Unlocking Mix-Basis Potential: Geometric Approach for Combined Attacks

Kai Hu[1,4,5,6], Chi Zhang[2], Chengcheng Chang[1,4,5,6], Jiashu Zhang[1], Meiqin Wang[1,4,6(✉)], and Thomas Peyrin[3]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, China.
kai.hu@sdu.edu.cn, chengcheng.chang@mail.sdu.edu.cn, joshua020827@163.com, mqwang@sdu.edu.cn,
[2] School of Mathematics, Shandong University, Jinan, China.
zhangchi010301@gmail.com
[3] Nanyang Technological University, Singapore.
thomas.peyrin@ntu.edu.sg
[4] State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, Qingdao, China.
[5] Quancheng Laboratory, Jinan 250103, China.
[6] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China.

Abstract. This paper explores the possibility of using different bases in Beyne's geometric approach, a flexibility that was theoretically proposed in Beyne's doctoral thesis but has not been adopted in real cryptanalytic attacks despite its potential to unify multiple attack paradigms. We revisit three bases from previous geometric approach papers and extend them to four extra ones determined by simple rules. With the final seven bases, we can obtain 7^{2d} different basis-based attacks in the d-th-order spaces, where the *order* is defined as the number of messages used in one sample during the attack. All these attacks can be studied in unified automatic search methods.

We provide several demonstrative applications of this framework. First, we show that by choosing an alternative pair of bases, the divisibility property analyzed by Beyne and Verbauwhede with ultrametric integral cryptanalysis (ASIACRYPT 2024) can be interpreted as a single element rather than as a linear combination of elements of the transition matrix; thus, the property can be studied in a unified way as other geometric approach applications. Second, we revisit the multiple-of-2^t property (EUROCRYPT 2017) under our new framework and present new multiple-of-2^t distinguishers for SKINNY-64 that surpass the state-of-the-art results, from the perspectives of both first-order and second-order attacks. Finally, we give a closed formula for differential-linear approximations without any assumptions, even confirming that the two differential-linear approximations of SIMECK-32 and SIMECK-48 found by Hadipour *et al.* are deterministic independently of concrete key values.

Keywords: Cryptanalysis, Geometric Approach, Automatic Search, Mix-Basis

1 Introduction

A secure symmetric-key primitive (block cipher, stream cipher, cryptographic permutation, *etc.*) is expected to have an indistinguishable behavior from an idealized one. In practice, whether the primitive meets this expectation is tested by cryptanalysis: confidence is brought about by continuous analyses performed by the community. There are many attack techniques in the toolbox of cryptanalysts, such as differential [10], linear [27], and integral [23] cryptanalysis, as well as some combined ones such as differential-linear attacks [24]. After creating a cipher, designers and third-party cryptanalysts test its resistance against all state-of-the-art cryptanalytic methods, and it is deemed secure only if it resists all of them with sufficient security margin.

One issue with this process is that there are too many different types of attacks, and testing all of them is a very tedious task. In addition, being secure against all known attacks is not foolproof against potential new attacks. A well-known example is the boomerang attack on COCONUT98 [36], which was designed to be secure against differential and linear cryptanalysis, but was quickly broken by this newly introduced technique. Sometimes, even for well-studied ciphers, unexpected properties are uncovered many years after publication. At Eurocrypt 2017, a structural property [17] (later named the multiple-of-8 property and multiple-of-n property [14]; in this paper, we call it multiple-of-2^t as n is always divisible by 2^t for a certain t) was found for the 5-round Advanced Encryption Standard (AES) [15]. This was surprising as AES has been carefully studied for almost 30 years, yet this simple property remained undiscovered. Furthermore, although some cryptanalytic methods have been widely used to evaluate the security of cryptographic algorithms, they may not yet be fully understood. For example, before 2015, integral cryptanalysis was already one of the most mature cryptanalytic methods. However, Todo's discovery of the division property [34,35] and the following theories on parity sets [13] and monomial predictions [20] revealed a close relationship between integral cryptanalysis and the theory of Boolean functions of cryptographic algorithms – an evident connection in hindsight that had not been truly utilized in integral attacks. More recently, Beyne and Verbauwhede applied the geometric approach [4] to integral cryptanalysis [8], significantly deepening the community's understanding of the integral attack and division property once again. This suggests that the current knowledge of cryptanalysis remains relatively shallow.

A possible explanation for this situation is that cryptanalysis remains a task heavily based on the experience of cryptanalysts. Although the field has achieved great progress in the past four decades, it is fair to say that the community still knows little about the underlying principles and interconnections of various cryptanalytic methods. Usually, new attacks are found based on the good intuition of the cryptanalysts rather than on some systematic methods. If a unified theory could be developed to describe all (or a large family of) attacks and could be used to discover new ones, it would be extremely beneficial for the advancement of the field.

Recently, the *geometric approach* proposed by Beyne [6] has shown the potential to bring about an interesting change in cryptanalysis. This technique has been successfully used to reinterpret linear [4], (quasi-d-)differential [7,37] and integral cryptanalysis [8], overcoming many difficulties that could not be solved by classical methods. Based on this theory, Beyne and Verbauwhede proposed a new attack called *ultrametric integral cryptanalysis* [5] and characterized the divisibility property of the frequency of a ciphertext monomial evaluating to 1, which was impossible before.

The key point of the geometric approach is to view the input and output spaces of a cipher as free vector spaces and treat the cipher as a linear map in the high-dimensional spaces. The geometric approach benefits from the extensive knowledge and tools already developed in linear algebra.

In the following, we assume the plaintext and ciphertext spaces of a cipher $\mathcal{E} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are $(\mathbb{F}_2^n)^d = \mathbb{F}_2^n \times \mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n$, where $\times$ represents the Cartesian product, and $(\mathbb{F}_2^n)^d$ is called a d-th-order space which will be formally defined in Definition 2. Choosing a field $\mathbb{K}$ and regarding all vectors in $(\mathbb{F}_2^n)^d$, denoted by $(\delta_u, 0 \le u < 2^{dn})$[1], as a generating set, a free vector space over $\mathbb{K}$ can be induced as

$$\mathbb{K}[(\mathbb{F}_2^n)^d] = \left\{ \sum_u k_u \delta_u : k_u \in \mathbb{K}, u = 0, 1, \ldots, 2^{dn} - 1 \right\}.$$

The pushforward operation $\mathcal{T}^{\mathcal{E}}$ is induced from the cipher $\mathcal{E}$, which is a linear map that sends a vector of $\mathbb{K}[(\mathbb{F}_2^n)^d]$ to another in the same space. Here, $(\delta_u, 0 \le u < 2^{dn})$ plays the role of the standard basis, under which the corresponding matrix of $\mathcal{T}^{\mathcal{E}}$ is uniquely determined, denoted by $T^{\mathcal{E}}$, which is called the transition matrix of $\mathcal{E}$. When we choose a different basis for $\mathcal{T}^{\mathcal{E}}$, denoted by $(\beta_u, 0 \le u < 2^{dn})$, with the change-of-basis matrix being P that satisfies

$$(\delta_0, \delta_1, \ldots, \delta_{2^{dn}-1}) = (\beta_0, \beta_1, \ldots, \beta_{2^{dn}-1})P,$$

the corresponding matrix of $\mathcal{T}^{\mathcal{E}}$ becomes another matrix under the new basis $(\beta_u, 0 \le u < 2^{dn})$, denoted by $A^{\mathcal{E}}$, that is *similar* to $T^{\mathcal{E}}$, *i.e.*, $A^{\mathcal{E}} = PT^{\mathcal{E}}P^{-1}$. This process can also be performed in a dual way by considering the function space from $\mathbb{F}_2^n$ to $\mathbb{K}$.

With a new proper basis, Beyne found that the elements of $A^{\mathcal{E}}$ would be related to some attacks. For example, when $d = 1$ and the new basis is chosen as $(\chi_u, u = 0, 1, \ldots, 2^n - 1)$, where $\chi_u = [(-1)^{u^\top x}, 0 \le x < 2^n]$ that is a column vector of 2^n length ($u^\top x$ representing the dot product of u and x), the element at the u-th column and v-th row of $A^{\mathcal{E}}$ is

$$A^{\mathcal{E}}_{v,u} = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{u^\top x + v^\top \mathcal{E}(x)}, \tag{1}$$

[1] We use the natural way to interpret a vector $u \in \mathbb{F}_2^n$ as an integer $\sum_{0 \le i < n} u_i 2^{n-1-i}$ where u_0 is the most significant bit.

which corresponds to a linear approximation of $\mathcal{E}$ with input and output masks being u and v respectively [4].

From another perspective, for every pair (v, u), $A^{\mathcal{E}}_{v,u}$ can serve as a statistic on a set of inputs and outputs, so it provides an opportunity for cryptanalysts to check if it follows the same probability distribution as a random permutation. In linear cryptanalysis, for example, the expected value of $A^{\mathcal{R}}_{v,u}$ in Equation (1) of a random permutation $\mathcal{R}$ is zero, so if $A^{\mathcal{E}}_{v,u}$ significantly deviates from 0, we can distinguish $\mathcal{E}$ from $\mathcal{R}$. To make the distinguishing process easier, an attacker prefers to choose a pair (v, u) with the largest possible absolute deviation of $A^{\mathcal{E}}_{v,u}$ from zero, which corresponds to the process of finding a good pair of input and output masks in linear cryptanalysis. In theory, we can also check the variances or any other values to do the distinguishing attacks, as long as it is possible to compare with a random permutation.

With various bases and different d, various transition matrices can be obtained. Their elements can be regarded as different statistics of inputs and outputs, providing opportunities (in theory) to compare the cipher with a random permutation. The linear [4], (quasi-d-)differential [7,37], integral [8], and ultrametric integral attacks [5], all follow a similar philosophy. In each of these previous applications of the geometric approach, the same kind of basis[2] is always chosen for the input and output spaces. Such a same-basis configuration works perfectly except for the ultrametric integral cryptanalysis: This attack describes the divisibility of the number of times that a ciphertext monomial value is equal to 1 occurs under a set of specifically-chosen plaintexts. Given a cipher $\mathcal{E} : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the divisibility property is defined as[3]

$$\sum_{x \preceq u} \tau(\mathcal{E}^v(x)) \equiv 0 \mod 2^t \tag{2}$$

where $\mathcal{E}^v(x)$ is the product of coordinates of $\mathcal{E}(x)$ according to the support of v whose values are 0 or 1, and the function $\tau : \mathbb{F}_2^n \to \mathbb{Q}$ maps elements of $\mathbb{F}_2$ to their integer equivalents in $\mathbb{Q}$, *i.e.*, $\tau(0) = 0$ and $\tau(1) = 1$. When $t = 1$, this is simply the zero-sum property studied by integral cryptanalysis. To study this property, Beyne and Verbauwhede chose the basis as $(\mu_u, 0 \le u < 2^n)$, where $\mu_u = [(-1)^{\mathsf{wt}(u \oplus v)} \tau(u^v), 0 \le v < 2^n]$ ($\mathsf{wt}(v)$ represents the Hamming weight of x)[4]. The corresponding transition matrix element is

$$A^{\mathcal{E}}_{v,u} = \sum_{x \preceq u} (-1)^{\mathsf{wt}(u \oplus x)} \tau(\mathcal{E}^v(x)) \tag{3}$$

By comparing Equations (2) and (3), one can observe that Equation (3) cannot be used to study Equation (2) in a direct way due to the existence of $(-1)^{\mathsf{wt}(u \oplus x)}$.

[2] In this paper, when we write same basis/different bases, by default we mean same kind of basis/different kinds of bases. For example, linear bases for $\mathbb{K}[\mathbb{F}_2^n]$ and $\mathbb{K}[\mathbb{F}_2^m]$ are the same (kind of) basis, although they are bases for different spaces.

[3] The partial order $x \preceq u$ for $x, u \in \mathbb{F}_2^n$ is defined as: for all indices, $x_i < u_i$ if we regard x_i and u_i as integers.

[4] In [5], this basis is equivalently written as $\sum_{x \preceq u} (-1)^{\mathsf{wt}(u \oplus x)} \delta_x$.

This is because the left-hand of Equation (2) does not equal any single element of $A^{\mathcal{E}}$ in Equation (3), which makes the description of ultrametric integral cryptanalysis different from the other applications of the geometric approach, and more techniques are required to describe this attack.

Our contributions. In [6, Section 2.4.2], Beyne discussed the possibility of using different bases in the geometric approach. However, such flexibility has never been adopted in concrete cryptanalytic attacks despite its potential to unify multiple attack paradigms. In this paper, we show that the geometric approach with different bases is indeed more flexible and will contain more attacks. Given a pair of (same or different) bases, one can obtain the corresponding transition matrix. The elements of the matrix can serve as statistics that provide opportunities for an attacker to examine whether the cipher's input and output samples follow the same distribution as a random permutation.

This way, given a set of t different bases, t^2 attacks can be naturally defined by them. We call these attacks a family of basis-based attacks defined on the t bases. This paper first recalls three bases used in previous geometric approach papers, then introduces three rules to generate four new bases from these three known ones. To characterize the number of messages in a sample exploited in an attack, we also define the *order* of a space and an attack. Bases that are used in higher-order attacks can be generated from first-order bases by the Kronecker product. Finally, from the seven bases used in our work, 7^{2d} attacks are obtained for the d-th-order cases, including many known and unknown attacks. All these attacks can be studied in a unified automatic search method. This has significantly enlarged the scope of the geometric approach.

An immediate benefit of allowing different bases is that the geometric approach can now be applied to describe combined attacks such as differential-linear cryptanalysis [24]. Choosing the basis used in quasi-differential cryptanalysis [7] for the input space, and the basis used in linear cryptanalysis [4] (actually, a variant of this basis), we derive a closed formula for the differential-linear approximation without any independence assumption. Automatic search tools are also developed in a natural way to calculate/approximate the exact differential-linear correlation. By enumerating all trails, we managed to confirm that two differential-linear approximations of `SIMECK` variants recently found by Hadipour, Derbez, and Eichlseder are deterministic independently of keys [18].

Three more applications are provided to demonstrate the effectiveness of the geometric approach with different bases.

In Section 4, we revisit Beyne and Verbauwhede's ultrametric integral cryptanalysis that studies the divisibility property. With an alternative choice of bases, the divisibility property can be described as a simpler mix-basis attack, where the correlation expression derived from the bases corresponds exactly to a single element of the transition matrix. Thus, we can focus more on tracing trails from all round functions' transition matrices, rather than the linear combinations of the divisibility property of different input vectors. In Sections 5 and 6, we apply our framework to the multiple-of-2^t property, a generalized property of the multiple-of-8 property which was originally discovered for the 5-round AES [17].

This property reached only 5 rounds for SKINNY-64 before this paper, but our automatic search method derived from the geometric approach easily extends its length to 10 rounds. We also study the multiple-of-2^t property as a first-order attack. This is naturally similar to the original multiple-of-2^t property. We find a new distinguisher for SKINNY-64 that reaches 11 rounds, which is already of the same length as the integral distinguishers. The applications in Sections 5 and 6 provide examples of how to study the same property for different orders.

Paper organization. The remaining paper is organized as follows. Section 2 introduces the notations and recalls some background knowledge. In Section 3, we describe our main contribution. The following four sections give four examples of applications of how to use the geometric approach with different bases in cryptanalysis. Section 8 concludes the paper.

2 Preliminaries

2.1 Notations

We use double-struck uppercase letters such as $\mathbb{U}, \mathbb{V}$ to represent sets. Uniquely, $\mathbb{Q}$ is used for rational numbers and $\mathbb{N}$ is for all natural numbers. If $\mathbb{V}$ is a vector space, $\dim \mathbb{V}$ represents its dimension.

A column vector of length n whose values are chosen from a set $\mathbb{S}$ is written as $[x_0, x_1, \ldots, x_{n-1}] = [x_i, 0 \leq i < n] \in \mathbb{S}^n$. Its corresponding row vector is $[x_0, x_1, \ldots, x_{n-1}]^\top = [x_i, 0 \leq i < n]^\top$. If all elements of a vector can be calculated by a function $f(x)$ by enumerating x, this vector is also represented by $[f(x), 0 \leq x < n]$. For two vectors $x, y \in \mathbb{F}_2^n$, $x \succeq y$ means $x_i \geq y_i$ for all i. Similarly, $x \preceq y$ means $x_i \leq y_i$ for all i. x_i and y_i are regarded as integers for this comparison. $\oplus$ is the bit-wise addition modular 2 for two vectors in $\mathbb{F}_2^n$. A vector $x \in \mathbb{F}_2^n$ can be seen as an integer $\sum_{0 \leq i < n} x_i 2^{n-1-i}$ where x_0 is the most significant bit; the integer form of a vector is used for indices. $a||b \in \mathbb{F}_2^{n+m}$ is the concatenation of $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$.

Functions are denoted by calligraphic upper letters, such as $\mathcal{F}$ and $\mathcal{E}$. Matrices are represented by uppercase letters like A and T, *etc.* The element at the v-th row and u-th column of a matrix A is denoted by $A_{v,u}$, which is also called the (v, u)-element of A. When a matrix is a Kronecker product of multiple matrices, the row and column indices are written as vector tuples. For example, $A = B \otimes C$, $A_{(v_0,v_1),(u_0,u_1)} = B_{v_0,u_0} C_{v_1,u_1}$. An introduction to the Kronecker product can be found in [6, Section 2.2.3].

Similar to the vector, if all (v, u)-elements of a matrix can be calculated by a function $f_u(v)$ that is in $\mathbb{S}$ with enumerating u and v, the matrix is also represented by $A = [f_u(v)]_{v,u} \in \mathbb{S}^{n \times n}$, where $0 \leq v < n$ is the row index and $0 \leq u < n$ is the column index.

The matrix can also be written by its column vectors, such as $A = [f_u(v)]_{v,u} = (f_0, f_1, \ldots, f_{n-1})$, where $f_u = [f_u(v), 0 \leq v < n]$ is its u-th column vector.

We introduce several functions that have been extensively used in previous geometric approach papers and will play important roles in this work. For example, some of these functions are used to represent the matrices or vectors in the way above.

Function 1 ($\mathsf{wt}(\cdot)$) $\mathsf{wt}(\cdot) : \mathbb{F}_2^n \to \mathbb{N}$, *for any* $x \in \mathbb{F}_2^n$, $\mathsf{wt}(x)$ *is the Hamming weight of* x *defined by* $\mathsf{wt}(x) = \sum_{0 \le i < n} x_i$.

