-mask joint correlation, whose weight is 168.62; its data- and key-path components have weights 53.06 and 115.57, respectively. The cancelling RQ trail has zero masks throughout the data path. In the key path, its only nonzero ADD masks are $(u, v, w) = (\texttt{00000000}, \texttt{00000000}, \texttt{00000005})$ at round 12 and $(\texttt{05000000}, \texttt{00000000}, \texttt{00000000})$ at round 15.

[1] We use the convention $\Delta_1(x, x') = R(x) + x'$ and the SPECK master-key ordering $K = (l_2, l_1, l_0, k_0)$. Take $K = (\texttt{3F07}, \texttt{EFAF}, \texttt{38A7}, \texttt{8FE2})$ and $K' = (\texttt{810E}, \texttt{6062}, \texttt{F14E}, \texttt{1FC5})$. Their master-key RX-difference is $(\texttt{FF00}, \texttt{BF3D}, \texttt{8000}, \texttt{0000})$, and expanding the two keys gives exactly the twelve round-key RX-differences in Table 5. For $P = (\texttt{D989}\|\texttt{278B})$ and $P' = (\texttt{B343}\|\texttt{6F16})$, the input RX-difference is $(\texttt{0050}\|\texttt{2000})$. After twelve rounds, $C = (\texttt{E633}\|\texttt{42AA})$ and $C' = (\texttt{E069}\|\texttt{A958})$, giving $\Delta_1(C, C') = (\texttt{2C0E}\|\texttt{2C0C})$. Every intermediate data RX-difference also agrees with the table.

Table 6: RQ analysis of the SPECK RX characteristics from [ZZZW25]. The data and key columns give exact zero-mask weights.

Variant	Rounds	Data	Key	RQ result	Nonzero masks in the cancelling trail
SPECK48/96	15	42.23	82.74	compatible	–
SPECK64/128	17	53.06	115.57	incompatible	key ADDs 12 and 15
SPECK96/144	16	78.81	131.57	incompatible	data ADDs 12–13; key ADDs 7–13
SPECK96/144	17	90.23	140.98	incompatible	key ADDs 7, 9, and 11
SPECK128/256	23	111.55	238.40	incompatible	key ADDs 7, 8, and 10–19
SPECK128/256	24	127.96	253.81	incompatible	key ADDs 7, 8, 10–13, 15–19, and 21

The output mask of the key-schedule modular addition in round 12 propagates through the intervening key-schedule updates and, after the prescribed rotation, becomes the input mask of the key-schedule modular addition in round 15. After accounting for the sign contributed by the relevant round-constant XOR, the product of the RQTM correlations is $-p$. As in the explicit SIMECK48/96 analysis of Section 4.2.1, mask propagation carries a key constraint between active nonlinear operations, while the correlation sign records whether the propagated constraints agree or contradict. Here, the negative sign yields the cancelling correlation $-p$. The other four incompatible cases admit the same RQ interpretation; their active data/key regions are listed in Table 6, so repeating the bit-level argument for each case is unnecessary. This illustrates that the RQ framework can detect and localize consistency failures.

4.4 Revisiting RXDR Attacks on SIMECK48/96

Chen *et al.* [CZX+23] constructed a 21-round rotational-XOR differential rectangle (RXDR) distinguisher for SIMECK48/96 by combining a 14-round RX characteristic with a 7-round differential distinguisher. The published estimate assigns the RX characteristic probability $p = 2^{-12}$ in the data path and $p_k = 2^{-24}$ in the key path, while the differential distinguisher has probability $\tilde{q} = 2^{-22.52}$. Consequently, they estimated the RXDR probability as $p^2 2^{-n} \tilde{q} = 2^{-94.52}$ and the weak-key class size as $2^{96} p_k = 2^{72}$.

Our joint RQ analysis gives exactly four trails, all with data-path correlation 2^{-12} and with key-path correlations 2^{-24}, -2^{-25}, -2^{-25}, and 2^{-26}. The key-path sum is therefore 2^{-26} rather than 2^{-24}, and the corresponding joint correlations sum to an ERXP of 2^{-38} rather than the published estimate $p \cdot p_k = 2^{-36}$. Consequently, the weak-key class size is 2^{70} rather than 2^{72}.

A direct Monte Carlo verification of the full 14-round characteristic would require an impractical number of samples, and verifying the even less probable complete RXDR event would be harder still. We therefore test the reduced characteristic obtained by removing the first four and the last round. The reduced RX characteristic has four rotational-quasidifferential trails with joint data-key correlations 2^{-22}, -2^{-23}, -2^{-23}, and 2^{-24}, whose sum is 2^{-24} rather than 2^{-22}. We experimentally verified this result using 2^{20} random keys and 2^{20} random plaintext pairs, obtaining an estimated probability of $2^{-23.8}$, which closely matches the predicted value 2^{-24}. The retained rounds contain the nonzero-mask key transitions responsible for the discrepancy, whereas the removed boundary rounds multiply all four correlations by the same factor 2^{-14} and do not change their relative signs or cancellation. Thus, the experiment isolates the relevant key-dependent cancellation at a measurable probability; it does not estimate the full characteristic or RXDR distinguisher.

The same phenomenon appears in the 17-round RX characteristic underlying the optimal 20-round RXDR distinguisher of [CZX+23]. Our analysis shows that its key probability is 2^{-34} rather than the reported value 2^{-32}. As a result, the corresponding weak-key class size is reduced from 2^{64} to 2^{62}.

5 Conclusion

In this paper, we introduced the first framework for rotational-XOR (RX) cryptanalysis based on the geometric approach. Inspired by the quasidifferential framework of Beyne and Rijmen [BR22], we developed the rotational-quasidifferential framework and derived exact expressions for RX characteristic probabilities in both fixed-key and average-key settings. This eliminates the need for the independence assumptions commonly used in previous analyses. We applied the proposed framework to SPECK, Alzette, SIMON, and SIMECK and revisited several existing cryptanalytic results. In particular, we reproduced the known incompatible SPECK32/64 characteristics and repaired the 12-round case. We also applied the same analysis to six SPECK RX characteristics [ZZZW25], identifying equal-magnitude, opposite-sign RQ trails that prove five of them incompatible. For Alzette, the signed RQ sums explained experimentally observed deviations from probability estimates obtained by multiplying independent ADD transitions. Our analyses validated the theoretical predictions of the rotational-quasidifferential framework, explained incompatibilities of RX characteristics, and refined the understanding of weak-key classes in rotational-XOR differential rectangle attacks. Overall, this work establishes a geometric framework for RX cryptanalysis and demonstrates that exact characteristic-level analysis can expose dependencies and incompatibilities hidden by probability estimates based on round independence.

