Revisiting Integral Distinguishers using Subspace Trails and Generalized Derivatives

Noureddine El-Asri, Kirpa Garg, and Valentin Suder

University of Rouen Normandy – LITIS UR 4108
Avenue de l'Université 76800 Saint-Étienne-du-Rouvray - France
{noureddine.el-asri1,kirpa.garg,valentin.suder}@univ-rouen.fr

Abstract. A framework for mounting integral attacks against block ciphers is discussed, using the propagation of subspaces and generalized derivatives. The proposed distinguisher exhibits a lower bound on the number of rounds for which a cipher remains vulnerable to integral attacks. This work also highlights potential applications of generalized derivatives in the analysis of Arithmetization-Oriented encryption schemes over finite fields of arbitrary characteristic. To illustrate the results, applications to various AES-like Substitution-Permutation Networks are provided.

Keywords: Subspace trails, subspace propagation, generalized derivatives, integral distinguishers, block ciphers, AES-like SPN ciphers

1 Introduction

Integral cryptanalysis and its variants are among the most effective techniques for analysing block ciphers. The method introduced by Knudsen and Wagner [21] exploits structured multisets of plaintexts whose components sum to zero after a certain number of rounds. Since then, integral cryptanalysis has been generalized and refined in several directions, including higher order and partial integrals [21], zero-sum distinguishers [1], and systematic frameworks such as the division property [29]. These approaches reveal how algebraic structure within the cipher induces predictable properties at the output.

Later on, a distinct cryptanalytic approach has emerged that exploits invariant subspaces of a block cipher's round function, known as the invariant subspace attack [22]. This technique was later generalized by Grassi et al. [18], who introduced subspace trails as a powerful and unifying framework for studying how subspaces propagate through block cipher constructions. Nevertheless, the notion of subspace trails has been defined inconsistently in the literature: several non-equivalent definitions [18,23,19] have been used interchangeably across different works, which may lead to ambiguity in both theoretical analysis and practical applications.

In this article, we present a framework for mounting integral attacks against block ciphers that exploits the propagation of subspaces and utilizes generalized

derivatives [27]. The distinguisher proposed in our work relies on how the algebraic degree growth behaves as a function of the number of rounds, yielding a lower bound on the number of rounds for which the cipher remains vulnerable to the proposed integral attack.

The strategy employed in our approach is an extension of the technique used by Beyne et al. [4], where the authors analyze arithmetization-oriented (AO) hash functions using invariant subspaces [22] in order to skip rounds in their attacks. Since we are focusing on encryption schemes, the notion of subspace trails, which is not affected by key addition, is more relevant than invariant subspaces, which are dependent on key addition.

We use our general methodology to analyse various AES-like Substitution-Permutation Network (SPN) ciphers, for instance AES [11], Midori-64 [2], Klein-64 [15], SKINNY-64 [3] and re-discover some previously known results. More interestingly, using our proposed integral distinguisher based on generalized derivatives, we provide a different explanation for the results obtained by Beyne and Verbauwhede [5] concerning AES-prime [25]. Especially, for some well defined keys, we obtain the same integral properties as those in [5] with less data for four, five and six rounds of AES-prime.

Tables 1 and 2 summarize some applications of the framework developed in this article. We present the best key independent zero-sum integral distinguisher for 7-round SKINNY-64, and a key dependent zero-sum integral distinguisher for reduced 5 and 6-round AES-prime. Table 3 (c.f. Section 5.2) presents an overview of the existing distinguishers on AES, together with our results.

Rounds ℓ	Algebraic Degree	Data	Reference
5	$\leq 3^5$	2^{32}	Corollary 4
6	$\leq 3^6$	2^{32}	Remark 13
7	≤ 47	2^{48}	Remark 14

Table 1. Parameters of the key independent zero-sum integral distinguisher for SKINNY-64 with the maximum number of rounds ℓ.

Rounds ℓ	Data	Number of Weak keys	Reference
1-5	p	$\geq p^{13}$	Theorem 4
6	p^4	$\geq N_I$	Example 5

Table 2. Zero-sum integral property for restricted master keys K on AES-prime with a maximum number of rounds ℓ.

This article is organised as follow. After recalling the notation and basic results in Section 2, we review existing definitions of subspace trails and analyze their relationships in Section 3, demonstrating that they are not equivalent. We then introduce a method to get an integral distinguisher based on subspace trails and higher order generalized derivatives for iterated SPN ciphers in Section 4. Finally, we illustrate our results by applying them to AES [11], Midori-64 [2], Klein-64 [15], SKINNY-64 [3] and AES-prime [25] (summarize in Table 4) in Section 5. Finally, we provide concluding remarks together with a summary and directions for future work.

2 Preliminaries

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime p called the characteristic, and $\mathbb{F}_q^*$ be the multiplicative group of non-zero elements of $\mathbb{F}_q$.

We define the algebraic degree of a function as follows (see [8, Definition 1] for $q = 2$).

Definition 1 (ANF and Algebraic Degree). *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a q-ary function. Its Algebraic Normal Form (ANF) is the unique representation of f as a multivariate polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n)$. The ANF is of maximum degree $q-1$ in each variable, so*

$$f(x_1, \ldots, x_n) = \sum_{u=(u_1,u_2,\cdots,u_n)\in[0,q-1]^n} a_u x^u,$$

where $a_u \in \mathbb{F}_q$ for all u and $x^u = \prod_{i=1}^n x_i^{u_i}$. The algebraic degree of f is

$$\deg_q(f) := \max\left\{ \sum_{i=1}^n u_i \;\middle|\; u = (u_1, u_2, \cdots, u_n) \in [0, q-1]^n,\, a_u \neq 0 \right\}.$$

For a vectorial function

$$F : \mathbb{F}_q^n \to \mathbb{F}_q^n, \quad x \mapsto (F_1(x), \ldots, F_n(x)),$$

its algebraic degree is $\deg_q(F) := \max_{1\leq i\leq n}(\deg_q(F_i))$. Here, $\deg_q(F)$ means the algebraic degree of F when seen as a function over $\mathbb{F}_q^n$.

Definition 2 (Derivative functions). *Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\alpha \in \mathbb{F}_q^n$. The derivative of F in the direction α is defined as*

$$\Delta_\alpha F(x) = F(x + \alpha) - F(x), \quad \forall x \in \mathbb{F}_q^n.$$

The derivative of order d along the directions $\alpha_i \in \mathbb{F}_q$, for $i = 1, \cdots, d$ is defined by

$$\Delta_{\alpha_1,\ldots,\alpha_d} F(x) = \Delta_{\alpha_1} \Delta_{\alpha_2,\ldots,\alpha_d} F(x).$$

We will denote $\Delta_S F(x) := \Delta_{\alpha_1,\ldots,\alpha_d} F(x)$, where $S = \{\alpha_1, \ldots, \alpha_d\}$. Note that

$$\Delta_{\alpha_1,\ldots,\alpha_d} F = \Delta_{\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(d)}} F$$

for all σ belonging to the symmetric group of order d.

Proposition 1. *With the same notation as in Definition 2,*

$$\deg_q(\Delta_S F) \leq \deg_q(F) - |S|$$

where $|S|$ denotes the cardinality of the set S.

Next, we define block ciphers, since we will consider attacks on them in the subsequent sections.

Definition 3 (Block cipher). *Let $n \geq 1$ and $\kappa \geq 1$. A block cipher $\mathcal{E}$ is a family of keyed functions $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ where for every $K \in \mathbb{F}_q^\kappa$, the function $\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a permutation of $\mathbb{F}_q^n$.*

Definition 4 (ℓ-Round Iterated Block Cipher). *Let $\ell \geq 1$. An ℓ-round iterated block cipher with a round function $\mathcal{R} : \mathbb{F}_q^\kappa \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a family of permutations*

$$\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n,$$

parameterized by a key $K \in \mathcal{K}$, constructed as a composition of ℓ round transformations from the round function $\mathcal{R}$ as follows:

Let the key K determine a sequence of round keys *$K \to (k_1, k_2, \ldots, k_\ell), k_i \in \mathbb{F}_q^\kappa$. Then the encryption of a plaintext $M \in \mathbb{F}_q^n$ into a ciphertext $C \in \mathbb{F}_q^n$ is done recursively as*

$$\begin{cases} x_0 = M, & \textit{(plaintext)}, \\ x_i = \mathcal{R}(k_i, x_{i-1}) = \mathcal{R}_{k_i}(x_{i-1}), & i = 1, 2, \ldots, \ell, \\ \mathcal{E}_K(M) = x_\ell = C, & \textit{(ciphertext)}. \end{cases}$$

Each round function $\mathcal{R}(k_i, \cdot)$ is assumed to be invertible, ensuring that the overall cipher $\mathcal{E}_K$ is invertible.

We denote by $\bar{\mathcal{E}} = \{\bar{\mathcal{E}}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ the corresponding decryption scheme with decryption round function $\bar{\mathcal{R}}$ where $\bar{\mathcal{R}}(k, \mathcal{R}(k, x)) = x$ for all $x \in \mathbb{F}_q^n$ and $k \in \mathbb{F}_q^\kappa$.

Remark 1. Equivalently, the block cipher can be written as

$$\mathcal{E}_K = \mathcal{R}_{k_\ell} \circ \mathcal{R}_{k_{\ell-1}} \circ \cdots \circ \mathcal{R}_{k_1},$$

where each $\mathcal{R}_{k_i} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ for $1 \leq i \leq \ell$ is the i-th round transformation derived from the round function $\mathcal{R}$ and subkey k_i.

Remark 2. Very commonly, $\mathcal{R}_k(x) = \mathcal{R}(x + k)$, and thus $\bar{\mathcal{R}}_k(x) = \mathcal{R}^{-1}(x) - k$.

Definition 5 (Substitution-Permutation Network (SPN)). *Let $q = p^n$ where p is a prime number and n is a positive integer. Let $S_1, \cdots, S_n$ be invertible functions over $\mathbb{F}_q$ and $\mathcal{L} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an invertible linear function. An SPN is an ℓ-round iterated block cipher with round function*

$$\begin{aligned} \mathcal{R} : \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ (x_1, \ldots, x_n) &\mapsto \mathcal{L}\left((S_1(x_1), \ldots, S_n(x_n))^T\right), \end{aligned}$$

i.e, $\mathcal{R} := \mathcal{L} \circ \mathcal{S}$ where $\mathcal{S}(x_1, \ldots, x_n) = (S_1(x_1), \ldots, S_n(x_n))$.

Integral distinguishers are powerful cryptanalytic tools that exploit structured properties of large input sets to distinguish block ciphers from random permutations. They were originally introduced in the form of the Square attack against SPN ciphers by Daemen, Knudsen, and Rijmen [9], and later formalized as integral cryptanalysis by Knudsen and Wagner [21]. We recall the definition of an integral distinguisher as follows.

Definition 6 (Integral Distinguisher). *Let $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$, where $K \in \mathbb{F}_q^\kappa$, be an ℓ-round iterated block cipher and $\mathbb{X} \subseteq \mathbb{F}_q^n$. If the sum of the ciphertexts over $\mathbb{X}$ satisfies*

$$\sum_{x \in \mathbb{X}} \mathcal{E}_K(x) = c$$

for some constant c that does not depend on the key K, then $\mathbb{X}$ is said to be an integral distinguisher for the block cipher. When $c = 0$, we call $\mathbb{X}$ a zero-sum integral distinguisher and the block cipher is said to exhibit a zero-sum property.

3 Subspace trails

While subspace trail cryptanalysis was introduced by Grassi et al. [18] over finite fields of even characteristic, the term remains inconsistently applied across the literature, with multiple definitions [23,19]. More precisely, these definitions [18,23,19] are often used interchangeably, even though they are not equivalent. For the sake of clarity, we restate these three definitions in the setting of finite fields of arbitrary characteristic p as follows. Here, the canonical inner product in $\mathbb{F}_p^n$ denoted by $\langle \cdot, \cdot \rangle$ is defined as $\langle u, v \rangle = \sum_{i=1}^n u_i v_i$ for $u, v \in \mathbb{F}_p^n$.

