Multi-Diagonal Truncated Differentials and Ciphertext-Only Attacks on Reduced-Round AES

Orhun Kara[1,2] and Can Balıkçı[1]

[1] Department of Mathematics, İzmir Institute of Technology, Gulbahce Campus, İzmir, Türkiye
[2] Computational Sciences and Engineering, İzmir Institute of Technology, Gulbahce Campus, İzmir, Türkiye

orhunkara@iyte.edu.tr, canbalikci@iyte.edu.tr

Abstract. We present the first ciphertext-only distinguishing attack on 5-round AES and a key-recovery attack on 6-round AES for all key sizes under ASCII-encoded English-language plaintext distributions, as well as additional ciphertext-only results under uniform ASCII distributions.

Our attacks are enabled by a new analytical framework for estimating truncated differential probabilities in 5-round AES, a problem that remains largely unresolved beyond restricted configurations. Existing approaches, relying on statistical sampling, integral cryptanalysis, or differential distribution tables of super S-boxes, are primarily limited to settings with a single active diagonal in the plaintext and a single passive inverse diagonal in the ciphertext. Our method extends this line of work by providing analytical estimates over a substantially broader range of configurations.

We construct this framework by combining precise computations of MDS-level transition probabilities with a systematic enumeration of truncated differential characteristic classes. By organizing characteristics into equivalence classes defined by diagonal propagation patterns, we enable structured aggregation of probability contributions. This approach captures configurations with a single active diagonal in the plaintext and arbitrary passive inverse diagonals in the ciphertext, as well as the complementary setting involving multiple active diagonals in the plaintext and a single passive inverse diagonal in the ciphertext.

Our results are validated through independent derivations, consistency checks against prior work, and computer-aided enumeration. More broadly, the framework offers a systematic approach to truncated differential analysis of AES and potentially other AES-like SPN ciphers.

Keywords: Ciphertext-only attack, Differential attack, Cryptanalysis, Truncated differential attack, Block cipher, AES, SPN cipher, DDT

1 Introduction

Block ciphers are fundamental to modern cryptography and serve as essential components in a wide range of cryptographic constructions, including message authentication codes and hash functions. Among them, the Advanced Encryption Standard (AES), standardized by NIST [15], is one of the most widely deployed symmetric

encryption algorithms. It is used in protocols such as TLS, GSM-5G, and WPA, as well as in applications such as file encryption and secure messaging (e.g., WhatsApp).

AES has undergone extensive cryptanalysis over more than 25 years. Various distinguishing techniques have been proposed, many of which form the foundation of key recovery attacks. Among the earliest and most studied approaches are Square [16], Meet-in-the-Middle (MITM) [12, 13], biclique [8], and zero-difference attacks [3].

Differential cryptanalysis, introduced by Biham and Shamir [7], remains one of the most powerful tools in the arsenal of cryptanalysts. Several extensions have since been developed, including impossible differentials [6], truncated and higher-order differentials [22], boomerang attacks [31], and differential-linear attacks [23].

AES is believed to resist differential-type attacks in its full-round form, but a variety of significant results exist for reduced-round variants. One major line of work is truncated differential cryptanalysis. Grassi et al. [20] introduced the "multiple-of-8" distinguisher for 5-round AES, the first construction that exploits a structural invariant across inverse diagonals. However, its extension to key recovery and more rounds is limited by the need to recover the final-round subkey. Bao et al. [2] proposed an integral-based truncated distinguisher for 5-round AES using a structured plaintext with a single active byte, revealing a passive inverse diagonal and exploiting non-uniform behavior in the fourth round. This leads to both a 5-round distinguisher and a 6-round key recovery attack, but relies on a specific input structure.

Here, a diagonal refers to the image of a column under the inverse `ShiftRows` operation of AES, while an inverse diagonal refers to the image of a column under the `ShiftRows` operation (see Figure 1). The `ShiftRows` operation denotes the standard cyclic row permutation used in AES.

Mixture differential cryptanalysis [17] builds on subspace mixing ideas to construct a 4-round distinguisher and extend it to 5 and 6 rounds via a truncated differential step. Although it enables a 6-round key recovery attack, its reliance on a single appended round limits further scalability.

The exchange attack [4] exploits column and diagonal symmetries to construct exchange-invariant plaintext sets, yielding a key-independent distinguisher up to 6-round AES. While it achieves a statistically detectable bias over exchange structures, its design does not naturally extend beyond six rounds due to its reliance on a single exchange step.

1.1 Problem statement and limitations of existing approaches

A central feature of truncated differential cryptanalysis of AES is that it abstracts away the exact byte values of active differences, focusing instead on whether each byte is active or passive across rounds. In this model, both the input and output difference values of an active byte are ignored, and the analysis tracks only the propagation pattern of being active or passive within a truncated differential characteristic.

While the computation of probabilities for such characteristics over multiple rounds is well understood, these values provide a coarse approximation of the true differ-

ential behavior. In particular, they yield lower bounds on the corresponding differential probabilities and have not, in the settings considered in the literature, led to distinguishers beyond four rounds of AES.

In contrast, the computation of full truncated differential probabilities is substantially more complex. It requires accounting for the combinatorial structure of all involved characteristics, rather than focusing on a single one. This introduces significant analytical and computational challenges and necessitates techniques beyond standard truncated differential modeling.

Three main approaches have been proposed for computing 5-round truncated differential probabilities of AES. The first is a statistical sampling approach introduced by Grassi and Rechberger [18], which estimates expectations and variances of certain truncated differentials by combining random variables. The second is the method of Bao et al. [2], which extends an integral distinguisher to compute probabilities of a different class of truncated differentials by exploiting high collision probabilities of functions with a balanced property. The third is the approach of Chang et al. [10], which defines 32×8 and 32×16 super S-boxes derived from 2-round AES structures and introduces algorithms for computing their differential distribution tables (DDTs).

A key structural property of 2-round AES is that a passive diagonal in the plaintext difference leads to a passive column after one round, which in turn gives rise to a passive inverse diagonal (see the second part of Lemma 2 and Figure 4). This behavior underpins several cryptanalytic techniques, including impossible differential [25], truncated differential [2], mixture [17], exchange [4], and subspace-invariant attacks [20].

Motivated by this property, a central question in truncated differential cryptanalysis is the following: given a plaintext pair with m **active** bytes confined to a single diagonal, what is the probability that i specified inverse diagonals are **passive** at the output of 5-round AES, while the remaining inverse diagonals are unrestricted? We denote this probability by $\chi(m \to i^+)$. Here, the superscript $+$ is introduced to indicate that at least i inverse diagonals are passive. We illustrate this notation through four examples in Figure 2 for $\chi(3 \to 2^+)$, where the first two inverse diagonals are specified to be passive.

Despite its central role in AES cryptanalysis, the problem of computing $\chi(m \to i^+)$ for general parameters m and i remains only partially understood even for 5-round AES. To date, only a small number of works have addressed restricted instances for 5-round AES, and its extension to higher rounds remains only partially explored.

Grassi and Rechberger [18] provide a partial result for $i = 1$, presenting a weighted average over m that approximates the scenario with $m = 4$ active bytes in a diagonal. More precisely, they compute the probability that a diagonal is active in a plaintext pair without specifying the exact number of active bytes within that diagonal, which yields a rough estimate for $\chi(4 \to 1^+)$.

Bao et al. [2] consider only the case $m = i = 1$ (i.e., $\chi(1 \to 1^+)$) by extending the integral distinguisher for a single active byte in the plaintext, where activeness is defined as the byte taking all possible values (see Proposition 1).

Chang et al. [10] study the same problem considered by Bao et al. and introduce algorithms for computing the DDTs of specific super S-boxes. Using these techniques, they first compute 4-round differentials whose plaintexts contain a single active byte and whose ciphertexts contain one or two passive bytes at specified positions, while all remaining bytes are unrestricted. By extending these differentials by one round, they obtain $\chi(1 \to 1^+)$ and $\chi(1 \to 2^+)$.

Chang et al. exploit the amplified bias in the conditional probability $\frac{\chi(1\to 2^+)}{\chi(1\to 1^+)}$ in their 5-round truncated differential distinguisher and extend the underlying differential structure by one additional round to obtain a 6-round characteristic. Notably, the bias is positive for $\chi(1 \to 1^+)$ and negative for $\chi(1 \to 2^+)$ (see Figure 6).