Several interesting directions remain for future research. Recent developments in the mix-basis framework [HZC+25] suggest combining RQ bases with other basis choices. Such combinations may reveal new distinguishers or previously unexplored cryptanalytic properties. Finally, it would be interesting to extend the rotational-quasidifferential framework beyond RX characteristics. Potential targets include rotational-XOR differential rectangle attacks [CZX+23], rotational differential-linear cryptanalysis [LSL21, LNS+23, NSLL22], and rotational-linear attacks [XWL21]. In particular, He *et al.* [HHN+26] identify an independence-free geometric treatment as an important complementary direction; the framework developed here may provide a foundation for such an extension. More broadly, combining the RQ basis with suitable basis choices may enable exact analyses of rotational combined attacks, as the mix-basis framework has done for boomerang attacks [CHH+25, CHPW26].

References

[AL16] Tomer Ashur and Yunwen Liu. Rotational cryptanalysis in the presence of constants. *IACR Trans. Symm. Cryptol.*, 2016(1):57–70, 2016.

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

[Bey21] Tim Beyne. A geometric approach to linear cryptanalysis. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 36–66. Springer, Cham, December 2021.

[Bey23] Tim Beyne. *A Geometric Approach to Symmetric-Key Cryptanalysis*. PhD thesis, KU Leuven, Leuven, Belgium, June 2023.

[BLU25] Alex Biryukov, Baptiste Lambin, and Aleksei Udovenko. Exact formula for RX-differential probability through modular addition for all rotations. *IACR Trans. Symm. Cryptol.*, 2025(1):542–591, 2025.

[BR22] Tim Beyne and Vincent Rijmen. Differential cryptanalysis in the fixed-key model. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part III*, volume 13509 of *LNCS*, pages 687–716. Springer, Cham, August 2022.

[BS93] Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round DES. In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 487–496. Springer, Berlin, Heidelberg, August 1993.

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

[BV24] Tim Beyne and Michiel Verbauwhede. Ultrametric integral cryptanalysis. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part VII*, volume 15490 of *LNCS*, pages 392–423. Springer, Singapore, December 2024.

[CHH+25] Chengcheng Chang, Hosein Hadipour, Kai Hu, Muzhou Li, and Meiqin Wang. Mix-basis geometric approach to boomerang distinguishers. *IACR Trans. Symm. Cryptol.*, 2025(3):693–728, 2025.

[CHPW26] Chengcheng Chang, Kai Hu, Shuo Peng, and Haoyang Wang. An exact four-wise framework for boomerang cryptanalysis. Cryptology ePrint Archive, Paper 2026/1473, 2026.

[CZX+23] Siwei Chen, Mingming Zhu, Zejun Xiang, Runqing Xu, Xiangyong Zeng, and Shasha Zhang. Rotational-xor differential rectangle cryptanalysis on simon-like ciphers. In Mike Rosulek, editor, *Topics in Cryptology - CT-RSA 2023 - Cryptographers' Track at the RSA Conference 2023, San Francisco, CA, USA, April 24-27, 2023, Proceedings*, Lecture Notes in Computer Science, pages 305–330. Springer, 2023.

[HHN+26] Jiahui He, Kai Hu, Zhongfeng Niu, Bart Preneel, and Meiqin Wang. Revisiting differential-linear cryptanalysis via a walsh-transform perspective. Cryptology ePrint Archive, Paper 2026/2013, 2026.

[HZC+25] Kai Hu, Chi Zhang, Chengcheng Chang, Jiashu Zhang, Meiqin Wang, and Thomas Peyrin. Unlocking mix-basis potential: Geometric approach for combined attacks. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part V*, volume 16004 of *LNCS*, pages 293–334. Springer, Cham, August 2025.

[KN10] Dmitry Khovratovich and Ivica Nikolic. Rotational cryptanalysis of ARX. In Seokhie Hong and Tetsu Iwata, editors, *FSE 2010*, volume 6147 of *LNCS*, pages 333–346. Springer, Berlin, Heidelberg, February 2010.

[KNP+15] Dmitry Khovratovich, Ivica Nikolic, Josef Pieprzyk, Przemyslaw Sokolowski, and Ron Steinfeld. Rotational cryptanalysis of ARX revisited. In Gregor Leander, editor, *FSE 2015*, volume 9054 of *LNCS*, pages 519–536. Springer, Berlin, Heidelberg, March 2015.

[KW02] Lars R. Knudsen and David Wagner. Integral cryptanalysis. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 112–127. Springer, Berlin, Heidelberg, February 2002.

[LLA+20] Jinyu Lu, Yunwen Liu, Tomer Ashur, Bing Sun, and Chao Li. Rotational-xor cryptanalysis of simon-like block ciphers. In *Information Security and Privacy – 25th Australasian Conference, ACISP 2020*, pages 105–124. Springer, 2020.

[LLA+22] Jinyu Lu, Yunwen Liu, Tomer Ashur, Bing Sun, and Chao Li. Improved rotational-xor cryptanalysis of simon-like block ciphers. *IET Inf. Secur.*, 16(4):282–300, 2022.

[LMM91] Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 17–38. Springer, Berlin, Heidelberg, April 1991.

[LNS+23] Yunwen Liu, Zhongfeng Niu, Siwei Sun, Chao Li, and Lei Hu. Rotational differential-linear cryptanalysis revisited. *Journal of Cryptology*, 36(1):3, January 2023.

[LSL21] Yunwen Liu, Siwei Sun, and Chao Li. Rotational cryptanalysis from a differential-linear perspective - practical distinguishers for round-reduced FRIET, Xoodoo, and Alzette. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 741–770. Springer, Cham, October 2021.

[LWRA17] Yunwen Liu, Glenn De Witte, Adrián Ranea, and Tomer Ashur. Rotational-xor cryptanalysis of reduced-round SPECK. *IACR Trans. Symmetric Cryptol.*, 2017(3):24–36, 2017.

[Mat94] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 386–397. Springer, Berlin, Heidelberg, May 1994.

[NSLL22] Zhongfeng Niu, Siwei Sun, Yunwen Liu, and Chao Li. Rotational differential-linear distinguishers of ARX ciphers with arbitrary output linear masks. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 3–32. Springer, Cham, August 2022.

[SG13] Ernst Schulte-Geers. On CCZ-equivalence of addition mod 2^n. *DCC*, 66(1-3):111–127, 2013.

[SRB21] Sadegh Sadeghi, Vincent Rijmen, and Nasour Bagheri. Proposing an milp-based method for the experimental verification of difference-based trails: application to speck, SIMECK. *Des. Codes Cryptogr.*, 89(9):2113–2155, 2021.

[XLSL19] Wenqian Xin, Yunwen Liu, Bing Sun, and C. Li. Improved cryptanalysis on siphash. In *Cryptology and Network Security*, 2019.

[XWL21] Yaqi Xu, Baofeng Wu, and Dongdai Lin. Rotational-linear attack: A new framework of cryptanalysis on ARX ciphers with applications to chaskey. In Debin Gao, Qi Li, Xiaohong Guan, and Xiaofeng Liao, editors, *ICICS 21, Part I*, volume 12919 of *LNCS*, pages 192–209. Springer, Cham, November 2021.

[ZZZW25] Yuhan Zhang, Lei Zhang, Yafei Zheng, and Wenling Wu. A new automatic framework for searching rotational-XOR differential characteristics in ARX ciphers. *DCC*, 93(6):2013–2054, 2025.