Function 2 ($(-1)^{u^\top(\cdot)}$) *Let* $u \in \mathbb{F}_2^n$, *we define* $(-1)^{u^\top(\cdot)} : \mathbb{F}_2^n \to \mathbb{Q}$ *as*

$$(-1)^{u^\top x} = \begin{cases} 1 & \text{if } u^\top x = 0, \\ -1 & \text{if } u^\top x = 1, \end{cases}$$

where $u^\top x$ means the dot product of u and x, *i.e.*, $u^\top x = \sum_{0 \le i < n} u_i x_i \bmod 2$. Another popular form of this function is written as $\chi_u(\cdot)$.

Function 3 ($\delta_u(\cdot)$) *Let* $u \in \mathbb{F}_2^n$, *we define* $\delta_u(\cdot) : \mathbb{F}_2^n \to \mathbb{Q}$ *as*

$$\delta_u(x) = \begin{cases} 1 & \text{if } x = u, \\ 0 & \text{otherwise.} \end{cases}$$

Remark. In this paper, the notation "δ_u" (rather than "$\delta_u(\cdot)$") is also used to represent the unit vector whose u-th element is 1. This interpretation is natural when we express it as $\delta_u = [\delta_u(x), 0 \le x < 2^n]$.

Function 4 ($(\cdot)^u$) *Let* $u \in \mathbb{F}_2^n$, *we define* $(\cdot)^u : \mathbb{F}_2^n \to \mathbb{Q}$ *as*

$$x^u = \begin{cases} 1 & \text{if } x \succeq u, \\ 0 & \text{otherwise.} \end{cases}$$

Note that in [5] and many previous papers, x^u is defined as a value in $\mathbb{F}_2$. To transform x^u into values in $\mathbb{Q}$, a Teichmüller lift

$$\tau : \mathbb{F}_2 \to \mathbb{Q}, \tau(0) = 0, \tau(1) = 1$$

is applied to x^u. However, since this paper only works in $\mathbb{Q}$, we by default use x^u as a value in $\mathbb{Q}$ to omit the notation τ for the sake of a simpler description.

Function 5 ($u^{(\cdot)}$) *Let* $u \in \mathbb{F}_2^n$, *we define* $u^{(\cdot)} : \mathbb{F}_2^n \to \mathbb{Q}$ *as*

$$u^x = \begin{cases} 1 & \text{if } x \preceq u, \\ 0 & \text{otherwise.} \end{cases}$$

Similarly to $(\cdot)^u$, we also omit the τ function and regard u^x by default as a rational number.

2.2 Brief Introduction to Beyne's Geometric Approach

This paper will discuss how to choose and combine different bases in Beyne's geometric approach, as well as generating new bases from existing ones by simple rules. Thus, in this subsection, we will only introduce how to describe an attack with a chosen basis and the usage of automatic search tools in the one-dimensional case [6, Section 2.4]. The geometric approach actually has a larger scope, for more content such as the multidimensional theory [6, Section 2.5] and deriving bases from group or monoid characters, we refer readers to [6,4,7,5]. Mathematical background knowledge about representations of finite groups and monoids can also be found in textbooks such as [30] and [31].

Consider a function $\mathcal{E} : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Beyne introduced the geometric approach, which is a way to use linear algebra techniques to analyze the properties of $\mathcal{E}$ [6]. There are two methods for this purpose. One is to work in free vector spaces, and the other is to start from function spaces. The two methods are dual to each other, so we will only introduce the first one here. Let $\mathbb{K}$ be any field,

$$\mathbb{K}[\mathbb{F}_2^n] = \left\{ \sum_{u \in \mathbb{F}_2^n} a_u \delta_u, a_u \in \mathbb{K}, u \in \mathbb{F}_2^n \right\}$$

is called a free vector space over $\mathbb{K}$ with $\mathbb{F}_2^n$ as the generating set. $\mathbb{K}[\mathbb{F}_2^n]$ is a vector space, and $(\delta_0, \delta_1, \ldots, \delta_{2^n-1})$ is the standard basis. In this paper, we tend to write the basis as a matrix like $[\delta_u(v)]_{v,u}$ by placing the u-th basis vector into the u-th column of $[\delta_u(v)]_{v,u}$.

The pushforward operation of $\mathcal{E}$ is defined as

$$\mathcal{T}^{\mathcal{E}} : \mathbb{K}[\mathbb{F}_2^m] \to \mathbb{K}[\mathbb{F}_2^n], \quad \sum_{u \in \mathbb{F}_2^n} a_u \delta_u \mapsto \sum_{u \in \mathbb{F}_2^n} a_u \delta_{\mathcal{E}(u)}.$$

Let $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, $\mathcal{E}(u) = v$ is equivalent to $\mathcal{T}^{\mathcal{E}}(\delta_u) = \delta_v = \delta_{\mathcal{E}(u)}$. One can easily verify that $\mathcal{T}^{\mathcal{E}}$ is a linear map. Under the standard basis, the matrix of $\mathcal{T}^{\mathcal{E}}$ can be derived, which is denoted by $T^{\mathcal{E}} \in \mathbb{K}^{2^m \times 2^n}$ with its (v, u)-element being $T^{\mathcal{E}}_{v,u} = \delta_v(\mathcal{E}(u))$.

Note that $\mathcal{T}^{\mathcal{E}}$ is a linear map, thus, with doing a change-of-basis for the input and output spaces we can obtain different matrices.

Suppose the new basis is $[\alpha_u(v)]_{v,u}$ (the lengths of basis vectors for the input and output spaces are implicit). The change-of-basis matrix for the standard basis and the new basis is $P_n \in \mathbb{K}^{2^n \times 2^n}$ and $P_m \in \mathbb{K}^{2^m \times 2^m}$,

$$[\delta_u(v)]_{v,u} = [\alpha_u(v)]_{v,u} P_n \text{ (input) and } [\delta_u(v)]_{v,u} = [\alpha_u(v)]_{v,u} P_m \text{ (output).}$$

The matrix of $\mathcal{T}^{\mathcal{E}}$ under the basis $[\alpha_u(v)]_{v,u}$ is then

$$A^{\mathcal{E}} = P_m T^{\mathcal{E}} P_n^{-1}. \tag{4}$$

Note that $[\delta_u(v)]_{v,u}$ is an identity matrix, thus $P_m = [\alpha_u(v)]^{-1}_{v,u}$ and $P_n^{-1} = [\alpha_u(v)]_{v,u}$. Here we assume $[\alpha_u(v)]^{-1}_{v,u}$ can be represented by a compact form,

denoted by $[\alpha_u(v)]^{-1}_{v,u} = [\alpha^\star_u(v)]_{v,u}$. Therefore

$$A^{\mathcal{E}} = [\alpha^\star_u(v)]_{v,u} T^{\mathcal{E}} [\alpha_u(v)]_{v,u}.$$

The (v,u)-element of A can be obtained by left-multiplying a unit row vector $\delta_v^\top$, followed by the right-multiplication of a unit column vector δ_u, as

$$\begin{aligned}
A^{\mathcal{E}}_{v,u} &= \delta_v^\top [\alpha^\star_u(v)]_{v,u} T^{\mathcal{E}} [\alpha_u(v)]_{v,u} \delta_u \\
&= [\alpha^\star_0(v), \alpha^\star_1(v), \ldots, \alpha^\star_{2^m-1}(v)]^\top T^{\mathcal{E}} [\alpha_u(0), \alpha_u(1), \ldots, \alpha_u(2^n-1)] \\
&= \left[\sum_{x \in \mathbb{F}_2^m} \alpha^\star_x(v) \delta_x(\mathcal{E}(0)), \ldots, \sum_{x \in \mathbb{F}_2^n} \alpha^\star_x(v) \delta_x(\mathcal{E}(2^n-1)) \right]^\top [\alpha_u(0), \ldots, \alpha_u(2^n-1)] \\
&= \sum_{x \in \mathbb{F}_2^n} \alpha^\star_{\mathcal{E}(x)}(v) \cdot \alpha_u(x)
\end{aligned} \tag{5}$$

The formula of $A^{\mathcal{E}}_{v,u}$ is called the *correlation expression* of the approximation (u,v). As mentioned before, the correlation expression can be seen as a statistic, which might follow different probability distributions for $\mathcal{E}$ being a random function or a cipher.

In the following, we revisit the applications of the geometric approach to linear [4], differential [7], and ultrametric integral cryptanalysis [5]. In this paper, the free vector spaces are always over $\mathbb{K} := \mathbb{Q}$.

Geometric approach to linear cryptanalysis. In [4], Beyne chose the linear basis as $[(-1)^{u^\top v}]_{v,u}$, whose inverse satisfies $[(-1)^{u^\top v}]^{-1}_{v,u} = 2^{-n}[(-1)^{u^\top v}]_{v,u}$. With Equation (5), the transition matrix for linear cryptanalysis has the (v,u)-element as

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

Geometric approach to differential cryptanalysis. In differential cryptanalysis, the input of $\mathcal{E}$ can be considered as a value and a difference, *i.e.*, $(x_0, x_0 \oplus x_1) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. Thus, the free vector spaces induced from the input and output spaces are $\mathbb{Q}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$.

In [7], Beyne and Rijmen chose the quasi-differential basis as

$$[(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1} = [(-1)^{u_0^\top v_0} \delta_{u_1}(v_1)]_{(v_0,v_1),(u_0,u_1)}.$$

According to the calculation rule of the Kronecker product, $(M_0 \otimes M_1)^{-1} = M_0^{-1} \otimes M_1^{-1}$, thus

$$\begin{aligned}
[(-1)^{u_0^\top v_0} \delta_{u_1}(v_1)]^{-1}_{(v_0,v_1),(u_0,u_1)} &= [(-1)^{u_0^\top v_0}]^{-1}_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]^{-1}_{v_1,u_1} \\
&= [2^{-n}(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}.
\end{aligned}$$

With Equation (5), the $((v_0, v_1), (u_0, u_1))$-element of the quasi-differential transition matrix is

$$A^{\mathcal{E}}_{(v_0,v_1),(u_0,u_1)} = 2^{-n} \sum_{\substack{x_0 \in \mathbb{F}_2^n \\ \mathcal{E}(x_0) \oplus \mathcal{E}(x_0 \oplus u_1) = v_1}} (-1)^{u_0^\top x_0 \oplus v_0^\top \mathcal{E}(x_0)}.$$

In [37], Wang *et al.* managed to extend the quasi-differential framework to d-differential cryptanalysis [33], with choosing the quasi-d-differential basis

$$[(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1} \otimes \cdots \otimes [\delta_{u_{d-1}}(v_{d-1})]_{v_{d-1},u_{d-1}}.$$

Geometric approach to ultrametric integral cryptanalysis. In [5], Beyne and Verbauwhede introduced the ultrametric integral cryptanalysis to study divisibility properties. The ultrametric integral basis is chosen as $[(-1)^{\mathsf{wt}(u \oplus v)} u^v]_{v,u}$, whose inverse is $[(-1)^{\mathsf{wt}(u \oplus v)} u^v]^{-1}_{v,u} = [u^v]_{v,u}$. According to Equation (5), the (v, u)-element of the ultrametric integral transition matrix is

$$A^{\mathcal{E}}_{v,u} = \sum_{x \preceq u} (-1)^{\mathsf{wt}(u \oplus x)} \mathcal{E}^v(x).$$

2.3 Propagation of Transition Matrix, Metric, and Automatic Search

Calculating the (v, u)-element of a transition matrix $A^{\mathcal{E}}$ according to the correlation expression is challenging, as it usually requires enumerating a variable in a large size of set, *e.g.*, $\mathbb{F}_2^n$. However, the transition matrices enjoy the following property.

Theorem 1 (Propagation of transition matrices [7,4]). *The transition matrix of $\mathcal{E} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ satisfies:*

(1) If $\mathcal{E} = \mathcal{E}_{s_0} || \cdots || \mathcal{E}_{s_{m-1}}$, $A^{\mathcal{E}} = \bigotimes_{i=0}^{m-1} A^{\mathcal{E}_i}$.
(2) if $\mathcal{E} = \mathcal{E}_{r-1} \circ \cdots \circ \mathcal{E}_1 \circ \mathcal{E}_0$, $A^{\mathcal{E}} = A^{\mathcal{E}_{r-1}} \cdot \cdots \cdot A^{\mathcal{E}_1} \cdot A^{\mathcal{E}_0}$.

According to Theorem 1, if $\mathcal{E} = \mathcal{E}_{r-1} \circ \mathcal{E}_{r-2} \circ \cdots \circ \mathcal{E}_0$ we have

$$A^{\mathcal{E}}_{u_r,u_0} = \sum_{u_{r-1},u_{r-2},\ldots,u_1} \prod_{i=0}^{r-1} A^{\mathcal{E}_i}_{u_{i+1},u_i}. \tag{6}$$

$A^{\mathcal{E}}_{u_r,u_0}$ is equal to the sum of *correlations* of all trails with input and output *masks* being u_0 and u_r, respectively.

Definition 1 (Approximation, trail and correlation [4]). *In Equation (6), the mask pair (u_0, u_r) is called an approximation, $\sum_{u_{r-1},\ldots,u_1} \prod_{i=0}^{r-1} A^{\mathcal{E}_i}_{u_{i+1},u_i}$ is called its correlation. $(u_0, u_1, \ldots, u_r)$ is called a trail belonging to (u_0, u_r). $\prod_{i=0}^{r-1} A^{\mathcal{E}_i}_{u_{i+1},u_i}$ is called the correlation of this trail.*

Therefore, $A^{\mathcal{E}}_{u_r,u_0}$ is the sum of the correlations of all trails belonging to the approximation (u_0, u_r). The search for a trail or the enumeration of trails has been extensively studied in previous articles related to automatic search, such as [28,32], which can be and have been reused in a natural way for the search of trails in the geometric approach [6]. In Appendix B, we give a high-level description of the current automatic search methods.

To use the correlation expression of $A^{\mathcal{E}}_{u_r,u_0}$ for a distinguishing attack, two types of *metrics* are known. The first is the Archimedean absolute value of $A^{\mathcal{E}}_{u_r,u_0}$ such as the correlation in linear attacks or the probability in differential attacks. The values for a cipher and a random permutation are expected to follow different probability distributions that can be distinguished with some samples. The second is to use the 2-adic absolute value[5] of $A^{\mathcal{E}}_{u_r,u_0}$, which can show if $A^{\mathcal{E}}_{u_r,u_0}$ is a multiple of a certain number (divisibility property). The 2-adic absolute value of a rational number $x = 2^t \frac{r}{s}$ with r and s being co-prime odd integers and t is an integer, is equal to 2^{-t}, denoted by $|x|_2 = 2^{-t}$. For example, as Beyne and Verbauwhede recently showed, the zero-sum property in integral cryptanalysis is equivalent to saying that the weight of the output Boolean function under some input sets is a multiple of 2. Thus, it is natural to consider whether the weight is also a multiple of 2^t $(t \geq 2)$. This metric has been introduced and well studied in [5]. According to the definition of the 2-adic absolute value on $\mathbb{Q}$, $A^{\mathcal{E}}_{u_r,u_0} \equiv 0 \bmod 2^t$ is equivalent to saying $|A^{\mathcal{E}}_{u_r,u_0}|_2 \leq 2^{-t}$.

Since the number of trails can be too large to exhaust, in most cases, only one or a small percentage of trails that have the most significant correlations can be searched and used. These trails are called dominant trails [6]. In the first metric, the sum of dominant trails cannot ensure that the approximation is always sound. Yet, in the second metric, due to the ultrametric triangle inequality $|x + y|_2 \leq \max\{|x|_2, |y|_2\}$, the correlation of the dominant trails can bound the summed correlations of all trails.

3 Geometric Approach While Allowing Different Bases

In [6, Section 2.4.2], Beyne showed that the transition matrices obtained for each round function under different bases have analogous propagation properties with the same bases case. However, prior related papers have not explored this possibility. In this section, we demonstrate how to use this idea in real cryptanalysis by combining different bases for the input and output spaces to describe new attacks, which enhances the geometric approach significantly. We also introduce the general framework for the geometric approach in the higher-order case.

3.1 Using Different Basis for Input and Output Spaces

Consider $\mathcal{E} : \mathbb{F}_2^n \to \mathbb{F}_2^m$. An attack on $\mathcal{E}$ can use samples $(p_0, p_1, \ldots, p_{d-1}) \in (\mathbb{F}_2^n)^d$ and corresponding $(c_0, c_1, \ldots, c_{d-1}) \in (\mathbb{F}_2^m)^d$ for a distinguishing or key-recovery

[5] As implied by [5], using p-adic absolute value as a metric is also possible, but this paper only focuses on 2-adic absolute value case.

attack, where $c_i = \mathcal{E}(p_i)$ for $0 \leq i < d$. For a specific distinguishing attack, the experimental correlation is calculated from $(p_0, p_1, \ldots, p_{d-1})$ and $(c_0, c_1, \ldots, c_{d-1})$ and reflects some statistical properties of the cipher. If the correlation of the target cipher follows a different probability distribution from a random function, we can perform a distinguishing attack with some computational resources. The number of sample components, *i.e.*, d, is an important information about the attack, defining the order of the input and output spaces. We call this number *the order of an attack*.

Definition 2 (The order of an attack). *The number d of $(\mathbb{F}_2^n)^d$ is called the order of the space $(\mathbb{F}_2^n)^d$. An attack that uses samples in a d-th-order space is called the d-th-order attack.*

For the sake of convenience, in the following we will say that a d-th-order attack on $\mathcal{E} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is an attack on $\mathcal{E}^{\times d} : (\mathbb{F}_2^n)^d \to (\mathbb{F}_2^m)^d$ (but in the cases when the order is clear, "$\times d$" might be omitted for simplicity). For example, differential cryptanalysis is a typical second-order attack as it uses a pair of messages, so we say that the differential attack is on $\mathcal{E}^{\times 2} : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^m)^2$. Furthermore, note that in a d-th ($d > 1$) order attack, in fact we are more interested in the difference between the i-th ($i \geq 1$) and the first component of the sample. Thus, we consider the input and output of $\mathcal{E}^{\times d}$ as

$$(p_0, p_0 \oplus p_1, \ldots, p_0 \oplus p_{d-1}) \text{ and } (c_0, c_0 \oplus c_1, \ldots, c_0 \oplus c_{d-1}),$$

which is similar to the setting of polytopic attacks [33]. In the following, by default we will use $(x_0, \Delta_1, \ldots, \Delta_{d-1})$ to represent the input of an attack where Δ_i ($i \geq 1$) is the difference between the i-th and the first element, *i.e.*, $\Delta_i = x_0 \oplus x_i$, and we will use $(\mathcal{E}(x_0), \mathcal{D}_{\Delta_1}\mathcal{E}(x_0), \ldots, \mathcal{D}_{\Delta_{d-1}}\mathcal{E}(x_0))$ to represent the output where $\mathcal{D}_\Delta\mathcal{E}(x) = \mathcal{E}(x) \oplus \mathcal{E}(x \oplus \Delta)$ is the derivative of $\mathcal{E}$ in direction Δ, evaluated on x. In this paper, for second-order attacks we use (x, Δ) and $(\mathcal{E}(x), \mathcal{D}_\Delta\mathcal{E}(x))$ for the input and output pairs, respectively. Such a writing style can simplify the notation.