Two related and more challenging problems arise when we retain the same plaintext difference condition, namely a plaintext pair with exactly one active diagonal, and modify the condition on the ciphertext differences for 5-round AES. The first problem concerns the probability that **at least** i inverse diagonals remain passive, denoted $\Pr[m \to i^+]$. The second concerns the probability that **exactly** i inverse diagonals remain passive, denoted $\Pr[m \to i]$. We illustrate example cases for $\Pr[3 \to 2]$ and $\Pr[3 \to 2^+]$ in Figure 2.

The literature on these questions remains limited. Bao et al. [2] provide a rough estimate of $\Pr[1 \to 1^+]$, which yields an upper bound for $\Pr[1 \to 1]$ in 5-round AES. Grassi and Rechberger [18] propose a similar ad hoc approach for $\Pr[4 \to 1^+]$, based on a weighted average over m to approximate the case $m = 4$; their method ignores joint probabilities and instead multiplies the probability that a given inverse diagonal is passive while the others are active by four (see Remark 1). Rønjom [27] recomputes both $\Pr[1 \to 1^+]$ and $\Pr[4 \to 1^+]$ using a weight-transition probability matrix.

We revisit these probabilities and derive refined analytical estimates using our framework, thereby extending the existing results (see the third part of Theorem 1).

Another direction for extending the results of Grassi and Rechberger [18], Bao et al. [2], Chang et al. [10], and Rønjom [27] is to consider the number of active diagonals in plaintext pairs for 5-round AES. We address the problem of computing truncated differential probabilities when more than one diagonal in the plaintext pair is active.

To formalize this setting, we introduce the notation $\Pr[i \Rightarrow m]$ and study the corresponding probability distributions. Specifically, for a plaintext pair that is active in i specified diagonals and passive in the remaining diagonals, $\Pr[i \Rightarrow m]$ denotes the probability that the corresponding ciphertext pair has exactly one active inverse diagonal, containing exactly m passive bytes. We derive these probabilities within our framework.

Moreover, when a plaintext pair contains m_1 and m_2 active bytes in two active diagonals, we study the associated truncated differential probabilities under the same framework. In particular, we compute the probability that the corresponding ciphertext pair has three passive inverse diagonals and one active inverse diagonal, with the passive bytes in the active inverse diagonal distributed across a specified set of j columns.

The statistical sampling approach of Grassi and Rechberger [18], the byte-permutation summation method based on integral techniques proposed by Bao et al. [2], and the computation of differential distribution tables (DDTs) of super S-boxes by Chang et al. [10] primarily focus on specific classes of truncated differential distinguishers associated with particular input structures, due to the inherent limitations of these methods.

In contrast, our analytical framework enables more flexible probability computations and allows the systematic derivation of a broader range of truncated differential distinguishers. An important consequence of this framework is that it naturally supports ciphertext-only cryptanalysis in the truncated differential setting.

We consider two plaintext models in Electronic Codebook (ECB) mode: natural English encoded in ASCII, and sequences of independent uniformly distributed ASCII-encoded bytes. In both settings, we construct the first ciphertext-only distinguisher for 5-round AES and the first ciphertext-only key-recovery attack on 6-round AES under such plaintext assumptions. Further details are provided in Section 1.2.

ECB is commonly used as a canonical abstraction in cryptanalytic analysis to isolate the behavior of the underlying block cipher independently of mode-specific transformations. Our results concern the permutation structure of AES and are not intended to model practical deployment scenarios.

1.2 Expanded overview of our contributions

Building on our analytical framework, we refine and extend 5-round truncated differential distinguishers to previously unexplored configurations, leading to new attacks on reduced-round AES. Our approach enables flexible probability computations and the systematic derivation of a broader class of truncated differentials within a unified analytical setting.

Primary contributions and insights:

- **A general analytical framework:** Existing distinguishers rely on frequency deviations within specific subspaces, permutation-sum techniques, or algorithms for computing the DDTs of super S-boxes, which may limit scalability.

  We introduce a flexible and general analytical framework for estimating truncated differential probabilities across AES rounds.

  By combining transition probabilities at the level of the AES diffusion layer with an exhaustive enumeration of truncated differential characteristics sharing identical probabilities, our framework yields accurate analytical estimates across a broader class of configurations.

- **Revisiting and extending 5-round truncated differentials:** Our results, summarized in Theorem 1, both confirm and substantially extend prior work of Grassi and Rechberger [18], Bao et al. [2], and Chang et al. [10]. We extend the analysis to **13 additional** (m, i) **configurations** for $\chi(m \to i^+)$ beyond the previously studied cases $\chi(4 \to 1^+)$, $\chi(1 \to 1^+)$, and $\chi(1 \to 2^+)$. Furthermore, all **16 cases** (m, i) for $\Pr[m \to i]$ are derived for the first time. For $\Pr[m \to i^+]$,

Property	Rounds	Data	Type	Cost	Ref.
Yoyo	5	$2^{26.8}$	ACC	$2^{24.8}$ XOR + $2^{26.8}$ MA	[28]
Yoyo**	5	$2^{30.65}$	ACC	$2^{28.65}$ XOR + $2^{30.65}$ MA	[26]
Truncated Differential	5	2^{68}	CP	$2^{73.3}$ MA	[2]
Truncated Differential	5	$2^{42.59}$	CP	$2^{42.91}$ E	[10]
Prob. Mixture Diff.	5	2^{55}	CP	$2^{71.5}$ M $\approx 2^{64.9}$ E	[21]
Trun. Dif. via Mean	5	$2^{48.96}$	CP	$2^{52.6}$ M $\approx 2^{46}$ E	[18]
Multiple-8	5	2^{32}	CP	$2^{35.6}$ M $\approx 2^{29}$ E	[20]
Exchange Attack	5	2^{30}	CP	2^{30} E	[4]
Truncated Differential	5	$2^{86.4}$	C-O	$2^{92.8}$ MA	Section 6.1
Truncated Differential	5	$2^{96.5}$	C-O*	$2^{103.1}$ MA	Section 6.1
Yoyo	6	$2^{123.8}$	ACC	$2^{122.8}$ XOR + $2^{123.8}$ MA	[28]
Yoyo**	6	$2^{129.15}$	ACC	$2^{128.15}$ XOR + $2^{129.15}$ MA	[26]
Truncated Differential	6	$2^{89.43}$	CP	$2^{96.52}$ MA	[2]
Zero Difference	6	$2^{122.8}$	ACC	$2^{121.8}$ XOR	[28]
Exchange Attack	6	$2^{88.2}$	CP	$2^{88.2}$ E	[4]
Truncated Boomerang	6	2^{87}	ACC	2^{87} E	[5]
Boomerang Chain	6	$2^{76.57}$	ACPC	$2^{76.57}$ E	[32]
Truncated Differential	6	$2^{62.88}$	ACPC	$2^{63.42}$ E	[10]

Table 1: Secret-Key Truncated Differential Distinguishers for 5- and 6-Round AES. The data are given in terms of chosen plaintext/ciphertext (CP/CC), adaptive chosen plaintext/ciphertext (ACP/ACC), adaptively chosen plaintexts and ciphertexts (ACPC), ciphertext-only (C-O) (English-ASCII plaintext in ECB mode), or ciphertext-only (C-O)* (uniform-ASCII plaintext in ECB mode). The time complexity is in encryptions (E), memory accesses (MA), or XOR operations (XOR). Values marked with "**" are the corrected versions of the values reported in [28].

we refine previously known estimates and provide solutions for **14 additional configurations**, yielding accurate analytical results for 5-round AES.

– **Extension to multiple active diagonals:** Prior work is restricted to plaintext pairs with a single active diagonal. We extend the analysis to configurations with multiple active diagonals, thus capturing the joint propagation behavior induced by the AES diffusion layer.

Our framework can be formulated in the decryption direction of AES and combined with the symmetry of AES induced by the omission of the `MixColumns` operation in the last round. As an application, in Theorem 3, we compute $\Pr[i \Rightarrow m]$ for $i \in \{1, 2, 3, 4\}$ and $m \in \{0, 1, 2, 3\}$, denoting the probability that exactly m bytes are passive within a fixed inverse diagonal, given a plaintext pair with i active diagonals.