A Fixed-Key Analysis

We consider only the data path and treat the round keys as independent constants, without taking the key schedule into account. This isolates key dependencies arising from the data path.

We analyzed the RX characteristics used to construct the rotational-XOR differential rectangle distinguishers in Tables 14, 15, and 19 of [CZX+23]. We did not observe any key dependency in these relatively short characteristics. We did, however, identify an error in the SIMON48/72 characteristics reported in Table 19: the RX-difference in either the key or the data should be $0x284920$ instead of $0x284900$.

We next consider the 20-round RX characteristic for SIMECK32/64 presented in Table 6 of [LLA+20], which also appears as Table 18 in [LLA+22]. We focus on the part from rounds 11 to 14, shown in Table 7. This is the shortest segment that exhibits nontrivial key dependence and therefore provides a convenient illustrative example.

Table 7: Part of the RX characteristic in [LLA+20, LLA+22] from rounds 11 to 14.

Key RX-difference	Data RX-difference
0013	(000a||0006)
000a	(0001||000a)
0004	(0002||0001)
	(0001||0002)

We enumerated all RQ trails corresponding to the segment in Table 7. Summing their correlations gives the exact probability

$$2^{-8} + (-1)^{k_5^2} 2^{-9} + (-1)^{k_{11}^2} 2^{-9} + (-1)^{k_5^2 + k_{11}^2} 2^{-10} = 2^{-10}(2 + (-1)^{k_5^2})(2 + (-1)^{k_{11}^2}),$$

where k_j^i is the j-th bit of the i-th round key.

To validate this result, we generated 10,000 random round-key triples (k^1, k^2, k^3) and, for each triple, constructed a corresponding related-key triple satisfying the target RX relation. For each related-key pair, we tested 2^{20} random plaintext pairs satisfying the prescribed RX-difference relation. The results are shown in Figure 2.

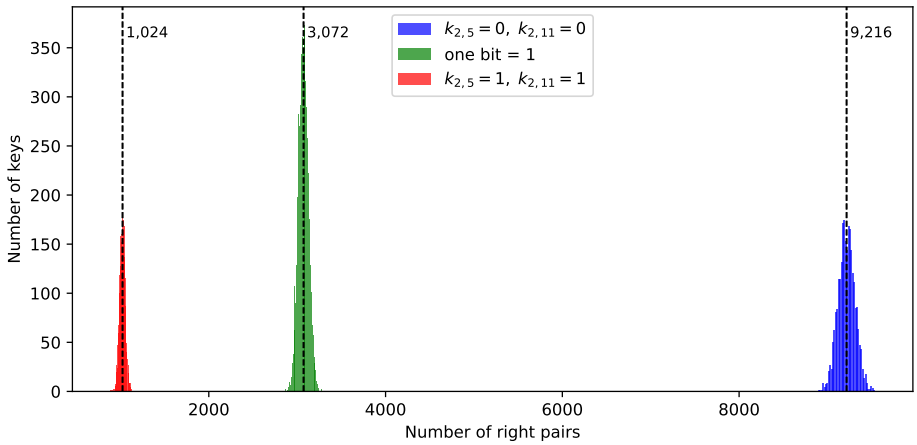

Figure 2: Histogram of the number of right pairs for 10,000 random round-key triples and 2^{20} plaintext pairs, showing agreement with the predicted key-dependent probabilities.

The histogram confirms the predicted three probability classes determined by k_5^2 and k_{11}^2. The left, middle, and right clusters correspond to probabilities 2^{-10}, $3 \cdot 2^{-10}$, and $9 \cdot 2^{-10}$, respectively. The middle cluster is approximately twice as high because it contains the two key conditions $(k_5^2, k_{11}^2) = (0, 1)$ and $(1, 0)$, whereas each of the other classes contains one.

Table 8 gives the complete 20-round RX characteristic, and Table 9 extends the analysis by grouping RQ trails according to their round-key masks.

Table 8: 20-round RX characteristic for SIMECK32/64.

Round	key RX-difference	data RX-difference
0	0004	(0000||0004)
1	0000	(0000||0000)
2	0001	(0000||0000)
3	0002	(0001||0000)
4	0002	(0000||0001)
5	0005	(0003||0000)
6	0001	(0000||0003)
7	0002	(0002||0000)
8	000a	(0004||0002)
9	0002	(0000||0004)
10	0000	(0006||0000)
11	0013	(000a||0006)
12	000a	(0001||000a)
13	0004	(0002||0001)
14	0000	(0001||0002)
15	0001	(0000||0001)
16	0000	(0000||0000)
17	0002	(0000||0000)
18	0006	(0002||0000)
19	0007	(0000||0002)
20		(0005||0000)
Prob.	2^{-34}	2^{-26}

To study key dependence, we enumerated all rotational-quasidifferential trails with absolute correlation at least 2^{-34} and summarized the resulting groups in Table 9. More precisely, the trails are grouped according to the tuple of round-key masks $(k^9, \ldots, k^{14})$, where k^i denotes the corresponding round-key mask in round i. All trails have zero key masks in the remaining rounds.

Table 9 shows that there are 23 distinct round-key-mask groups. Let $u_1, \ldots, u_{23} \in \mathbb{F}_2^{96}$ denote the corresponding masks. The first four groups in Table 9 are exactly those contributing to the rounds 11–14 segment in Table 7, and hence explain its key dependence.

Table 9: Rotational-quasidifferential trail groups for the 20-round RX characteristic of SIMECK32/64, classified by round-key masks.

Group correlation	sign	round-key mask (k^9–k^{14})
2^{-26}	+1	0000 0000 0000 0000 0000 0000
2^{-27}	+1	0000 0000 0000 0000 0800 0000
	+1	0000 0000 0000 0000 0020 0000
2^{-28}	+1	0000 0000 0000 0000 0820 0000
	+1	0000 0000 0000 0040 0800 0000
2^{-29}	+1	0000 0000 0000 0040 0820 0000
	-1	0800 0400 0a00 0100 0200 0400
	-1	0800 0400 0a20 0100 0200 0400
2^{-30}	-1	0800 0400 0a20 0100 0220 0400
	-1	0800 0400 0a20 0110 0200 0400
	-1	0800 0440 0a20 0100 0200 0400
	-1	0800 0400 0a20 0100 0a00 0400
	-1	0800 0400 0a00 0100 0a00 0400
	-1	0800 0400 0a00 0100 0220 0400
	-1	0800 0400 0a00 0110 0200 0400
	-1	0800 0440 0a00 0100 0200 0400
2^{-33}	+1	0020 0010 0028 0044 0808 0010
2^{-34}	+1	0020 0010 0028 0044 0828 0010
	+1	0020 0030 0028 0044 0808 0010
	+1	0020 0010 0038 0044 0818 0010
	+1	0020 0010 0028 0064 0838 0010
	+1	0020 0010 0028 4044 0808 0010
	+1	0020 0010 8028 0044 8808 0010

B RX Characteristics Used in Previous Work

B.1 SPECK RX Characteristics

Liu *et al.* [LWRA17] presented the 11- and 12-round SPECK32/64 RX characteristics reproduced in Tables 10 and 11. Both are incompatible, as analyzed in Section 4.2.3. The compatible 12-round replacement is already given in Table 5 and is therefore not repeated here.