Consider the d-th-order space $(\mathbb{F}_2^n)^d$ and the rational field $\mathbb{Q}$, the free vector space can be induced as $\mathbb{Q}[(\mathbb{F}_2^n)^d]$, where elements in $(\mathbb{F}_2^n)^d$ is a basis of $\mathbb{Q}[(\mathbb{F}_2^n)^d]$. It is similar to the cases we have discussed in Section 2, but we choose different bases for the input and output free vector spaces here.

For $\mathcal{E}^{\times d} : (\mathbb{F}_2^n)^d \to (\mathbb{F}_2^m)^d$, let $\mathcal{T}^{\mathcal{E}^{\times d}}$ be the pushforward operation of $\mathcal{E}^{\times d}$ that maps a standard basis of $\mathbb{Q}[(\mathbb{F}_2^n)^d]$ to a standard basis of $\mathbb{Q}[(\mathbb{F}_2^m)^d]$, *i.e.*, $\mathcal{T}^{\mathcal{E}^{\times d}}(\delta_u) = \delta_{\mathcal{E}^{\times d}(u)}$ where $u \in (\mathbb{F}_2^n)^d$. Under the standard basis, the corresponding matrix of $\mathcal{T}^{\mathcal{E}^{\times d}}$ is denoted by $T^{\mathcal{E}^{\times d}}$ with $T^{\mathcal{E}^{\times d}}_{v,u} = \delta_v(\mathcal{E}^{\times d}(u))$.

Suppose we choose two bases for the input and output spaces which satisfy

$$[\delta_u(v)]_{v,u} = [\alpha_u(v)]_{v,u}P \text{ (input) and } [\delta_u(v)]_{v,u} = [\beta_u(v)]_{v,u}Q \text{ (output)},$$

where $P \in \mathbb{F}_2^{2^n \times 2^n}$ and $Q \in \mathbb{F}_2^{2^m \times 2^m}$ are the corresponding change-of-basis matrices. A new transition matrix of $\mathcal{E}^{\times d}$ can be deduced similarly to Equation (4)

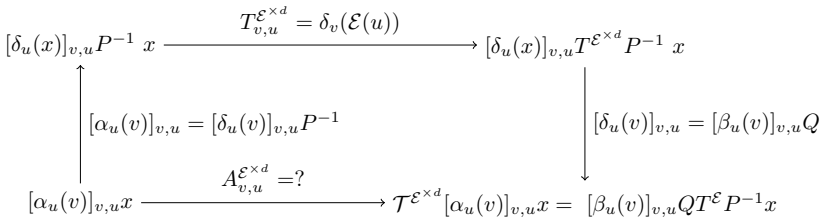

Fig. 1: An illustration of the geometric approach on a cryptanalysis with two different bases. Note $P^{-1} = [\alpha_u(x)]_{x,u}$ and $Q = [\beta_u(x)]^{-1}_{x,u}$. Given a vector $[\alpha_u(x)]_{x,u}x$ where x is the coordinate under the basis $[\alpha_u(x)]_{x,u}$. After the change-of-basis operation in the input space, it becomes a vector represented by $[\delta_u(x)]_{x,u}$, and then transformed by $\mathcal{T}^{\mathcal{E}^{\times d}}$ to $[\delta_u(x)]_{x,u}T^{\mathcal{E}^{\times d}}P^{-1}x$ ($T^{\mathcal{E}^{\times d}}$ is the corresponding matrix of $\mathcal{T}^{\mathcal{E}^{\times d}}$ under the basis $[\delta_u(x)]_{x,u}$). After the change-of-basis operation in the output space, it becomes to the final form under the basis $[\beta_u(x)]_{x,u}$ whose coordinate is $QT^{\mathcal{E}}P^{-1}x$.

as

$$A^{\mathcal{E}^{\times d}} = Q\ T^{\mathcal{E}^{\times d}}\ P^{-1}, \tag{7}$$

Clearly, $P^{-1} = [\alpha_u(v)]_{v,u}$ and $Q = [\beta_u(v)]^{-1}_{v,u}$. If $Q = [\beta_u(v)]^{-1}_{v,u}$ can also be represented in a compact way, say $Q = [\beta^{\star}_u(v)]_{v,u}$, the (v,u)-element of $A^{\mathcal{E}^{\times d}}$ can be obtained similar to Equation (5) by multiplying to the left a row unit vector $\delta_v^{\top}$ and multiplying to the right a column unit vector δ_u, as

$$\begin{aligned} A^{\mathcal{E}^{\times d}}_{v,u} &= {\delta_v}^{\top}\ A^{\mathcal{E}^{\times d}}\ \delta_u = \delta_v^{\top}\ (Q\ T^{\mathcal{E}^{\times d}}\ P^{-1})\ \delta_u \\ &= [\beta^{\star}_y(v), 0 \le y < 2^{dn}]^{\top}\ T^{\mathcal{E}^{\times d}}\ [\alpha_u(x), 0 \le x < 2^{dn}] \\ &= \sum_{x \in (\mathbb{F}_2^n)^{\otimes d}} \beta^{\star}_{\mathcal{E}^{\otimes d}(x)}(v)\ \alpha_u(x) \end{aligned} \tag{8}$$

An illustration is provided in Figure 1.

Depending on whether the two bases for the input and output spaces are the same, we divide attacks into two kinds.

Definition 3 (Same-basis and mix-basis attack). *An attack on*

$$\mathcal{E}^{\times d} : (\mathbb{F}_2^n)^d \to (\mathbb{F}_2^m)^d$$

is called a same-basis attack if the bases chosen for the input and output spaces are the same; otherwise, a mix-basis attack.

This partition is crucial for calculating the transition matrix from those of its composite functions. Most modern ciphers are constructed from smaller component functions, so computing the whole transition matrix of the cipher should handle the propagation properties of the transition matrices of its components.

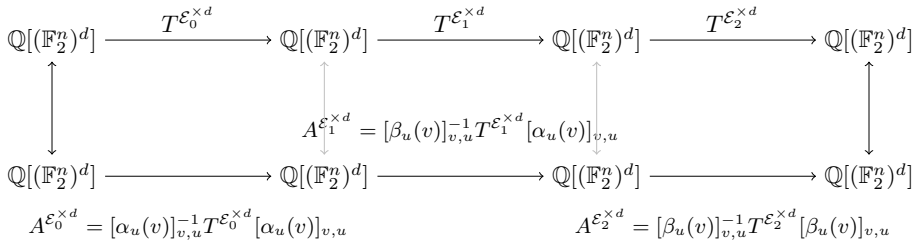

Fig. 2: The illustration of the proof for Proposition 1. For $\mathcal{E}_0^{\times d}$, both the input and output bases are $[\alpha_u(v)]_{v,u}$. For $\mathcal{E}_1^{\times d}$, the input basis is $[\alpha_u(v)]_{v,u}$ and the output basis is $[\beta_u(v)]_{v,u}$. For $\mathcal{E}_2^{\times d}$, both the input and output bases are $[\beta_u(v)]_{v,u}$.

Consider a d-th-order attack on $\mathcal{E}^{\times d} = \mathcal{E}_2^{\times d} \circ \mathcal{E}_1^{\times d} \circ \mathcal{E}_0^{\times d}$, *i.e.*, $\mathcal{E}^{\times d}$ divided into three parts. When we choose the same basis for the input and output spaces of $\mathcal{E}^{\times d}$, the attack is a same-basis attack. According to Theorem 1, the transition matrix of $\mathcal{E}^{\times d}$ is the product of the transition matrices of $\mathcal{E}_2^{\times d}$ and $\mathcal{E}_1^{\times d}$ and $\mathcal{E}_0^{\times d}$. However, things are a bit more complicated for a mix-basis attack because different bases are used for different parts of the cipher. We have the following proposition, which is actually a direct corollary of [6, Theorem 2.5].

Proposition 1 (Propagation of the mix-basis transition matrices). *For $\mathcal{E}^{\times d} = \mathcal{E}_2^{\times d} \circ \mathcal{E}_1^{\times d} \circ \mathcal{E}_0^{\times d}$, suppose that we select $[\alpha_u(v)]_{v,u}$ for the input space of $\mathcal{E}^{\times d}$ (it is also the input space of $\mathcal{E}_0^{\times d}$) and $[\beta_u(v)]_{v,u}$ for the output space of $\mathcal{E}^{\times d}$ (it is also the output space of $\mathcal{E}_2^{\times d}$). Denote the transition matrix of $\mathcal{E}^{\times d}$ under the two bases by $A^{\mathcal{E}^{\times d}}$. Then we have*

$$A^{\mathcal{E}^{\times d}} = A^{\mathcal{E}_2^{\times d}} A^{\mathcal{E}_1^{\times d}} A^{\mathcal{E}_0^{\times d}}$$

where $A^{\mathcal{E}_0^{\times d}}$ is the transition matrix of $\mathcal{E}_0^{\times d}$ under the same input and output basis $[\alpha_u(v)]_{v,u}$, $A^{\mathcal{E}_1^{\times d}}$ is the transition matrix of $\mathcal{E}_1^{\times d}$ under the input basis $[\alpha_u(v)]_{v,u}$ and output basis $[\beta_u(v)]_{v,u}$, and $A^{\mathcal{E}_2^{\times d}}$ is the transition matrix of $\mathcal{E}_2^{\times d}$ under the same input and output basis $[\beta_u(v)]_{v,u}$.

The proof is obvious with Equation (7), so we omit it. An illustration is provided in Figure 2.

Corollary 1. *Suppose $\mathcal{E}^{\times d} = \mathcal{E}_{r-1}^{\times d} \circ \cdots \circ \mathcal{E}_0^{\times d}$. Choose $r+1$ bases $[\alpha_u(v)]_{v,u}^{(i)}, 0 \leq i < r+1$, denote the transition matrix of $\mathcal{E}_i^{\times d}$ under the input basis $[\alpha_u(v)]_{v,u}^{(i)}$ and output basis $[\alpha_u(v)]_{v,u}^{(i+1)}$ by $A^{\mathcal{E}_i^{\times d}}$. Therefore, the transition matrix of $\mathcal{E}^{\otimes d}$ under the input basis $[\alpha_u(v)]_{v,u}^{(0)}$ and output basis $[\alpha_u(v)]_{v,u}^{(r)}$ can be calculated by*

$$A^{\mathcal{E}^{\times d}} = A^{\mathcal{E}_{r-1}^{\times d}} A^{\mathcal{E}_{r-2}^{\times d}} \cdots A^{\mathcal{E}_0^{\times d}}.$$

3.2 Basis of First-Order Spaces and Attacks

In this subsection, we revisit three bases for the first-order spaces that have been used in the previous geometric approach and introduce rules to generate new bases based on these existing bases.

Linear cryptanalysis. In [4], Beyne introduced the geometric approach for the first time and applied it to linear cryptanalysis. The basis he chose for the linear cryptanalysis can be represented by

Basis 1 (Linear basis [4]) $[(-1)^{u^\top v}]_{v,u}$.

Quasi-differential cryptanalysis. In [7], Beyne and Rijmen introduced the quasi-differential technique. Differential cryptanalysis is a second-order attack whose input and output spaces are second-order spaces. Beyne and Rijmen chose the quasi-differential basis as follows,

$$[(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1} = [(-1)^{u_0^\top v_0}\delta_{u_1}(v_1)]_{(v_0,v_1),(u_0,u_1)}.$$

The first part of the quasi-differential basis is for the value, which is just the linear basis. The second part is for the difference, which is the standard basis.

Basis 2 (Standard basis [7]) $[\delta_u(v)]_{v,u}$.

Ultrametric integral cryptanalysis. In [5], Beyne and Verbauwhede introduced the ultrametric integral cryptanalysis to study the divisibility property, where the ultrametric integral basis was used.

Basis 3 (Ultrametric integral basis [5]) $[(-1)^{\mathrm{wt}(u\oplus v)}v^u]_{v,u}$.

Next, we introduce three simple rules that can generate new bases based on existing ones. These rules follow a simple fact that any 2^{nd} linearly independent vectors can serve as a basis for a d-th-order space.

Remark. In theory, any operation that preserves the rank of a matrix can be used to generate new bases here. However, practical applications of the geometric approach usually require basis matrices with compact representation (*i.e.*, all elements can be calculated by a function), and an arbitrary operation might break the compact representation. Thus, we restrain ourselves in this paper to the following three rules, maintaining compact representations for the three bases introduced above and leaving it as a future work to explore more possibilities of more rules.

Rule 1 (Inverse) *If* $[\alpha_u(x)]_{v,u}$ *is a basis,* $[\alpha_u(v)]^{-1}_{v,u}$ *is also a basis.*

Rule 2 (Transpose) *If* $[\alpha_u(x)]_{v,u}$ *is a basis,* $[\alpha_u(v)]^{\top}_{v,u}$ *is also a basis.*

Table 1: Seven bases of the first-order space concluded from previous geometric approach papers and induced from Rules 1, 2 and 3. The usage of their effects of these bases for the input and output have been shown in Equation (8).

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

Rule 3 (Scale) *If* $[\alpha_u(v)]_{v,u}$ *is a basis,* $[k\alpha_u(v)]_{v,u}$ *is a basis, where* $k \neq 0$ *belongs to the corresponding field, in this paper the field is* $\mathbb{Q}$.

According to these three rules, we obtain four more bases.

Basis 4 (Inverse of linear basis) $[2^{-n}(-1)^{u^\top v}]_{v,u}$.

It is easy to check $[2^{-n}(-1)^{u^\top v}]_{v,u} \cdot [(-1)^{u^\top v}]_{v,u} = \text{Identity}$.

Basis 5 (Inverse of ultrametric integral basis) $[u^v]_{v,u}$.

It is easy to check $[u^v]_{v,u} \cdot [(-1)^{\mathsf{wt}(u\oplus v)}u^v]_{v,u} = \text{Identity}$.

Basis 6 (Transpose of ultrametric integral basis) $[(-1)^{\mathsf{wt}(u\oplus v)}v^u]_{v,u}$.

Basis 7 (Inverse and transpose of ultrametric integral basis) $[v^u]_{v,u}$.

When choosing specific bases for the input and output spaces, we can use Equation (8) to calculate the element in the corresponding transition matrix. The $\beta^{\star}_{\mathcal{E}^{\times d}(x)}(v)$ and $\alpha_u(x)$ calculated according to the matrix composed of the bases are called *effects*. We list them for the seven bases above in Table 1. These effects can help us quickly write the correlation expression, *i.e.*, the formula of the element of the corresponding transition matrix, based on the chosen bases.

Combining these seven bases for the input and output spaces, 49 different attacks, including 7 same-basis and 42 mix-basis ones, are generated. We list them in Tables 6 and 7.

Remark. One may doubt if some of them can be called "attacks". For example, when choosing $[\delta_u(v)]_{v,u}$ for both input and output spaces, the statistic

$$A^{\mathcal{E}}_{v,u} = \sum_{x=u,\mathcal{E}(x)=v} 1$$

says nothing except $\mathcal{E}(u) = v$. Whether we should regard it as an attack depends on the definition of "attacks". On the one hand, considering $\mathcal{E}$ as a public permutation, knowing $\mathcal{E}(u) = v$ is indeed useful to distinguish $\mathcal{E}$ from a random permutation. On the other hand, when $\mathcal{E}$ is key-dependent, $A^{\mathcal{E}}_{v,u} = \sum_{x=u,\mathcal{E}(x)=v} 1$ means there is a deterministic invariant behavior of $\mathcal{E}$ independently of the key (practically, this statistic should always be influenced by the secret key for a secure cipher). Therefore, we still include such simple statistics as attacks.

3.3 Basis of Higher-Order Spaces and Attacks

For a d-th-order attack, the input and output spaces are also d-th-order. In theory, any 2^{dn} linearly independent vectors can serve as a set of bases and lead to a basis-based attack. However, a random basis is difficult to handle if it does not have a compact representation. Thus, inspired by the quasi-differential cryptanalysis [7], we generate a basis for higher-order spaces by the tensor product of first-order space bases.

Proposition 2 (Basis for $\mathbb{K}[(\mathbb{F}_2^n)^d]$). *For a d-th-order space $\mathbb{K}[(\mathbb{F}_2^n)^d]$, we choose bases for each of its d components, denoted by $[\alpha_u(v)]^{(i)}_{v,u}$. $\bigotimes_{0\le i<d}[\alpha_u(v)]^{(i)}_{v,u}$ is a basis of $\mathbb{K}[(\mathbb{F}_2^n)^d]$.*

Proof. This is from the calculation rules for the tensor product. Since $[\alpha_u(v)]^{(i)}_{v,u}$ spans to $\mathbb{K}[\mathbb{F}_2^n]$, $\bigotimes_{0\le i<d}[\alpha_u(v)]^{(i)}_{v,u}$ spans to $\bigotimes_{0\le i<d}\mathbb{K}[(\mathbb{F}_2^n)] = \mathbb{K}[(\mathbb{F}_2^n)^d]$.

To compute Equation (8), we need the inverses of the basis matrices. Proposition 3 gives a simple way of calculating.

Proposition 3 (Inverse of a higher-order basis matrix). *Suppose that $\bigotimes_{0\le i<d}[\alpha_u(v)]^{(i)}_{v,u}$ is a basis of $\mathbb{K}[(\mathbb{F}_2^n)^d]$. Then, $\bigotimes_{0\le i<d}\left([\alpha_u(v)]^{(i)}_{v,u}\right)^{-1}$ is the inverse of $\bigotimes_{0\le i<d}[\alpha_u(v)]^{(i)}_{v,u}$, which is also a basis of $\mathbb{K}[(\mathbb{F}_2^n)^d]$.*

Proof. This directly follows from the fact that the inverse matrix of $A \otimes B$ is $A^{-1} \otimes B^{-1}$.