We further analyze structured multi-diagonal settings (Theorems 2 and 4), including configurations with (m_1, m_2) active bytes distributed across two di-

agonals. This leads to the identification of **72 new truncated differentials** for 5-round AES, all arising from previously unexplored multi-diagonal configurations.

– **Verification and consistency:** Our results are supported by multiple layers of validation. First, key statements are independently derived through alternative analytical arguments. Second, our results are consistent with all previously known special cases in the literature. Third, we perform a computer-assisted enumeration to validate local transition behavior and selected global probability computations. Consistency across independent analytical derivations and computational methods provides supporting evidence for the correctness of our results.

  We also verify parts of Theorem 1 by providing an alternative proof for each part in Section 4.3, and we verify the common input and output pair scenarios of Theorems 1, Theorem 2, Theorem 3, and Theorem 4 against each other in Section 5.1. Moreover, the fact that two different methods of computing our probabilities yield the same results can be considered a partial verification of our calculations.

– **Ciphertext-only cryptanalysis:** We construct a distinguisher for 5-round AES and a key-recovery attack on 6-round AES using truncated differentials with multiple active diagonals. Our analysis considers ASCII-encoded English plaintexts for all key sizes, as well as uniformly distributed ASCII plaintexts for AES-192 and AES-256, both in ECB mode.

  The uniform-ASCII model assumes that plaintext bytes are drawn uniformly at random over the ASCII alphabet prior to encryption, yielding a conservative baseline with minimal statistical structure. Under this model, the resulting ciphertext distributions are less biased than those arising from natural language, making our attacks applicable beyond language-dependent settings.

  Our attacks rely on the observation that the overall bias in the ciphertext-only setting is jointly determined by the distribution of active diagonals in plaintext pairs and the structural redundancies inherent in natural-language plaintexts encoded in ASCII, which amplify deviations from the random-permutation model. When these effects are considered together, the dominant contribution to the bias arises from plaintext pairs containing exactly one passive diagonal. In this case, the structural redundancy and the differential behavior reinforce each other, leading to the largest deviation from the random-permutation baseline. Consequently, this case provides the main contribution to the distinguisher in Equation 10 for $i = 3$. Our ciphertext-only attacks exploit this combined mechanism.

  The complexities of the distinguishing attacks, including prior work and our construction, are summarized in Table 1. For English-ASCII plaintexts, the time complexity of our 6-round attack is $2^{113.4}$ additions for AES-128 and AES-192, and 2^{131} encryptions for AES-256. The corresponding data complexity is $2^{99.2}$ ciphertexts, and the memory complexity is $2^{106.4}$ bytes.

  Under the uniform-ASCII assumption, the time complexity of the same attack is $2^{133.6}$ additions for AES-192 and 2^{131} encryptions for AES-256. The data

complexity is $2^{109.3}$ ciphertexts, and the memory complexity is $2^{126.6}$ bytes. The complexity does not improve over brute-force search for AES-128.

All probability computations and resulting attacks are derived within the heuristic framework commonly used in truncated differential cryptanalysis. In particular, we adopt the standard independence assumption across rounds for truncated differential probabilities. Under this approximation, the propagation of active–passive patterns through successive rounds is treated as approximately independent for the purpose of probability estimation, as is customary in the analysis of AES and related SPN ciphers. Further details on these modeling assumptions are discussed in Section 2.2.

Within this framework, our approach combines precise transition probabilities at the level of the `MixColumns` operation with exhaustive enumeration of all contributing truncated differential characteristics, yielding analytical estimates that refine prior results under the same assumption.

We illustrate the truncated differential probabilities relative to the corresponding random-permutation probabilities, as well as their deviations from 1 in Figures 6, 8 and Tables 2, 3. Normalization by the corresponding random-permutation probabilities makes the distinguishing effect directly visible, while deviations from 1 provide a convenient representation of the bias magnitude. These visualizations illustrate how the truncated differential probabilities vary from the random-permutation case across different parameter configurations.

The data complexities of our attacks are computed independently of these visualizations by applying standard distinguishing formulas to the corresponding truncated differential and random-permutation probabilities, following the methodology of [29]. In particular, Equation 13 is used throughout the attack analysis to estimate the required data complexity.

Paper organization. Section 2 introduces AES, notation, and assumptions. Section 3 reviews prior results in our notation and shows that they can be recovered within our framework for the case of a single active diagonal in the input and a single passive inverse diagonal in the output. Section 4 extends these results to the case of a single active diagonal and multiple passive inverse diagonals, while Section 5 further generalizes the framework to an arbitrary number of active diagonals with a single passive inverse diagonal. Section 6 describes the ciphertext-only attacks. Section 7 concludes the paper with future work and open problems.

2 A short definition of AES, notation and assumptions

In this section, we provide a short description of AES and introduce our notation, which we utilize throughout the paper.

2.1 Definition of AES

AES (Advanced Encryption Standard) is defined by the NIST FIPS 197 standard [15]. We briefly introduce the fundamental building blocks of the cipher; its design philosophy is described in detail in [11]. The AES encryption algorithm has a block length of 128 bits and three different variants corresponding to key lengths of 128,

192, and 256 bits. These variants use 10, 12, and 14 rounds, respectively. The internal states are represented as 4×4 matrices of bytes. The round functions are described below:

`SubBytes` (SB): A byte-level transformation in which a nonlinear S-box maps each 8-bit input to an 8-bit output.

`ShiftRows` (SR): A linear transformation that rotates row-i to the left by i bytes (for $i = 0, 1, 2, 3$).

`MixColumns` (MC): A linear operation defined by a 4×4 matrix multiplication over $GF(2^8)$: each column of the state is multiplied by the `MixColumns` matrix.

`AddRoundKey` (AK): XOR the state with the round key.

The inverses of the operations SB, SR, and MC are denoted as SB^{-1}, SR^{-1}, and MC^{-1}, respectively. First, the plaintext is XORed with the *whitening key*. In the final round, the `MixColumns` (MC) operation is omitted. Let us denote the i-th column of the j-th subkey RK_j by $KW\{4j + i - 1\}$. RK_0 is the whitening key. Then, the columns $KW\{k\}$ can be computed as follows:

$$\begin{cases} KW\{k-N\} \oplus f\big(KW\{k-1\}\big) \oplus r\{k \text{ div } N\}, & \text{if } k \bmod N = 0, \\ KW\{k-N\} \oplus g\big(KW\{k-1\}\big), & \text{if } k \bmod N = 4 \text{ and } N = 8, \\ KW\{k-N\} \oplus KW\{k-1\}, & \text{otherwise.} \end{cases}$$

where $N = 4, 6, 8$ for 128-, 192-, and 256-bit key lengths, respectively. The functions f and g are specific nonlinear permutations in a column, and $r\{k\}$ is constant for $k \in \{0, 1, \ldots, 43/51/59\}$.

Fig. 1: Illustration of the diagonal and inverse diagonal byte positions in an AES state. The green, yellow, purple, and orange colors represent the bytes in the first, second, third, and fourth diagonals and inverse diagonals, respectively.

2.2 Our notation and assumptions

k-bit r-round AES is referred to as r-round AES-k. There is no MC operation in the r-th round. Plaintext, ciphertext, and key are denoted by P, C, and K, respectively. The outputs of the AK, SB, SR, and MC operations in the i-th round are represented by AK_i, SB_i, SR_i, and MC_i, respectively. Additionally, the difference of a pair is represented by Δ. That is, ΔP and ΔC represent the plaintext

difference and ciphertext difference, respectively, while ΔAK_i, ΔSB_i, ΔSR_i and ΔMC_i denote the difference of the pair at the outputs of AK_i, SB_i, SR_i and MC_i, respectively. The bytes of a state are represented by $[\cdot]$. For example, the outputs of the MC operation in the second round for bytes that are located in the second and third positions are denoted as $MC_2[1,2]$. Byte numbers are arranged as follows: 0, 1, 2, and 3 in the first column; 4, 5, 6, and 7 in the second column; 8, 9, 10, and 11 in the third column; and 12, 13, 14, and 15 in the last column. The byte positions corresponding to the diagonals and inverse diagonals are illustrated in Figure 1.