The same work presented a 13-round SPECK96/144 characteristic. Applying the RQ framework to the printed differences makes the error local: at round 7, the zero input differences and the printed key RX-difference `000000000010` require the modular-addition output difference `000000000013`, whose zero-mask RQTM coefficient is zero. Keeping every other published difference fixed, replacing that key RX-difference by `000000000002` removes the impossible transition. The corrected characteristic in Table 12 has data- and key-path zero-mask weights 37.98 and 106.08, respectively, matching the reported rounded values. This agreement, together with an explicit right pair, shows that the printed value is a typographical error and that the corrected characteristic is compatible. [2]

[2]We use $\Delta_1(x, x') = R(x) + x'$ and the SPECK96/144 master-key order $K = (l_1, l_0, k_0)$. Take $K =$ (`814D7718C18C`, `34CC88DDAA02`, `8AEFB5DFA3F0`) and $K' =$ (`029AEE338819`, `699903F35504`, `15DF6BBD4FE0`). For $P =$ (`D2132F593A07`‖`33B666CC3939`) and $P' =$ (`A4265CBA740F`‖`676CCD987273`), expanding the keys and encrypting the plaintexts reproduces every round-key and intermediate data RX-difference in Table 12.

Table 10: Published 11-round RX characteristic for SPECK32/64 from [LWRA17].

Round	key RX-difference	data RX-difference
0	0000	(0000||0000)
1	0000	(0000||0000)
2	0000	(0000||0000)
3	0001	(0000||0000)
4	0000	(0000||0000)
5	0003	(0000||0000)
6	0200	(0000||0000)
7	0205	(0200||0200)
8	0801	(0000||0800)
9	2001	(0000||2000)
10	aa0b	(0000||8000)
11		(2a0b||2a09)
Prob.	$2^{-45.32}$	$2^{-22.15}$

Table 12: Corrected 13-round RX characteristic for SPECK96/144 from [LWRA17]. The bold entry corrects the printed value `000000000010`.

Round	key RX-difference	data RX-difference
0	000000020801	(000002080000||000000000001)
1	000000000008	(000000000000||000000000008)
2	000000000240	(000000000000||000000000040)
3	000000000000	(000000000200||000000000000)
4	000000000000	(000000000000||000000000000)
5	000000000000	(000000000000||000000000000)
6	000000000001	(000000000000||000000000000)
7	**000000000002**	(000000000000||000000000000)
8	07000000001e	(000000000003||000000000003)
9	390000000001	(000000000018||000000000000)
10	090100000010	(010000000000||010000000000)
11	100800000091	(080000000010||000000000010)
12	767707000425	(000000000080||000000000000)
13		(f67707000425||f67707000425)
Prob.	$2^{-106.08}$	$2^{-37.98}$

The complete SPECK characteristics from [ZZZW25] used in Section 4.3 are given in Tables 13, 14, 15, and 16. The published 16-round SPECK96/144 characteristic is the prefix through round 16 of Table 15, with key- and data-path weights 131.57 and 78.81, respectively. Likewise, the 23-round SPECK128/256 characteristic is the prefix through round 23 of Table 16, with key- and data-path weights 238.40 and 111.55.

Table 11: Published incompatible 12-round RX characteristic for SPECK32/64 from [LWRA17].

Round	key RX-difference	data RX-difference
0	0000	(0050||2000)
1	0100	(8000||0000)
2	0001	(0000||0000)
3	0000	(0000||0000)
4	0001	(0000||0000)
5	0000	(0000||0000)
6	0001	(0000||0000)
7	0200	(0000||0000)
8	0206	(0200||0200)
9	0800	(0000||0800)
10	2001	(0000||2000)
11	a40e	(0000||8000)
12		(240e||240c)
Prob.	$2^{-59.08}$	$2^{-25.57}$

Table 13: 15-round SPECK48/96 RX characteristic from [ZZZW25].

Round	key RX-difference	data RX-difference
0	000090	(909000||001000)
1	000080	(008000||000000)
2	000000	(000000||000000)
3	000000	(000000||000000)
4	000000	(000000||000000)
5	000000	(000000||000000)
6	000001	(000000||000000)
7	000001	(000000||000000)
8	000001	(000000||000000)
9	010011	(000001||000001)
10	100080	(000010||000018)
11	890391	(000089||000049)
12	c80002	(000248||000000)
13	000801	(000000||000000)
14	974119	(000800||000800)
15	–	(974910||970910)
Prob.	$2^{-82.74}$	$2^{-42.23}$

Table 14: 17-round SPECK64/128 RX characteristic from [ZZZW25].

Round	key RX-difference	data RX-difference
0	00000090	(00909000||00001000)
1	00000080	(00008000||00000000)
2	00000000	(00000000||00000000)
3	00000000	(00000000||00000000)
4	00000000	(00000000||00000000)
5	00000000	(00000000||00000000)
6	00000001	(00000000||00000000)
7	00000001	(00000000||00000000)
8	00000003	(00000000||00000000)
9	0700001f	(00000003||00000003)
10	38000000	(00000018||00000000)
11	01000000	(00000000||00000000)
12	08010002	(01000000||01000000)
13	0009000a	(09000003||01000003)
14	00000050	(00000008||08000010)
15	02000242	(00000040||400000c0)
16	04401142	(02000202||02000400)
17	–	(04421540||14423540)
Prob.	$2^{-115.57}$	$2^{-53.06}$

Table 15: 17-round SPECK96/144 RX characteristic from [ZZZW25]. Its 16-round prefix is also analyzed in Section 4.3.

Round	key RX-difference	data RX-difference
0	000000020801	(000002080000||000000000001)
1	000000000008	(000000000000||000000000008)
2	000000000240	(000000000000||000000000040)
3	000000000000	(000000000200||000000000000)
4	000000000000	(000000000000||000000000000)
5	000000000000	(000000000000||000000000000)
6	000000000001	(000000000000||000000000000)
7	000000000002	(000000000000||000000000000)
8	07000000001e	(000000000003||000000000003)
9	390000000003	(000000000018||000000000000)
10	0f0100000000	(010000000000||010000000000)
11	00080000001f	(080000000000||000000000000)
12	090101000002	(00000000001f||00000000001f)
13	480109000002	(0001010000f8||000101000000)
14	020000010002	(000009010002||000801010002)
15	000009080000	(000801090100||004809010110)
16	104249000110	(004808080810||020840000090)
17	–	(024a41080998||120841080d18)
Prob.	$2^{-140.98}$	$2^{-90.23}$

Table 16: 24-round SPECK128/256 RX characteristic from [ZZZW25]. Its 23-round prefix is also analyzed in Section 4.3.