Therefore, combining the seven first-order bases in Table 1, 7^d different d-th-order bases are obtained. The 7^d different bases lead to 7^{2d} attacks including 7^d same-basis attacks and $7^{2d} - 7^d$ mix-basis attacks. Again, similar to the first-order case, not all of them look interesting, but we still see them as attacks to keep the theory intact. The effects of 49 bases for the second-order case are listed in Tables 8 and 9.

To quickly derive the correlation expression of an attack, we can use a similar method with first-order attacks. Either we can write all attacks according to the effects of the bases and check if some are interesting, or we can write the correlation expression we are interested in and see if there are proper bases that can lead to this attack.

3.4 Trail Search for Mix-Basis Attacks

Recalling Theorem 1 and Equation (6), all (resp. some) trails are clustered and their correlations are added to compute (resp. approximate) the transition matrix elements. For the mix-basis attacks following Proposition 1 and Corollary 1, transition matrices are calculated based on the corresponding input and output bases, which completely follows the same method as the same-basis attacks like linear [4], quasi-differential [7] and ultrametric integral cryptanalysis [5].

In terms of the metrics, the case of mix-basis attacks is also the same as that of same-basis attacks. We can study the value of the correlation expression by adding the correlations of trails, or look into the divisibility property by studying their 2-adic absolute values. In this paper, we do not have a specific rule for how to choose the metric, but we try both to see if we can get interesting attacks.

4 Example I: An Alternative Pair of Bases for Divisibility Property

4.1 Revisiting the Ultrametric Integral Cryptanalysis from [5]

In [5], Beyne and Verbauwhede introduced ultrametric integral cryptanalysis to describe the divisibility property. The divisibility property is a generalization of the integral property [23], interpolating between bits that sum to zero (divisibility by 2) and saturated bits (divisibility by 2^{n-1} for 2^n inputs). Given $u \in \mathbb{F}_2^n$, suppose $\mathbb{U}_u = \{x \in \mathbb{F}_2^n : x \preceq u\}$ is a structure of the plaintexts, the divisibility studies if

$$\sum_{x \in \mathbb{U}_u} \mathcal{E}^v(x) = \sum_{x \preceq u} \mathcal{E}^v(x) \equiv 0 \bmod 2^t. \tag{9}$$

To study it, Beyne and Verbauwhede chose the ultrametric integral basis as

$$[(-1)^{\mathsf{wt}(u \oplus v)} u^v]_{v,u}.$$

Denote the change-of-basis matrix between $[(-1)^{\mathsf{wt}(u \oplus v)} u^v]_{v,u}$ and the standard basis $[\delta_u(v)]_{v,u}$ by P, *i.e.*,

$$[\delta_u(v)]_{v,u} = [(-1)^{\mathsf{wt}(u \oplus v)} u^v]_{v,u} P.$$

Each element in $\mathbb{Q}[\mathbb{U}_u]$ can be expressed by a linear combination of basis vectors in $[(-1)^{\mathsf{wt}(u \oplus v)} u^v]_{v,u} = (\mu_0, \mu_1, \ldots, \mu_{2^n-1})$, thus $\delta_{\mathbb{U}_u} := \sum_{x \in \mathbb{U}_u} \delta_x = \sum_{x \preceq u} \delta_x$ is

$$\delta_{\mathbb{U}_u} = \sum_{\nu \preceq u} 2^{\mathsf{wt}(u) - \mathsf{wt}(\nu)} \mu_\nu.$$

Let the transition matrix of $\mathcal{E}$ under the basis $[(-1)^{\mathsf{wt}(u \oplus v)} u^v]_{v,u}$ be $A^{\mathcal{E}}$, we have

$$A^{\mathcal{E}}_{v,\nu} = \delta_v^\top A^{\mathcal{E}} \delta_\nu = \delta_v^\top P \; T^{\mathcal{E}} \; P^{-1} \delta_\nu = P_v T^{\mathcal{E}} \mu_\nu,$$

where P_v is the v-th row of P. The corresponding summation of the ciphertext is

$$\sum_{x\preceq u}\mathcal{E}^v(x)=\sum_{x\in\mathbb{U}_u}P_vT^{\mathcal{E}}\delta_x=P_vT^{\mathcal{E}}\delta_{\mathbb{U}_u}=\sum_{\nu\preceq u}2^{\mathsf{wt}(u)-\mathsf{wt}(\nu)}P_vT^{\mathcal{E}}\mu_\nu$$
$$=\sum_{\nu\preceq u}2^{\mathsf{wt}(u)-\mathsf{wt}(\nu)}A^{\mathcal{E}}_{v,\nu}.$$

There is an equivalence between $\sum_{x\preceq u}\mathcal{E}^v(x)\equiv 0 \bmod 2^t$ $(t\leq \mathsf{wt}(u))$ and $\left|\sum_{x\preceq u}\mathcal{E}^v(x)\right|_2\leq 2^{-t}$. According to the ultrametric triangle inequality of the 2-adic absolute value $|x+y|_2\leq \max\{|x|_2,|y|_2\}$,

$$\left|\sum_{x\preceq u}\mathcal{E}^v(x)\right|_2=\left|\sum_{\nu\preceq u}2^{\mathsf{wt}(u)-\mathsf{wt}(\nu)}A^{\mathcal{E}}_{v,\nu}\right|_2\leq\max_{\nu\preceq u}2^{\mathsf{wt}(\nu)-\mathsf{wt}(u)}\left|A^{\mathcal{E}}_{v,\nu}\right|_2.$$

Thus, if we prove $\max_{\nu\preceq u}2^{\mathsf{wt}(\nu)-\mathsf{wt}(u)}\left|A^{\mathcal{E}}_{v,\nu}\right|_2\leq 2^{-t}$, we verify that $\sum_{x\preceq u}\mathcal{E}^v(x)\equiv 0 \bmod 2^t$. For those ν satisfying $\mathsf{wt}(\nu)\leq\mathsf{wt}(u)-t$, $\max_{\nu\preceq u}2^{\mathsf{wt}(\nu)-\mathsf{wt}(u)}\left|A^{\mathcal{E}}_{v,\nu}\right|_2\leq 2^{-t}$ is already valid. For ν satisfying $\mathsf{wt}(\nu)>\mathsf{wt}(u)-t$, we need to verify that $\left|A^{\mathcal{E}}_{v,\nu}\right|_2\leq 2^{-t-wt(\nu)+\mathsf{wt}(u)}$ which can be done by searching for trails. That is, the divisibility in Equation (9) is studied in an indirect way. The reason is that the vector corresponding to the input set $\mathbb{U}_u$ is not any column index of the matrix derived from the ultrametric integral basis.

4.2 An Alternative Method for Divisibility Property

Using two different bases for the input and output, we can derive a matrix whose (v,u)-element is exactly $\sum_{x\preceq u}\mathcal{E}^v(x)$, *i.e.*,

$$A^{\mathcal{E}}_{v,u}=\sum_{x\preceq u}\mathcal{E}^v(x).$$

Note that $A^{\mathcal{E}}_{v,u}=\sum_{x\preceq u}\mathcal{E}^v(x)=\sum_{x\in\mathbb{F}_2^n}u^x\mathcal{E}^v(x)$. According to Table 1, if we want a term u^x, we can choose the basis

$$[u^v]_{v,u}$$

for the input space. For $\mathcal{E}^v(x)$, we can choose the basis

$$[(-1)^{\mathsf{wt}(u\oplus v)}u^v]_{v,u}$$

for the output space. The (v,u)-element of the transition matrix under these two bases is

$$A^{\mathcal{E}}_{v,u}=\sum_{x\in\mathbb{F}_2^n}u^x\mathcal{E}^v(x)=\sum_{x\preceq u}\mathcal{E}^v(x).$$

Since the bases for the input and output spaces are different, this attack belongs to the mix-basis attacks. To characterize the propagation of the transition matrices, we divide an r-round cipher $\mathcal{E}$ into three parts

$$\mathcal{E} = \mathcal{E}_2 \circ \mathcal{E}_1 \circ \mathcal{E}_0,$$

where $\mathcal{E}_0$, $\mathcal{E}_1$ and $\mathcal{E}_2$ are three consecutive parts of $\mathcal{E}$ whose number of rounds are respectively r_0, r_1 and r_2 that satisfy $r_0 + r_1 + r_2 = r$.

For $\mathcal{E}_0$, the transition matrix is obtained in the same-base attack framework under the basis $[u^v]_{v,u}$ for the input and output spaces. Thus, the (v,u)-element of the transition $A^{\mathcal{E}_0}$ is

$$A^{\mathcal{E}_0}_{v,u} = \sum_{x \in \mathbb{F}_2^n} u^x \cdot (-1)^{\mathsf{wt}(v \oplus \mathcal{E}(x))} \mathcal{E}^v(x) = \sum_{x \preceq u} (-1)^{\mathsf{wt}(v \oplus \mathcal{E}(x))} \mathcal{E}^v(x). \tag{10}$$

For $\mathcal{E}_2$, the transition matrix is also obtained in the same-basis attack framework under the basis $[(-1)^{\mathsf{wt}(u \oplus x)} u^v]_{v,u}$ for both the input and output spaces. Thus, the (v,u)-element of the transition $A^{\mathcal{E}_2}$ is

$$A^{\mathcal{E}_2}_{v,u} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathsf{wt}(u \oplus x)} u^x \cdot \mathcal{E}^v(x) = \sum_{x \preceq u} (-1)^{\mathsf{wt}(u \oplus x)} \mathcal{E}^v(x). \tag{11}$$

Note that $A^{\mathcal{E}_2}$ is just the transition matrix of ultrametric integral cryptanalysis derived by Beyne and Verbauwhede.

For $\mathcal{E}_1$, the transition matrix is derived from the same bases for $\mathcal{E}$, so the (v,u)-element of this transition matrix is

$$A^{\mathcal{E}_1}_{v,u} = \sum_{x \in \mathbb{F}_2^n} u^x \cdot \mathcal{E}^v(x) = \sum_{x \preceq u} \mathcal{E}^v(x). \tag{12}$$

Finally,

$$A^{\mathcal{E}} = A^{\mathcal{E}_2} A^{\mathcal{E}_1} A^{\mathcal{E}_0}.$$

The automatic search can be done with the same methods introduced in Section 2.3 and [5], with the 2-adic absolute value $|\cdot|_2$ being the metric. The targets of ultrametric integral cryptanalysis and our alternative attack are the same; our method cannot find more distinguishers than ultrametric integral cryptanalysis. However, our method does not require any more techniques in the automatic search. We give an example on how to use the automatic search model for our alternative attack and re-find the ultrametric integral distinguishers for 9-round `PRESENT` in Appendix C.

5 Example II: First-Order Multiple-of-2^t Property

The multiple-of-2^t property was found for the first time by Grassi, Rechberger, and Rønjom [17] for 5-round AES. For $\mathcal{E} : \mathbb{F}_2^n \to \mathbb{F}_2^m$, this property shows that there exist two non-trivial linear subspaces $\mathbb{U}$ and $\mathbb{V}$ of $\mathbb{F}_2^n$ satisfying: for any

coset of $\mathbb{U}$, say $c \oplus \mathbb{U}$, the number of distinct pairs $\{x, y\}$ satisfying $x \neq y$ in $c \oplus \mathbb{U}$ such that $\mathcal{E}(x)$ and $\mathcal{E}(y)$ belong to the same coset of $\mathbb{V}$ is always divisible by 2^t. Later, Boura, Canteaut, and Coggia extended this property to more ciphers [14]. For example, they found that SKINNY [3] has multiple-of-2^{h-1} properties, where $h \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14\}$ according to different subspace trails found by the methods of [25]. However, since this proof heavily relies on the subspace trail, the rounds for SKINNY's multiple-of-2^t property still stop at 5 rounds.

Inspired by ultrametric integral cryptanalysis [5], it is possible to choose a pair of bases to describe the multiple-of-2^t property. The original multiple-of-2^t property works for pairs of messages, so it should be studied as a second-order attack. Interestingly, similar ideas are also applicable for the first-order case, where we go to study the divisibility property of the number of inputs and outputs that are in certain subspaces. In the following, we first describe the first-order multiple-of-2^t attack, as we obtain better results than the second-order multiple-of-2^t attack for SKINNY-64. The methods are also applicable in theory to other ciphers such as AES. However, modelling the heavy AES components such as the 8-bit Sbox and the MDS matrix remains an important obstacle, so we will only focus on SKINNY-64 in this paper.

We first define the first-order multiple-of-2^t property.

Definition 4 (First-order multiple-of-2^t property). *For $\mathcal{E} : \mathbb{F}_2^n \to \mathbb{F}_2^m$, let $a, u \in \mathbb{F}_2^n$, $b, v \in \mathbb{F}_2^m$ and $u \neq \mathbf{1}^n$, $v \neq \mathbf{1}^m$, where $\mathbf{1}^n$ (resp. $\mathbf{1}^m$) is the bit vector with all its n (resp. m) coordinates being 1. If the size of*

$$\{x : a \oplus x \preceq u, \mathcal{E}(x) \oplus b \preceq v\}$$

is divisible by 2^t, we say $\mathcal{E}$ has a first-order multiple-of-2^t property with respect to a, u, b and v.

Denoting $\mathcal{F}(x) = \mathcal{E}(x \oplus a) \oplus b$, *i.e.*, $\mathcal{F}$ is a function with XORing constants before and after $\mathcal{E}$, this property can be characterized by the following correlation expression,

$$A^{\mathcal{F}}_{v,u} = \sum_{x \oplus a \preceq u, \mathcal{E}(x) \oplus b \preceq v} 1 = \sum_{x \preceq u, \mathcal{F}(x) \preceq v} 1 = \sum_{x \in \mathbb{F}_2^n} \underbrace{u^x}_{\substack{\text{effect of} \\ \text{input basis}}} \underbrace{v^{\mathcal{F}(x)}}_{\substack{\text{effect of} \\ \text{output basis}}}. \tag{13}$$

Checking Table 1, it suffices to choose the input basis as $[u^v]_{v,u}$ and the output basis $[(-1)^{\mathsf{wt}(u \oplus v)} v^u]_{v,u}$, to generate a mix-basis attack. $\mathcal{E}$ is divided into three parts, as $\mathcal{E} = \mathcal{E}_2 \circ \mathcal{E}_1 \circ \mathcal{E}_0$, then $\mathcal{F} = \oplus_b \circ \mathcal{E}_2 \circ \mathcal{E}_1 \circ \mathcal{E}_0 \circ \oplus_a$, where $\oplus_a(x) = x \oplus a$, $\oplus_b(x) = x \oplus b$, and $\mathcal{E}_1$ is usually set as a single layer of Sboxes.

For $\mathcal{E}'_0 = \mathcal{E}_0 \circ \oplus_a$, the same-basis attack with the basis $[u^v]_{v,u}$ is applied. The correlation expression is

$$A^{\mathcal{E}'_0}_{v,u} = \sum_{x \preceq u} (-1)^{\mathsf{wt}(\mathcal{E}'_0(x) \oplus v)} (\mathcal{E}'_0(x))^v. \tag{14}$$

Since $\oplus_a : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be seen as n parallel bit-XOR operations, we have $A^{\oplus_a} = \bigotimes_{0 \le i < n} A^{\oplus_{a_i}}$, where

$$A^{\oplus_{a_i}} = \begin{bmatrix} (-1)^{a_i} & 0 \\ a_i & 1 \end{bmatrix}. \tag{15}$$

Similarly, for $\mathcal{E}_2' = \oplus_a \circ \mathcal{E}_2$, the same-basis attack with the basis $[(-1)^{\mathsf{wt}(u \oplus v)} v^u]_{v,u}$ is applied. The correlation expression is

$$A^{\mathcal{E}_2}_{v,u} = \sum_{x \succeq u} (-1)^{\mathsf{wt}(x \oplus u)} v^{\mathcal{E}(x)}. \tag{16}$$

For $\oplus_b : \mathbb{F}_2^m \to \mathbb{F}_2^m$ such that $A^{\oplus_b} = \bigotimes_{0 \le i < m} A^{\oplus_{b_i}}$, we have

$$A^{\oplus_{b_i}} = \begin{bmatrix} (-1)^{b_i} & b_i \\ 0 & 1 \end{bmatrix}. \tag{17}$$

Finally, the input basis $[u^v]_{v,u}$ and output basis $[(-1)^{\mathsf{wt}(u \oplus v)} v^u]_{v,u}$ are applied to $\mathcal{E}_1$ to get its correlation expression that is the same as Equation (13).

The automatic search model is constructed based on the transition matrix of each part of $\mathcal{F}$. To study if $A^{\mathcal{F}}_{v,u}$ is divisible by 2^t, we check if $|A^{\mathcal{F}}_{v,u}|_2 \le 2^{-t}$; this can be done by proving that there is no trail whose correlation is larger than 2^{-t}. Due to the ultrametric triangle inequality $|x+y|_2 \le \max\{|x|_2, |y|_2\}$ of the 2-adic absolute value, we can search for a trail that connects u and v with the largest 2-adic absolute value. If this largest value is 2^{-t}, then we know $|A^{\mathcal{F}}_{v,u}|_2 \le 2^{-t}$ and $A^{\mathcal{F}}_{v,u} \equiv 0 \bmod 2^t$.

Choice of the position of $\mathcal{E}_1$. If all trails can be exhausted, the position of $\mathcal{E}_1$ does not affect the final correlation $A^{\mathcal{F}}_{v,u}$. However, in this paper, we only give the upper bound on the 2-adic absolute value of the correlation by searching for a trail that has the largest 2-adic absolute value, and thus the position of $\mathcal{E}_1$ does affect the results. No matter where $\mathcal{E}_1$ is positioned, all the upper bounds that we obtain are real. In our applications, we will try all possibilities for the position of $\mathcal{E}_1$ and choose the tightest bound as the final result.

Application to SKINNY-64. We apply the above method to round-reduced SKINNY-64 (the specification of SKINNY-64 is provided in Appendix A.2) for checking its first-order multiple-of-2^t property. We divide r rounds of SKINNY-64 into three parts as $\mathcal{E} = \mathcal{E}_2 \circ \mathcal{E}_1 \circ \mathcal{E}_0$ with $\mathcal{E}_1$ being one layer of Sboxes. According to Equations (14), (13), (16), the transition matrices for components of $\mathcal{E}_0$, $\mathcal{E}_1$ and $\mathcal{E}_2$ can be constructed. The $\oplus_a$ and $\oplus_b$ operations are modeled with Equations (15) and (17). In our model, we do not specify concrete values for a and b, and regard a, b as unknown constants. Thus, our results work for any constants a and b. Next, we give more details about our automatic search model for SKINNY-64.