Definition 7 (Orthogonal Subspace Trail). *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ and $(U_0, \ldots, U_r)$ be a set of $r+1$ subspaces with $\dim(U_i) \leq \dim(U_{i+1})$. If, for each $i = 0, \ldots, r-1$ and for each $a_i \in U_i^\perp$, there exists a (unique) $a_{i+1} \in U_{i+1}^\perp$, where $U^\perp := \{ v \in \mathbb{F}_p^n \mid \langle u, v \rangle = 0$ for all $u \in U\}$ for any subspace $U \subseteq \mathbb{F}_p^n$, such that*

$$F(U_i + a_i) \subseteq U_{i+1} + a_{i+1},$$

then $(U_0, U_1, \ldots, U_r)$ is a subspace trail of length r. We denote this by

$$U_0 \xrightarrow{F} U_1 \xrightarrow{F} U_2 \xrightarrow{F} \cdots \xrightarrow{F} U_r.$$

Another definition of subspace trails was proposed by Leander et al. [23].

Definition 8 (Complete Subspace Trail). *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ and $(U_0, \ldots, U_r)$ be a set of $r+1$ subspaces with $\dim(U_i) \leq \dim(U_{i+1})$. If, for each $i = 0, \ldots, r-1$ and for each $a_i \in \mathbb{F}_p^n$, there exists a (unique) $a_{i+1} \in \mathbb{F}_p^n$ such that*

$$F(U_i + a_i) \subseteq U_{i+1} + a_{i+1},$$

then $(U_0, U_1, \ldots, U_r)$ is a subspace trail of length r, denoted by

$$U_0 \overset{F}{\rightrightarrows} U_1 \overset{F}{\rightrightarrows} U_2 \overset{F}{\rightrightarrows} \cdots \overset{F}{\rightrightarrows} U_r.$$

There is yet another formulation of subspace trails, introduced by Grassi et al.[19], where the main distinction lies in considering the complement space rather than the full space.

Definition 9 (Complement Subspace Trail). *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ and $(U_0, \ldots, U_r)$ be a set of $r+1$ subspaces with $\dim(U_i) \leq \dim(U_{i+1})$. If, for each $i = 0, \ldots, r-1$ and for each $a_i \in \mathbb{F}_p^n$, there exists a (unique) $a_{i+1} \in U_{i+1}^{\complement}$, where $U_{i+1}^{\complement} := \mathbb{F}_p^n \setminus U_{i+1}$ is the complement of U_{i+1}, such that*

$$F(U_i + a_i) \subseteq U_{i+1} + a_{i+1},$$

then $(U_0, U_1, \ldots, U_r)$ is a subspace trail of length r.

Furthermore, when all the relations in Definitions 7, 8, and 9 become equalities, the trail is said to be a constant dimensional or *exact* subspace trail with respect to that definition.

Remark 3. For a function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ and a sequence of subspaces $(U_0, U_1, \ldots, U_r)$ such that $\dim(U_i) \leq \dim(U_{i+1})$ for all $0 \leq i \leq r-1$, if additionally $U_i + U_i^{\perp} = \mathbb{F}_p^n$ for each i, and we have an orthogonal subspace trail (Definition 7)

$$U_0 \xrightarrow{F} U_1 \xrightarrow{F} U_2 \xrightarrow{F} \cdots \xrightarrow{F} U_r$$

then it is also a complete subspace trail (Definition 8), that is,

$$U_0 \overset{F}{\rightrightarrows} U_1 \overset{F}{\rightrightarrows} U_2 \overset{F}{\rightrightarrows} \cdots \overset{F}{\rightrightarrows} U_r.$$

The following example highlights how Definition 7, Definition 8 and Definition 9 differ from each other.

Example 1. Define a function $F : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ as $F(x, y) = (xy + x, xy)$. Let $U = \mathbb{F}_2 \times (1, 1) = U^{\perp}$ and $V = \mathbb{F}_2 \times (0, 1)$ be subspaces of $\mathbb{F}_2^2$. Then we have,

$$F((0,0) + U) = F(U) = \{F(0,0), F(1,1)\} = \{(0,0), (0,1)\} = V$$

and,

$$F((1,1) + U) = \{F(1,1), F(0,0)\} = \{(0,1), (0,0)\} = V.$$

Therefore for every $a \in U^{\perp}$, there exists $b \in V^{\perp}$ such that $F(a+U) = b+V$. However for $x = (1, 0) \in \mathbb{F}_{2^2} \setminus U^{\perp}$,

$$F(x + U) = F((1,0) + U) = \{F(1,0), F(0,1)\} = \{(1,0), (0,0)\}$$

is not contained in any coset of V. This implies that Definition 8 and Definition 9 do not hold here.

In the subsequent sections, as we don't want ourselves to be bothered with the key addition, we focus on Definition 8.

4 Skipping rounds using subspace trails and subspace chains.

In this section, we present the main idea of our paper, using exact subspace trails, generalized derivatives and subspace chains to explain or improve existing attacks. To be as general as possible, we work over finite fields of arbitrary characteristic p. Recently, Salagean and Ozbudak [27,28] used discrete derivatives (see definition 2) to interpret a new kind of higher order derivatives more convenient when working over arbitrary characteristic as a way to generalize almost perfect non-linear functions and differential uniformity [26]. They referred to it as generalized derivatives, defined as follows.

Definition 10 (Generalized derivative functions). *The generalized derivative of a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ in a direction $\alpha \in \mathbb{F}_{p^n}$ is defined as*

$$\nabla_\alpha F(x) := \sum_{i \in \mathbb{F}_p} F(x + i\alpha) = \Delta\underbrace{\alpha, \alpha, \ldots, \alpha}_{p-1} F(x).$$

Remark 4. ∇ behaves like a derivative, in particular, when $p = 2$, $\nabla_\alpha F = \Delta_\alpha F$.

Definition 11 (Higher order generalized derivative functions). *The higher order generalized derivative of a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ in the $\mathbb{F}_p$-linearly independent directions $\alpha_1, \alpha_2, \cdots, \alpha_m \in \mathbb{F}_{p^n}$ is defined as*

$$\nabla_S F(x) := \nabla_{\alpha_1, \ldots, \alpha_m} F(x) = \nabla_{\alpha_1} \nabla_{\alpha_2} \ldots \nabla_{\alpha_m} F(x),$$

where $S = \{\alpha_1, \ldots, \alpha_m\}$.

Proposition 2. *With the same notation as in Definition 11,*

$$\deg_p(\nabla_S F) \leq \deg_p(F) - |S| \times (p - 1).$$

The following Lemma links the notion of higher order generalized derivatives introduced in Definition 11 to the notion of integrals in Definition 6 when the set $\mathbb{X}$ is an affine subspace. The proof can be derived from the explicit expression used by Winter et al. [30] for computing higher order derivatives.

Lemma 1. *Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a function and let p be the characteristic of the finite field $\mathbb{F}_q$. Let $U = \mathbb{F}_p\alpha_1 + \cdots + \mathbb{F}_p\alpha_m$ be an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_q^n$ of dimension m. Then*

$$\forall x \in \mathbb{F}_q^n, \quad \nabla_{\alpha_1, \ldots, \alpha_m} F(x) = \sum_{u \in U} F(x + u).$$

Remark 5. Let U be a subspace of $\mathbb{F}_p^n$, and let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two $\mathbb{F}_p$-basis of U. Since the higher order generalized derivative is independent of the choice of basis, or, more precisely,

$$\nabla_{\mathcal{B}_1} F = \nabla_{\mathcal{B}_2} F,$$

for any function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$, we (by abuse of notation) write $\nabla_U F$ instead of $\nabla_{\mathcal{B}_1} F$ or $\nabla_{\mathcal{B}_2} F$.

Remark 6. Note that, from Lemma 1, computing $\nabla_U F(x)$ requires $p^{\dim_{\mathbb{F}_p}(U)}$ calls of the function F. While doing it the usual way needs $2^{\dim_{\mathbb{F}_p}(U)\times(p-1)}$ calls. This is significant because, when p is a large prime, which is usually preferable (see for instance [13]), for instance $p = 2^7 - 1$, computing it the usual way, that is as a regular higher order derivative, requires

$$2^{(p-1)\times\dim_{\mathbb{F}_p}(U)} = 2^{(2^7-2)\times\dim_{\mathbb{F}_p}(U)} = 2^{126\times\dim_{\mathbb{F}_p}(U)}$$

calls for the function F which is comparatively larger than the number of calls required using Lemma 1, that is

$$p^{\dim_{\mathbb{F}_p}(U)} = (2^7-1)^{\dim_{\mathbb{F}_p}(U)} \sim 2^{7\times\dim_{\mathbb{F}_p}(U)}.$$

The following theorem is our main observation.

Theorem 1. *Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a function such that $F = R_2 \circ R_1$ for some functions $R_1, R_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Suppose that there exists an exact complete subspace trail $U \overset{R_1}{\to} V$. Then*

$$\forall a \in \mathbb{F}_q^n,\ \exists\ b_a \in \mathbb{F}_q^n, \quad \nabla_U F(a) = \nabla_V R_2(b_a). \tag{1}$$

Proof. Let $a \in \mathbb{F}_q^n$. By Definition 8, there exists $b_a \in \mathbb{F}_q^n$ such that

$$F(a+U) = R_2 \circ R_1(a+U) = R_2(b_a + V).$$

Since, U and V are of the same dimension, we have

$$\sum_{u\in U} F(a+u) = \sum_{v\in V} R_2(b_a+v).$$

□

Figure 1 illustrates the idea of Theorem 1.

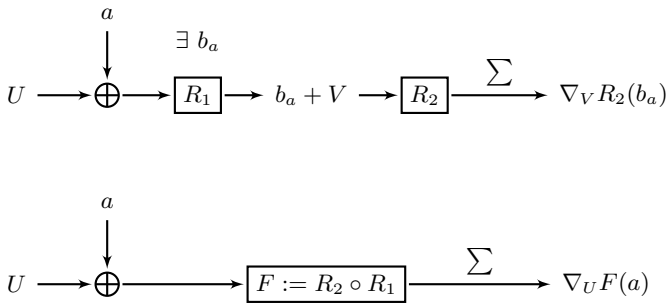

Fig. 1. Schematic idea behind Theorem 1.

Remark 7. In [4], the authors skipped rounds in order to obtain a zero-sum. Here, we use a higher order generalized derivative to obtain Equality (1).

For a function $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ written as $F(x) = \big(F^{(1)}(x), F^{(2)}(x), \ldots, F^{(n)}(x)\big)$, each function $F^{(i)} : \mathbb{F}_q^n \to \mathbb{F}_q$ is called a *coordinate function* of F. In the following result, we restate Theorem 1 in terms of the coordinate functions rather than the full vectorial function. This formulation is helpful because it can provide a distinguisher for some coordinate functions even when the properties of the complete round function are not fully known.

Corollary 1. *Let $F(F^{(1)}, F^{(2)}, \cdots, F^{(n)}) : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Suppose that $F = R_2 \circ R_1$ for some functions $R_1, R_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$, then $F(x) = (R_2^{(1)} \circ R_1(x), R_2^{(2)} \circ R_1(x), \cdots, R_2^{(n)} \circ R_1(x))$. Suppose also that there exists an exact complete subspace trail $U \overset{R_1}{\rightrightarrows} V$. Then for every $1 \leq i \leq n$, we have*

$$\forall a \in \mathbb{F}_q^n,\ \exists\ b_a \in \mathbb{F}_q^n, \quad \nabla_U F^{(i)}(a) = \nabla_V R_2^{(i)}(b_a).$$

Proof. The proof follows directly from Theorem 1. □

Theorem 1 allows us to skip the part R_1 in the sense that the sum over the subspace U of the full function $F = R_2 \circ R_1$ reduces to the sum of the last part R_2 over a subspace V having the same dimension as U. Moreover, in conjunction with Proposition 2, we have the following property on ℓ-round iterated block cipher schemes.