Round	key RX-difference	data RX-difference
0	0000000000000090	(0000000000909000||0000000000001000)
1	0000000000000080	(0000000000008000||0000000000000000)
2	0000000000000000	(0000000000000000||0000000000000000)
3	0000000000000000	(0000000000000000||0000000000000000)
4	0000000000000000	(0000000000000000||0000000000000000)
5	0000000000000000	(0000000000000000||0000000000000000)
6	0000000000000001	(0000000000000000||0000000000000000)
7	0000000000000001	(0000000000000000||0000000000000000)
8	0000000000000007	(0000000000000000||0000000000000000)
9	070000000000003f	(0000000000000007||0000000000000007)
10	3800000000000000	(0000000000000038||0000000000000000)
11	0100000000000000	(0000000000000000||0000000000000000)
12	0801000000000003	(0100000000000000||0100000000000000)
13	0009000000000003	(0900000000000002||0100000000000002)
14	00000000000000f0	(0100000000000000||0900000000000010)
15	0100010000000002	(0901000000000080||4101000000000000)
16	0640080000000001	(4008000000000002||4800000000000000)
17	80c0000000000007	(c000000000000000||8000000000000002)
18	04410001000000f1	(0000000000000004||0000000000000010)
19	1149400900000009	(0041000100000081||0041000100000001)
20	8892000100000004	(9208010801000008||9000010001000000)
21	8000410901000004	(0000090009010004||8000010001010000)
22	0117880108000001	(0400400000080104||0400480008000100)
23	4dae800901000032	(0113c04100000900||2111804140000100)
24	–	(6cbe10080000013a||643212020000093b)
Prob.	$2^{-253.81}$	$2^{-127.96}$

B.2 Alzette RX Characteristics

Table 17 gives the three four-step Alzette RX characteristics used in Section 4.1, following the data released with [BLU25]. Here $c_0 =$ `b7e15162` and $c_7 =$ `c2b3293d` are public Alzette constants. For each step, the final column gives the input and output RX-differences $(\alpha_i, \beta_i, \delta_i)$ of its modular addition; the last row of each characteristic has no following addition.

Table 17: Four-step Alzette RX characteristics used in the full-data-path RQ analysis.

(c, γ)	Step	State RX-difference	ADD RX-difference $(\alpha_i, \beta_i, \delta_i)$
$(c_7, 12)$	0	(0088ec24||0044e400)	(0088ec24,0089c800,0000e424)
	1	(f0201132||00a0c000)	(f0201132,60000050,70200102)
	2	(8000f414||0021f810)	(8000f414,0021f810,8020fc04)
	3	(70000912||00600019)	(70000912,60001900,f0001012)
	4	(0020e504||1072f019)	–
$(c_0, 1)$	0	(085ff001||042df000)	(085ff001,085be000,0003f000)
	1	(d82003a7||07ddf000)	(d82003a7,f80003ee,10200fb4)
	2	(c803fc13||0007f810)	(c803fc13,0007f810,d803fc07)
	3	(00200fa0||b000001f)	(00200fa0,00001fb0,00200ff0)
	4	(d803fc57||bff0003f)	–
$(c_7, 2)$	0	(803e0200||401f8000)	(803e0200,803f0000,007f0200)
	1	(c8008fca||3f1d8000)	(c8008fca,c0001f8e,08008fc4)
	2	(c07f020e||78ff8400)	(c07f020e,78ff8400,487f8202)
	3	(80000fc8||e8008004)	(80000fc8,008004e8,808004e0)
	4	(48ff892a||ece00084)	–

B.3 SIMECK RX Characteristics

In [LLA+20], Lu *et al.* presented a 27-round RX characteristic for SIMECK48/96 and a 35-round RX characteristic for SIMECK64/128. For reference, these characteristics are reproduced in Table 18 and Table 19, respectively.

In [CZX+23], Chen *et al.* constructed two RXDR distinguishers for SIMECK48/96: a 21-round distinguisher obtained by combining a 14-round RX characteristic and a 7-

round differential distinguisher, and a 20-round distinguisher obtained by combining a 17-round RX characteristic and a 3-round differential distinguisher. For reference, the corresponding 14-round and 17-round RX characteristics are reproduced in Table 20 and Table 21, respectively.

The exact probabilities of these characteristics are re-evaluated in Section 4 by enumerating the corresponding rotational-quasidifferential trails.

Table 18: 27-round RX characteristic for SIMECK48/96.

Round	key RX-difference	data RX-difference
0	000004	(000001||000006)
1	000000	(000000||000001)
2	000002	(000001||000000)
3	000003	(000001||000001)
4	000002	(000001||000001)
5	000000	(000000||000001)
6	000003	(000001||000000)
7	000003	(000000||000001)
8	000004	(000002||000000)
9	000000	(000000||000002)
10	000002	(000002||000000)
11	00000e	(000004||000002)
12	000002	(000000||000004)
13	000000	(000006||000000)
14	000013	(00000c||000006)
15	00000c	(000001||00000c)
16	000004	(000002||000001)
17	000000	(000001||000002)
18	000002	(000001||000001)
19	000002	(000001||000001)
20	000001	(000000||000001)
21	000000	(000000||000000)
22	000003	(000000||000000)
23	000004	(000003||000000)
24	000004	(000002||000003)
25	000000	(000001||000002)
26	00000d	(000000||000001)
27		(00000c||000000)
Prob.	2^{-52}	2^{-42}

Table 19: 35-round RX characteristic for SIMECK64/128.

Round	key RX-difference	data RX-difference
0	00000006	(00000001||00000004)
1	00000000	(00000000||00000001)
2	00000003	(00000001||00000000)
3	00000002	(00000001||00000001)
4	00000000	(00000000||00000001)
5	00000002	(00000001||00000000)
6	00000003	(00000000||00000001)
7	00000004	(00000002||00000000)
8	00000000	(00000000||00000002)
9	00000002	(00000002||00000000)
10	0000000a	(00000004||00000002)
11	00000001	(00000000||00000004)
12	00000001	(00000005||00000000)
13	00000013	(0000000a||00000005)
14	0000000c	(00000002||0000000a)
15	00000005	(00000002||00000002)
16	00000001	(00000001||00000002)
17	00000002	(00000001||00000001)
18	00000002	(00000001||00000001)
19	00000002	(00000001||00000001)
20	00000003	(00000001||00000001)
21	00000002	(00000001||00000001)
22	00000003	(00000001||00000001)
23	00000000	(00000000||00000001)
24	00000002	(00000001||00000000)
25	00000003	(00000000||00000001)
26	00000006	(00000002||00000000)
27	00000000	(00000000||00000002)
28	00000002	(00000002||00000000)
29	0000000a	(00000004||00000002)
30	00000000	(00000000||00000004)
31	00000000	(00000004||00000000)
32	00000010	(0000000c||00000004)
33	0000000c	(00000000||0000000c)
34	00000005	(00000000||00000000)
35		(00000005||00000000)
Prob.	2^{-72}	2^{-54}

Table 20: 14-round RX characteristic for SIMECK48/96.