For a component $\mathcal{S}$ which might be an Sbox in SC or an LBox in the MC (the MixColumn operation of SKINNY-64 can be split into 16 parallel 4-bit Sboxes,

Table 2: The first-order multiple-of-2^t property of SKINNY-64 from 6 to 11 rounds. The input/output values represent u and v, respectively. The constants in $\oplus_a$ and $\oplus_b$ are set as unknown constants; thus, these distinguishers work for any a and b.

Rnd.	Input/Output Value	Multiple-of-2^t	Configure
6	0fff'ffff'ffff'ffff → ffff'f0ff'ffff'ffff	2^{47}	$3+1+2$
7	0fff'ffff'ffff'ffff → ffff'f0ff'ffff'ffff	2^{42}	$3+1+3$
8	0fff'ffff'ffff'ffff → ffff'f0ff'ffff'ffff	2^{29}	$4+1+3$
9	0fff'ffff'ffff'ffff → ffff'f0ff'ffff'ffff	2^{17}	$4+1+4$
10	0fff'ffff'ffff'ffff → ffff'f0ff'ffff'ffff	2^{8}	$4+1+5$
11	0fff'ffff'ffff'ffff → ffff'f0ff'ffff'ffff	2^{1}	$3+1+7$

which are called LBox, see Appendix A.2 for more details), given the input mask u and output mask v, the vectors $\big(u, v, -\log(|A^{\mathcal{S}}_{v,u}|_2)\big)$ are modeled with the automatic search tool language, in a classical way.

For operations such as SR, directly modifying variables suffices. For AC and ART operations, known and unknown constants are XORed with the state, so Equations (15) and (17) are used in models.

Finally, we want to maximize the product of correlations of all components along a trail. Since each correlation x is transformed as $-\log(x)$, the equivalent optimization goal becomes minimizing the sum of these negative logarithms. This is similar to the popular manipulation of the probability in differential cryptanalysis.

Results. The longest first-order multiple-of-2^t property reaches 11 rounds for SKINNY-64, as shown in Table 2. The 11-round SKINNY-64 has a first-order multiple-of-2 property, which has the same length as the longest integral distinguishers [16].

From first-order to second-order multiple-of-2^t distinguishers. Suppose $\mathcal{E}$ has a first-order multiple-of-2^t property with respect to a and b, and $b \in \mathbb{F}_2^m$. Let $c = n - \mathsf{wt}(v)$, so c is the length of the constant part of the output coset, it is equivalent to say that all messages in $\{x : x \oplus a \preceq u\}$ are divided into 2^c sets, and the size of each set is divisible by 2^t. From each set, we can combine the values into pairs whose differences related to the c bits are zero, and the number of ordered pairs is a multiple of (at least) 2^{t-1}. This is because if $x = p \times 2^t$, then $x(x-1)/2 = p^2 \times 2^{2t-1} - p \times 2^{t-1} \equiv 0 \bmod 2^{t-1}$. That is, the whole number of ordered pairs from all 2^c sets is also divisible by at least 2^{t-1}. From Table 2, we can obtain a multiple-of-16 property for the 10-round SKINNY-64, whereas currently the best one only reaches 5 rounds [14]. In the next section, we will develop a mix-basis attack to describe the second-order multiple-of-2^t property, and replay the same results with the automatic search method.

6 Example III: Second-Order Multiple-of-2^t Property

In this section, we apply the geometric approach to the second-order multiple-of-2^t property and construct the automatic search model for SKINNY-64. The automatic search model can replay the same second-order multiple-of-2^t property described at the end of Section 5. Currently, though the same method also works for heavier ciphers such as AES in theory, the complicated 8-bit Sbox and MDS matrix make it difficult to construct efficient search models. Thus, we leave it as a future work for these heavy ciphers.

We first recall the formal definition of the second-order multiple-of-2^t property.

Definition 5 (Second-order multiple-of-2^t property [17][6]). *For $\mathcal{E}: \mathbb{F}_2^n \to \mathbb{F}_2^m$, let $a, u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$ and $u \neq \mathbf{1}^n$, $v \neq \mathbf{1}^m$. If the size of*

$$\{\{x, y\} : x \neq y, a \oplus x \preceq u, a \oplus y \preceq u, \mathcal{E}(x) \oplus \mathcal{E}(y) \preceq v\}$$

is divisible by 2^t, we say $\mathcal{E}$ has a second-order multiple-of-2^t property with respect to a, u and v.

The property should be described as a second-order attack, as two values are in a sample. Let $\mathcal{F}(x) = \mathcal{E}(x \oplus a) \oplus b$, we first try the following correlation expression,

$$A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} = \sum_{\substack{x \preceq u_0, \Delta \preceq u_1 \\ \mathcal{F}(x) \preceq v_0, \mathcal{D}_\Delta \mathcal{F}(x) \preceq v_1}} 1 = \sum_{x \in \mathbb{F}_2^n, \Delta \in \mathbb{F}_2^n} \underbrace{u_0^x u_1^\Delta}_{\text{effect of input basis}} \underbrace{v_0^{\mathcal{F}(x)} v_1^{\mathcal{D}_\Delta \mathcal{F}(x)}}_{\text{effect of output basis}} \tag{18}$$

where $u_0 = u_1 = u$ and $v_0 = \mathbf{1}^m, v_1 = v$. The condition $v_0 = \mathbf{1}^m$ is required as the value x is not restricted at all.

By checking the effects of bases in Tables 8 and 9, to construct this correlation expression, the input basis can be chosen as $[u_0^{v_0}]_{v_0,u_0} \otimes [u_1^{v_1}]_{v_1,u_1}$, and the output basis is chosen as $[(-1)^{\mathsf{wt}(v_0 \oplus u_0)} v_0^{u_0}]_{v_0,u_0} \otimes [(-1)^{\mathsf{wt}(v_1 \oplus u_1)} v_1^{u_1}]_{v_1,u_1}$.

Note that the multiple-of-2^t property is to count the number of distinct pairs, while the number counted by Equation (18) is the ordered pairs (*i.e.*, $\{a, b\}$ are counted twice). Besides, the trivial pairs such as $\{a, a\}$ are also counted once. To address this problem, we have the following proposition.

Proposition 4. *When $u_0 = u_1 = u$, $v_0 = \mathbf{1}, v_1 = v$, and $2^{\mathsf{wt}(u)-1} \equiv 0 \bmod 2^t$,*

$$A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} = \sum_{\substack{x \preceq u_0, \Delta \preceq u_1 \\ \mathcal{F}(x) \preceq v_0, \mathcal{D}_\Delta \mathcal{F}(x) \preceq v_1}} 1 \equiv 0 \bmod 2^{t+1}$$

is equivalent to

$$|\{\{x, y\} : x \neq y, x \preceq u, y \preceq u, \mathcal{F}(x) \oplus \mathcal{F}(y) \preceq v\}| \equiv 0 \bmod 2^t.$$

[6] This property is summarized from [17] by ourselves.

Proof. Among the $A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)}$ pairs, there are $2^{\mathsf{wt}(u)}$ trivial ones. After excluding these trivial pairs, there are $A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} - 2^{\mathsf{wt}(u)}$ non-trivial ordered pairs. Thus, $(A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} - 2^{\mathsf{wt}(u)})/2$ is the number of distinct unordered pairs. Since $A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} \equiv 0 \bmod 2^{t+1}$, we have $A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} = p \times 2^{t+1}$ for a certain p. Therefore,

$$\left(A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} - 2^{\mathsf{wt}(u)}\right)/2 = \left(p \times 2^{t+1} - 2^{\mathsf{wt}(u)}\right)/2 = p \times 2^t - 2^{\mathsf{wt}(u)-1}.$$

Thus, $2^{\mathsf{wt}(u)-1} \equiv 0 \bmod 2^t$ leads to $(A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} - 2^{\mathsf{wt}(u)})/2 \equiv 0 \bmod 2^t$.

Conversely, from $\left(A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} - 2^{\mathsf{wt}(u)}\right)/2 \equiv 0 \bmod 2^t$ and $2^{\mathsf{wt}(u)-1} \equiv 0 \bmod 2^t$, we know that $A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} \equiv 0 \bmod 2^{t+1}$. □

Similar to ultrametric integral cryptanalysis [5], $A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)} \equiv 0 \mod 2^t$ is equivalent to $|A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)}|_2 \leq 2^{-t}$. Then the second-order multiple-of-2^t property of $\mathcal{E}$ can be modeled by a mix-basis attack on $\mathcal{F}$.

Similar to the first-order case, $\mathcal{E}$ is divided into three parts, as $\mathcal{E} = \mathcal{E}_2 \circ \mathcal{E}_1 \circ \mathcal{E}_0$, and $\mathcal{E}_1$ is a single Sbox layer. Thus $\mathcal{F} = \oplus_b \circ \mathcal{E}_2 \circ \mathcal{E}_1 \circ \mathcal{E}_0 \circ \oplus_a$.

For $\mathcal{E}'_0 = \mathcal{E}_0 \circ \oplus_a$, the same-basis attack with the basis $[u_0^{v_0}]_{v_0,u_0} \otimes [u_1^{v_1}]_{v_1,u_1}$ is applied. The correlation expression is

$$A^{\mathcal{E}'_0}_{(v_0,v_1),(u_0,u_1)} = \sum_{\substack{x \preceq u_0, \Delta \preceq u_1 \\ \mathcal{E}'_0(x) \succeq v_0, \mathcal{D}_\Delta \mathcal{E}'_0(x) \succeq v_1}} (-1)^{\mathsf{wt}(v_0 \oplus \mathcal{E}'_0(x))} (-1)^{\mathsf{wt}(v_1 \oplus \mathcal{D}_\Delta \mathcal{E}'_0(x))}$$

Since $\oplus_a : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be seen as n parallel bit-XOR operations, thus we have $A^{\oplus_a} = \bigotimes_{0 \leq i < n} A^{\oplus_{a_i}}$, where

$$A^{\oplus_{a_i}} = \begin{bmatrix} (-1)^{a_i} & 0 & 0 & 0 \\ 0 & (-1)^{a_i} & 0 & 0 \\ a_i & 0 & 1 & 0 \\ 0 & a_i & 0 & 1 \end{bmatrix}$$

Similarly, for $\mathcal{E}'_2 = \oplus_a \circ \mathcal{E}_2$, the same-basis attack with the basis $[(-1)^{\mathsf{wt}(u_0 \oplus v_0)} v_0^{u_0}]_{v_0,u_0} \otimes [(-1)^{\mathsf{wt}(u_0 \oplus v_0)} v_0^{u_0}]_{v_0,u_0}$ is applied. The correlation expression is

$$A^{\mathcal{E}'_2}_{(v_0,v_1),(u_0,u_1)} = \sum_{\substack{x \succeq u_0, \Delta \succeq u_1 \\ \mathcal{E}'_2(x) \preceq v_0, \mathcal{D}_\Delta \mathcal{E}'_2(x) \preceq v_1}} (-1)^{\mathsf{wt}(u_0 \oplus x)} (-1)^{\mathsf{wt}(u_1 \oplus \Delta)}$$

For $\oplus_b : \mathbb{F}_2^m \to \mathbb{F}_2^m$ such that $A^{\oplus_b} = \bigotimes_{0 \leq i < m} A^{\oplus_{b_i}}$, we have

$$A^{\oplus_{b_i}} = \begin{bmatrix} (-1)^{b_i} & 0 & b_i & 0 \\ 0 & (-1)^{b_i} & 0 & b_i \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Finally, the input basis $[u_0^{v_0}]_{v_0,u_0} \otimes [u_1^{v_1}]_{v_1,u_1}$ and output basis $[(-1)^{\mathsf{wt}(u_0 \oplus v_0)} v_0^{u_0}]_{v_0,u_0} \otimes [(-1)^{\mathsf{wt}(u_1 \oplus v_1)} v_1^{u_1}]_{v_1,u_1}$ are applied to $\mathcal{E}_1$ to get its correlation expression that is the same as Equation (18).

The automatic search model is constructed based on the transition matrix of each part of $\mathcal{F}$. To study if $A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)}$ is divisible by 2^t, we check if $|A^{\mathcal{F}}_{(v_0,v_1),(u_0,u_1)}|_2 \leq 2^{-t}$ similarly to the first-order case.

Application to SKINNY-64. The automatic search model for SKINNY-64 for the second-order multiple-of-2^t property is analogous to Section 5, except that the vectors here are

$$(u_0, u_1, v_0, v_1, -\log(|A^{\mathcal{S}}_{(v_0,v_1),(u_0,u_1)}|_2))$$

for an operation $\mathcal{S}$.

Results and discussions. Up to 10 rounds, we can find new second-order multiple-of-2^t properties for SKINNY-64, by the automatic search model. These distinguishers are identical to those derived by analyzing the first-order multiple-of-2^t properties for SKINNY-64. However, the second-order multiple-of-2^t property has the potential to be better than the first-order case, as the sum of several numbers that are not divisible by 2^t can still be a multiple of 2^t. Thus, the potential of the automatic search model for the second-order multiple-of-2^t property has not been fully explored, which we leave as future work.

7 Example IV: Differential-Linear Cryptanalysis

Differential-linear (DL) cryptanalysis was originally proposed by Langford and Hellman in 1994 [24]. In this attack, a cipher $\mathcal{E}$ is decomposed into two sub-ciphers as $\mathcal{E} = \mathcal{E}_1 \circ \mathcal{E}_0$, where a differential for $\mathcal{E}_0$ and a linear approximation for $\mathcal{E}_1$ are considered. The bias of this DL approximation can be estimated accordingly under some independence assumptions.

As pointed out in [9], experiments are required to verify the estimated bias when possible because the underlying assumptions may fail. A closed formula for the DL bias, from Blondeau, Leander, and Nyberg [11], is given under the sole assumption that $\mathcal{E}_0$ and $\mathcal{E}_1$ are independent. Let $\varepsilon[\delta \xrightarrow{\mathcal{E}_0} \gamma]$ denote the correlation of a DL distinguisher over $\mathcal{E}_0$ with the input difference δ and output mask γ, and $c[\gamma \xrightarrow{\mathcal{E}_1} \lambda]$ denote the linear correlation with input and output masks γ and λ, respectively, over $\mathcal{E}_1$. Then, based on the independence assumption between $\mathcal{E}_0$ and $\mathcal{E}_1$, a DL distinguisher over $\mathcal{E} = \mathcal{E}_1 \circ \mathcal{E}_0$ with input difference δ and output mask λ has the exact correlation

$$\varepsilon[\delta \xrightarrow{\mathcal{E}} \lambda] = \sum_{\gamma} \varepsilon[\delta \xrightarrow{\mathcal{E}_0} \gamma] c^2[\gamma \xrightarrow{\mathcal{E}_1} \lambda]. \tag{19}$$

Recently, new methods to estimate the DL bias have been proposed. For example, Bar-On *et al.* proposed the Differential-Linear Connectivity Table (DLCT) [1], Liu *et al.* introduced the algebraic transitional form (DATF) to approximate

Table 3: The second-order multiple-of-2^t property on SKINNY-64 from 6 to 10 rounds. the input/output mask pairs represent $(u_0, u_1)/(v_0, v_1)$. The constants in $\oplus_a$ and $\oplus_b$ are set as unknown constants; thus, these distinguishers work for any a and b.

Rnd.	Input/Output Value-Difference Pairs	Multiple -of-$2n$(-n)	Config.
6	(0fff′ffff′ffff′ffff, 0fff′ffff′ffff′ffff) ↓ (ffff′ffff′ffff′ffff, ffff′f0ff′ffff′ffff)	$2^{47}(2^{46})$	$2+1+3$
7	(0fff′ffff′ffff′ffff, 0fff′ffff′ffff′ffff) ↓ (ffff′ffff′ffff′ffff, ffff′f0ff′ffff′ffff)	$2^{42}(2^{41})$	$3+1+3$
8	(0fff′ffff′ffff′ffff, 0fff′ffff′ffff′ffff) ↓ (ffff′ffff′ffff′ffff, ffff′f0ff′ffff′ffff)	$2^{29}(2^{28})$	$4+1+3$
9	(0fff′ffff′ffff′ffff, 0fff′ffff′ffff′ffff) ↓ (ffff′ffff′ffff′ffff, ffff′f0ff′ffff′ffff)	$2^{17}(2^{16})$	$4+1+4$
10	(0fff′ffff′ffff′ffff, 0fff′ffff′ffff′ffff) ↓ (ffff′ffff′ffff′ffff, ffff′f0ff′ffff′ffff)	$2^{8}(2^{7})$	$4+1+5$

the bias [26] followed by [19], Hadipour, Derbez and Eichlseder generalized the DLCT to more rounds [18], and Peng *et al.* combined the truncated differential for a precise estimation of the DL bias [29].

7.1 Closed Formula without Independence Assumption

Using our notations, the DL approximation over a cipher $\mathcal{E}$ with an input difference δ and an output mask λ can be described by the following statistic

$$A^{\mathcal{E}}_{(v_0,v_1),(u_0,u_1)} = 2^{-n} \sum_{x\in\mathbb{F}_2^n, \Delta=u_1} (-1)^{u_0^\top x \oplus v_0^\top \mathcal{E}(x) \oplus v_1^\top \mathcal{D}_\Delta \mathcal{E}(x)}, \tag{20}$$

where $u_0 = v_0 = 0$, $u_1 = \delta$ and $v_1 = \lambda$. Indeed, after replacing u_0, v_0, u_1, v_1 with $0, 0, \delta, \lambda$, the above equation becomes

$$\varepsilon[\delta \xrightarrow{\mathcal{E}} \lambda] = A^{\mathcal{E}}_{(0,\lambda),(0,\delta)} = 2^{-n} \sum_{x\in\mathbb{F}_2^n, \Delta=\delta} (-1)^{v_1^\top \mathcal{D}_\Delta \mathcal{E}(x)}.$$

By checking the effects in Tables 8 and 9, Equation (20) can be obtained with the geometric approach with the input basis $[(-1)^{u^\top v}]_{v,u} \otimes [\delta_u(v)]_{v,u}$ and output basis $[2^{-n}(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [(-1)^{u_1^\top v_1}]_{v_1,u_1}$ (or another basis $[(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [2^{-n}(-1)^{u_1^\top v_1}]_{v_1,u_1}$).