A byte in a pair is considered active if there is a non-zero difference between two components of the pair and passive if both components have the same value at that byte position. A vector $V = (v_0, v_1, v_2, v_3)$ can be a column, a row, a diagonal (SR^{-1} of a column), or an inverse diagonal (SR of a column). A vector (of a pair) is active if it contains at least one active byte and fully active if all its bytes are active. A vector is passive if all its bytes are passive.

As usual, $\binom{n}{j}$ denotes the binomial coefficient, defined as $\binom{n}{j} = \dfrac{n!}{j!(n-j)!}$ where ! is the factorial notation. We define the function

$$\delta_m = \begin{cases} 1, & \text{if } m > 0, \\ 0, & \text{if } m \leq 0 \end{cases}$$

for the integer value $m \in \mathbb{Z}$ in our probability computations. We denote the minimum of i and j by $\min\{i, j\}$.

We note that, in all our probability computations, we always consider the number of **passive bytes** or **passive inverse diagonals** in the outputs, as counting passiveness in the output is more straightforward.

$P_{i,j}$: The probability that i active bytes in a column produce j passive bytes at specific positions and $4 - j$ active bytes at the other positions through the MC operation. Since this probability does not depend on the actual positions, we do not specify them in our notation. In general, we omit positions in the probabilities whenever they have no effect.

P_{i,j^+}: The probability that i active bytes in a column produce passive bytes at specific j positions through the MC operation, and the remaining bytes can be either passive or active. Note that $P_{i,0^+} = 1$ by definition.

$\Pr[m \to i]$: Let m bytes in one given diagonal be active, and the remaining bytes be passive, for a given pair of plaintexts, where $m \in \{1, 2, 3, 4\}$. Then, the probability that exactly i inverse diagonals are passive and the remaining $4 - i$ are active in the corresponding ciphertext pair after 5 rounds of AES encryption is denoted by $\Pr[m \to i]$ for $0 \leq i \leq 3$.

$\Pr[m \to i^+]$: Let m bytes in one given diagonal be active, and the remaining bytes be passive, for a given pair of plaintexts, where $m \in \{1, 2, 3, 4\}$. Then, the probability that at least i inverse diagonals are passive in the corresponding ciphertext pair after 5 rounds of AES encryption is denoted by $\Pr[m \to i^+]$ for $0 \leq i \leq 3$.

$\chi(m \to i^+)$: Let m bytes in one given diagonal be active, and the remaining bytes be passive, for a given pair of plaintexts, where $m \in \{1, 2, 3, 4\}$. Then, the probability that given i inverse diagonals are passive after 5 rounds of AES encryption is denoted by $\chi(m \to i^+)$ for $0 \leq i \leq 3$.

Note that the probability for $i = 0$ is 1 by definition. This corresponds to the case where no condition is imposed on the ciphertext pair. That is, $\chi(m \to 0^+) := 1$ for any m.

Figure 2 shows some example scenarios for a given (m, i) pair under the notations $\Pr[m \to i]$, $\Pr[m \to i^+]$, and $\chi(m \to i^+)$.

$\Pr[i \Rightarrow m]$: Assume that i given diagonals of a plaintext pair are active and the other diagonals are passive. Then, the probability that the corresponding ciphertext pair for 5-round AES has given three passive inverse diagonals and one active inverse diagonal, with exactly m passive bytes in that active inverse diagonal is denoted by $\Pr[i \Rightarrow m]$.

$SB^{in}_{out}(\alpha[i_1, \ldots, i_j], \beta)$: The set of all pairs in byte positions $i_1, i_2, \ldots, i_j$ of the `SubBytes` operation that produce the given input $\alpha[i_1, \ldots, i_j]$ and output difference $\beta[i_1, \ldots, i_j]$ in the positions $[i_1, \ldots, i_j]$.

$SB^{in}_{out}(\alpha[i_1, \ldots, i_j], \beta) = \bigotimes_{\ell=1}^{j} SB^{in}_{out}(\alpha[i_\ell], \beta)$, for an input–output difference of the `SubBytes` operation at positions $i_1, i_2, \ldots, i_j$, where $\bigotimes$ denotes the tensor product of the vectors. For any fixed position i, the set $SB^{in}_{out}(\alpha[i_\ell], \beta)$ is either empty or contains 2 or 4 elements, as determined by the S-box DDT. Then, $SB^{in}_{out}(\alpha[i_1, \ldots, i_j], \beta)$ is empty if and only if at least one of the $SB^{in}_{out}(\alpha[i_\ell], \beta)$ is empty.

Our assumptions We follow the standard modeling framework used in the analysis of AES and related SPN ciphers, in which round-to-round differences and internal column-wise differences are assumed not to introduce significant systematic dependencies that would bias probability computations.

At the S-box level, we adopt the commonly used single S-box modeling hypothesis. For a fixed non-zero input difference ΔX, if X is sampled uniformly at random among values consistent with ΔX, then the solutions of

$$SB(X) \oplus SB(X \oplus \Delta X) = \Delta Y \tag{1}$$

are modeled using the standard per-S-box transition probabilities induced by the AES differential distribution table. This approximation, which captures the known non-uniformities of the S-box, is widely used and supported empirically in prior work, including [18, 2].

Across distinct S-boxes, we treat difference outcomes as approximately independent for the purpose of probability estimation, as is standard in truncated differential analyses. This abstraction neglects dependencies induced by the linear layer that are difficult to track analytically, but enables tractable aggregation of probabilities across rounds.

Under these assumptions, probabilities of round transitions are combined within the usual heuristic framework of truncated differential analysis. In particular, we

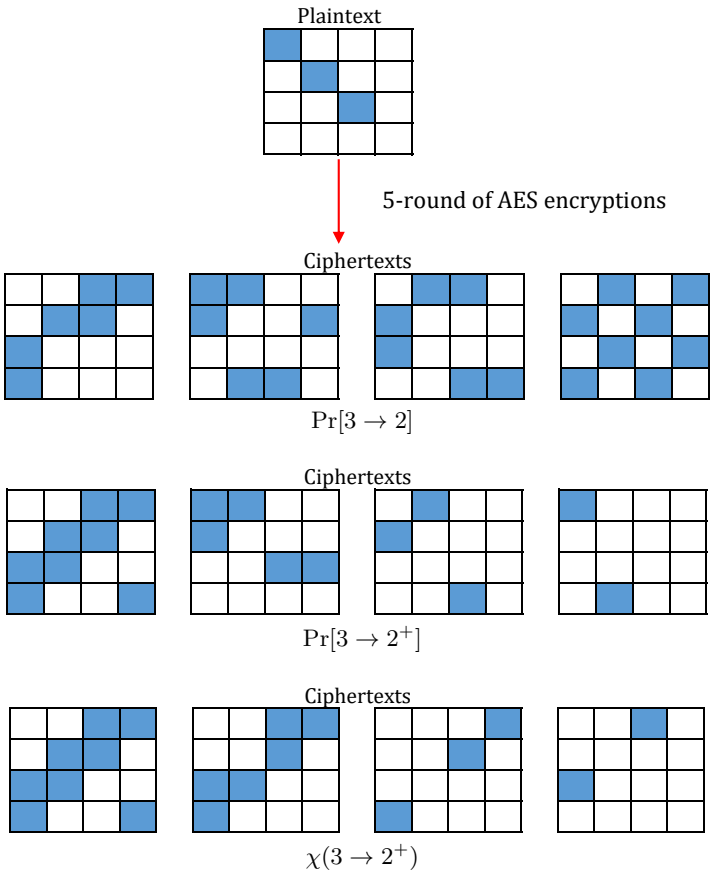


Fig. 2: Representative ciphertext examples for the events $\Pr[3 \to 2]$, $\Pr[3 \to 2^+]$, and $\chi(3 \to 2^+)$, all obtained from the same plaintext pair with three active bytes in the first diagonal. The event $\Pr[3 \to 2]$ corresponds to exactly two passive inverse diagonals; four representative (non-exhaustive) examples are shown. The event $\Pr[3 \to 2^+]$ corresponds to at least two passive inverse diagonals. Finally, $\chi(3 \to 2^+)$ denotes the case where two specified inverse diagonals are passive; here, the first and second inverse diagonals are fixed to be passive, while the remaining diagonals are unrestricted.

assign per-`MixColumns` probabilities to the linear constraints induced by input differences and combine contributions corresponding to effectively independent transitions across rounds.