Round	key RX-difference	data RX-difference
0	000114	(000000||000110)
1	000008	(000004||000000)
2	000004	(000000||000004)
3	000000	(000000||000000)
4	000002	(000000||000000)
5	000006	(000002||000000)
6	000002	(000000||000002)
7	000000	(000000||000000)
8	000008	(000000||000000)
9	000005	(000008||000000)
10	000007	(000015||000008)
11	000015	(000000||000015)
12	000000	(000000||000000)
13	00006f	(000000||000000)
14		(00006f||000000)
Prob.	2^{-24}	2^{-12}

Table 21: 17-round RX characteristic for SIMECK48/96.

Round	key RX-difference	data RX-difference
0	000114	(000000||000110)
1	000008	(000004||000000)
2	000004	(000000||000004)
3	000000	(000000||000000)
4	000002	(000000||000000)
5	000006	(000002||000000)
6	000002	(000000||000002)
7	000000	(000000||000000)
8	000008	(000000||000000)
9	000005	(000008||000000)
10	000007	(000015||000008)
11	000015	(000000||000015)
12	000000	(000000||000000)
13	000008	(000000||000000)
14	000019	(000008||000000)
15	000013	(000009||000008)
16	00001e	(000000||000009)
17		(000017||000000)
Prob.	2^{-32}	2^{-18}

C Connection with Existing Works

C.1 Bitwise AND

Beyne and Rijmen derived a closed-form expression for the quasidifferential transition matrix (QDTM) of the bitwise AND operation in Theorem 5.1 of [BR22]. For convenience, we restate their result using the notation of this paper.

Theorem 12. *Let $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ be defined by $F(x, y) = x \wedge y$. For differences $a, b, c \in \mathbb{F}_2^n$ and masks $u, v, w \in \mathbb{F}_2^n$, it holds that $D^F_{(w,c),(u\|v,a\|b)} \neq 0$ if and only if*

$$c \preccurlyeq a \vee b, \qquad u \vee v \preccurlyeq a \vee b \vee w, \qquad a \wedge u + b \wedge v = c \wedge w.$$

Moreover, whenever these conditions hold,

$$D^F_{(w,c),(u\|v,a\|b)} = 2^{-\mathrm{wt}(a\vee b)-\mathrm{wt}(w\wedge\bar{a}\wedge\bar{b})}(-1)^{(\bar{a}\wedge u+c\wedge v)^\top(\bar{b}\wedge v+c\wedge u)+(u\wedge v)^\top(c+a\wedge b\wedge\bar{c})}.$$

We now compare the AND-QDTM of Theorem 12 with the AND-RQTM derived in Theorem 7. When the rotation offset is $\gamma = 0$, the rotation operator reduces to the identity map. At the level of the underlying bases, the rotational-quasidifferential basis therefore reduces to the ordinary quasidifferential basis. Consequently, the RQTM is expected to reduce to the QDTM. The following proposition verifies this equivalence directly from the two closed-form expressions.

Proposition 3. *Let $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ be defined by $F(x, y) = x \wedge y$. For rotation offset $\gamma = 0$, the AND-RQTM coefficient from Theorem 7 satisfies*

$$A^F_{(w,c),(u\|v,a\|b)} = D^F_{(w,c),(u\|v,a\|b)},$$

where the right-hand side is the AND-QDTM coefficient of Theorem 12. In particular, the two expressions have identical nonzero conditions, absolute values, and signs.

Proof. For $\gamma = 0$, we have $R = R^{-1} = I$. Therefore, the auxiliary variables appearing in the AND-RQTM expression of Theorem 7 reduce to $p = b, q = a,$ and $r = c + a \wedge b$.

We first compare the nonzero conditions. The first nonzero condition of the AND-RQTM in Theorem 7 is $q \wedge u + p \wedge v + w \wedge r = w \wedge p \wedge q$. Substituting $p = b$, $q = a$, and $r = c + a \wedge b$ gives

$$a \wedge u + b \wedge v + w \wedge (c + a \wedge b) = w \wedge a \wedge b.$$

Since $w\wedge(c+a\wedge b) = w\wedge c+w\wedge a\wedge b$, the terms $w\wedge a\wedge b$ cancel, yielding $a\wedge u+b\wedge v = c\wedge w$. This is exactly the third nonzero condition of the AND-QDTM in Theorem 12.

Next, the second nonzero condition of the AND-RQTM becomes

$$\bar{a} \wedge \bar{b} \wedge \big((c + a \wedge b) \vee u \vee v\big) \preccurlyeq w.$$

We analyze this condition coordinate-wise. Suppose first that $a_i \vee b_i = 1$. Then $\bar{a}_i\bar{b}_i = 0$, so the second AND-RQTM condition imposes no restriction at coordinate i. The first two AND-QDTM conditions, $c_i \leq a_i \vee b_i$ and $u_i \vee v_i \leq a_i \vee b_i \vee w_i$, are also automatically satisfied.

It remains to consider the case $a_i = b_i = 0$. Then $r_i = c_i$. The first AND-RQTM condition reduces to $c_i w_i = 0$, whereas the second condition reduces to $c_i \vee u_i \vee v_i \leq w_i$. If $c_i = 1$, the latter condition forces $w_i = 1$, contradicting $c_i w_i = 0$. Hence, $c_i = 0$. The remaining condition is therefore $u_i \vee v_i \leq w_i$.

Combining the two cases over all coordinates gives $c \preccurlyeq a \vee b$ and $u \vee v \preccurlyeq a \vee b \vee w$. Together with $a \wedge u + b \wedge v = c \wedge w$, these are precisely the three nonzero conditions of Theorem 12. Thus, the AND-RQTM and AND-QDTM have identical support when $\gamma = 0$.

We next compare the absolute values. The AND-RQTM formula in Theorem 7 gives, for $\gamma = 0$,

$$\left|A^F_{(w,c),(u\|v,a\|b)}\right| = 2^{-n+\mathrm{wt}(\bar{a}\wedge\bar{b}\wedge\bar{w})}.$$

The three vectors $a\vee b, \bar{a}\wedge\bar{b}\wedge w,$ and $\bar{a}\wedge\bar{b}\wedge\bar{w}$ have pairwise disjoint supports and partition the n coordinates. Consequently, $n = \mathrm{wt}(a\vee b) + \mathrm{wt}(\bar{a}\wedge\bar{b}\wedge w) + \mathrm{wt}(\bar{a}\wedge\bar{b}\wedge\bar{w})$. It follows that $-n + \mathrm{wt}(\bar{a}\wedge\bar{b}\wedge\bar{w}) = -\mathrm{wt}(a\vee b) - \mathrm{wt}(\bar{a}\wedge\bar{b}\wedge w)$. Therefore,

$$\left|A^F_{(w,c),(u\|v,a\|b)}\right| = 2^{-\mathrm{wt}(a\vee b)-\mathrm{wt}(w\wedge\bar{a}\wedge\bar{b})},$$

which is exactly the absolute value of the AND-QDTM coefficient in Theorem 12.

Finally, we compare the signs. Since the bitwise AND operation acts independently on each coordinate, both transition coefficients factor into products of one-bit contributions. For $\gamma = 0$, the sign exponent of the AND-RQTM in Theorem 7 becomes

$$\mathrm{wt}((\bar{a}\wedge r\wedge u)\vee(u\wedge v\wedge w)\vee(a\wedge r\wedge v)),$$

where $r = c + a\wedge b$.