Theorem 2. *Let $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ be an ℓ-round iterated block cipher with round function $\mathcal{R} : \mathbb{F}_q^\kappa \times \mathbb{F}_q^n \to \mathbb{F}_q^n$. Let $K \to \{k_1, \ldots, k_\ell\} \subset \mathbb{F}_q^\kappa$ be any round keys and suppose that there exist linear subspaces $U_0, U_1, \ldots, U_m$ of $\mathbb{F}_q^n$ having the same $\mathbb{F}_p$-dimension s such that*

$$U_0 \overset{\mathcal{R}_{k_1}}{\rightrightarrows} U_1 \overset{\mathcal{R}_{k_2}}{\rightrightarrows} \cdots \overset{\mathcal{R}_{k_m}}{\rightrightarrows} U_m.$$

Then, if the algebraic degree satisfies

$$\deg_p(\mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_{m+1}}) \leq s \times (p-1) \tag{2}$$

we get

$$\sum_{u \in U_0} \mathcal{E}_K(x+u) = c_K$$

for every $x \in \mathbb{F}_q^n$ where $c_K \in \mathbb{F}_q^n$ is a key-dependent constant vector.

Proof. Let $\mathcal{E}_K = \mathcal{E}_K^{(2)} \circ \mathcal{E}_K^{(1)}$, where

$$\mathcal{E}_K^{(1)} = \mathcal{R}_{k_m} \circ \mathcal{R}_{k_{m-1}} \circ \cdots \circ \mathcal{R}_{k_1},\ \text{and},\ \mathcal{E}_K^{(2)} = \mathcal{R}_{k_\ell} \circ \mathcal{R}_{k_{\ell-1}} \circ \cdots \circ \mathcal{R}_{k_{m+1}}.$$

As $U_i \overset{\mathcal{R}_{k_i}}{\rightrightarrows} U_{i+1}$ for all $0 \leq i \leq m-1$, we have $U_0 \overset{\mathcal{E}_K^{(1)}}{\rightrightarrows} U_m$. Thus, for all $x \in \mathbb{F}_q^n$, there exists $y_x \in \mathbb{F}_q^n$ such that

$$\sum_{u \in U_0} \mathcal{E}_K(x+u) = \sum_{u \in U_m} \mathcal{E}_K^{(2)}(y_x + u) = \nabla_{\alpha_1, \cdots, \alpha_s} \mathcal{E}_K^{(2)}(y_x)$$

where $\alpha_1, \cdots, \alpha_s$ is an $\mathbb{F}_p$-basis of U_m. Since $\deg_p(\mathcal{E}_K^{(2)}) \leq s \times (p-1)$, then

$$\deg_p(\nabla_{\alpha_1,\cdots,\alpha_s}\mathcal{E}_K^2) \leq \deg_p(\mathcal{E}_K^{(2)}) - s \times (p-1) \leq 0$$

for all $x \in \mathbb{F}_q^n$. This is the desired claim. □

In the typical setting, where $\mathcal{R}_k(x) = \mathcal{R}(x+k)$ for all $k, x \in \mathbb{F}_q^n$. we have the following result.

Corollary 2. *Let $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ be an ℓ-round iterated block cipher with round function $\mathcal{R} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and such that $\mathcal{R}_k(x) = \mathcal{R}(x+k)$ is a one-round encryption. Let $K \to \{k_1, \ldots, k_\ell\} \subset \mathbb{F}_q^n$ be any round keys and suppose that there exist linear subspaces $U_0, U_1, \ldots, U_m$ of $\mathbb{F}_q^n$ having the same $\mathbb{F}_p$-dimension s such that they define a complete exact subspace trail for $\mathcal{R}$*

$$U_0 \overset{\mathcal{R}}{\rightrightarrows} U_1 \overset{\mathcal{R}}{\rightrightarrows} \cdots \overset{\mathcal{R}}{\rightrightarrows} U_m.$$

Then, if the algebraic degree of the last m rounds satisfy

$$\deg_p(\mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_{\ell-m}}) \leq s \times (p-1) \tag{3}$$

we get

$$\sum_{u \in U_0} \mathcal{E}_K(x+u) = c_K$$

for every $x \in \mathbb{F}_q^n$ where $c_K \in \mathbb{F}_q^n$ is a key-dependent constant vector.

Proof. One can easily see that, if $\mathcal{R}_k(x) = \mathcal{R}(x+k)$, then $U_i \overset{\mathcal{R}}{\rightrightarrows} U_{i+1} \iff U_i \overset{\mathcal{R}_{k_i}}{\rightrightarrows} U_{i+1}$. The result then directly follows from the well known property: $\deg_p(F \circ G) \leq \deg_p(F) \times \deg_p(G)$. □

Remark 8. If we denote $d := \deg_p(\mathcal{R})$ and $d^{\ell-m+1} < n(p-1)$ then

$$d^{\ell-m} \leq s \times (p-1) \iff \ell \leq m + \log_d(s \times (p-1)).$$

The quantity $m + \log_d(s \times (p-1))$ is particularly high when p, m, and/or s are big and d is small, which is the case for several ciphers (AES-prime [25] for instance). For example, if $m = 2$, $p = 2^{31}-1$, $s = 12$ and $d = 5$, then the integral holds if the number of rounds ℓ verifies $\ell \leq 16$.

We can get similar results, if we restrict ourselves to coordinate functions of the encryption function, as explained in the following corollary.

Corollary 3. *Let $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ be an ℓ-round iterated block cipher with round function $\mathcal{R} : \mathbb{F}_q^\kappa \times \mathbb{F}_q^n \to \mathbb{F}_q^n$. Let $K \to \{k_1, \ldots, k_\ell\} \subset \mathbb{F}_q^\kappa$ be any round keys and suppose that there exist $m < \ell$ linear subspaces $U_0, U_1, \ldots, U_m$ of $\mathbb{F}_q^n$ having the same $\mathbb{F}_p$-dimension s such that*

$$U_0 \overset{\mathcal{R}_{k_1}}{\rightrightarrows} U_1 \overset{\mathcal{R}_{k_2}}{\rightrightarrows} \cdots \overset{\mathcal{R}_{k_m}}{\rightrightarrows} U_m.$$

If there exist $i \in \{1, \ldots, n\}$ *such that the coordinate function verifies*

$$\deg_p \left((\mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_{\ell-m}})^{(i)} \right) \leq s \times (p-1). \tag{4}$$

Then

$$\sum_{u \in U_0} (\mathcal{E}_K(x+u))^{(i)} = c_K$$

for every $x \in \mathbb{F}_q^n$ *where* $c_K \in \mathbb{F}_q^n$ *is a key-dependent constant vector.*

Remark 9. If $\kappa = n$ and $\mathcal{R}_k(x) = \mathcal{R}(x+k)$, then Corollary 2 can also be restated in terms of the coordinate functions of $\mathcal{R}$, as done in the above Corollary 3.

Our results can be extended to more rounds in some cases using the following definition of subspace chains mentioned by Boeuf et al. in [6].

Definition 12 (Subspace chains). *Let* $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *be a function and let* $U_0, \ldots, U_r$ *be* $\mathbb{F}_p$*-linear subspaces of* $\mathbb{F}_q^n$ *with* $a_0, \ldots, a_r \in \mathbb{F}_q^n$*. Then the sequence of pairs* $(U_0, a_0), \ldots, (U_r, a_r)$ *is said to be a subspace chain of* F *if* $F(a_i + U_i) \subseteq a_{i+1} + U_{i+1}$ *for any* $0 \leq i \leq r-1$*. The chain is said to be exact, if*

$$F(a_i + U_i) = a_{i+1} + U_{i+1} \quad \forall\ 0 \leq i \leq r-1.$$

Definition 13 (Germs of subspaces by a function). *Let* U *be a* $\mathbb{F}_p$*-linear subspace of* $\mathbb{F}_q^n$ *and* $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *be a function. We define the germs of the subspace* U *by a function* F *as*

$$\Gamma_F(U) = \left\{ a \in \mathbb{F}_q^n \;\middle|\; F(a+U) \text{ is an } \mathbb{F}_p\text{-affine subspace of } \mathbb{F}_q^n \right\}.$$

Remark 10. Note that if $a \in \Gamma_F(U)$, then $a + u \in \Gamma_F(U)$ for any $u \in U$, i.e. $|\Gamma_F(U)| \geq |U|$. This implies that either $|\Gamma_F(U)| = 0$ or $|\Gamma_F(U)| \geq |U|$.

Next, we suppose that the key scheduling algorithm which produces $(k_0, \ldots, k_\ell)$ from K is as follows: $\psi_i(K) = k_i$ where $\psi_i : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a bijection.

Theorem 3. *Let* $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ *be an* ℓ*-round iterated block cipher with round function* $\mathcal{R} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *and such that* $\mathcal{R}_k(x) = \mathcal{R}(x+k)$ *is a one-round encryption. Suppose that there exists an exact complete subspace trail*

$$U_0 \overset{\mathcal{R}}{\to} U_1 \overset{\mathcal{R}}{\to} \cdots \overset{\mathcal{R}}{\to} U_m$$

having the same $\mathbb{F}_p$*-dimension* s*. Furthermore, suppose that* $|\Gamma_{\mathcal{R}}(U_m)| > 0$*. Then, for any* $x \in \mathbb{F}_q^n$*, there exist* $|\Gamma_{\mathcal{R}}(U_m)|$ *keys* K *such that, if the algebraic degree verifies*

$$\deg_p(\mathcal{R})^{\ell-m-1} \leq s \times (p-1) \tag{5}$$

then

$$\sum_{u \in U_0} \mathcal{E}_K(x+u) = c_K$$

where $c_K \in \mathbb{F}_q^n$ *is a key-dependent constant vector.*

Proof. Let $K \to k_0, \ldots, k_\ell$ be round keys. As $U_0 \overset{\mathcal{R}}{\rightrightarrows} U_1 \overset{\mathcal{R}}{\rightrightarrows} \cdots \overset{\mathcal{R}}{\rightrightarrows} U_m$, then for any $x \in \mathbb{F}_q^n$, there exists $y \in \mathbb{F}_q^n$ such that $\mathcal{R}_{k_{m-1}} \circ \cdots \circ \mathcal{R}_{k_0}(x + U_0) = y + U_m$. Thus, if $y + k_m \in \Gamma_{\mathcal{R}}(U_m)$, then there exist $z \in \mathbb{F}_q^n$ and a linear subspace V of $\mathbb{F}_q^n$ of the same dimension as U_m such that $\mathcal{R}_{k_m}(y + U_m) = z + V$. We can skip $m + 1$ rounds as

$$\sum_{u \in U_0} \mathcal{E}_K(x + u) = \sum_{v \in V} \mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_{m+1}}(z + v).$$

As a consequence, if $\deg_p(\mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_{m+1}}) \leq s \times (p-1)$, then $\deg_p(\sum_{u \in U_0} \mathcal{E}_K(x + u)) \leq 0$. □

Remark 11. If the inequalities (2), (3), (4) and (5) are strict, then the sum will be zero, independently of the key K.

5 Applications to AES-like SPN ciphers

In this section, we first recall the general design of the Advanced Encryption Standard (AES) [11] as well as definitions and preliminary results about the existing complete subspace trails. We then present our results on ciphers that follow the same design principle as the AES, which we call AES-like SPN ciphers, first on binary fields, and finally on AES-prime.

5.1 AES

The AES is a SPN cipher that operates on 128-bit blocks and supports key sizes of 128, 192, and 256 bits. It consists of multiple rounds, where each round applies a sequence of transformations combining linear diffusion and nonlinear substitution. The internal state of AES is represented as a 4×4 matrix of bytes in $\mathbb{F}_{2^8}$, constructed using the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$ over $\mathbb{F}_2$. For AES-128, the cipher applies a total of 10 rounds to the state. Each round performs the following four operations on the state matrix:

1. `SubBytes` (S-Box): a nonlinear, invertible byte-wise substitution defined over $\mathbb{F}_{2^8}$, applying the same 8-bit to 8-bit S-Box in parallel to all 16 bytes of the state,
2. `ShiftRows` (SR): a cyclic shift of the rows of the 4×4 state array,
3. `MixColumns` (MC): a linear diffusion layer that multiplies each column by a constant 4×4 invertible matrix over $\mathbb{F}_{2^8}$,
4. `AddRoundKey` (ARK): a bitwise XOR with a 128−bit round key derived from the master key.

The cipher begins with an initial AddRoundKey operation before the first round, and the final round omits the MixColumns step. One round of AES can be described as $\mathcal{R}_K(x) = \mathrm{K} \oplus \mathrm{MC} \circ \mathrm{SR} \circ \text{S-Box}(x)$.