Unlike several prior approaches, we compute the probabilities of `MixColumns` transitions exactly (see Lemma 2) and explicitly enumerate all truncated differential characteristics contributing to a given event. In particular, we systematically ap-

ply the inclusion-exclusion principle when evaluating probabilities for conditions involving exactly or at least i passive inverse diagonals.

Finally, we note that these modeling assumptions are heuristic in nature and do not hold exactly for AES. Such assumptions are standard in the literature, and within this framework our approach provides a systematic characterization of truncated differential behavior relative to prior methods. These idealizations are not expected to materially affect the resulting attack complexities for the configurations considered, and all results are derived within this modeling framework.

Chang et al. [10] compute the average value $\chi(1 \to 1^+)$ without relying on an independence assumption. In our framework, we obtain $\chi(1 \to 1^+) \approx 2^{-32} + 2^{-53.983}$, whereas Chang et al. derive a closely matching value via a direct DDT-based computation without the independence assumption $2^{-32} + 2^{-53.815}$. The comparison in Figure 6 illustrates the corresponding bias behavior under these two estimations.

3 A simple rederivation of previous results via our framework

We note that, under the setting and notation introduced in Section 2.2, the results of Bao et al. [2], Grassi and Rechberger [18], and Chang et al. [10] can be derived within our framework.

In this section, we re-derive these results in a unified manner via a single proposition, which reduces the previously separate analyses to a common analytical form.

This implies that the three results can be viewed as special cases of a single analytical framework, which further extends to additional truncated differential configurations considered in Sections 4 and 5.

Proposition 1. *For 5-round AES, we have* $\chi(1 \to 1^+) = P^4_{4,1^+}$, $\chi(1 \to 2^+) = P^4_{4,2^+}$, *and*

$$\chi(4 \to 1^+) = \sum_{\ell=0}^{2} \binom{4}{\ell} \cdot P_{4,\ell} \cdot P^4_{4-\ell,1^+}.$$

Proof. It is trivial that a single active byte leads to all bytes being active at the end of the second round. Therefore, the probability that a given diagonal is passive at the end of the third round, and hence that the corresponding inverse diagonal is passive at the end of the fifth round, is

$$\chi(1 \to 1^+) = P^4_{4,1^+}.$$

Similarly, the probability that a single active byte leads to two given inverse diagonals being passive at the end of the fifth round is

$$\chi(1 \to 2^+) = P^4_{4,2^+}.$$

Four active bytes in a single diagonal result in ℓ passive bytes in a given column at the end of the first round with probability $\binom{4}{\ell} \cdot P_{4,\ell}$. These ℓ passive bytes imply

the presence of $4-\ell$ fully active columns at the end of the second round and, consequently, $4-\ell$ active bytes in each column after the `ShiftRows` operation in the third round. The subsequent `MixColumns` operation in the third round produces a given passive diagonal with probability $P^4_{4-\ell,1^+}$, which in turn leads to a given passive inverse diagonal.

We impose the restriction $4-\ell > 1$, that is, $\ell \leq 2$, since the `MixColumns` matrix is MDS and the number of active input bytes must be strictly greater than the number of passive output bytes. Therefore, the overall probability is given by

$$\chi(4 \to 1^+) = \sum_{\ell=0}^{2} \binom{4}{\ell} \cdot P_{4,\ell} \cdot P^4_{4-\ell,1^+}.$$

The probability $P_{4,1^+}$ is given by

$$P_{4,1^+} = \frac{1}{2^8} + \frac{1}{2^8 \cdot (2^8-1)^3},$$

which will be derived in Lemma 1. Therefore,

$$\chi(1 \to 1^+) = P^4_{4,1^+} = \left(\frac{1}{2^8} + \frac{1}{2^8 \cdot (2^8-1)^3}\right)^4.$$

Bao et al. [2] derive this result by extending the integral distinguisher of AES and computing the collision probability of two distinct inputs to a function obtained by summing four independent permutations.

Chang et al. [10] compute the average probability that a given byte position is passive as $2^{-8} + 2^{-31.816}$ for 4-round AES, using a method based on the differential distribution table (DDT) of the corresponding super S-box. This value is slightly smaller than $P_{4,1^+} = 2^{-8} + 2^{-31.983}$. The difference can be attributed to index dependencies between byte positions in the internal AES states across consecutive rounds, as analyzed in [10]. Their approach does not rely on an independence assumption across rounds, since it directly computes the DDTs of super S-boxes. Overall, these results indicate that the independence assumptions in our analysis introduce only minor inaccuracies, and our estimates remain close to those of Chang et al. [10].

Let us consider the case analyzed by Grassi and Rechberger [18], namely when four active bytes appear in a single diagonal of a plaintext pair. If there is only one active byte at the end of the first round, then all bytes become active by the end of the third round. Consequently, only configurations with two, three, or four active bytes at the end of the first round can lead to a given passive inverse diagonal at the third round. Figure 3 illustrates the characteristics grouped according to these three partitions.

We generalize these observations to the case of an arbitrary number of passive inverse diagonals for 5-round AES in Theorem 1. This result highlights the effectiveness and flexibility of our approach, allowing previous results to be recovered in a clear and natural manner and extended within the framework established by our partitioning method (see Section 4.2).

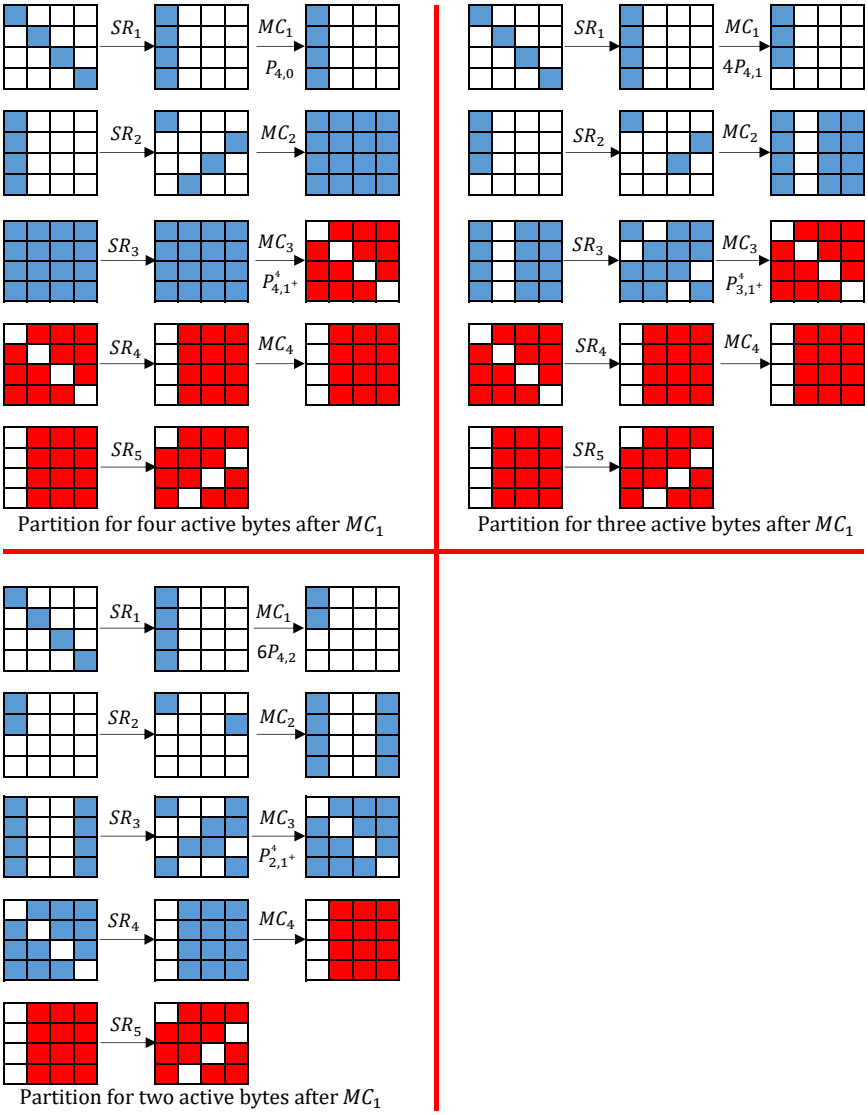


Fig. 3: Illustration of three partitions of the setting considered by Grassi and Rechberger [18], as referenced in Proposition 1. Blue boxes denote active bytes, white boxes denote passive bytes, and red boxes denote free positions (which may be active or passive). The partitions are defined according to the number of active bytes after MC_1 and contain 1, 4, and 6 characteristics, respectively. For each output column of MC_3 and MC_4 corresponding to an active input column, at least one red box in that column must be active.