Therefore, we can treat the DL attacks as a mix-basis attack. We first divide $\mathcal{E}$ into three parts as $\mathcal{E} = \mathcal{E}_2 \circ \mathcal{E}_1 \circ \mathcal{E}_0$. For $\mathcal{E}_0$, the quasi-differential cryptanalysis [7] is applied, and the transition matrix is denoted by $A^{\mathcal{E}_0}$. For $\mathcal{E}_1$, Equation (20) is used for the correlation expression, and the transition matrix is denoted by $A^{\mathcal{E}_1}$. For $\mathcal{E}_2$, the correlation expression derived with the same basis $2^{-n}[(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [(-1)^{u_1^\top v_1}]_{v_1,u_1}$ for the input/output spaces is

$$A^{\mathcal{E}_2}_{(v_0,v_1),(u_0,u_1)} = 2^{-2n} \sum_{x\in\mathbb{F}_2^n, \Delta\in\mathbb{F}_2^n} (-1)^{u_0^\top x \oplus v_0^\top \mathcal{E}(x) \oplus u_1^\top \Delta \oplus v_1^\top \mathcal{D}_\Delta \mathcal{E}(x)}$$

The transition matrix of $\mathcal{E}$ with input basis $[(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}$ and output basis $[2^{-n}(-1)^{u_0^\top v_0}]_{v_0,u_0} \otimes [(-1)^{u_1^\top v_1}]_{v_1,u_1}$ is calculated by

$$A^{\mathcal{E}} = A^{\mathcal{E}_2} A^{\mathcal{E}_1} A^{\mathcal{E}_0}$$

Setting $u_0 = v_0 = 0$, $u_1 = \delta$ and $v_1 = \lambda$, we get

$$\varepsilon[\delta \xrightarrow{\mathcal{E}} \lambda] = A^{\mathcal{E}}_{(0,\lambda),(0,\delta)} = \sum_{(\theta_0,\theta_1),(\gamma_0,\gamma_1)} A^{\mathcal{E}_2}_{(0,\lambda),(\theta_0,\theta_1)} \, A^{\mathcal{E}_1}_{(\theta_0,\theta_1),(\gamma_0,\gamma_1)} \, A^{\mathcal{E}_0}_{(\gamma_0,\gamma_1),(0,\delta)}. \tag{21}$$

Equation (21) can be the closed formula for the DL approximation correlation. Inherent in the geometric approach, such a formula holds without independence assumptions. Using the automatic search tools to trace all trails derived from Equation (21), we can get the exact correlation.

When treating $\mathcal{E}_1 \circ \mathcal{E}_0$ as a whole part and considering $\mathcal{E}_1 \circ \mathcal{E}_0$ and $\mathcal{E}_2$ as two independent parts, we can get the same Blondeau-Leander-Nyberg formula from Equation (21). The details are given in Appendix D.

7.2 Automatic Search for DL Approximation

Like previous applications, it is easy to develop an automatic search model to look for DL distinguishers on a cipher. For a given input difference δ and an output mask λ, we can use trails to approximate Equation (20). If we can exhaust all possible trails, the sum of all trail correlations is the exact DL approximation.

In [18], Hadipour *et al.* extended the DLCT to cover more rounds to give an efficient and precise method to estimate the correlation of DL approximations. They applied the method to the block cipher `SIMECK` and obtained the currently best-known DL distinguishers. Among the DL distinguishers they found, there are two deterministic DL approximations, one for `SIMECK`-32 and one for `SIMECK`-48, as shown in Table 4. However, as Hadipour *et al.*'s model was set based on the classical assumption that the consecutive rounds are independent, it is difficult to know if these deterministic DL approximations hold for all the key values. This is actually a challenge for almost all classical cryptanalysis methods. The geometric approach, as shown in previous applications, inherently works well without independence assumptions, as long as we can exhaust all trails.

Table 4: Two deterministic DL approximations of SIMECK found by Hadipour *et al.* [18].

Cipher	Round	Input Diff	Output Mask	Cor.
SIMECK-32	7	00001000	00000400	1
SIMECK-48	8	000000020000	000000010000	1

We set the automatic search tools for the two DL distinguishers. Our automatic search model is able to exhaust all trails for the two DL approximations, thus calculating the exact correlations of them. According to our search results, the sum of correlations of trails with non-zero masks for the values (which means the concrete key values would affect the final correlation) is always zero. The sum of correlations of trails with zero masks for the values (which means the key values would not affect the final correlation) is finally 1. Therefore, we confirm that the two DL approximations have exactly 1 correlation, without being affected by the key bits.

8 Conclusion

This paper extends Beyne's geometric approach by allowing using two different bases for the input and output spaces. We utilized three previously known bases and generated four new ones according to some simple rules. Based on these seven bases, we defined a family of *basis-based* attacks. For a d-th-order, the seven bases lead to 7^{2d} attacks. The basis-based attacks provide a systematic way to generate new ones rather than the classical intuitive method. Our extension makes the geometric approach more flexible and able to describe/predict more types of attacks. Inherent to the geometric approach, all basis-based attacks can be studied with a similar automatic search method. The core is to track the propagation trails and estimate the correlations according to certain metrics. We provided four example applications to show how to take some basis-based attacks into practice, including an alternative way for the divisibility property studied by ultrametric integral cryptanalysis, multiple-of-2^t properties for the first-order and second-order attacks, and finally, the differential-linear attacks.

There are many future works. For example, one can explore how to quickly check all these basis-based attacks and identify the most threatening one for a certain cipher. Besides, Corollary 1 is not really used in this paper; it is interesting to study how to find a "best basis chain" that can connect the bases for the input and output spaces of each round that brings the best dominant trail [5, Theorem 2.2], which can reduce the search burden significantly. Additionally, the potential of the second-order multiple-of-2^t properties requires a deeper exploration. Finally, it would be interesting to study more possibilities of the bases, in addition to the ones presented by this paper.

Acknowledgements. The authors thank Christof Beierle, who shepherded our paper, and the anonymous reviewers, whose insightful comments significantly improved the quality of this paper. This research is supported by the National Key R&D Program of China (Grant No. 2024YFA1013000, 2023YFA1009500), the National Natural Science Foundation of China (Grant No. 62032014, U2336207), Department of Science & Technology of Shandong Province (No.SYS202201), Quan Cheng Laboratory (Grant No. QCLZD202301, QCLZD202306). Kai Hu is supported by the National Cryptologic Science Fund of China (2025NCSF02007), the National Natural Science Foundation of China (62402283), the Natural Science Foundation of Shandong Province (2025HWYQ-025), the Natural Science Foundation of Jiangsu Province (BK20240420) and Program of Qilu Young Scholars of Shandong University. Meiqin Wang is also supported by the the National Cryptologic Science Fund of China (2025NCSF01013). Thomas Peyrin is supported by the Singapore NRF Investigatorship grant NRF-NRFI08-2022-0013.

References

1. Bar-On, A., Dunkelman, O., Keller, N., Weizman, A.: DLCT: A new tool for differential-linear cryptanalysis. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I. Lecture Notes in Computer Science, vol. 11476, pp. 313–342. Springer (2019). https://doi.org/10.1007/978-3-030-17653-2_11, https://doi.org/10.1007/978-3-030-17653-2_11
2. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK lightweight block ciphers. In: Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, June 7-11, 2015. pp. 175:1–175:6. ACM (2015). https://doi.org/10.1145/2744769.2747946, https://doi.org/10.1145/2744769.2747946
3. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9815, pp. 123–153. Springer (2016). https://doi.org/10.1007/978-3-662-53008-5_5, https://doi.org/10.1007/978-3-662-53008-5_5
4. Beyne, T.: A geometric approach to linear cryptanalysis. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13090, pp. 36–66. Springer (2021). https://doi.org/10.1007/978-3-030-92062-3_2, https://doi.org/10.1007/978-3-030-92062-3_2
5. Beyne, T.: A geometric approach to linear cryptanalysis. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I. Lecture Notes in Com-

puter Science, vol. 13090, pp. 36–66. Springer (2021). https://doi.org/10.1007/978-3-030-92062-3_2, https://doi.org/10.1007/978-3-030-92062-3_2

6. Beyne, T.: A geometric approach to symmetric-key cryptanalysis. Ph.D. thesis, KU Leuven, Leuven, Belgium (2023), https://lirias.kuleuven.be/retrieve/713998, doctoral thesis
7. Beyne, T., Rijmen, V.: Differential cryptanalysis in the fixed-key model. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13509, pp. 687–716. Springer (2022). https://doi.org/10.1007/978-3-031-15982-4_23, https://doi.org/10.1007/978-3-031-15982-4_23
8. Beyne, T., Verbauwhede, M.: Integral cryptanalysis using algebraic transition matrices. IACR Trans. Symmetric Cryptol. **2023**(4), 244–269 (2023). https://doi.org/10.46586/TOSC.V2023.I4.244-269, https://doi.org/10.46586/tosc.v2023.i4.244-269
9. Biham, E., Dunkelman, O., Keller, N.: Enhancing differential-linear cryptanalysis. In: Zheng, Y. (ed.) Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2501, pp. 254–266. Springer (2002). https://doi.org/10.1007/3-540-36178-2_16, https://doi.org/10.1007/3-540-36178-2_16
10. Biham, E., Shamir, A.: Differential Cryptanalysis of the Full 16-Round DES. In: Brickell, E.F. (ed.) Advances in Cryptology - CRYPTO '92. LNCS, vol. 740, pp. 487–496. Springer (1992). https://doi.org/10.1007/3-540-48071-4_34, https://doi.org/10.1007/3-540-48071-4_34
11. Blondeau, C., Leander, G., Nyberg, K.: Differential-linear cryptanalysis revisited. J. Cryptol. **30**(3), 859–888 (2017). https://doi.org/10.1007/S00145-016-9237-5, https://doi.org/10.1007/s00145-016-9237-5
12. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings. Lecture Notes in Computer Science, vol. 4727, pp. 450–466. Springer (2007). https://doi.org/10.1007/978-3-540-74735-2_31, https://doi.org/10.1007/978-3-540-74735-2_31
13. Boura, C., Canteaut, A.: Another view of the division property. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9814, pp. 654–682. Springer (2016). https://doi.org/10.1007/978-3-662-53018-4_24, https://doi.org/10.1007/978-3-662-53018-4_24
14. Boura, C., Canteaut, A., Coggia, D.: A general proof framework for recent AES distinguishers. IACR Trans. Symmetric Cryptol. **2019**(1), 170–191 (2019). https://doi.org/10.13154/TOSC.V2019.I1.170-191, https://doi.org/10.13154/tosc.v2019.i1.170-191
15. Daemen, J., Rijmen, V.: AES and the Wide Trail Design Strategy. In: Knudsen, L.R. (ed.) Advances in Cryptology - EUROCRYPT 2002. LNCS, vol. 2332, pp. 108–109. Springer (2002). https://doi.org/10.1007/3-540-46035-7_7, https://doi.org/10.1007/3-540-46035-7_7

16. Derbez, P., Fouque, P.: Increasing precision of division property. IACR Trans. Symmetric Cryptol. **2020**(4), 173–194 (2020). https://doi.org/10.46586/TOSC.V2020.I4.173-194, https://doi.org/10.46586/tosc.v2020.i4.173-194
17. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round AES. In: Coron, J., Nielsen, J.B. (eds.) Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II. Lecture Notes in Computer Science, vol. 10211, pp. 289–317 (2017). https://doi.org/10.1007/978-3-319-56614-6_10, https://doi.org/10.1007/978-3-319-56614-6_10
18. Hadipour, H., Derbez, P., Eichlseder, M.: Revisiting differential-linear attacks via a boomerang perspective with application to aes, ascon, clefia, skinny, present, knot, twine, warp, lblock, simeck, and SERPENT. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 14923, pp. 38–72. Springer (2024). https://doi.org/10.1007/978-3-031-68385-5_2, https://doi.org/10.1007/978-3-031-68385-5_2
19. Hu, K., Peyrin, T., Tan, Q.Q., Yap, T.: Revisiting higher-order differential-linear attacks from an algebraic perspective. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part III. Lecture Notes in Computer Science, vol. 14440, pp. 405–435. Springer (2023). https://doi.org/10.1007/978-981-99-8727-6_14, https://doi.org/10.1007/978-981-99-8727-6_14
20. Hu, K., Sun, S., Wang, M., Wang, Q.: An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube attacks, and key-independent sums. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2020. LNCS, vol. 12491, pp. 446–476. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_15, https://doi.org/10.1007/978-3-030-64837-4_15
21. Jean, J.: TikZ for Cryptographers. https://www.iacr.org/authors/tikz/ (2016)
22. Jean, J., Nikolic, I., Peyrin, T.: Tweaks and keys for block ciphers: The TWEAKEY framework. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II. Lecture Notes in Computer Science, vol. 8874, pp. 274–288. Springer (2014). https://doi.org/10.1007/978-3-662-45608-8_15, https://doi.org/10.1007/978-3-662-45608-8_15
23. Knudsen, L.R., Wagner, D.A.: Integral Cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) Fast Software Encryption - FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer (2002). https://doi.org/10.1007/3-540-45661-9_9, https://doi.org/10.1007/3-540-45661-9_9
24. Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis. In: Desmedt, Y. (ed.) Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings. Lecture Notes in Computer Science, vol. 839, pp. 17–25. Springer (1994). https://doi.org/10.1007/3-540-48658-5_3, https://doi.org/10.1007/3-540-48658-5_3
25. Leander, G., Tezcan, C., Wiemer, F.: Searching for subspace trails and truncated differentials. IACR Trans. Symmetric Cryptol. **2018**(1), 74–100

(2018). https://doi.org/10.13154/TOSC.V2018.I1.74-100, https://doi.org/10.13154/tosc.v2018.i1.74-100
26. Liu, M., Lu, X., Lin, D.: Differential-linear cryptanalysis from an algebraic perspective. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III. Lecture Notes in Computer Science, vol. 12827, pp. 247–277. Springer (2021). https://doi.org/10.1007/978-3-030-84252-9_9, https://doi.org/10.1007/978-3-030-84252-9_9
27. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer (1993). https://doi.org/10.1007/3-540-48285-7_33, https://doi.org/10.1007/3-540-48285-7_33
28. Mouha, N., Wang, Q., Gu, D., Preneel, B.: Differential and linear cryptanalysis using mixed-integer linear programming. In: Wu, C., Yung, M., Lin, D. (eds.) Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers. Lecture Notes in Computer Science, vol. 7537, pp. 57–76. Springer (2011). https://doi.org/10.1007/978-3-642-34704-7_5, https://doi.org/10.1007/978-3-642-34704-7_5
29. Peng, T., Zhang, W., Weng, J., Ding, T.: New approaches for estimating the bias of differential-linear distinguishers. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 14923, pp. 174–205. Springer (2024). https://doi.org/10.1007/978-3-031-68385-5_6, https://doi.org/10.1007/978-3-031-68385-5_6
30. Serre, J.P.: Linear Representations of Finite Groups, Graduate Texts in Mathematics, vol. 42. Springer-Verlag, New York, 1st edn. (1977). https://doi.org/10.1007/978-1-4684-9458-7, translated from the French original by Leonard L. Scott
31. Steinberg, B.: Representation Theory of Finite Monoids. Universitext, Springer International Publishing, Cham, Switzerland, 1st edn. (2016). https://doi.org/10.1007/978-3-319-43932-3
32. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I. Lecture Notes in Computer Science, vol. 8873, pp. 158–178. Springer (2014). https://doi.org/10.1007/978-3-662-45611-8_9, https://doi.org/10.1007/978-3-662-45611-8_9
33. Tiessen, T.: Polytopic Cryptanalysis. In: Fischlin, M., Coron, J. (eds.) Advances in Cryptology - EUROCRYPT 2016. LNCS, vol. 9665, pp. 214–239. Springer (2016). https://doi.org/10.1007/978-3-662-49890-3_9, https://doi.org/10.1007/978-3-662-49890-3_9
34. Todo, Y.: Structural evaluation by generalized integral property. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Crypto-

graphic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9056, pp. 287–314. Springer (2015). https://doi.org/10.1007/978-3-662-46800-5_12, https://doi.org/10.1007/978-3-662-46800-5_12

35. Todo, Y., Morii, M.: Bit-based division property and application to simon family. In: Peyrin, T. (ed.) Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9783, pp. 357–377. Springer (2016). https://doi.org/10.1007/978-3-662-52993-5_18, https://doi.org/10.1007/978-3-662-52993-5_18
36. Wagner, D.A.: The boomerang attack. In: Knudsen, L.R. (ed.) Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings. Lecture Notes in Computer Science, vol. 1636, pp. 156–170. Springer (1999). https://doi.org/10.1007/3-540-48519-8_12, https://doi.org/10.1007/3-540-48519-8_12
37. Wang, L., Song, L., Wu, B., Rahman, M., Isobe, T.: Revisiting the boomerang attack from a perspective of 3-differential. IEEE Trans. Inf. Theory **70**(7), 5343–5357 (2024). https://doi.org/10.1109/TIT.2023.3324738, https://doi.org/10.1109/TIT.2023.3324738
38. Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.: The simeck family of lightweight block ciphers. In: Güneysu, T., Handschuh, H. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings. Lecture Notes in Computer Science, vol. 9293, pp. 307–329. Springer (2015). https://doi.org/10.1007/978-3-662-48324-4_16, https://doi.org/10.1007/978-3-662-48324-4_16

Appendix

A Specifications of SKINNY-64, PRESENT and SIMECK

A.1 Specifications of PRESENT

PRESENT is a 64-bit block cipher supporting 80-bit and 128-bit keys designed by Bogdanov *et al.* in 2007 [12]. The design is a SPN construction consisting of a round key addition, a 4-bit Sbox layer, and a bit permutation layer. The S-box is specified as follows:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S[x]	c	5	6	b	9	0	a	d	3	e	f	8	4	7	1	2

The bit permutation and the entire round function are both illustrated in Figure 3.

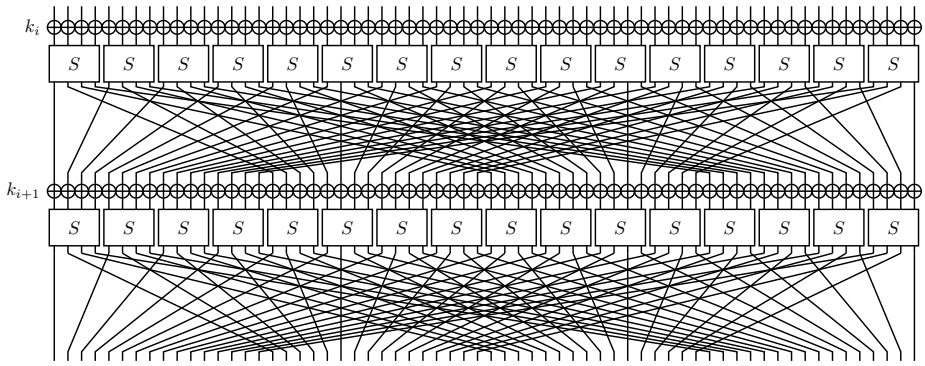

Fig. 3: Round function of PRESENT. The figure is taken from [21].