We now recall the exact subspace trail through two rounds of AES [18] . To do this, we define four families of subspaces of the space $\mathbb{F}_{2^8}^{4\times 4}$ over $\mathbb{F}_{2^8}$:=

$\mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$, which are essential to AES. Let $E = \{e_{0,0}, \ldots, e_{3,3}\}$ denote the set of unit vectors of $\mathbb{F}_{2^8}^{4\times 4}$, where $e_{i,j}$ has a single 1 in the i-th row and j-th column and 0 elsewhere. For example, $e_{0,1}$ corresponds to the following matrix:

$$e_{0,1} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Definition 14 (Column spaces). *The column spaces $\mathcal{C}_i$ are defined as*

$$\mathcal{C}_i = \mathrm{Span}_{\mathbb{F}_{2^8}}\{e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i}\}.$$

Definition 15 (Diagonal spaces). *The diagonal spaces $\mathcal{D}_i$ are defined as*

$$\mathcal{D}_i = \mathrm{Span}_{\mathbb{F}_{2^8}}\{e_{0,i}, e_{1,i+1}, e_{2,i+2}, e_{3,i+3}\}.$$

Definition 16 (Inverse-Diagonal spaces). *The inverse-diagonal spaces $\mathcal{ID}_i$ are defined as*

$$\mathcal{ID}_i = SR(\mathcal{C}_i) = \mathrm{Span}_{\mathbb{F}_{2^8}}\{e_{0,i}, e_{1,i-1}, e_{2,i-2}, e_{3,i-3}\}.$$

Definition 17 (Mixed spaces). *The mixed spaces $\mathcal{M}_i$ are defined as*

$$\mathcal{M}_i = MC(\mathcal{ID}_i).$$

Definition 18. *Given $I \subseteq \{0,1,2,3\}$ where $0 < |I| \leq 3$, we define*

$$\mathcal{C}_I = \bigoplus_{i\in I} \mathcal{C}_i, \quad \mathcal{D}_I = \bigoplus_{i\in I} \mathcal{D}_i, \quad \mathcal{ID}_I = \bigoplus_{i\in I} \mathcal{ID}_i, \quad \mathcal{M}_I = \bigoplus_{i\in I} \mathcal{M}_i.$$

Remark 12. For the round function $\mathcal{R}$ of any AES-like cipher with linear layer $\mathcal{L} = \mathrm{MC}\circ\mathrm{SR}$ and S-box $\mathcal{S}$, the subspaces $\mathcal{D}_I, \mathcal{C}_I$ and $\mathcal{M}_I$ can be seen as following

$$\mathcal{M}_I = MC(SR(\mathcal{C}_I)) = \mathcal{L}(\mathcal{C}_I) \quad \text{and} \quad \mathcal{C}_I = SR(\mathcal{D}_I).$$

Since MixColumns affects only the constant columns, thus $\mathrm{MC}(\mathcal{C}_I) = \mathcal{C}_I$. Therefore, $\mathcal{L}(\mathcal{D}_I) = \mathcal{C}_I$.

Note that the dimension of any of the four spaces over $\mathbb{F}_{2^8}$ in Definition 18 is 4 times the cardinality of I. We now state the subspace trails defined using these four families of subspaces, as introduced by Grassi et al. [18].

Lemma 2. *[18] Let $I \subseteq \{0,1,2,3\}$ with $0 < |I| \leq 3$ and $a \in \mathcal{D}_I^{\perp}$. There exists a unique $b \in \mathcal{C}_I^{\perp}$ such that*

$$\mathcal{R}_K(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b.$$

Lemma 3. *[18] Let $I \subseteq \{0,1,2,3\}$ with $0 < |I| \leq 3$ and $a \in \mathcal{C}_I^{\perp}$. There exists a unique $b \in \mathcal{M}_I^{\perp}$ such that*

$$\mathcal{R}_K(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b.$$

From the above two lemmas, there exists an exact two-round orthogonal subspace trail:

$$\mathcal{D}_I \xrightarrow{\mathcal{R}_K} \mathcal{C}_I \xrightarrow{\mathcal{R}_K} \mathcal{M}_I.$$

Since $\mathcal{D}_I \oplus \mathcal{D}_I^{\perp} = \mathcal{C}_I \oplus \mathcal{C}_I^{\perp} = \mathcal{M}_I \oplus \mathcal{M}_I^{\perp} = \mathbb{F}_{2^8}^{4\times 4}$, we apply Remark 3 to obtain

$$\mathcal{D}_I \overset{\mathcal{R}_K}{\rightrightarrows} \mathcal{C}_I \overset{\mathcal{R}_K}{\rightrightarrows} \mathcal{M}_I.$$

This shows that AES has an exact two round subspace trail with respect to both Definition 7 and Definition 8.

In a similar way, there exists an exact complete subspace trail

$$\mathcal{M}_I \overset{\bar{\mathcal{R}}}{\rightrightarrows} \mathcal{C}_I \overset{\bar{\mathcal{R}}}{\rightrightarrows} \mathcal{D}_I,$$

for the decryption round function $\bar{\mathcal{R}} = \bar{\mathcal{S}} \circ \bar{\mathcal{L}}$ of AES, where, $\bar{\mathcal{L}} = \mathcal{L}^{-1}$, and $\bar{\mathcal{S}} = \mathcal{S}^{-1}$. The following lemma states this formally.

Lemma 4. *Let $I \subseteq \{0,1,2,3\}$ with $0 < |I| \leq 3$ and $a \in \mathbb{F}_q^n$. There exists $b \in \mathbb{F}_q^n$ such that*

$$\bar{\mathcal{R}}(\mathcal{M}_I \oplus a) = \mathcal{C}_I \oplus b.$$

and for $c \in \mathbb{F}_q^n$, there exists $d \in \mathbb{F}_q^n$ such that

$$\bar{\mathcal{R}}(\mathcal{C}_I \oplus c) = \mathcal{D}_I \oplus d.$$

Proof. We only prove the claim $\mathcal{M}_I \overset{\bar{\mathcal{R}}}{\rightrightarrows} \mathcal{C}_I$, since the other identity $\mathcal{C}_I \overset{\bar{\mathcal{R}}}{\rightrightarrows} \mathcal{D}_I$ follows by an identical argument. For any $a \in \mathbb{F}_q^n$,

$$\bar{\mathcal{R}}(\mathcal{M}_I \oplus a) = \bar{\mathcal{S}} \circ \bar{\mathcal{L}}(\mathcal{M}_I \oplus a) = \bar{\mathcal{S}}\Big(\bar{\mathcal{L}}(\mathcal{M}_I) \oplus \bar{a}\Big), \quad \text{where} \quad \bar{a} = \bar{\mathcal{L}}(a).$$

Since, $\mathcal{M}_I = \mathcal{L}(\mathcal{C}_I)$ from Remark 12, we have $\bar{\mathcal{S}}\Big(\bar{\mathcal{L}}(\mathcal{M}_I) \oplus \bar{a}\Big) = \bar{\mathcal{S}}\Big(\mathcal{C}_I \oplus \bar{a}\Big)$. Also, because $\bar{\mathcal{S}}$ is bijective and acts independently on each byte, it maps the additive coset $\mathcal{C}_I + \bar{a}$ to another additive coset $\mathcal{C}_I + b$, where $b = (b_{i,j})$ with $b_{i,j} = \bar{\mathcal{S}}(\bar{a}_{i,j})$ for each byte (i,j). □

5.2 AES-like SPN ciphers in even characteristic

AES has been widely studied through key-independent distinguishers, especially those based on integral and differential-integral techniques. The Square attack of Daemen et al. [9] first demonstrated a 4-round zero-sum property, forming the basis for subsequent improvements. Partial-sum refinements [14] expanded

this idea, enabling more efficient 4-round distinguishers. Later developments introduced new structural integral properties, such as the multiple-of-8 distinguisher [17] and mixture differential techniques [16], which extended to 4–6 rounds with significantly reduced data. The most recent progress combines Fast Hadamard Transform (FHT), partial sums, and data packing to obtain a 6-round key-independent distinguisher [12]. Table 3 summarizes these key developments.

Distinguisher	**Rounds**	**Data**	**Reference**
Square / Saturation	4	2^{32}	[9]
Square + Partial Sums	4	6×2^{32}	[14]
Multiple-of-8 Integral	4	2^{33}	[17]
Mixture Differential	4–6	2^{17}–2^{26}	[16]
FHT + partial sums + Packing	6	2^{32}	[12]
Zero-sum Integral	$1-2$	2^{8}	Proposition 3
Zero-sum Integral	3	2^{32}	Corollary 4
Zero-sum Integral	4	2^{64}	Corollary 5

Table 3. Key-Independent Distinguishers on Reduced-Round AES

Here, we present some applications of our results discussed in Section 4 to AES-like SPN ciphers over the finite fields of even characteristic. Our goal is to demonstrate how exact subspace trails can be used to construct distinguishers for such SPN ciphers. Although our approach does not improve upon the best existing attacks, we include these applications to illustrate the usefulness and generality of our framework.

One may recall that Boura, Canteaut, and Coggia [7] provided exact complete subspace trails for several other AES-like SPN ciphers, replacing the subspaces $\mathcal{D}_I$, $\mathcal{C}_I$, and $\mathcal{M}_I$ with analogous constructions. With a slight abuse of notation, we continue to denote these subspaces by $\mathcal{D}_I$, $\mathcal{C}_I$, and $\mathcal{M}_I$ when referring to those AES-like SPN ciphers. Their framework applies to ciphers such as Midori-64 [2], Klein-64 [15], and SKINNY-64 [3]. As a direct consequence of Corollary 2 applied to the above mentioned AES-like SPN ciphers, we derive the following corollary.

Corollary 4. *Let $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ be an ℓ-round AES-like SPN block cipher, where $q = 2^m$, with round function $\mathcal{R}$ and a two-round exact complete subspace trail*

$$\mathcal{D}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{C}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{M}_I,$$

$\dim_{\mathbb{F}_2}(\mathcal{D}_I) = \dim_{\mathbb{F}_2}(\mathcal{C}_I) = \dim_{\mathbb{F}_2}(\mathcal{M}_I) = 4 \times m \times |I|$, $1 \le |I| \le 3$. *Therefore, if*

$$\ell \le 2 + \log_{\deg_2(\mathcal{R})}(4 \times m \times |I|), \tag{6}$$

then

$$\sum_{u \in \mathcal{D}_I} \mathcal{E}_K(x+u) = c_K, \qquad \text{for every } x \in \mathbb{F}_q^n \text{ and every key } K,$$

where $c_K \in \mathbb{F}_q^n$ is a key-dependent constant vector.

Proof. The proof follows directly from Lemma 2, Lemma 3 and Corollary 2. □

In Table 4, we present the maximum number of rounds for various AES-like SPN ciphers, assuming the algebraic degree grows exponentially, for which our approach (Corollary 4) yields a distinguisher.

Cipher	q	n	$\deg_2(\mathcal{R})$	ℓ	d	Data
AES	2^8	16	7	4	64	2^{64}
Midori-64	2^4	16	3	5	32	2^{32}
Klein-64	2^4	16	3	5	32	2^{32}
Skinny-64	2^4	16	3	5	32	2^{32}

Table 4. Parameters of the zero-sum integral distinguisher for AES-like SPN ciphers over $\mathbb{F}_q^n$ with round function $\mathcal{R}$, maximum number of rounds ℓ and the dimension of an exact subspace trail d.

For the round decryption function, we obtain the following.

Corollary 5. *Let $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ be an ℓ-round AES-like SPN block cipher over $\mathbb{F}_q$, where $q = 2^m$. Let $\bar{\mathcal{E}} = \{\bar{\mathcal{E}}_K : \mathbb{F}_q^n \to \mathbb{F}_q^n\}_K$ denote the corresponding decryption scheme with decryption round function $\bar{\mathcal{R}}$ and a two-round exact complete subspace trail*

$$\mathcal{M}_I \overset{\bar{\mathcal{R}}}{\to} \mathcal{C}_I \overset{\bar{\mathcal{R}}}{\to} \mathcal{D}_I,$$

$\dim_{\mathbb{F}_2}(\mathcal{D}_I) = \dim_{\mathbb{F}_2}(\mathcal{C}_I) = \dim_{\mathbb{F}_2}(\mathcal{M}_I) = 4 \times m \times |I|$, *with* $1 \le |I| \le 3$. *Therefore, if*

$$\ell \le 2 + \log_{\deg_2(\bar{\mathcal{R}})}(4 \times m \times |I|),$$

then

$$\sum_{u \in \mathcal{M}_I} \bar{\mathcal{E}}_K(x+u) = c_k, \qquad \text{for every } x \in \mathbb{F}_q^n \text{ and key } K$$

where $c_K \in \mathbb{F}_q^n$ is a key-dependent constant vector.