4 Generalizations of Grassi and Rechberger [18], Bao et al. [2], and Chang et al. [10] in a single diagonal

In this section, we generalize the results of Grassi and Rechberger [18], Bao et al. [2], and Chang et al. [10], restricting our attention to plaintext pairs containing a single active diagonal, as in the previous works. In Grassi and Rechberger [18], this diagonal contains four active bytes, whereas both Bao et al. [2] and Chang et al. [10] consider a single active byte.

We extend these analyses by allowing an arbitrary number of active bytes within the active plaintext diagonal and, more importantly, by removing the restriction on the number of passive inverse diagonals in the ciphertext pair. In particular, for any $i = 0, 1, 2, 3$, we compute the probabilities that a given set of i inverse diagonals is passive, as well as the probabilities that the ciphertext pair contains exactly i passive inverse diagonals, a scenario not previously studied.

Moreover, both Grassi and Rechberger [18] and Bao et al. [2] provide only rough estimates for the probability that **at least** one inverse diagonal is passive in the cases $m = 4$ and $m = 1$ active bytes, respectively. By contrast, our framework not only provides more accurate probability estimates for these events but also generalizes them by computing the probability that the ciphertext pair contains at least i passive inverse diagonals.

These generalizations are formalized in Theorem 1. The statements in this section and the associated probability expressions are derived under the standard independence assumption used in truncated differential cryptanalysis of AES and related SPN ciphers, as described in Section 2.2. Under this assumption, round-wise transition probabilities are combined multiplicatively, and the resulting values are analytical estimates within the adopted model.

4.1 Preliminaries

In this section, we introduce the core concepts used throughout the paper and apply them to a detailed truncated differential analysis of 5-round AES.

We first derive exact probabilities for the number of passive bytes at specified positions within a column, as well as for the event that a column remains fully active after the `MixColumns` operation. While such statements are often used in a heuristic or approximate form in prior analyses, we provide precise probability expressions together with concise proofs in Lemma 1.

This lemma serves as a fundamental building block in our subsequent computations of truncated differential characteristics. In particular, the exact treatment of `MixColumns` transition probabilities enables more accurate evaluation of truncated differential probabilities for 5-round AES.

Lemma 1. *Let an MC matrix be a 4×4 MDS matrix (maximum distance separable) over the extension field $GF(2^n)$. Assume an input pair of two distinct randomly selected columns has i active words before the MC operation. Then,*

1. *the probability of having exactly $j \geq 0$ passive words at specific positions (and the other words are free) after the MC operation is given by*

$$P_{i,j^+} = \frac{\delta_{i-j}}{(2^n-1)^j} - j \cdot \left(\frac{\delta_{i-j-1}}{(2^n-1)^{j+1}} - \frac{\delta_{i-j-2}}{(2^n-1)^{j+2}} \right); \tag{2}$$

2. *and the probability of having only $j \geq 0$ passive words at specific positions, and the other words are active in the corresponding output column after the MC operation is given by*

$$P_{i,j} = \frac{\delta_{i-j}}{(2^n-1)^j} - \frac{4 \cdot \delta_{i-j-1}}{(2^n-1)^{j+1}} + \frac{10 \cdot \delta_{i-j-2}}{(2^n-1)^{j+2}} - \frac{20 \cdot \delta_{i-j-3}}{(2^n-1)^{j+3}}. \tag{3}$$

Proof. 1. The `MixColumns` transition probability does not depend on the specific ordering of active input words, and likewise the $\binom{4}{j}$ placements of j passive output words all have the same probability. Therefore, without loss of generality and for notational simplicity, we may assume that the active input words occupy the first i positions and the passive output words occupy the last j positions (that is, the first $4-j$ words are free). We then consider a column of the `MixColumns` operation with the first i input words active and the first j output words passive. The number of elements satisfying this condition is obtained by solving the system of equations given below, and dividing this quantity by $(2^n-1)^i$ yields P_{i,j^+}.

$$\begin{cases} 2x_1 + \delta_{i-1} \cdot 3x_2 + \delta_{i-2} \cdot x_3 + \delta_{i-3} \cdot x_4 = \delta_{4-j} \cdot y_1, \\ x_1 + \delta_{i-1} \cdot 2x_2 + \delta_{i-2} \cdot 3x_3 + \delta_{i-3} \cdot x_4 = \delta_{3-j} \cdot y_2, \\ x_1 + \delta_{i-1} \cdot x_2 + \delta_{i-2} \cdot 2x_3 + \delta_{i-3} \cdot 3x_4 = \delta_{2-j} \cdot y_3, \\ 3x_1 + \delta_{i-1} \cdot x_2 + \delta_{i-2} \cdot x_3 + \delta_{i-3} \cdot 2x_4 = \delta_{1-j} \cdot y_4, \\ x_1 \neq 0, \ \ldots, \ x_i \neq 0, \ x_{i+1} = \ldots = x_4 = 0, \\ y_1, \ldots, y_{4-j} \text{ are free.} \end{cases} \tag{4}$$

We first solve this system for the case $i = 4$; the other cases follow by a similar argument. For $i = 4$, there are initially four active words at the input of the MC operation; we now enumerate all possible cases.

For $j = 3$, this yields a homogeneous system of three linear equations in four variables. The solution to this homogeneous system is given by $x_4 = a \cdot x_1, x_3 = b \cdot x_1, x_2 = c \cdot x_1$, where all variables depend on the single variable x_1. Because x_1 can be any non-zero value, there are (2^n-1) solutions. Since the total number of inputs is $(2^n-1)^4$, we obtain $P_{4,3^+} = \frac{(2^n-1)}{(2^n-1)^4} = \frac{1}{(2^n-1)^3}$.

For $j = 2$, we get a homogeneous system of two equations in four variables. Its solution can be written as $ax_1 + bx_2 = cx_3, dx_1 + ex_2 = fx_4$, expressing x_3 and x_4 in terms of x_1 and x_2. We obtain $(2^n-1) \cdot (2^n-3) = (2^n-1)^2 - 2 \cdot (2^n-1)$ different cases that guarantee non-zero values for x_3 and x_4. Since the total number of inputs is $(2^n-1)^4$, we obtain $P_{4,2^+} = \frac{1}{(2^n-1)^2} - \frac{2}{(2^n-1)^3}$.

For $j = 1$, we obtain the linear equation $x_4 = ax_1 + bx_2 + cx_3$ involving four variables. Here, x_1 can be any of the (2^n-1) non-zero elements. The expression $ax_1 + bx_2$ can be either zero or non-zero. If $ax_1 + bx_2 \neq 0$, then x_1 has (2^n-1) choices, x_2 must avoid one specific value (so (2^n-2) options), and x_3 must also be

non-zero and independent (again (2^n-2) options). This gives $(2^n-1)\cdot(2^n-2)^2$ solutions. If $ax_1+bx_2=0$, then for each of the 2^n-1 choices of x_1 there is exactly one x_2 satisfying the equation, and x_3 can again be any non-zero value. This results in $(2^n-1)\cdot 1\cdot(2^n-1)$ solutions. Summing both cases, the total number of valid solutions is $(2^n-1)\cdot(2^n-2)^2+(2^n-1)^2$. Since the total number of possible non-zero input combinations is $(2^n-1)^4$, we obtain $P_{4,1^+}=\frac{1}{(2^n-1)}-\frac{1}{(2^n-1)^2}+\frac{1}{(2^n-1)^3}$.

The δ_m function is defined to satisfy the condition $i>j$ for P_{i,j^+}, and for $j\geq 2$, factoring out j from the second and third terms yields the expression given in part *(1)* of Lemma 1. Similar steps can be performed for $i=3,2,1$. Moreover, the case $P_{i,0^+}=1$ is trivial. This completes the proof of part *(1)*.