A.2 Specifications of SKINNY-64

The block cipher family SKINNY was presented at CRYPTO 2016 [3] designed under the TWEAKEY framework [22], whose goal is to compete with the NSA design SIMON [2] in terms of hardware/software performance. According to the length of block and tweakey, the SKINNY family consists of 6 different members represented as SKINNY-n-t, where $n \in \{64, 128\}$ and $t \in \{n, 2n, 3n\}$, which respectively represent the sizes of block and tweakey. Here we introduce the 64-bit version of SKINNY, *i.e.*, SKINNY-64, under the single tweakey model. SKINNY-64 is chosen as its Sbox is 4-bit. Since the multiple-of-n property is described as a 2nd order attack, it is equivalent to describe the propagation for an 8-bit Sbox ciphers in the classical automatic search.

The round function of SKINNY-64 comprises five operations as SubCells (SC), AddConstants (AC), AddRoundTweakey (ART), ShiftRows (SR) and MixColumns (MC), see Figure 4. So a round of SKINNY-64 can be written as

$$R = \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{ART} \circ \mathsf{AC} \circ \mathsf{SC}.$$

1. SC: SC is the only non-linear layer of SKINNY-64, using a 4-bit Sbox S as follows,

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S[x]	c	6	9	0	1	a	2	b	3	8	5	d	4	e	7	f

2. AC and ART: In the AC operation, a 6-bit round-based constant is XORed with the top two cells of the first column, and a constant 2 is XORed with the third cell of the first column. In the ART operation, a 8-cell round key is XORed with the first two rows of the state.
3. SR: SR circularly shifts the i-th row of the internal state to right with i nibbles, where $i = 0, 1, 2, 3$.
4. MC: MC multiplies four nibbles of each state column with the binary matrix M. The details of M are listed below,

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Since the non-zero elements in this matrix are only 1, the MC operation can be decomposed into 4 parallel small operations called Lbox, denoted by LBox. Let the input and output of M is x and y, $(y_i, y_{i+4}, y_{i+8}, y_{i+12} = \mathsf{L}(x_i, x_{i+4}, x_{i+8}, x_{i+12}) = (x_0 \oplus x_2 \oplus x_3, x_0, x_1 \oplus x_2, x_0 \oplus x_2)$, for $i \in \{0, 1, 2, 3\}$.

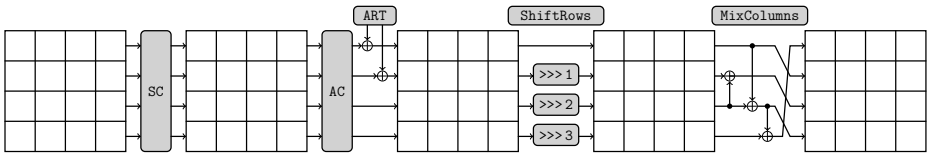

Fig. 4: Round function of SKINNY-64. The figure is taken from [21].

A.3 Specifications of SIMECK

SIMECK is a family of lightweight block ciphers proposed at CHES 2015 [38]. The design is similar to SIMON. The SIMECK family consists of several family members SIMECK-$2n/4n$ operating on n-bit words with a state size of $2n$ bits and a key

size of $4n$ bits for $n \in \{16, 24, 32\}$. In round i, the $2n$-bit input state of round i is split into two n-bit words (L_i, R_i) and updated with a Feistel-based round function F to produce (L_{i+1}, R_{i+1}) using the n-bit round key K_i. The round function is a quadratic Feistel function using bitwise XOR $(x \oplus y)$, bitwise AND $x \wedge y$, and cyclic left-shifts by c bits $(x \lll c)$ (see Figure 5):

$$R_{i+1} = L_i$$
$$L_{i+1} = R_i \oplus K_i \oplus (L_i \wedge (L_i \lll 5)) \oplus (L_i \lll 1).$$

The round key K_i is produced using a similar nonlinear update function. The total number of rounds is 32 rounds for SIMECK 32/64 (referred to as SIMECK-32 for short), 36 rounds for SIMECK 48/96 (referred to as SIMECK-48).

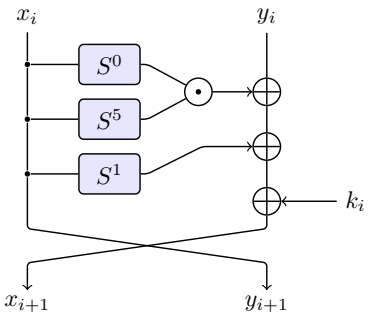

Fig. 5: Round function of SIMECK. The figure is adapted from [21].

B High-Level Viewpoint of Automatic Search for Geometric Approach

In the past decade, automatic search methods have been very popular in cryptanalysis and many classical attack techniques have been modeled. The idea is to express a cryptanalytic problem into a constrained problem, such as Mixed Integer Linear Programming (MILP) or the Satisfiability Problem (SAT), then use off-the-shelf solvers to complete the search. The results are then translated into solutions for the original cryptanalytic problem.

In the case of the geometric approach, the transition matrix is naturally suitable to be modeled in such frameworks.

First, the cipher is divided into many small components, such as Sboxes, bit permutations, and even XORs, ANDs, or COPYs (aka. Branches, where a bit is copied into 2 or multiple bits). Then, each component can be viewed as a "function" (the COPY function is also viewed as a function with one input and two outputs), the correlation expression derived after choosing two bases for the input and output is then applied to the function. For a function $\mathcal{F} : \mathbb{F}_2^n \longrightarrow$

$\mathbb{F}_2^m$ (note that n and m are usually small as they are the components of the target cipher), we traverse all input and output values. For the d-th-order attack, the input and output vectors should be $u_0||u_1||\dots||u_{d-1}$ and $v_0||v_1||\dots||v_{d-1}$, respectively. Then, according to the statistic, a value related to the input/output vectors, denoted by c, is obtained. Values $c \neq 0$ are then made into an entry:

$$(u_0, u_1, \cdots, u_{d-1}, v_0, v_1, \cdots, v_{d-1}, M(c)),$$

where $M(c)$ represents the values after applying some measures to c (usually forcing it to a positive integer number). For example, if one targets a probability, then $M(c)$ is usually $-\log(c)$. While for the divisibility property, $M(c) = -\log(|c|_2)$ where $|c|_2$ is the 2-adic absolute value of c. Usually, such an entry will be edited as bit strings.

All these entries with $c \neq 0$ will be called *valid propagations*. We generate corresponding variables for the input and output of $\mathcal{F}$, then we can use a set of inequalities, CNF constraints, or other methods to make sure that these variables have to be one of these valid propagations.

Finally, we define an objective function that usually sums up all variables from $M(c)$, and we use a solver to search for one trail that makes the summation maximum or minimum. Sometimes, one can also want to search for all valid trails.

We recommend that readers refer to previous research on the geometric approach, such as [7] and [5], for a deeper understanding of how automation is applied in this field.

C Automatic Search for the Simplified Ultrametric Integral Crytanalysis

We replay here the ultrametric integral attack, but in the simplified way described in Section 4. Setting $u =$ `fffffffffffffffe`, we obtain the same results for 9 rounds of `PRESENT` as for [5]. We divide the 9-round `PRESENT` without the last bit permutation into 3 parts: $\mathcal{E}_0$ covers the first 4 rounds, $\mathcal{E}_1$ covers the Sbox layer of the 5th round, and $\mathcal{E}_2$ covers the remaining 4 rounds. The transition matrices of the Sboxes of $\mathcal{E}_0$, $\mathcal{E}_1$ and $\mathcal{E}_2$ can be computed according to Equations (10), (12) and (11). The transition matrix of $\mathcal{E}_2$ is the same as the one in [5], but we still provide it here for a better comparison among the three matrices of the `PRESENT` Sbox.

Now let us consider the propagation. For the Sbox layer, we first construct the transition matrices for a single Sbox, which is not difficult since the correlation expressions of the three matrices we constructed earlier already exist. Based on the transition matrix of a single Sbox, the propagation rules of the Sbox layer can be conveniently characterized: `PRESENT`'s Sbox layer consists of 16 Sboxes, we have $A_{v,u}^{S_0||\cdots||S_{15}} = \prod_{i=0}^{15} A_{v_i,u_i}^{S_i}$, where $A^{S_0||\cdots||S_{15}}$ is the transition matrix of the Sbox layer and A^{S_i} is the transition matrix of the i-th Sbox.

For the bit permutation layer P, one can easily obtain that for all the three matrices, $M_{v,u} \neq 0$ if and only if $v = P(u)$. For the round key layer $K(x) = x \oplus k$, we can regard it as 64 parallel 2-input-1-output functions, so we have

$$A^K = \bigotimes_{i=0}^{63} A^{K_i} = \bigotimes_{i=0}^{63} \begin{bmatrix} (-1)^{k_i} & 0 \\ k_i & 1 \end{bmatrix} \text{(for } \mathcal{E}_0\text{)}, A^K = \bigotimes_{i=0}^{63} A^{K_i} = \bigotimes_{i=0}^{63} \begin{bmatrix} 1 & 0 \\ k_i & (-1)^{k_i} \end{bmatrix} \text{(for } \mathcal{E}_2\text{)},$$

Our goal is to obtain the 2-adic value of $A^{\mathcal{E}}_{v,u} = \sum_{y \preceq u} \mathcal{E}^v(y)$. Because of the triangle inequality of 2-adic value, we have

$$\left|A^{\mathcal{E}}_{u_r,u_0}\right|_2 \leq \max_{u_{r-1},u_{r-2},\ldots,u_2} \left|\prod_{i=0}^{r-1} A^{\mathcal{E}^i}_{u_{i+1},u_i}\right|_2.$$

Therefore, we only need to utilize an automated search tool to find the path that maximizes the 2-adic value of $\prod_{i=0}^{r-1} A^{\mathcal{E}^i}_{u_{i+1},u_i}$ according to the propagation rules mentioned above. Table 5 presents the search results for 9-round `PRESENT`.

Table 5: Divisibility property for the integral distinguisher on 9-round `PRESENT` searched by our simplified method, with input set $\{x : x \preceq \texttt{fffffffffffffffe}\}$. The number of times the i-th output bit equals one is divisible by 2^{b_i}. These results are completely the same as [5].

bit i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
theoretical b_i	2	1	1	1	2	0	0	0	2	0	0	0	2	0	0	0
	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
	1	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0
	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	1	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0
	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
	1	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0

D Obtain Blondeau-Leander-Nyberg Formula from Geometric Approach

Given Equation (21), and taking $\mathcal{E}_1 \circ \mathcal{E}_0$ as a whole part, we get

$$\varepsilon[\delta \xrightarrow{\mathcal{E}} \lambda] = A^{\mathcal{E}}_{(0,\lambda),(0,\delta)} = \sum_{(\gamma_0,\gamma_1)} A^{\mathcal{E}_2}_{(0,\lambda),(\gamma_0,\gamma_1)} A^{\mathcal{E}_1 \circ \mathcal{E}_0}_{(\gamma_0,\gamma_1),(0,\delta)},$$

we can set $\gamma_0 = 0$ to force $\mathcal{E}_1 \circ \mathcal{E}_0$ and $\mathcal{E}_2$ to be independent. Indeed, $A^{\mathcal{E}_1 \circ \mathcal{E}_0}_{(\gamma_0=0,\gamma_1),(0,\delta)}$ represents the correlation of a DL approximation of $\mathcal{E}_1 \circ \mathcal{E}_0$ with the input difference δ and the output mask γ_1. The independence of $\mathcal{E}_1 \circ \mathcal{E}_0$ and $\mathcal{E}_2$ is equivalent to say that the intermediate values at the connection point can be any values, which is equivalent to $\gamma_0 = 0$.

Note that

$$
\begin{aligned}
A^{\mathcal{E}_2}_{(0,\lambda),(0,\gamma_1)} &= 2^{-2n} \sum_{x\in\mathbb{F}_2^n, \Delta\in\mathbb{F}_2^n} (-1)^{\gamma_1^\top \Delta \oplus \lambda^\top \mathcal{D}_\Delta \mathcal{E}(x)} \\
&= 2^{-2n} \sum_{x\in\mathbb{F}_2^n, x\oplus\Delta\in\mathbb{F}_2^n} (-1)^{\gamma_1^\top x \oplus \gamma_1^\top (x\oplus\Delta) \oplus \lambda^\top \mathcal{E}(x) \oplus \lambda^\top \mathcal{E}(x\oplus\Delta)} \\
&= \left(2^{-n} \sum_{x\in\mathbb{F}_2^n} (-1)^{\gamma_1^\top x \oplus \lambda^\top \mathcal{E}(x)}\right) \left(2^{-n} \sum_{x\oplus\Delta\in\mathbb{F}_2^n} (-1)^{\gamma_1^\top (x\oplus\Delta) \oplus \mathcal{E}(x\oplus\Delta))}\right) \\
&= c^2[\gamma_1 \xrightarrow{\mathcal{E}_2} \lambda].
\end{aligned}
$$

Thus, Equation (21) becomes to

$$
\begin{aligned}
\varepsilon[\delta \xrightarrow{\mathcal{E}} \lambda] = A^{\mathcal{E}}_{(0,\lambda),(0,\delta)} &= \sum_{(0,\gamma_1)} A^{\mathcal{E}_2}_{(0,\lambda),(0,\gamma_1)} A^{\mathcal{E}_1\circ\mathcal{E}_0}_{(0,\gamma_1),(0,\delta)} = \sum_{0||\gamma_1} A^{\mathcal{E}_2}_{(0,\lambda),(0,\gamma_1)} A^{\mathcal{E}_1\circ\mathcal{E}_0}_{(0,\gamma_1),(0,\delta)} \\
&= \sum_{\gamma_1} \varepsilon[\delta \xrightarrow{\mathcal{E}_1\circ\mathcal{E}_0} \gamma_1] A^{\mathcal{E}_2}_{(0,\lambda),(0,\gamma_1)} = \sum_{\gamma_1} \varepsilon[\delta \xrightarrow{\mathcal{E}_1\circ\mathcal{E}_0} \gamma_1] c^2[\gamma_1 \xrightarrow{\mathcal{E}_2} \lambda]
\end{aligned}
$$

which is exactly Equation (19).

Table 6: First-order attacks (first part)

Output/Input	$[\delta_u(v)]_{v,u}$	$[(-1)^{u^\top v}]_{v,u}$	$[2^{-n}(-1)^{u^\top v}]_{v,u}$	$[u^v]_{v,u}$
$[\delta_u(v)]_{v,u}$	$\sum_{x=u,\mathcal{E}(x)=v} 1$	$\sum_{\substack{x\in\mathbb{F}_2^n \\ \mathcal{E}(x)=v}} (-1)^{u^\top x}$	$2^{-n}\sum_{\substack{x\in\mathbb{F}_2^n \\ \mathcal{E}(x)=v}} (-1)^{u^\top x}$	$\sum_{\substack{x\preceq u \\ \mathcal{E}(x)=v}} 1$
$[(-1)^{u^\top v}]_{v,u}$	$2^{-n}\sum_{x=u}(-1)^{v^\top \mathcal{E}(x)}$	$2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x\oplus v^\top \mathcal{E}(x)}$	$2^{-2n}\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x\oplus v^\top \mathcal{E}(x)}$	$2^{-n}\sum_{x\preceq u}(-1)^{v^\top \mathcal{E}(x)}$
$[2^{-n}(-1)^{u^\top v}]_{v,u}$	$\sum_{x=u}(-1)^{v^\top \mathcal{E}(x)}$	$\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x\oplus v^\top \mathcal{E}(x)}$	$2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x\oplus v^\top \mathcal{E}(x)}$	$\sum_{x\preceq u}(-1)^{v^\top \mathcal{E}(x)}$
$[u^v]_{v,u}$	$\sum_{x=u}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}\mathcal{E}^v(x)$	$\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}\mathcal{E}^v(x)$	$2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}\mathcal{E}^v(x)$	$\sum_{x\preceq u}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}\mathcal{E}^v(x)$
$[(-1)^{\mathsf{wt}(u\oplus v)}u^v]_{v,u}$	$\sum_{x=u}\mathcal{E}^v(x)$	$\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x}\mathcal{E}^v(x)$	$2^{-n}\sum_{x\in\mathbb{F}_2^n}\mathcal{E}^v(x)$	$\sum_{x\preceq u}\mathcal{E}^v(x)$
$[v^u]_{v,u}$	$\sum_{x=u}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}v^{\mathcal{E}(x)}$	$\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}v^{\mathcal{E}(x)}$	$2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}v^{\mathcal{E}(x)}$	$\sum_{x\preceq u}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}v^{\mathcal{E}(x)}$
$[(-1)^{\mathsf{wt}(u\oplus v)}v^u]_{v,u}$	$\sum_{x=u}v^{\mathcal{E}(x)}$	$\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x}v^{\mathcal{E}(x)}$	$2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{u^\top x}v^{\mathcal{E}(x)}$	$\sum_{x\preceq u}v^{\mathcal{E}(x)}$

Table 7: First-order attacks (second part)