Proof. The proof follows directly from Lemma 4 and Corollary 2. □

Example 2. (AES) In the case of AES-128, the round function $\mathcal{R} : \mathbb{F}_{2^8}^{4\times 4} \to \mathbb{F}_{2^8}^{4\times 4}$ has algebraic degree 7. For $\mathcal{D}_I$ with $|I| = 2$, since $r = 2$ is the largest integer such that

$$7^r < 4 \times 2 \times 8 = 64,$$

we obtain the following distinguisher for four rounds of the AES

$$\sum_{u \in \mathcal{D}_I} \mathcal{E}_K(x+u) = 0, \qquad \text{for every } x \in \mathbb{F}_{2^8}^{4\times 4} \text{ and key } K.$$

Similarly, since the decryption round function $\bar{\mathcal{R}}$ has an algebraic degree at most 7, we have a zero-sum integral distinguisher on 4-round for the AES. Moreover, by using Remark 2, we can even have a zero-sum integral distinguisher for five

rounds of decryption function of AES. This follows because when we decrypt the last three rounds of AES, for the cipher text $C \in \mathbb{F}_q^n$, we get

$$\bar{\mathcal{R}}(\bar{\mathcal{R}}(\bar{\mathcal{R}}(C) - k_\ell) - k_{\ell-1}) - k_{\ell-2}$$

for keys $\{k_{\ell-2}, k_{\ell-1}, k_\ell\} \in \mathbb{F}_q^n$. Here, we do not include a whitening key after the last round. Therefore, using Corollary 5 and after decrypting the last three round of AES with $C \in \mathcal{R}(\mathcal{M}_I)$, we get

$$\begin{aligned}\bar{\mathcal{R}}(\bar{\mathcal{R}}(\bar{\mathcal{R}}(\mathcal{R}(\mathcal{M}_I)) - k_\ell) - k_{\ell-1}) - k_{\ell-2} &= \bar{\mathcal{R}}(\bar{\mathcal{R}}(\mathcal{M}_I - k_\ell) - k_{\ell-1}) - k_{\ell-2} \\ &= b + \mathcal{D}_I,\end{aligned}$$

for some $b \in \mathbb{F}_{2^8}^{4\times 4}$, which is an additive coset of $\mathcal{D}_I$ for keys $\{k_{\ell-2}, k_{\ell-1}, k_\ell\} \in \mathbb{F}_q^n$. This allows us to skip three rounds of decryption instead of two. Hence, we get a 5-round zero-sum integral distinguisher for keys $\{k_{\ell-4}, \ldots, k_\ell\} \in \mathbb{F}_q^n$ as follows

$$\sum_{x \in \mathcal{R}(\mathcal{M}_I)} \bar{\mathcal{R}}_{k_{\ell-4}} \circ \cdots \circ \bar{\mathcal{R}}_{k_\ell}(x) = \sum_{u \in \mathcal{D}_I} \bar{\mathcal{R}}_{k_{\ell-4}} \circ \bar{\mathcal{R}}_{k_{\ell-3}}(b+u) = 0.$$

Remark 13. Using the same technique as in Example 2, and looking at the decryption function of Midori-64, Skinny-64 and Klein-64, we get a zero-sum integral distinguisher on their 6-round decryption using 2^{32} data.

Next, we illustrate the number of rounds required for AES-like SPN ciphers with exponential algebraic degrees growth in Figure 2. The lower bound on the number of rounds of AES-like SPN ciphers with round function $\mathcal{R}$ to prevent the integral properties discussed in this section follows from inequality (6), by using the exact complete subspace trail $\mathcal{D}_I \overset{\mathcal{R}}{\Rightarrow} \mathcal{C}_I \overset{\mathcal{R}}{\Rightarrow} \mathcal{M}_I$ with $|I| = 3$. The inequality (6) assumes an exponential growth in the algebraic degree of the round function as a function of the number of rounds. The algebraic degree of the round function $\mathcal{R}$ is equal to the algebraic degree of the S-box: $d = \deg_2(S)$, and when $q = 2^m$, this value can take any integer between 2 and $m - 1$.

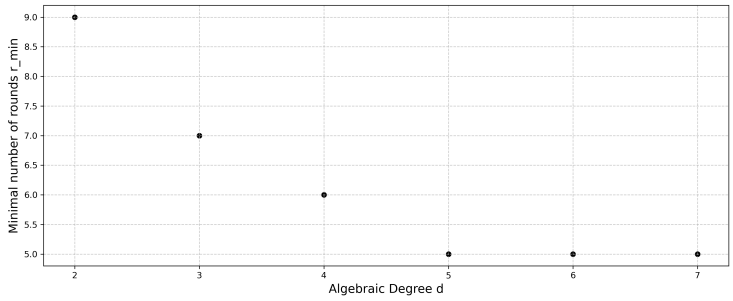

Fig. 2. Minimal number of rounds required for AES-like SPN ciphers to be resistant to the presented integrals, as a function of the algebraic degree, when $q = 2^8$

Remark 14. We can actually go further if the algebraic degree d growth is not exponential in ℓ rounds. For instance, in the case of SKINNY-64, Hebborn et al. [20] show that the algebraic degree of its round function lies between 39 and 47 instead of 3^5 after 5 rounds. Therefore, using the exact complete subspace trail

$$\mathcal{D}_I \overset{\mathcal{R}_{k_0}}{\Rightarrow} \mathcal{C}_I \overset{\mathcal{R}_{k_1}}{\Rightarrow} \mathcal{M}_I$$

with $|I| = 3$ to skip two rounds, and the fact that

$$\deg_2(\mathcal{R}_{k_6} \circ \mathcal{R}_{k_5} \circ \mathcal{R}_{k_4} \circ \mathcal{R}_{k_3} \circ \mathcal{R}_{k_2}) \leq 47 < 12 \times 4 = 48$$

for all keys $k_2, k_3, k_4, k_5, k_6 \in \mathbb{F}_{2^4}^{4\times 4}$, we obtain the following zero-sum integral distinguisher for seven rounds of SKINNY-64 by applying Theorem 2

$$\sum_{u \in \mathcal{D}_I} \mathcal{R}_{k_6} \circ \mathcal{R}_{k_5} \circ \mathcal{R}_{k_4} \circ \mathcal{R}_{k_3} \circ \mathcal{R}_{k_2} \circ \mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x+u) = 0,$$

for every $x \in \mathbb{F}_{2^4}^{4\times 4}$ and $k_0, k_1, k_2, k_3, k_4, k_5, k_6 \in \mathbb{F}_{2^4}^{4\times 4}$. To the best of our knowledge, this is the best zero-sum integral distinguisher on reduced round Skinny-64.

Remark 15. Based on Corollary 3 and [20, Table 7], we can, in fact, get an integral distinguisher on 8-round Skinny64. In [20, Table 7], the authors give an upper bound on the algebraic degree of every coordinate $i \in \{0, \ldots, 15\}$ function after 6-round encryption. This is because the 6-round coordinate functions for $i \in \{4, 5, 6, 7\}$ have algebraic degree at most 47, instead of 3^5.

Now we give the one dimensional exact complete subspace trail for the round function $\mathcal{R}$ of AES-like SPN ciphers. In what follows, $\mathcal{L} = MC \circ SC$ where MC and SC denotes the MixColumns and ShiftColumns operation of AES-like SPN ciphers, respectively.

Proposition 3. *Let $\{e_{i,j} \mid 0 \leq i, j \leq 3\}$ be the set of unit vectors of $\mathbb{F}_{2^8}^{4\times 4}$, and $\mathcal{R}$ be the round function of AES-like SPN ciphers. Then, for any $a \in \mathbb{F}_q^n$, there exists a unique $b \in \mathbb{F}_q^n$ such that for any $0 \leq i, j \leq 3$,*

$$\mathcal{R}(a \oplus \mathbb{F}_q\, e_{i,j}) = b \oplus \mathbb{F}_q\, \mathcal{L}(e_{i,j}).$$

Proof. The proof is similar to that of Lemma 2. □

Remark 16. From Proposition 3, we have a one-round exact subspace trail that further gives us a two-round zero-sum integral distinguisher for AES, using Corollary 2. Moreover, it is already known that there exists a zero-sum integral distinguisher for three rounds of AES using q data, namely the square attack [10]. However, we are not able to achieve such a result with our approach. The reason is that the existence of a subspace trail guarantees a zero-sum integral distinguisher after a certain number of rounds, depending on the algebraic degree growth. The converse does not necessarily hold, that is the existence of a zero-sum integral distinguisher does not imply the existence of a subspace trail or a degree growth deficiency.

Leander et al. [23] studied the length of the longest complete subspace trails for AES-like SPN ciphers. Motivated by their work, we investigate the length of the longest subspace trails for various AES-like SPN ciphers with respect to Definition 7. Carrying out an analysis for Midori-64, we identified what appears to be a typo in the article by Liu and Yang [24]. Specifically, the authors define certain subspaces $\mathcal{D}_I, \mathcal{C}_I, \mathcal{M}_I$, and $\mathcal{W}_I$ of $\mathbb{F}_{2^4}^{4\times 4}$. However, the subspace $\mathcal{W}_I$ as defined in the article does not match the subspace that is actually used throughout their subsequent analysis. Furthermore, they claim the existence of a three-round exact complete subspace trail $\mathcal{D}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{C}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{M}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{W}_I$ where $\mathcal{R}$ is the round function for Midori-64. We observe that the final step $\mathcal{M}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{W}_I$ does not hold under any of the definitions of $\mathcal{W}_I$ provided in their manuscript. Therefore, the claimed exact subspace trail appears to be incorrect, though the results in the article [24] are still valid since they are not based on the exactness of the subspace trail from $\mathcal{M}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{W}_I$.

5.3 AES-prime

In this subsection, we apply the theoretical results of Section 4 on AES-prime, introduced by Masure et al. in [25]. Particularly, with our approach, we find the same integral properties of AES-prime given by Tim Beyne and Michiel Verbauwhede in [5]. We also extend these integral properties on more rounds for some weak keys that we are going to introduce.

AES-prime, as described in [25], consists on adapting the standard AES design to $\mathbb{F}_p$ where p is a large prime, using only additions and multiplications over the chosen prime field. The main design components remain the same: the key is a vector of 16 elements of $\mathbb{F}_p$ and the state is considered as a 4 by 4 table of $\mathbb{F}_p$ elements. We recall the main components of AES-prime as follows

1. **State and Field:** AES-prime operates on a 4×4 state matrix of elements in the prime field $\mathbb{F}_p$, where $p = 2^7 - 1 = 127$.
2. **SubBytes (S-box):** applies a non-linear permutation $S : \mathbb{F}_{127} \to \mathbb{F}_{127}$ independently to each element $s_{i,j}$, $0 \leq i, j \leq 3$ of the state, given by

$$S(x) = x^5 + 2 \qquad (\deg_p S = 5)$$

3. **ShiftRows:** performs a cyclic left shift on the rows of the state matrix. If the state rows are indexed $0, 1, 2, 3$, the transformation is:
   - Row i: cyclic left shift by i position, for $0 \leq i \leq 3$.
4. **MixColumns:** mixes the data within each column via multiplication by a constant MDS matrix M over $\mathbb{F}_{127}$. For each state column c,

$$\begin{pmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{pmatrix} = M \cdot c = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 16 \\ 1 & 4 & 16 & 2 \\ 1 & 16 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix} \pmod{127}.$$

5. **AddRoundKey:** combines the state with the round key k_i using addition in $\mathbb{F}_{127}$: $s'_{i,j} = s_{i,j} + k_{i,j}$.

Table 5 resumes some known properties of AES-prime.