Thus, it suffices to compare the sign exponents coordinate-wise. Under the common nonzero conditions derived above, the one-bit exponent of the AND-RQTM is given by

(a_i, b_i)	AND-RQTM sign exponent
$(0,0)$	$u_i v_i$
$(0,1)$	$c_i u_i$
$(1,0)$	$c_i v_i$
$(1,1)$	$\bar{c}_i v_i$

On the other hand, the one-bit contribution to the exponent of the AND-QDTM in Theorem 12 is

$$(\bar{a}_i u_i + c_i v_i)(\bar{b}_i v_i + c_i u_i) + u_i v_i (c_i + a_i b_i \bar{c}_i).$$

Evaluating this expression for the four possibilities $(a_i, b_i) \in \mathbb{F}_2^2$, subject to the corresponding common nonzero conditions, yields

(a_i, b_i)	AND-QDTM sign exponent
$(0,0)$	$u_i v_i$
$(0,1)$	$c_i u_i$
$(1,0)$	$c_i v_i$
$(1,1)$	$\bar{c}_i v_i$.

Hence, the sign contributions of the AND-RQTM and AND-QDTM agree at every coordinate. Their complete signs are therefore identical.

We conclude that, for $\gamma = 0$, the AND-RQTM and AND-QDTM have the same support, absolute value, and sign. Therefore,

$$A^F_{(w,c),(u\|v,a\|b)} = D^F_{(w,c),(u\|v,a\|b)}.$$

□

The same equivalence can also be seen directly from the definitions of the two bases. For $\gamma = 0$, we have

$$\begin{aligned}\rho_{u,a}(x,y) &= \chi_u(x)\delta_a(R^0(x)+y)\\ &= \chi_u(x)\delta_a(x+y)\\ &= \beta_{u,a}(x,y).\end{aligned}$$

Hence, the rotational-quasidifferential basis is exactly the quasidifferential basis when $\gamma = 0$. Accordingly, their change-of-basis operators coincide, and therefore $A^F = D^F$.

Proposition 3 verifies this reduction explicitly for the closed-form transition coefficients of the bitwise AND operation.

C.2 Modular Addition

Biryukov, Lambin, and Udovenko [BLU25] derived a validity criterion and an exact probability formula for RX-differentials through modular addition for every nonzero rotation offset. For comparison with the RQTM, we first restate their Theorems 1 and 2 using the notation and one-based bit indexing of this paper.

Theorem 13 ([BLU25])**.** *Let $F(x,y) = x \boxplus y$, let $R = R^{\gamma}$ for $1 \le \gamma < n$, and define*

$$P_{\mathrm{RX}}(a, b \to c) = \Pr_{x,y}\big[(R(x)+a) \boxplus (R(y)+b) = R(x \boxplus y) + c\big].$$

Write

$$a_R = a\big|_{\{1,\dots,\gamma\}}, \qquad a_L = a\big|_{\{\gamma+1,\dots,n\}},$$

and define b_L, b_R, c_L, c_R analogously. Let $\xi = a + b + c$ and

$$\theta = (I + \mathrm{SHL})(\xi), \qquad \zeta = \mathrm{SHL}\big((a+c) \vee (b+c)\big),$$

where SHL *denotes a one-bit logical left shift. Then*

$$P_{\mathrm{RX}}(a, b \to c) > 0 \iff \theta_i \le \zeta_i \quad \text{for every } i \notin \{1, \gamma+1\}. \tag{3}$$

For an m-bit triple (α, β, Δ), let

$$d = \#\big\{i \in \{1, \dots, m-1\} : (\alpha_i, \beta_i, \Delta_i) \notin \{000, 111\}\big\}$$

and define

$$\mathcal{T}_m(\alpha, \beta, \Delta, \omega) = 2^{-d-1} + \mathbf{1}_{\alpha+\beta+\Delta \in \{0^m, 1^m\}}(-1)^{\omega} 2^{-m-1}.$$

Whenever the equivalent conditions in Equation (3) hold,

$$P_{\mathrm{RX}}(a, b \to c) = \mathcal{T}_{n-\gamma}(a_L, b_L, c_L, \xi_1)\mathcal{T}_{\gamma}(a_R, b_R, c_R, \xi_{\gamma+1}).$$

We now compare Theorem 13 with the modular-addition RQTM in Theorem 8.

Proposition 4 (Zero-mask specialization of the modular-addition RQTM)**.** *Under the notation of Theorem 13,*

$$A^{F}_{(0,c),(0\|0,a\|b)} = P_{\mathrm{RX}}(a, b \to c).$$

Consequently, the zero-mask RQTM entry is nonzero exactly under Equation (3), and, whenever it is nonzero,

$$A^{F}_{(0,c),(0\|0,a\|b)} = \mathcal{T}_{n-\gamma}(a_L, b_L, c_L, \xi_1)\mathcal{T}_{\gamma}(a_R, b_R, c_R, \xi_{\gamma+1}).$$

Thus, the zero-mask support and value obtained from Theorem 8 agree exactly with Theorem 13.

Proof. Applying Equation (1) to $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{n}$ and setting all input and output masks to zero gives

$$\begin{aligned} A^{F}_{(0,c),(0\|0,a\|b)} &= 2^{-2n}\#\big\{(x,y) : F(R(x)+a, R(y)+b) = R(F(x,y)) + c\big\} \\ &= P_{\mathrm{RX}}(a, b \to c), \end{aligned}$$

which proves the first equality. It remains to verify directly that the closed form of Theorem 8 reduces to the support and value in Theorem 13.

When $u = v = w = 0$, the CCZ-transformed masks satisfy $u' = v' = w' = 0$, and hence $s_0 = 0$. The one-bit support conditions for $\phi_i(s, r)$ reduce to

$$s(r + p_i q_i) = 0, \qquad \bar{p}_i \bar{q}_i r \le s, \tag{4}$$

and every supported coefficient is nonnegative, with

$$\phi_i(s,r) = 2^{-1+\bar{p}_i\bar{q}_i\bar{s}}.$$

Here

$$p = R^{-1}(a+c), \qquad q = R^{-1}(b+c).$$

Substituting these expressions and the definition of r_0 into Equation (4), and eliminating λ, μ, η, and τ, gives

$$\theta_i \le \zeta_i \qquad \text{for every } i \notin \{1, \gamma+1\}.$$

The variables τ and η range over the two boundary values at positions 1 and $\gamma+1$, so the two omitted positions impose no support condition. Hence, the zero-mask RQTM entry is nonzero exactly under Equation (3).