2. We provide our proof for this part only in the case $i=4$, as in part *(1)*. The other cases are similar and can easily be deduced from the case $i=4$. We also consider the situation where, besides j passive words, the remaining $4-j$ words are active. We then perform analogous calculations for $j=1,2,3$. First, when $j=3$, the one remaining word is necessarily active, so no further calculation is required. We thus obtain $P_{4,3}=P_{4,3^+}=\frac{1}{(2^n-1)^3}$.

For $j=2$, the expression for $P_{4,2^+}$ from part *(1)* also counts cases in which one additional passive word is present. By subtracting these, we get: $(2^n-1)^2-2\cdot(2^n-1)-2\cdot(2^n-1)=(2^n-1)^2-4\cdot(2^n-1)$. Thus, $P_{4,2}=\frac{1}{(2^n-1)^2}-\frac{4}{(2^n-1)^3}$.

For $j=1$, the expression for $P_{4,1^+}$ from part *(1)* also counts cases with two or three passive words. Therefore, subtracting the contributions for $j=2$ and $j=3$ yields $(2^n-1)^3-(2^n-1)^2+(2^n-1)-3\cdot((2^n-1)^2-4\cdot(2^n-1))-3\cdot(2^n-1)=(2^n-1)^3-4\cdot(2^n-1)^2+10\cdot(2^n-1)$. Since there are $(2^n-1)^4$ total cases, $P_{4,1}=\frac{1}{(2^n-1)}-\frac{4}{(2^n-1)^2}+\frac{10}{(2^n-1)^3}$.

One may introduce a delta function δ_m to enforce the condition $i>j$ for $P_{i,j}$, and analogous formulas follow immediately for $i=3,2,1$. The case $P_{i,0}$ is computed from $P_{i,0}=1-4P_{i,1}-6P_{i,2}-4P_{i,3}$. Thus, the proof of part *(2)* is complete.

Note 1. We can deduce the corresponding probabilities in Lemma 1 for the case of the `MixColumns` operation in AES by setting $n=8$. Note that we assume $n=8$ whenever we use the probabilities $P_{i,j}$ and P_{i,j^+} in our statements related to AES. We have verified these probabilities in practice by computing them for $n=8$ through our implementation. Moreover, part *(2)* of Lemma 1 is provided in recursive form in [14] for $n=8$, and it coincides with our result.

The following properties of the AES diffusion layer are fundamental and well known; however, we include their proofs for completeness.

Lemma 2. *Let a plaintext/ciphertext pair be given for at least 4-round AES encryption.*

1. *Assume the plaintext pair has only one active diagonal. Consequently, there is only one active column at the output of MC_1. Let $i\in\{1,2,3,4\}$ be the number of active bytes in that column. Then the output of MC_2 contains i fully active columns, and each of these columns contains i active bytes at the input of MC_3.*

2. *Let $j \in \{1, 2, 3, 4\}$. The plaintext pair has j passive diagonals if and only if there are j passive columns at the output of MC_1 if and only if the input of MC_2 contains j passive inverse diagonals.*

Proof. 1. Assume a given plaintext pair has only one active diagonal. After the SR_1 operation, the active bytes in the active diagonal are gathered into a single column, and thus the output of the MC_1 contains only one active column. If that column contains i active bytes, after the SR_2 operations each of those i active bytes is in a different column; therefore, every active column at the input of MC_2 contains exactly one active byte. By the branch number property, the output of MC_2 consists of i fully active columns. After the SR_3 operation, at the input of MC_3, each column contains i active bytes.

2. Assume a given plaintext pair has j passive diagonals. After the SR_1 operation, the input of the MC_1 contains j passive columns, and thus the output of the MC_1 contains j passive columns. After the SR_2 operation, the input of the MC_2 contains j passive inverse diagonals. The reverse implication is obtained by a similar argument. Moreover, Figure 4 shows an example for $j = 2$.

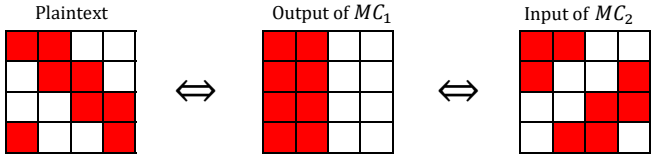


Fig. 4: An example of the second case of Lemma 2 for $j = 2$. White boxes represent passive bytes, while red boxes may be active or passive; however, in the first, second, and third patterns, at least one byte in the corresponding diagonal, column, and inverse diagonal, respectively, must be active.

Lemma 3 gives the relation between $\chi(m \to i^+)$ and $\Pr[m \to j]$ for arbitrary values of i and j, which we utilize in our computations.

Lemma 3. *Let a given plaintext pair for the 5-round AES encryption contain only m active bytes, all in one diagonal, for $1 \leq m \leq 4$. Then the following holds for $0 \leq i \leq 3$:*

$$\Pr[m \to i] = \binom{4}{i} \cdot \left[\chi(m \to i^+) - \delta_{3-i} \cdot \binom{4-i}{3-i} \cdot \chi(m \to (i+1)^+) + \right.$$
$$\left. \delta_{2-i} \cdot \binom{4-i}{2-i} \cdot \chi(m \to (i+2)^+) - \delta_{1-i} \cdot \binom{4-i}{1-i} \cdot \chi(m \to (i+3)^+) \right] \quad (5)$$

Proof. Assume a given plaintext pair has m ($1 \leq m \leq 4$) active bytes, all in one diagonal for 5-round AES encryption. In $\Pr[m \to i]$, there are i passive inverse

diagonals and $4-i$ active inverse diagonals at the end of 5-round AES encryption. Although $\chi(m \to i^+)$ has i passive inverse diagonals in specific positions, it is not guaranteed that the remaining $4-i$ inverse diagonals are active after the 5-round AES encryption. Therefore, one must exclude from $\chi(m \to i^+)$ the combinations of the $\chi(m \to (i+1)^+)$, $\chi(m \to (i+2)^+)$, and $\chi(m \to (i+3)^+)$ states to obtain $\Pr[m \to i]$.

In $\Pr[m \to i]$, the positions of the i passive diagonals are not specific, whereas in all the other terms the positions of the passive diagonals are specific. Therefore, each term on the right hand side of the equation is multiplied by $\binom{4}{i}$. In $\chi(m \to i^+)$, the i passive inverse diagonals are specific and the $\chi(m \to (i+1)^+)$ state is excluded from this term. In this case $i+1$ passive inverse diagonals can be obtained in $\binom{4-i}{3-i}$ different ways. Normally $\binom{4-i}{2-i}$ occurrences of $\chi(m \to (i+2)^+)$ must be excluded from the initial state; however, $\binom{4-i}{3-i} \cdot \binom{3-i}{2-i}$ occurrences of $\chi(m \to (i+2)^+)$ are excluded together with $\chi(m \to (i+1)^+)$. Since $\binom{4-i}{3-i} \cdot \binom{3-i}{2-i} - \binom{4-i}{2-i} = \binom{4-i}{2-i}$, $\binom{4-i}{2-i}$ occurrences of $\chi(m \to (i+2)^+)$ need to be added back. Similarly, for $\chi(m \to (i+3)^+)$, normally $\binom{4-i}{1-i}$ occurrences of $\chi(m \to (i+3)^+)$ must be excluded from the initial state; however, $\binom{4-i}{3-i} \cdot \binom{3-i}{1-i}$ occurrences of $\chi(m \to (i+3)^+)$ are excluded together with $\chi(m \to (i+1)^+)$ and $\binom{4-i}{2-i} \cdot \binom{2-i}{1-i}$ occurrences are included together with $\chi(m \to (i+2)^+)$; since $\binom{4-i}{3-i} \cdot \binom{3-i}{1-i} = \binom{4-i}{2-i} \cdot \binom{2-i}{1-i}$ they cancel each other out, and therefore $\binom{4-i}{1-i}$ occurrences of $\chi(m \to (i+3)^+)$ must be excluded from the initial state.

Finally, by adding δ functions for the constraints $i+1 \leq 3$, $i+2 \leq 3$, and $i+3 \leq 3$ corresponding to $\chi(m \to (i+1)^+)$, $\chi(m \to (i+2)^+)$, and $\chi(m \to (i+3)^+)$, respectively, the desired result is obtained.