Rounds ℓ	**data**	**Algebraic Degree**
$1-4$	p	5^ℓ
5	p^4	2002
6	p^8	2015

Table 5. Known integral properties of AES-prime and its algebraic degree growth through its round function, based on [5, Section 7.1].

In what follows, let $\mathcal{R} = \mathcal{L} \circ \mathcal{S}$ denote the round function of AES-prime, where $\mathcal{S}$ is the S-box layer and $\mathcal{L}$ is the linear layer consisting of the `ShiftRows` and `MixColumns` operations. For a round key $k_i \in \mathbb{F}_p^{4\times 4}$, we denote by $\mathcal{R}_{k_i}(x) = \mathcal{R}(x + k_i)$ the i-th encryption round.

Proposition 4. *Let $\{e_{i,j} \mid 0 \le i,j \le 3\}$ be the set of unit vectors of $\mathbb{F}_p^{4\times 4}$. Then, $\mathcal{R}$ has the following one dimensional exact complete subspace trail*

$$\mathbb{F}_p e_{i,j} \overset{\mathcal{R}}{\to} \mathbb{F}_p \mathcal{L}(e_{i,j}) \quad \text{for any } 1 \le i,j \le 3. \tag{7}$$

Proof. We only need to show that the S-box layer $\mathcal{S}$ maps any additive coset of $\mathbb{F}_p e_{i,j}$ to another additive coset of $\mathbb{F}_p e_{i,j}$. Let $a \in \mathbb{F}_p^{4\times 4}$. For $i,j \in \{0,1,2,3\}$ we have,

$$\begin{aligned}\mathcal{S}(a + u e_{i,j}) &= \left(\sum_{\substack{0\le m,n\le 3 \\ (m,n)\neq(i,j)}} S(a_{m,n})\, e_{m,n} \right) + S(a_{i,j} + u)\, e_{i,j} \\ &= b + S(a_{i,j} + u)\, e_{i,j} \in b + \mathbb{F}_p\, e_{i,j} \quad \forall u \in \mathbb{F}_p,\end{aligned}$$

where

$$b = \sum_{0\le m,n\le 3,\ (m,n)\neq(i,j)} S(a_{m,n}) e_{m,n}$$

does not depend on u. As S is a bijection, we have the following equality

$$\mathcal{S}(a + \mathbb{F}_p e_{i,j}) = b + \mathbb{F}_p e_{i,j}.$$

By applying the linear layer $\mathcal{L}$, we get $\mathcal{R}(a + \mathbb{F}_p e_{i,j}) = \mathcal{L}(b) + \mathbb{F}_p \mathcal{L}(e_{i,j})$. □

Remark 17. In Proposition 4, we can get a formula for the affine subspace $\mathcal{R}(a + \mathbb{F}_p e_{i,j})$ as follows

$$\begin{aligned}\mathcal{R}(a + \mathbb{F}_p e_{i,j}) &= \mathcal{L}\left(\sum_{0\le m,n\le 3,\ (m,n)\neq(i,j)} S(a_{m,n}) e_{m,n} + \mathbb{F}_p\, e_{i,j} \right) \\ &= \mathcal{L}\left(\mathcal{S}(a) - S(a_{i,j}) e_{i,j} + \mathbb{F}_p\, e_{i,j} \right) \\ &= \mathcal{L}(\mathcal{S}(a) + \mathbb{F}_p\, e_{i,j}) = \mathcal{R}(a) + \mathbb{F}_p\, \mathcal{L}(e_{i,j}).\end{aligned}$$

Hereafter, $K \to \{k_0, k_1, \ldots, k_s\}$ denotes the round keys $k_0, \ldots, k_s \in \mathbb{F}_p^{4\times 4}$ generated from a key scheduling algorithm using a master key $K \in \mathbb{F}_p^{4\times 4}$. The key scheduling algorithm used by the designers of AES-prime is $K \in \mathbb{F}_p^{4\times 4} \to (k, k, k, \ldots, k)$, that is the same key for all rounds. However, our arguments do not rely on this particular choice and remain valid for any key schedule. By using the one dimensional exact subspace trail (7) and Corollary 2, we describe a four-round zero-sum integral distinguisher on AES-prime using p data as follows.

Proposition 5. *Let $\{e_{i,j} \mid 0 \le i, j \le 3\}$ be the set of unit vectors of $\mathbb{F}_p^{4\times 4}$. For any round keys $K \to \{k_0, k_1, k_2, k_3, k_4\} \subset \mathbb{F}_p^{4\times 4}$, and any $x \in \mathbb{F}_p^{4\times 4}$, we have*

$$\sum_{u\in\mathbb{F}_p} \mathcal{R}_{k_3} \circ \mathcal{R}_{k_2} \circ \mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x + ue_{i,j}) = 0, \quad \text{for any } 1 \le i, j \le 3.$$

Proof. From Corollary 2, and by using the trail (7), we have a zero-sum integral distinguisher on ℓ rounds if ℓ verifies

$$\ell < 1 + \log_{deg_p(\mathcal{R})}(p-1).$$

As $p = 2^7 - 1$ and $\deg_p(\mathcal{R}) = 5$, we get

$$1 + \log_5(p-1) = 1 + \log_5(126) \simeq 4.005.$$

We thus have a zero-sum integral distinguisher on $\ell \in \{1, 2, 3, 4\}$ rounds using only p data (summing over a space of cardinality p). □

Furthermore, we give a 5-round zero-sum integral distinguisher on AES-prime using p^4 data. In fact, similarly to AES, AES-prime also has a two-round exact complete subspace trail

$$\mathcal{D}_I \overset{\mathcal{R}}{\Rightarrow} \mathcal{C}_I \overset{\mathcal{R}}{\Rightarrow} \mathcal{M}_I$$

of $\mathbb{F}_p$-dimension $4\times|I|$ where $I \subset \{0, 1, 2, 3\}$. The trail is defined the same way as in Subsection 5.1 (see Remark 12), and such that $\mathcal{C}_I = \mathcal{L}(\mathcal{D}_I)$ and $\mathcal{M}_I = \mathcal{L}(\mathcal{C}_I)$. Taking $|I| \in \{1, 2\}$, we get the following result.

Proposition 6. *Let $\mathcal{D}_I$ be the diagonal space where $I \subset \{0, 1, 2, 3\}$. For any round keys $K \to \{k_0, k_1, k_2, k_3, k_4, k_5\} \subset \mathbb{F}_p^{4\times 4}$, and any $x \in \mathbb{F}_p^{4\times 4}$, if $|I| = 1$, we have*

$$\sum_{u\in\mathcal{D}_I} \mathcal{R}_{k_4} \circ \mathcal{R}_{k_3} \circ \mathcal{R}_{k_2} \circ \mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x + u) = 0, \quad \forall\ 0 \le i, j \le 3,$$

and, if $|I| = 2$,

$$\sum_{u\in\mathcal{D}_I} \mathcal{R}_{k_5} \circ \mathcal{R}_{k_4} \circ \mathcal{R}_{k_3} \circ \mathcal{R}_{k_2} \circ \mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x + u) = 0, \quad \forall\ 0 \le i, j \le 3.$$

Proof. From Corollary 2, and, using the trail $\mathcal{D}_I \overset{\mathcal{R}}{\to} \mathcal{C}_I \overset{\mathcal{R}}{\to} \mathcal{M}_I$ with $|I| = 1$, we have a zero-sum integral distinguisher on ℓ rounds if ℓ verifies

$$\ell < 2 + \log_5(4 \times |I| \times (p-1)) = 2 + \log_5(4 \times (p-1)).$$

Since for AES-prime, $p = 2^7 - 1$, we have $2 + \log_5(4 \times (p-1)) \simeq 5.504$. Thus, AES-prime has a zero-sum integral distinguisher for $\ell \in \{1, 2, 3, 4, 5\}$ rounds using p^4 data.

Similarly, by taking $|I| = 2$, we get $2 + \log_5(4 \times 2 \times (p-1)) \simeq 6.296$ and by Corollary 2, we have a 6-round zero-sum integral distinguisher on AES-prime using p^8 data. □

The lower bound on the number of rounds of AES-prime with round function $\mathcal{R}$ to prevent the integral properties discussed in this section can be derived from formula (3):

$$r_{\min}(d) = \lfloor 3 + \log_d(3 \times 4 \times (p-1)) \rfloor, \tag{8}$$

by using the trail $\mathcal{D}_I \overset{\mathcal{R}}{\to} \mathcal{C}_I \overset{\mathcal{R}}{\to} \mathcal{M}_I$ with $|I| = 3$. This works on any AES-prime-like SPN. To illustrate this, let's consider the case of AES-prime field, i.e., $p = 2^7 - 1$. In this scenario, the algebraic degree of the round function $\mathcal{R}$ is equal to the algebraic degree of the S-box: $d = \deg_p(S)$. This value can take any integer between 2 and $p-1$. Figure 3 provides a graphical representation of the relationship (8). This expression (8) assumes an exponential growth in the algebraic degree of the round function as a function of the number of rounds, i.e. it is a generic bound.

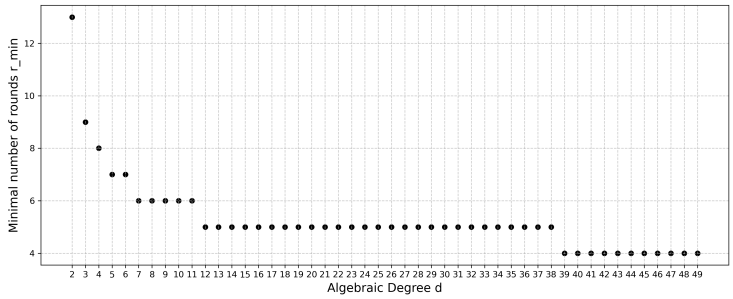

Fig. 3. Minimal number of rounds required for AES-prime to be resistant to the presented integrals as a function of the algebraic degree

Table 5 already summarized the zero-sum integral distinguishers discussed above and, as we can see, leads to the same conclusions as those obtained by Beyne et al. [5]. However, our arguments are based on different notions, that

are, the existence of exact subspace trails and the algebraic degree growth of the round function.

We can improve Proposition 5 and 6 when I is of cardinality 1. More precisely, some of these zero-sum integrals can be extended by one additional round for a restricted subset of master keys K. To do so, we use the notion of subspace chains and germs introduced in Definition 12 and Definition 13, respectively. Let us first recall a result of Boeuf, Canteaut and Perrin [6] that we adapt in the context of AES-prime. For $x \in \mathbb{F}_p^{4\times 4}$, define $\mathrm{supp}(x) := \{(i,j) \mid x_{i,j} \neq 0\}$.

Lemma 5 (Theorem 1 [6]). *Let $\mathcal{R} = \mathcal{L} \circ \mathcal{S}$ be the round function of an SPN over $\mathbb{F}_p^{4\times 4}$, where $\mathcal{L}$ is the linear layer and $\mathcal{S}$ the S-box layer with S-box $S(x) = x^\alpha + c$ over $\mathbb{F}_p$. Let $V = v_0 + \mathbb{F}_p v_1 + \cdots + \mathbb{F}_p v_m$ be a subspace of $\mathbb{F}_p^{4\times 4}$ such that $supp(v_i) \cap supp(v_j) = \emptyset$ for any $i \neq j$. Then*

$$\mathcal{R}(V) = \mathcal{R}(v_0) + \mathbb{F}_p\mathcal{L}(v_1) + \cdots + \mathbb{F}_p\mathcal{L}(v_m).$$

In AES-prime, the S-box is of the form $S(x) = x^\alpha + c$. From Lemma 5, we can estimate the germ's number for the round function $\mathcal{R}$: $|\Gamma_{\mathcal{R}}(\mathbb{F}_p\mathcal{L}(e_{i,j}))|$ (see Definition 13).