For the values, set

$$B_L = \frac{1}{2}\big(G_0(0) + (-1)^{\kappa}G_0(1)\big) = \frac{1}{2}\sum_{\lambda,\tau\in\mathbb{F}_2}(-1)^{\lambda\kappa}F_0(\lambda,\tau),$$
$$B_R = \frac{1}{2}\big(G_1(0) + G_1(1)\big) = \frac{1}{2}\sum_{\mu,\eta\in\mathbb{F}_2}(-1)^{\mu\eta}F_1(\mu,\eta).$$

Theorem 8 gives

$$A^F_{(0,c),(0\|0,a\|b)} = B_L B_R.$$

For a block of length m, each of the d nonconstant internal triples contributes a factor $1/2$, and the boundary condition contributes another factor $1/2$. The four-term block sum therefore evaluates to

$$2^{-d-1} + \mathbf{1}_{\alpha+\beta+\Delta\in\{0^m,1^m\}}(-1)^{\omega}2^{-m-1} = \mathcal{T}_m(\alpha,\beta,\Delta,\omega).$$

For the first block, $m = n-\gamma$, $(\alpha,\beta,\Delta) = (a_L, b_L, c_L)$, and $\omega = \xi_1$. For the second block, $m = \gamma$, $(\alpha,\beta,\Delta) = (a_R, b_R, c_R)$, and $\omega = \xi_{\gamma+1}$. Thus,

$$B_L = \mathcal{T}_{n-\gamma}(a_L, b_L, c_L, \xi_1), \qquad B_R = \mathcal{T}_{\gamma}(a_R, b_R, c_R, \xi_{\gamma+1}),$$

and multiplying the two identities proves the claimed value. □

Thus, the zero-mask case provides a consistency check against the known exact RX-differential probability. The general RQTM formula additionally determines the signed correlations for nonzero masks, which are needed when RX characteristic probabilities are expressed as sums of rotational-quasidifferential trails.

D Constraint-Based Modeling of Modular Addition

For practical constraint-based trail searches, it is useful to express $G_0(\lambda)$ and $G_1(\mu)$ without explicitly evaluating the corresponding sums of one-bit coefficients. The following proposition gives such a representation in terms of a support bit, a sign bit, and an integer weight.

For a set of coordinates $S \subseteq \{1,\dots,n\}$, we write x_S for the restriction of a vector x to S. Recall that $j = n-\gamma$, and let $I = \{1,\dots,j-1\}$ and $K = \{j+1,\dots,n-1\}$. An empty set of coordinates is interpreted in the natural way. For $\lambda, \mu \in \mathbb{F}_2$, set

$$s^{(0)}_{\lambda} = s_0 + \lambda U \qquad \text{and} \qquad s^{(1)}_{\mu} = s_0 + \mu V.$$

Proposition 5 (Modeling form of modular-addition RQTM)**.** *For every $\lambda, \mu \in \mathbb{F}_2$, there exist $a_\lambda^{(0)}, a_\mu^{(1)} \in \{0,1\}$, $J_\lambda^{(0)}, J_\mu^{(1)} \in \mathbb{F}_2$, and nonnegative integers $W_\lambda^{(0)}, W_\mu^{(1)}$ such that*

$$G_0(\lambda) = a_\lambda^{(0)}(-1)^{J_\lambda^{(0)}} 2^{-W_\lambda^{(0)}} \qquad \text{and} \qquad G_1(\mu) = a_\mu^{(1)}(-1)^{J_\mu^{(1)}} 2^{-W_\mu^{(1)}}.$$

More precisely, $a_\lambda^{(0)} = 1$ if and only if

$$q_I \wedge u_I' + p_I \wedge v_I' + (s_\lambda^{(0)})_I \wedge (r_0)_I = (s_\lambda^{(0)})_I \wedge p_I \wedge q_I,$$
$$\bar{p}_I \wedge \bar{q}_I \wedge \big((r_0)_I \vee u_I' \vee v_I'\big) \preceq (s_\lambda^{(0)})_I,$$

and

$$u_j' \vee v_j' \le (s_\lambda^{(0)})_j.$$

Whenever these conditions hold,

$$W_\lambda^{(0)} = |I| - \mathrm{wt}\Big(\bar{p}_I \wedge \bar{q}_I \wedge \overline{(s_\lambda^{(0)})_I}\Big) + (s_\lambda^{(0)})_j,$$
$$J_\lambda^{(0)} = \mathrm{wt}\Big(\Big[(\bar{q} \wedge r_0 \wedge u') \vee (u' \wedge v' \wedge s_\lambda^{(0)}) \vee (q \wedge r_0 \wedge v')\Big]_I\Big) + u_j' v_j' \pmod 2.$$

Similarly, $a_\mu^{(1)} = 1$ if and only if

$$q_K \wedge u_K' + p_K \wedge v_K' + (s_\mu^{(1)})_K \wedge (r_0)_K = (s_\mu^{(1)})_K \wedge p_K \wedge q_K,$$
$$\bar{p}_K \wedge \bar{q}_K \wedge \big((r_0)_K \vee u_K' \vee v_K'\big) \preceq (s_\mu^{(1)})_K,$$

and

$$(u_n' + \mu p_n) \vee (v_n' + \mu q_n) \le (s_\mu^{(1)})_n.$$

Whenever these conditions hold,

$$W_\mu^{(1)} = |K| - \mathrm{wt}\Big(\bar{p}_K \wedge \bar{q}_K \wedge \overline{(s_\mu^{(1)})_K}\Big) + (s_\mu^{(1)})_n,$$
$$J_\mu^{(1)} = \mathrm{wt}\Big(\Big[(\bar{q} \wedge r_0 \wedge u') \vee (u' \wedge v' \wedge s_\mu^{(1)}) \vee (q \wedge r_0 \wedge v')\Big]_K\Big)$$
$$+ \mu(r_0)_n + (u_n' + \mu p_n)(v_n' + \mu q_n) \pmod 2.$$

Consequently, writing the two factors of Theorem 8 as H_0 and H_1, respectively, gives

$$H_0 = a_0^{(0)}(-1)^{J_0^{(0)}} 2^{-W_0^{(0)}} + a_1^{(0)}(-1)^{J_1^{(0)}+\kappa} 2^{-W_1^{(0)}},$$
$$H_1 = a_0^{(1)}(-1)^{J_0^{(1)}} 2^{-W_0^{(1)}} + a_1^{(1)}(-1)^{J_1^{(1)}} 2^{-W_1^{(1)}}.$$

In particular,

$$H_0 = 0 \iff \big(a_0^{(0)} = a_1^{(0)} = 0\big)$$
$$\vee \ \big(a_0^{(0)} = a_1^{(0)} = 1,\, W_0^{(0)} = W_1^{(0)},\, J_0^{(0)} + J_1^{(0)} + \kappa = 1\big),$$

and

$$H_1 = 0 \iff \big(a_0^{(1)} = a_1^{(1)} = 0\big)$$
$$\vee \ \big(a_0^{(1)} = a_1^{(1)} = 1,\, W_0^{(1)} = W_1^{(1)},\, J_0^{(1)} + J_1^{(1)} = 1\big).$$

Remark 1. Proposition 5 is particularly convenient for constraint-based searches. Each branch $G_0(\lambda)$ or $G_1(\mu)$ is represented by a Boolean support condition, a sign bit, and an integer weight. Moreover, the vanishing of H_0 and H_1 can be detected using only support conditions, equality of integer weights, and parity conditions. Thus, the exact support and value of a modular-addition RQTM entry can be modeled without explicitly constructing the RQTM.