Output/Input	$[(-1)^{\mathsf{wt}(u\oplus v)}u^v]_{v,u}$	$[v^u]_{v,u}$	$[(-1)^{\mathsf{wt}(u\oplus v)}v^u]_{v,u}$
$[\delta_u(v)]_{v,u}$	$\sum_{\substack{x\preceq u\\ \mathcal{E}(x)=v}}(-1)^{\mathsf{wt}(u\oplus x)}$	$\sum_{\substack{x\succeq u\\ \mathcal{E}(x)=v}}1$	$\sum_{\substack{x\succeq u\\ \mathcal{E}(x)=v}}(-1)^{\mathsf{wt}(u\oplus x)}$
$[(-1)^{u^\top v}]_{v,u}$	$2^{-n}\sum_{x\preceq u}(-1)^{\mathsf{wt}(u\oplus x)}(-1)^{v^\top\mathcal{E}(x)}$	$2^{-n}\sum_{x\preceq u}(-1)^{v^\top\mathcal{E}(x)}$	$2^{-n}\sum_{x\succeq u}(-1)^{\mathsf{wt}(u\oplus x)}(-1)^{v^\top\mathcal{E}(x)}$
$[2^{-n}(-1)^{u^\top v}]_{v,u}$	$\sum_{x\preceq u}(-1)^{\mathsf{wt}(u\oplus x)}(-1)^{v^\top\mathcal{E}(x)}$	$\sum_{x\succeq u}(-1)^{v^\top\mathcal{E}(x)}$	$\sum_{x\succeq u}(-1)^{\mathsf{wt}(u\oplus x)}(-1)^{v^\top\mathcal{E}(x)}$
$[u^v]_{v,u}$	$\sum_{x\preceq u}(-1)^{\mathsf{wt}(u\oplus x)}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}\mathcal{E}^v(x)$	$\sum_{x\succeq u}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}\mathcal{E}^v(x)$	$\sum_{x\succeq u}(-1)^{\mathsf{wt}(u\oplus x)}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}\mathcal{E}^v(x)$
$[(-1)^{\mathsf{wt}(u\oplus v)}u^v]_{v,u}$	$\sum_{x\preceq u}(-1)^{\mathsf{wt}(u\oplus x)}\mathcal{E}^v(x)$	$\sum_{x\succeq u}\mathcal{E}^v(x)$	$\sum_{x\succeq u}(-1)^{\mathsf{wt}(u\oplus x)}\mathcal{E}^v(x)$
$[v^u]_{v,u}$	$\sum_{x\preceq u}(-1)^{\mathsf{wt}(u\oplus x)}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}v^{\mathcal{E}(x)}$	$\sum_{x\succeq u}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}v^{\mathcal{E}(x)}$	$\sum_{x\succeq u}(-1)^{\mathsf{wt}(u\oplus x)}(-1)^{\mathsf{wt}(v\oplus\mathcal{E}(x))}v^{\mathcal{E}(x)}$
$[(-1)^{\mathsf{wt}(u\oplus v)}v^u]_{v,u}$	$\sum_{x\preceq u}(-1)^{\mathsf{wt}(u\oplus x)}v^{\mathcal{E}(x)}$	$\sum_{x\succeq u}v^{\mathcal{E}(x)}$	$\sum_{x\succeq u}(-1)^{\mathsf{wt}(u\oplus x)}v^{\mathcal{E}(x)}$

Table 8: 49 Bases for the second-order attacks and their effects(first part)

Index	**Basis**	**Effect of input** $\alpha_u(x)$	**Effect of output** $\beta^{\star}_{\mathcal{E}(x)}(v)$
0	$[\delta_{u_0}(v_0)]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}$	$\delta_{u_0}(x)\delta_{u_1}(\Delta)$	$\delta_{v_0}(\mathcal{E}(x))\delta_{v_1}(\mathcal{D}_\Delta\mathcal{E}(x))$
1	$[\delta_{u_0}(v_0)]_{v_0,u_0} \otimes [2^{-n}(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$\delta_{u_0}(x)2^{-n}(-1)^{u_1^\top \Delta}$	$\delta_{v_0}(\mathcal{E}(x))(-1)^{v_1^\top \mathcal{D}_\Delta\mathcal{E}(x)}$
2	$[\delta_{u_0}(v_0)]_{v_0,u_0} \otimes [(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$\delta_{u_0}(x)(-1)^{u_1^\top \Delta}$	$\delta_{v_0}(\mathcal{E}(x))2^{-n}(-1)^{v_1^\top \mathcal{D}_\Delta\mathcal{E}(x)}$
3	$[\delta_{u_0}(v_0)]_{v_0,u_0} \otimes [{u_1}^{v_1}]_{v_1,u_1}$	$\delta_{u_0}(x){u_1}^{\Delta}$	$\delta_{v_0}(\mathcal{E}(x))(-1)^{\mathrm{wt}(v_1\oplus\mathcal{D}_\Delta\mathcal{E}(x))}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
4	$[\delta_{u_0}(v_0)]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1\oplus v_1)}{u_1}^{v_1}]_{v_1,u_1}$	$\delta_{u_0}(x)(-1)^{\mathrm{wt}(u_1\oplus\Delta)}{u_1}^{\Delta}$	$\delta_{v_0}(\mathcal{E}(x))(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
5	$[\delta_{u_0}(v_0)]_{v_0,u_0} \otimes [{v_1}^{u_1}]_{v_1,u_1}$	$\delta_{u_0}(x)\Delta^{u_1}$	$\delta_{v_0}(\mathcal{E}(x))(-1)^{\mathrm{wt}(v_1\oplus\mathcal{D}_\Delta\mathcal{E}(x))}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
6	$[\delta_{u_0}(v_0)]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1\oplus v_1)}{v_1}^{u_1}]_{v_1,u_1}$	$\delta_{u_0}(x)(-1)^{\mathrm{wt}(u_1\oplus\Delta)}\Delta^{u_1}$	$\delta_{v_0}(\mathcal{E}(x)){v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
7	$[2^{-n}(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}$	$2^{-n}(-1)^{u_0^\top x}\delta_{u_1}(\Delta)$	$(-1)^{v_0^\top \mathcal{E}(x)}\delta_{v_1}(\mathcal{D}_\Delta\mathcal{E}(x))$
8	$[2^{-n}(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [2^{-n}(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$2^{-n}(-1)^{u_0^\top x}2^{-n}(-1)^{u_1^\top \Delta}$	$(-1)^{v_0^\top \mathcal{E}(x)}(-1)^{v_1^\top \mathcal{D}_\Delta\mathcal{E}(x)}$
9	$[2^{-n}(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$2^{-n}(-1)^{u_0^\top x}(-1)^{u_1^\top \Delta}$	$(-1)^{v_0^\top \mathcal{E}(x)}2^{-n}(-1)^{v_1^\top \mathcal{D}_\Delta\mathcal{E}(x)}$
10	$[2^{-n}(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [{u_1}^{v_1}]_{v_1,u_1}$	$2^{-n}(-1)^{u_0^\top x}{u_1}^{\Delta}$	$(-1)^{v_0^\top \mathcal{E}(x)}(-1)^{\mathrm{wt}(v_1\oplus\mathcal{D}_\Delta\mathcal{E}(x))}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
11	$[2^{-n}(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1\oplus v_1)}{u_1}^{v_1}]_{v_1,u_1}$	$2^{-n}(-1)^{u_0^\top x}(-1)^{\mathrm{wt}(u_1\oplus\Delta)}{u_1}^{\Delta}$	$(-1)^{v_0^\top \mathcal{E}(x)}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
12	$[2^{-n}(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [{v_1}^{u_1}]_{v_1,u_1}$	$2^{-n}(-1)^{u_0^\top x}\Delta^{u_1}$	$(-1)^{v_0^\top \mathcal{E}(x)}(-1)^{\mathrm{wt}(v_1\oplus\mathcal{D}_\Delta\mathcal{E}(x))}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
13	$[2^{-n}(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1\oplus v_1)}{v_1}^{u_1}]_{v_1,u_1}$	$2^{-n}(-1)^{u_0^\top x}(-1)^{\mathrm{wt}(u_1\oplus\Delta)}\Delta^{u_1}$	$(-1)^{v_0^\top \mathcal{E}(x)}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
14	$[(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}$	$(-1)^{u_0^\top x}\delta_{u_1}(\Delta)$	$2^{-n}(-1)^{v_0^\top \mathcal{E}(x)}\delta_{v_1}(\mathcal{D}_\Delta\mathcal{E}(x))$
15	$[(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [2^{-n}(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$(-1)^{u_0^\top x}2^{-n}(-1)^{u_1^\top \Delta}$	$2^{-n}(-1)^{v_0^\top \mathcal{E}(x)}(-1)^{v_1^\top \mathcal{D}_\Delta\mathcal{E}(x)}$
16	$[(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$(-1)^{u_0^\top x}(-1)^{u_1^\top \Delta}$	$2^{-n}(-1)^{v_0^\top \mathcal{E}(x)}2^{-n}(-1)^{v_1^\top \mathcal{D}_\Delta\mathcal{E}(x)}$
17	$[(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [{u_1}^{v_1}]_{v_1,u_1}$	$(-1)^{u_0^\top x}{u_1}^{\Delta}$	$2^{-n}(-1)^{v_0^\top \mathcal{E}(x)}(-1)^{\mathrm{wt}(v_1\oplus\mathcal{D}_\Delta\mathcal{E}(x))}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
18	$[(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1\oplus v_1)}{u_1}^{v_1}]_{v_1,u_1}$	$(-1)^{u_0^\top x}(-1)^{\mathrm{wt}(u_1\oplus\Delta)}{u_1}^{\Delta}$	$2^{-n}(-1)^{v_0^\top \mathcal{E}(x)}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
19	$[(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [{v_1}^{u_1}]_{v_1,u_1}$	$(-1)^{u_0^\top x}\Delta^{u_1}$	$2^{-n}(-1)^{v_0^\top \mathcal{E}(x)}(-1)^{\mathrm{wt}(v_1\oplus\mathcal{D}_\Delta\mathcal{E}(x))}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
20	$[(-1)^{{u_0}^\top v_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1\oplus v_1)}{v_1}^{u_1}]_{v_1,u_1}$	$(-1)^{u_0^\top x}(-1)^{\mathrm{wt}(u_1\oplus\Delta)}\Delta^{u_1}$	$2^{-n}(-1)^{v_0^\top \mathcal{E}(x)}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
21	$[{u_0}^{v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}$	${u_0}^{x}\delta_{u_1}(\Delta)$	$(-1)^{\mathrm{wt}(v_0\oplus\mathcal{E}(x))}\mathcal{E}^{v_0}(x)\delta_{v_1}(\mathcal{D}_\Delta\mathcal{E}(x))$
22	$[{u_0}^{v_0}]_{v_0,u_0} \otimes [2^{-n}(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	${u_0}^{x}2^{-n}(-1)^{u_1^\top \Delta}$	$(-1)^{\mathrm{wt}(v_0\oplus\mathcal{E}(x))}\mathcal{E}^{v_0}(x)(-1)^{v_1^\top \mathcal{E}([(-1)^{\mathrm{wt}(u_0\oplus v_0)}{u_0}^{v_0}]_{v_0,u_0})}$
23	$[{u_0}^{v_0}]_{v_0,u_0} \otimes [(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	${u_0}^{x}(-1)^{u_1^\top \Delta}$	$(-1)^{\mathrm{wt}(v_0\oplus\mathcal{E}(x))}\mathcal{E}^{v_0}(x)2^{-n}(-1)^{v_1^\top \mathcal{D}_\Delta\mathcal{E}(x)}$

Table 9: 49 Bases for the second-order attacks and their effects (second part)

Index	Basis	Effect of input $\alpha_u(x)$	Effect of output $\beta^\star_{\mathcal{E}(x)}(v)$
24	$[{u_0}^{v_0}]_{v_0,u_0} \otimes [{u_1}^{v_1}]_{v_1,u_1}$	${u_0}^{x}{u_1}^{\Delta}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}\mathcal{E}^{v_0}(x)(-1)^{\mathrm{wt}(v_1 \oplus \mathcal{D}_\Delta\mathcal{E}(x))}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
25	$[{u_0}^{v_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1 \oplus v_1)}{u_1}^{v_1}]_{v_1,u_1}$	${u_0}^{x}(-1)^{\mathrm{wt}(u_1 \oplus \Delta)}{u_1}^{\Delta}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}\mathcal{E}^{v_0}(x)(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
26	$[{u_0}^{v_0}]_{v_0,u_0} \otimes [{v_1}^{u_1}]_{v_1,u_1}$	${u_0}^{x}\Delta^{u_1}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}\mathcal{E}^{v_0}(x)(-1)^{\mathrm{wt}(v_1 \oplus \mathcal{D}_\Delta\mathcal{E}(x))}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
27	$[{u_0}^{v_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1 \oplus v_1)}{v_1}^{u_1}]_{v_1,u_1}$	${u_0}^{x}(-1)^{\mathrm{wt}(u_1 \oplus \Delta)}\Delta^{u_1}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}\mathcal{E}^{v_0}(x){v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
28	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{u_0}^{v_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}{u_0}^{x}\delta_{u_1}(\Delta)$	$\mathcal{E}^{v_0}(x)\delta_{v_1}(\mathcal{D}_\Delta\mathcal{E}(x))$
29	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{u_0}^{v_0}]_{v_0,u_0} \otimes [2^{-n}(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}{u_0}^{x}2^{-n}(-1)^{{u_1}^\top\Delta}$	$\mathcal{E}^{v_0}(x)(-1)^{{v_1}^\top\mathcal{D}_\Delta\mathcal{E}(x)}$
30	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{u_0}^{v_0}]_{v_0,u_0} \otimes [(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}{u_0}^{x}(-1)^{{u_1}^\top\Delta}$	$\mathcal{E}^{v_0}(x)2^{-n}(-1)^{{v_1}^\top\mathcal{D}_\Delta\mathcal{E}(x)}$
31	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{u_0}^{v_0}]_{v_0,u_0} \otimes [{u_1}^{v_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}{u_0}^{x}{u_1}^{\Delta}$	$\mathcal{E}^{v_0}(x)(-1)^{\mathrm{wt}(v_1 \oplus \mathcal{D}_\Delta\mathcal{E}(x))}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
32	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{u_0}^{v_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1 \oplus v_1)}{u_1}^{v_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}{u_0}^{x}(-1)^{\mathrm{wt}(u_1 \oplus \Delta)}{u_1}^{\Delta}$	$\mathcal{E}^{v_0}(x)(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
33	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{u_0}^{v_0}]_{v_0,u_0} \otimes [{v_1}^{u_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}{u_0}^{x}\Delta^{u_1}$	$\mathcal{E}^{v_0}(x)(-1)^{\mathrm{wt}(v_1 \oplus \mathcal{D}_\Delta\mathcal{E}(x))}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
34	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{u_0}^{v_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1 \oplus v_1)}{v_1}^{u_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}{u_0}^{x}(-1)^{\mathrm{wt}(u_1 \oplus \Delta)}\Delta^{u_1}$	$\mathcal{E}^{v_0}(x){v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
35	$[{v_0}^{u_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}$	$x^{u_0}\delta_{u_1}(\Delta)$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}{v_0}^{\mathcal{E}(x)}\delta_{v_1}(\mathcal{D}_\Delta\mathcal{E}(x))$
36	$[{v_0}^{u_0}]_{v_0,u_0} \otimes [2^{-n}(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$x^{u_0}2^{-n}(-1)^{{u_1}^\top\Delta}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}{v_0}^{\mathcal{E}(x)}(-1)^{{v_1}^\top\mathcal{D}_\Delta\mathcal{E}(x)}$
37	$[{v_0}^{u_0}]_{v_0,u_0} \otimes [(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$x^{u_0}(-1)^{{u_1}^\top\Delta}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}{v_0}^{\mathcal{E}(x)}2^{-n}(-1)^{{v_1}^\top\mathcal{D}_\Delta\mathcal{E}(x)}$
38	$[{v_0}^{u_0}]_{v_0,u_0} \otimes [{u_1}^{v_1}]_{v_1,u_1}$	$x^{u_0}{u_1}^{\Delta}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}{v_0}^{\mathcal{E}(x)}(-1)^{\mathrm{wt}(v_1 \oplus \mathcal{D}_\Delta\mathcal{E}(x))}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
39	$[{v_0}^{u_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1 \oplus v_1)}{u_1}^{v_1}]_{v_1,u_1}$	$x^{u_0}(-1)^{\mathrm{wt}(u_1 \oplus \Delta)}{u_1}^{\Delta}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}{v_0}^{\mathcal{E}(x)}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
40	$[{v_0}^{u_0}]_{v_0,u_0} \otimes [{v_1}^{u_1}]_{v_1,u_1}$	$x^{u_0}\Delta^{u_1}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}{v_0}^{\mathcal{E}(x)}(-1)^{\mathrm{wt}(v_1 \oplus \mathcal{D}_\Delta\mathcal{E}(x))}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
41	$[{v_0}^{u_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1 \oplus v_1)}{v_1}^{u_1}]_{v_1,u_1}$	$x^{u_0}(-1)^{\mathrm{wt}(u_1 \oplus \Delta)}\Delta^{u_1}$	$(-1)^{\mathrm{wt}(v_0 \oplus \mathcal{E}(x))}{v_0}^{\mathcal{E}(x)}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
42	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{v_0}^{u_0}]_{v_0,u_0} \otimes [\delta_{u_1}(v_1)]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}x^{u_0}\delta_{u_1}(\Delta)$	${v_0}^{\mathcal{E}(x)}\delta_{v_1}(\mathcal{D}_\Delta\mathcal{E}(x))$
43	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{v_0}^{u_0}]_{v_0,u_0} \otimes [2^{-n}(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}x^{u_0}2^{-n}(-1)^{{u_1}^\top\Delta}$	${v_0}^{\mathcal{E}(x)}(-1)^{{v_1}^\top\mathcal{D}_\Delta\mathcal{E}(x)}$
44	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{v_0}^{u_0}]_{v_0,u_0} \otimes [(-1)^{{u_1}^\top v_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}x^{u_0}(-1)^{{u_1}^\top\Delta}$	${v_0}^{\mathcal{E}(x)}2^{-n}(-1)^{{v_1}^\top\mathcal{D}_\Delta\mathcal{E}(x)}$
45	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{v_0}^{u_0}]_{v_0,u_0} \otimes [{u_1}^{v_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}x^{u_0}{u_1}^{\Delta}$	${v_0}^{\mathcal{E}(x)}(-1)^{\mathrm{wt}(v_1 \oplus \mathcal{D}_\Delta\mathcal{E}(x))}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
46	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{v_0}^{u_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1 \oplus v_1)}{u_1}^{v_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}x^{u_0}(-1)^{\mathrm{wt}(u_1 \oplus \Delta)}{u_1}^{\Delta}$	${v_0}^{\mathcal{E}(x)}(\mathcal{D}_\Delta\mathcal{E}(x))^{v_1}$
47	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{v_0}^{u_0}]_{v_0,u_0} \otimes [{v_1}^{u_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}x^{u_0}\Delta^{u_1}$	${v_0}^{\mathcal{E}(x)}(-1)^{\mathrm{wt}(v_1 \oplus \mathcal{D}_\Delta\mathcal{E}(x))}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$
48	$[(-1)^{\mathrm{wt}(u_0 \oplus v_0)}{v_0}^{u_0}]_{v_0,u_0} \otimes [(-1)^{\mathrm{wt}(u_1 \oplus v_1)}{v_1}^{u_1}]_{v_1,u_1}$	$(-1)^{\mathrm{wt}(u_0 \oplus x)}x^{u_0}(-1)^{\mathrm{wt}(u_1 \oplus \Delta)}\Delta^{u_1}$	${v_0}^{\mathcal{E}(x)}{v_1}^{\mathcal{D}_\Delta\mathcal{E}(x)}$