Proposition 7. *Let $\mathcal{R}$ be the round function of AES-prime. Then, for any $a \in \mathbb{F}_p^{4\times 4}$, if $supp(a) \cap supp(\mathcal{L}(e_{i,j})) = \emptyset$, where $\{e_{i,j} \mid 0 \leq i,j \leq 3\}$ is the set of unit vectors of $\mathbb{F}_p^{4\times 4}$, $x \in \mathbb{F}_p^{4\times 4}$, we have*

$$\mathcal{R}(a + \mathbb{F}_p\mathcal{L}(e_{i,j})) = \mathcal{R}(a) + \mathbb{F}_p\mathcal{L} \circ \mathcal{L}(e_{i,j}) \quad \forall\ 0 \leq i,j \leq 3,$$

or in other words,

$$|\Gamma_{\mathcal{R}}(\mathbb{F}_p\mathcal{L}(e_{i,j}))| \geq p^{13} \quad \forall\ 0 \leq i,j \leq 3.$$

Proof. Let $a \in \mathbb{F}_p^{4\times 4}$, and suppose that $\mathrm{supp}(a) \cap \mathrm{supp}(\mathcal{L}(e_{i,j})) = \emptyset$ for some $0 \leq i,j \leq 3$. Then, from Lemma 5, it follows that

$$\mathcal{R}(a + \mathbb{F}_p\mathcal{L}(e_{i,j})) = \mathcal{R}(a) + \mathbb{F}_p\mathcal{L} \circ \mathcal{L}(e_{i,j}).$$

Therefore, $\mathcal{R}(a + u + \mathbb{F}_p\mathcal{L}(e_{i,j})) = \mathcal{R}(a) + \mathbb{F}_p\mathcal{L} \circ \mathcal{L}(e_{i,j})$ for any $u \in \mathbb{F}_p\mathcal{L}(e_{i,j})$.

Thus, if $a \in \mathbb{F}_p^{4\times 4}$ is such that $a = a_1 + a_2$ where $\mathrm{supp}(a_1) \cap \mathrm{supp}(\mathcal{L}(e_{i,j})) = \emptyset$ and $a_2 \in \mathbb{F}_p\mathcal{L}(e_{i,j})$, then

$$\mathcal{R}(a + \mathbb{F}_p\mathcal{L}(e_{i,j})) = \mathcal{R}(a_1) + \mathbb{F}_p\mathcal{L} \circ \mathcal{L}(e_{i,j}).$$

Observe that there exist $p \times p^{16 - w_H(\mathcal{L}(e_{i,j}))}$ of such elements a, where $w_H(\cdot)$ denotes the Hamming weight. In case of AES-prime, $w_H(\mathcal{L}(e_{i,j})) = 4$, i.e.

$$p \times p^{16 - w_H(\mathcal{L}(e_{i,j}))} = p \times p^{12} = p^{13}.$$

Hence, $|\Gamma_{\mathcal{R}}(\mathbb{F}_p\mathcal{L}(e_{i,j}))| \geq p^{13}$. □

Now we are ready to present our 5-round weak key distinguisher on AES-prime.

Theorem 4. *Let $\{e_{i,j} \mid 0 \leq i,j \leq 3\}$ be the set of unit vectors of $\mathbb{F}_p^{4\times 4}$, $x \in \mathbb{F}_p^{4\times 4}$ and $K \to \{k_0, k_1, k_2, k_3, k_4, k_5\} \subset \mathbb{F}_p^{4\times 4}$ be the round keys. If*

$$k_1 + b \in \Gamma_{\mathcal{R}}(\mathbb{F}_p\mathcal{L}(e_{i,j}))$$

where b is such that $\mathcal{R}(x + k_0 + \mathbb{F}_p e_{i,j}) = b + \mathbb{F}_p\mathcal{L}(e_{i,j})$, then

$$\sum_{u\in\mathbb{F}_p} \mathcal{R}_{k_4} \circ \mathcal{R}_{k_3} \circ \mathcal{R}_{k_2} \circ \mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x + ue_{i,j}) = 0, \quad \forall\ 0 \leq i,j \leq 3.$$

Proof. The proof follows directly from Theorem 3 using the trail (7) and Proposition 7. □

Example 3. To illustrate Theorem 4, we use the trail $\mathbb{F}_p e_{0,0} \overset{\mathcal{R}}{\to} \mathbb{F}_p\mathcal{L}(e_{0,0})$ (Proposition 4). First, we have

$$\mathcal{L}(e_{0,0}) = \begin{bmatrix} 1&0&0&0\\ 1&0&0&0\\ 1&0&0&0\\ 1&0&0&0 \end{bmatrix}$$

and for $a \in \mathbb{F}_p^{4\times 4}$, we have $\mathcal{R}(a) = M \times \left[S(a_{i,j})\right]_{i,j}$, $0 \leq i,j \leq 3$. A two rounds encryption of $x \in \mathbb{F}_p^{4\times 4}$ under AES-prime using a key $k \in \mathbb{F}_p^{4\times 4}$ is $\mathcal{R}(\mathcal{R}(x+k)+k)$. We first compute

$$\begin{aligned}\mathcal{R}(k + \mathbb{F}_p e_{0,0}) &= \mathcal{R}\left(\begin{bmatrix} 0 & k_{0,1} & k_{0,2} & k_{0,3}\\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3}\\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3}\\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix} + \mathbb{F}_p \begin{bmatrix} 1&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0 \end{bmatrix}\right)\\ &= M \times \begin{bmatrix} S(0) & S(k_{0,1}) & S(k_{0,2}) & S(k_{0,3})\\ S(k_{1,1}) & S(k_{1,2}) & S(k_{1,3}) & S(k_{1,0})\\ S(k_{2,2}) & S(k_{2,3}) & S(k_{2,0}) & S(k_{2,1})\\ S(k_{3,3}) & S(k_{3,0}) & S(k_{3,1}) & S(k_{3,2}) \end{bmatrix} + \mathbb{F}_p \begin{bmatrix} 1&0&0&0\\ 1&0&0&0\\ 1&0&0&0\\ 1&0&0&0 \end{bmatrix}\end{aligned}$$

and therefore $\mathcal{R}(\mathcal{R}(k + \mathbb{F}_p e_{0,0}) + k) =$

$$\mathcal{R}\left(M \times \begin{bmatrix} S(0) & S(k_{0,1}) & S(k_{0,2}) & S(k_{0,3})\\ S(k_{1,1}) & S(k_{1,2}) & S(k_{1,3}) & S(k_{1,0})\\ S(k_{2,2}) & S(k_{2,3}) & S(k_{2,0}) & S(k_{2,1})\\ S(k_{3,3}) & S(k_{3,0}) & S(k_{3,1}) & S(k_{3,2}) \end{bmatrix} + \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3}\\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3}\\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3}\\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix} + \mathbb{F}_p \begin{bmatrix} 1&0&0&0\\ 1&0&0&0\\ 1&0&0&0\\ 1&0&0&0 \end{bmatrix}\right).$$

Thus, if

$$M \times \begin{bmatrix} S(0)\\ S(k_{1,1})\\ S(k_{2,2})\\ S(k_{3,3}) \end{bmatrix} + \begin{bmatrix} k_{0,0}\\ k_{1,0}\\ k_{2,0}\\ k_{3,0} \end{bmatrix} = \begin{bmatrix} u\\ u\\ u\\ u \end{bmatrix} \tag{9}$$

for some $u \in \mathbb{F}_p$, then $\mathcal{R}(\mathcal{R}(k+\mathbb{F}_p e_{0,0})+k)$ will be an affine subspace of dimension 1 (see Lemma 5). We have p choices for $u \in \mathbb{F}_p$, p^3 choices for $K_{1,1}, K_{2,2}, K_{3,3}$ (because S is a bijection) and p^9 for the other key variables that are not in the Equation (9). We thus enumerate p^{13} keys $k \in \mathbb{F}_p^{4\times 4}$ such that $\mathcal{R}(\mathcal{R}(k+\mathbb{F}_p e_{0,0})+k)$ is an additive coset of $\mathbb{F}_p e_{0,0}$.

Proposition 7 allows us to have a zero-sum integral distinguisher on five rounds of AES-prime, using only p data, provided that the key is chosen according to the condition specified in Theorem 4. The number of such keys is greater than or equal to p^{13} over a total of p^{16} possible keys based on Proposition 7 (see Example 3). A similar strategy can be applied to obtain a zero-sum integral distinguisher for six rounds, in which case p^4 data is sufficient. The following proposition is a direct use of Lemma 5.

Proposition 8. *Let $I \subset \{0,1,2,3\}$ such that $|I| = 1$. Then,*

$$\mathcal{R}(\mathcal{M}_I) = \mathcal{R}(0) + \mathcal{L}(\mathcal{M}_I).$$

Proof. If $|I| = 1$, then there is a vector basis of $\mathcal{M}_I$ having pairwise disjoint supports. The result follows from Lemma 5. □

Example 4. If we take $I = \{0\}$, i.e. $\mathcal{C}_I = Span_{\mathbb{F}_p}\{e_{0,0}, e_{1,0}, e_{2,0}, e_{3,0}\}$, then $\mathcal{M}_I$ has the following vectors as a basis:

$$m_1 := \begin{bmatrix} 1&0&0&0\\ 1&0&0&0\\ 1&0&0&0\\ 1&0&0&0 \end{bmatrix},\ m_2 := \begin{bmatrix} 0&1&0&0\\ 0&2&0&0\\ 0&4&0&0\\ 0&16&0&0 \end{bmatrix},\ m_3 := \begin{bmatrix} 0&0&1&0\\ 0&0&4&0\\ 0&0&16&0\\ 0&0&12&0 \end{bmatrix},\ m_4 := \begin{bmatrix} 0&0&0&1\\ 0&0&0&16\\ 0&0&0&2\\ 0&0&0&4 \end{bmatrix}$$

and it is clear that m_1, m_2, m_3 and m_4 have a pairwise disjoint support.

Remark 18. Since the S-box of the AES is not of the form $x^\alpha + c$ (See Lemma 5), Proposition 8 holds for AES-prime, but not for AES.

Theorem 5. *Let $K \to \{k_0, k_1, k_2, k_3, k_4, k_5, k_6\} \subset \mathbb{F}_p^{4\times 4}$ be the round keys, $x \in \mathbb{F}_p^{4\times 4}$, and $|I| = 1$. If*

$$k_2 + b \in \Gamma_{\mathcal{R}}(\mathcal{M}_I)$$

where b is such that $\mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x + \mathcal{D}_I) = b + \mathcal{M}_I$, then

$$\sum_{u \in \mathcal{D}_I} \mathcal{R}_{k_5} \circ \mathcal{R}_{k_4} \circ \mathcal{R}_{k_3} \circ \mathcal{R}_{k_2} \circ \mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x + u) = 0.$$

Proof. Let $x \in \mathbb{F}_p^{4\times 4}$. Since we have the exact subspace trail $\mathcal{D}_I \overset{\mathcal{R}}{\Rightarrow} \mathcal{C}_I \overset{\mathcal{R}}{\Rightarrow} \mathcal{M}_I$, there exists an element $b \in \mathbb{F}_p^{4\times 4}$ such that $\mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x + \mathcal{D}_I) = b + \mathcal{M}_I$. If $k_2 + b \in \Gamma_{\mathcal{R}}(\mathcal{M}_I)$, then $\mathcal{R}_{k_2} \circ \mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}(x + \mathcal{D}_I)$ is an affine subspace. Using Proposition 8, we have $|\Gamma_{\mathcal{R}}(\mathcal{M}_I)| \geq |\mathcal{M}_I| = p^4$. It follows from Theorem 3 that we can skip the first three rounds, and have a zero-sum integral distinguisher over the remaining three rounds for AES-prime. □

Example 5. We take $I = \{0\}$ as in Example 4. A two-round encryption of $x \in \mathbb{F}_p^{4\times 4}$ under a key $k \in \mathbb{F}_p^{4\times 4}$ by AES-prime's round function is $\mathcal{R}(\mathcal{R}(x+k)+k)$, and by taking $x \in \mathcal{D}_I$, the quantity $\mathcal{R}(\mathcal{R}(\mathcal{D}_I+k)+k)$ is an additive coset of $\mathcal{M}_I$. To apply Theorem 5, we need

$$\mathcal{R}(\mathcal{R}(\mathcal{D}_I+k)+k)+k = \mathcal{M}_I.$$

From [18, Lemma 1 and 2], we know that

$$\mathcal{R}(\mathcal{R}(\mathcal{D}_I+k)+k)+k = \mathcal{R}(\mathcal{R}(k)+k)+k+\mathcal{M}_I,$$

and, if $\mathcal{R}(\mathcal{R}(k)+k)+k \in \mathcal{M}_I$ then,

$$\mathcal{R}(\mathcal{R}(\mathcal{R}(\mathcal{D}_I+k)+k)+k) = \mathcal{R}(0)+\mathcal{L}(\mathcal{M}_I).$$

Thus, for at least N_I number of keys, we have a zero-sum integral distinguisher on six rounds of AES-prime, where N_I denotes the number of $k \in \mathbb{F}_p^{4\times 4}$ such that $\mathcal{R}(\mathcal{R}(k)+k)+k \in \mathcal{M}_I$.

AES-prime decryption round Here, we briefly give some integral properties of AES-prime decryption round function, since the algebraic degree of the decryption round is comparatively high (101) to the encryption round (5). We denote by $\bar{\mathcal{R}} := \bar{\mathcal{S}} \circ \bar{\mathcal{L}}$ the decryption round of AES-prime, where $\bar{\mathcal{S}} : \mathbb{F}_p^{4\times 4} \to \mathbb{F}_p^{4\times 4}$ is the S-box layer with S-box $\bar{S}(x) = (x-2)^{101}$ and $\bar{\mathcal{L}} = \mathcal{L}^{-1}$. AES-prime decryption round has the following exact complete subspace trail.

Proposition 9. *Let $\bar{\mathcal{R}} : \mathbb{F}_p^{4\times 4} \to \mathbb{F}_p^{4\times 4}$ be AES-prime decryption round. We have*

$$\mathcal{M}_I \overset{\bar{\mathcal{R}}}{\to} \mathcal{C}_I \overset{\bar{\mathcal{R}}}{\to} \mathcal{D}_I.$$

Proof. For any $a \in \mathbb{F}_p^{4\times 4}$, we have

$$\bar{\mathcal{R}}(a+\mathcal{C}_I) = \bar{\mathcal{S}} \circ \bar{\mathcal{L}}(a+\mathcal{C}_I) = \bar{\mathcal{S}}(\bar{\mathcal{L}}(a)+\bar{\mathcal{L}}(\mathcal{C}_I)) = \bar{\mathcal{S}}(\bar{\mathcal{L}}(a)+\mathcal{D}_I)$$

as $\mathcal{C}_I = \mathcal{L}(\mathcal{D}_I)$. Since an S-box acts independently on the coordinates, $\bar{\mathcal{S}}$ maps an additive coset of $\mathcal{D}_I$ to another additive coset of $\mathcal{D}_I$, therefore there exists $b \in \mathbb{F}_p^{4\times 4}$ such that $\bar{\mathcal{R}}(a+\mathcal{C}_I) = b+\mathcal{D}_I$. One can prove $\mathcal{M}_I \overset{\bar{\mathcal{R}}}{\to} \mathcal{C}_I$ exactly the same way as above. □

We also have a one dimensional subspace trails for $\bar{\mathcal{R}}$. More precisely, we have the following.

Proposition 10. *Let $\bar{\mathcal{R}} : \mathbb{F}_p^{4\times 4} \to \mathbb{F}_p^{4\times 4}$ be AES-prime decryption round. Then $\bar{\mathcal{R}}$ satisfies*

$$\mathbb{F}_p\mathcal{L}(e_{i,j}) \overset{\bar{\mathcal{R}}}{\to} \mathbb{F}_p e_{i,j}$$

where $\{e_{i,j} \mid 0 \le i,j \le 3\}$ be the set of unit vectors of $\mathbb{F}_p^{4\times 4}$ for all $0 \le i,j \le 3$.

Proof. For all $a \in \mathbb{F}_p^{4\times 4}$, we have

$$\bar{\mathcal{R}}(a + \mathbb{F}_p\mathcal{L}(e_{i,j})) = \bar{\mathcal{S}} \circ \bar{\mathcal{L}}(a + \mathbb{F}_p\mathcal{L}(e_{i,j})) = \bar{\mathcal{S}}(\bar{\mathcal{L}}(a) + \mathbb{F}_p e_{i,j}) \quad \forall\ 0 \leq i, j \leq 3.$$

Since $\bar{\mathcal{S}}$ acts independently on every coordinate, $\bar{\mathcal{S}}$ maps any additive coset of $\mathbb{F}_p e_{i,j}$ to another additive coset of $\mathbb{F}_p e_{i,j}$. This ends the proof. □

From the trails defined in this subsection and by using Theorem 3, we can get several zero-sum integrals on reduced-round AES-prime decryption. In particular, we have a 4-round AES-prime decryption distinguishers using p^4 data respectively. Applying the technique from Example 2,

$$\bar{\mathcal{R}}(\bar{\mathcal{R}}(\bar{\mathcal{R}}(\mathcal{R}(\mathcal{M}_I)) - k_\ell) - k_{\ell-1}) - k_{\ell-2}$$

will be a coset of $\mathcal{D}_I$. Using the algebraic degree argument, we get the following zero-sum integral distinguisher when $|I| = 1$,

$$\sum_{C \in \mathcal{R}(\mathcal{M}_I)} \bar{\mathcal{R}}(\bar{\mathcal{R}}(\bar{\mathcal{R}}(\bar{\mathcal{R}}(C) - k_\ell) - k_{\ell-1}) - k_{\ell-2}) - k_{\ell-3} = 0.$$

The same technique can be used for a one dimensional exact complete subspace trail to have a 3-round AES-prime decryption distinguisher using p data.

6 Conclusions

We presented a unified and generic approach to mount integral attacks against block ciphers based on exact subspace trails and higher order generalized derivatives. Our main idea was to use exact subspace trails to skip initial rounds and, provided some criteria on the algebraic degree of the last rounds, we obtained an integral distinguisher on the whole encryption scheme. We were able to explain or improve some of the previously known results on AES-like SPN ciphers. Moreover, our distinguisher provides a lower bound on the number of rounds for which a cipher remains vulnerable to the proposed integral attack.

This work also highlighted potential applications of generalized derivatives and higher order generalized derivatives in the context of encryption schemes. In particular, they helped to explain previously known results differently or with less data for specific key configurations.

Future work includes extending these results to any arbitrary subspace trails and not only the exact complete ones. Second, it would be interesting to develop new tools to analyse block ciphers by studying the properties of higher order generalized derivatives of functions. Additionally, we plan to investigate the possibility of applying these techniques to improve key recovery attacks.

References

1. Aumasson, J.P., Meier, W.: Zero-sum distinguishers for reduced keccak-f and for the core functions of luffa and hamsi. rump session of Cryptographic Hardware and Embedded Systems-CHES **2009**, 67 (2009)

2. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A block cipher for low energy. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 411–436. Springer (2015)
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: Annual international cryptology conference. pp. 123–153. Springer (2016)
4. Beyne, T., Canteaut, A., Dinur, I., Eichlseder, M., Leander, G., Leurent, G., Naya-Plasencia, M., Sasaki, Y., Todo, Y., Wiemer, F.: Out of oddity – new cryptanalytic techniques against symmetric primitives optimized for integrity proof systems. In: Advances in Cryptology – CRYPTO 2020 – 40th Annual International Cryptology Conference, Proceedings. Lecture Notes in Computer Science, vol. 12172, pp. 299–328. Springer (2020). https://doi.org/10.1007/978-3-030-56877-1_11, https://doi.org/10.1007/978-3-030-56877-1_11
5. Beyne, T., Verbauwhede, M.: Integral cryptanalysis in characteristic p. In: Hanaoka, G., Yang, B.Y. (eds.) Advances in Cryptology – ASIACRYPT 2025. LNCS, vol. 16245, pp. 66–96. Springer Nature Singapore (2026). https://doi.org/10.1007/978-981-95-5018-0_3, artifact available at https://artifacts.iacr.org/asiacrypt/2025/a3
6. Boeuf, A., Canteaut, A., Perrin, L.: Propagation of subspaces in primitives with monomial sboxes: Applications to rescue and variants of the aes. IACR Transactions on Symmetric Cryptology **2023**(4), 270–298 (Dec 2023). https://doi.org/10.46586/tosc.v2023.i4.270-298, https://tosc.iacr.org/index.php/ToSC/article/view/11288
7. Boura, C., Canteaut, A., Coggia, D.: A general proof framework for recent aes distinguishers. IACR Transactions on Symmetric Cryptology **2019**(1), 170–191 (2019)
8. Bouvier, C., Canteaut, A., Perrin, L.: On the algebraic degree of iterated power functions. Des. Codes Cryptogr. **91**(3), 997–1033 (2023)
9. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher square. In: Biham, E. (ed.) Fast Software Encryption – FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer (1997)
10. Daemen, J., Rijmen, V.: AES proposal: Rijndael (1999)
11. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography, Springer, Berlin, Heidelberg (2002)
12. Dunkelman, O., Ghosh, S., Keller, N., Leurent, G., Marmor, A., Mollimard, V.: Partial sums meet fft: improved attack on 6-round aes. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 128–157. Springer (2024)
13. Dziembowski, S., Faust, S., Skórski, M.: Optimal amplification of noisy leakages. In: Kushilevitz, E., Malkin, T. (eds.) Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9563, pp. 291–318. Springer (2016). https://doi.org/10.1007/978-3-662-49099-0_11, https://doi.org/10.1007/978-3-662-49099-0_11
14. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.: Improved cryptanalysis of rijndael. In: Fast Software Encryption (FSE). pp. 213–230. Springer (2000)

15. Gong, Z., Nikova, S., Law, Y.W.: Klein: a new family of lightweight block ciphers. In: International workshop on radio frequency identification: security and privacy issues. pp. 1–18. Springer (2011)
16. Grassi, L.: Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced aes. IACR Transactions on Symmetric Cryptology pp. 133–160 (2018)
17. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round aes. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 289–317. Springer (2017)
18. Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to aes. IACR Transactions on Symmetric Cryptology **2016**(2), 192–225 (2016). https://doi.org/10.13154/tosc.v2016.i2.192-225, https://doi.org/10.13154/tosc.v2016.i2.192-225
19. Grassi, L., Rechberger, C., Schofnegger, M.: Proving resistance against infinitely long subspace trails: How to choose the linear layer. IACR Transactions on Symmetric Cryptology pp. 314–352 (2021)
20. Hebborn, P., Lambin, B., Leander, G., Todo, Y.: Lower bounds on the degree of block ciphers. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 537–566. Springer (2020)
21. Knudsen, L., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) Fast Software Encryption. pp. 112–127. Springer Berlin Heidelberg, Berlin, Heidelberg (2002)
22. Leander, G., Abdelraheem, M.A., AlKhzaimi, H., Zenner, E.: A cryptanalysis of printcipher: The invariant subspace attack. In: Annual Cryptology Conference. pp. 206–221. Springer (2011)
23. Leander, G., Tezcan, C., Wiemer, F.: Searching for subspace trails and truncated differentials. IACR Transactions on Symmetric Cryptology pp. 74–100 (2018)
24. Liu, W., Yang, Y.: The 7-round subspace trail-based impossible differential distinguisher of midori-64. Security and Communication Networks (2021)
25. Masure, L., Méaux, P., Moos, T., Standaert, F.X.: Effective and efficient masking with low noise using small-mersenne-prime ciphers. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 596–627. Springer (2023)
26. Nyberg, K.: Differentially uniform mappings for cryptography. 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. 55–64. Springer (1993). https://doi.org/10.1007/3-540-48285-7_6, https://doi.org/10.1007/3-540-48285-7_6
27. Özbudak, F., Salagean, A.: New generalized almost perfect nonlinear functions. Finite Fields Their Appl. **70**, 101796 (2021). https://doi.org/10.1016/J.FFA.2020.101796, https://doi.org/10.1016/j.ffa.2020.101796
28. Salagean, A., Özbudak, F.: Further constructions and characterizations of generalized almost perfect nonlinear functions. Cryptogr. Commun. **15**(6), 1117–1127 (2023). https://doi.org/10.1007/S12095-023-00647-1, https://doi.org/10.1007/s12095-023-00647-1
29. Todo, Y.: Structural evaluation by generalized integral property. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015. LNCS, vol. 9056, pp. 287–314. Springer (2015)

30. Winter, R., Salagean, A., Phan, R.C.W.: Comparison of cube attacks over different vector spaces. In: Groth, J. (ed.) Cryptography and Coding. pp. 225–238. Springer International Publishing, Cham (2015)