4.2 Generalization of Proposition 1

The following theorem presents three distinguishers for 5-round AES. The first part is well-known and is shown in [18] for the case $m = 4$ and in [2, 10] for the case $m = 1$; here m denotes the number of active bytes in the active diagonal of the plaintext pair. Note that we extend their results through simple arithmetic using our framework in Proposition 1. The second part has not, as far as we know, been studied in the literature and is introduced here for the first time. The third part appears in [2] only for the case $m = i = 1$, and in [18] only for the case $m = 4, i = 1$; the probability computations in both works are rough computations (see Remark 1). In [27], the cases in [2] and [18] are recomputed using a different technique. In contrast, we compute these probabilities for all pairs (m, i) with $m \in \{1, 2, 3, 4\}$ and $i \in \{0, 1, 2, 3\}$.

Theorem 1. *Assume that a given plaintext pair for the 5-round AES encryption contains m active bytes, all in one diagonal, where $1 \leq m \leq 4$. Then,*

1. *the probability that the corresponding ciphertext pair contains i passive inverse diagonals at specific positions for $0 \leq i \leq 3$ is*

$$\chi(m \to i^+) = \sum_{\ell=0}^{\min\{m,4-i\}-1} \binom{4}{\ell} \cdot P_{m,\ell} \cdot P^4_{4-\ell,i^+},$$

2. *the probability that the corresponding ciphertext pair contains exactly i passive inverse diagonals for $0 \leq i \leq 3$ is*

$$\Pr[m \to i] = \sum_{\ell=0}^{\min\{m,4-i\}-1} \binom{4}{\ell}\binom{4}{i} P_{m,\ell} \left(\sum_{j=0}^{3-\ell-i} \binom{4-i}{j} (-1)^j P^4_{4-\ell,(i+j)^+} \right),$$

3. *and the probability that the corresponding ciphertext pair contains at least i passive inverse diagonals is*

$$\Pr[m \to i^+] = \sum_{j=i}^{3} \Pr[m \to j].$$

Proof. 1. Assume a given plaintext pair has m active bytes, all in one diagonal. Let there be ℓ passive bytes in a column at the end of the first round, ensuring that the condition $m > \ell$ holds, with probability $\binom{4}{\ell} \cdot P_{m,\ell}$. From Lemma 2, it follows that at the input of MC_3, each column contains $4 - \ell$ active bytes. By Lemma 2, there must be i specific passive diagonals after MC_3 to obtain i specific passive inverse diagonals after 5-round encryption. For one column, the probability of transitioning from $4 - \ell$ active bytes to a state where specific i bytes are passive and the remaining bytes are free is $P_{4-\ell,i^+}$. Therefore, for all four columns, the probability is $P^4_{4-\ell,i^+}$. Additionally, due to the conditions $4 - \ell > i$ and $m > \ell$, the term $\min\{m - 1, i - 1\} - 1$ becomes the upper bound of the sum. Finally, by multiplying the obtained probabilities for each condition of m and summing them, the result is obtained. Moreover, the partitions for Theorem 1 (part *(1)*) with $m = 2$, $i = 2$ are presented in Figure 5; analogous arguments apply to the remaining cases.

2. The difference between part *(2)* and part *(1)* is that in *(2)* any i inverse diagonals are passive, rather than given i specific inverse diagonals as in *(1)* and, in addition, the remaining $4 - i$ inverse diagonals must be active. Hence, the proof follows the same procedure as in *(1)* up to the MC_3 operation. After five rounds of encryption, the probability of obtaining i passive inverse diagonals is $\binom{4}{i} \cdot P^4_{4-\ell,i^+}$ for MC_3; however, in this case, it is not necessary that all but one of the $4-i$ inverse diagonals be active. Therefore, from the $4 - i$ inverse diagonals, all $P^4_{4-\ell,(i+j)^+}$ scenarios that do not satisfy this condition under the constraint $j = 0$ to $4 - \ell > i + j$ must be excluded together with their combinations. Additionally, due to the condition $4 - \ell - i > j$, the term $3 - \ell - i$ becomes the upper bound of the sum. Finally, by multiplying the obtained probabilities for each condition of m and summing them, the result is obtained.

3. Assume a given plaintext pair has m active bytes, all in one diagonal. The event that at least i passive inverse diagonals occur in the ciphertext after 5-round encryption consists of all cases starting from exactly i passive inverse diagonals up to the case of three passive inverse diagonals. (For example, for $i = 1$ the event "at least one passive inverse diagonal" is the sum of the cases "exactly one", "exactly two", and "exactly three" passive inverse diagonals.) Thus, since in *(2)* the probability of exactly i passive inverse diagonals is $\Pr[m \to i]$, the desired expression for each m and i is obtained as the sum of the probabilities from $\Pr[m \to i]$ to $\Pr[m \to 3]$.

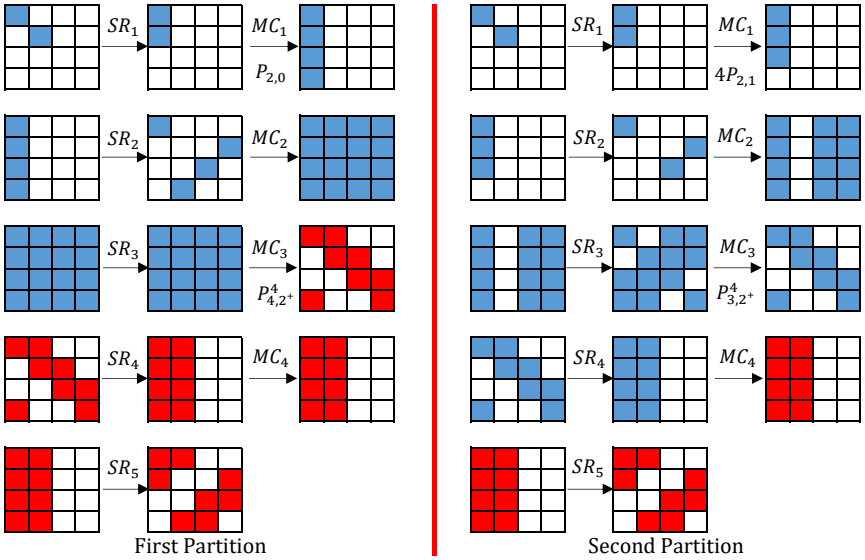


Fig. 5: Illustration of two partitions of the characteristics considered in Theorem 1, part *(1)*, for $i = m = 2$. The color coding follows Figure 3. The partition on the left corresponds to a fully active column after MC_1 and contains a single characteristic. The other partition corresponds to a column with three active bytes after MC_1 and contains four characteristics. For each output column of MC_3 and MC_4 corresponding to an active input column, at least one red box must be active.

Figure 6 shows, for each m and i, the deviations from 1 of the probability ratios obtained in Theorem 1 relative to the corresponding random permutation probabilities. To ensure correctness, all probabilities are independently recomputed using a computer implementation[3]. As observed in the figure, when m and i are fixed, the deviations of these ratios may appear almost equal across different probability measures. However, a closer inspection reveals that these deviations are in fact distinct. For example, when $m = 4$ and $i = 2$, the values of $\chi(4 \to 2^+)$, $\Pr[4 \to 2]$, and $\Pr[4 \to 2^+]$ are 0.0002179705383556, 0.000217970523646, and 0.0002179705285492, respectively.

Notice that in the expression $\Pr[m \to i]$ and the corresponding random permutation, there are exactly i passive inverse diagonal conditions. In contrast, in the expressions $\chi(m \to i^+)$ and $\Pr[m \to i^+]$, and in the corresponding random permutations, there are, in addition to exactly the i passive inverse diagonal conditions, also exactly $i+1$, $i+2$, and $i+3$ passive inverse diagonal conditions in the appropriate cases. However, in these cases, the dominant contribution in both $\chi(m \to i^+)$ and $\Pr[m \to i^+]$, as well as in the corresponding random permutation probabilities, comes from the probability of having exactly i passive inverse diagonal conditions.

[3] GitHub Code Repository

Therefore, for the same values of m and i, the values in Figure 6 are close to each other.

Remark 1. The probability $\Pr[m \to i^+]$ can be computed directly once $\Pr[m \to i]$ is known, as shown in Theorem 1. However, the existing literature does not approach the computation of $\Pr[m \to i^+]$ in this systematic manner. As a consequence, prior works restrict their analysis to the special cases $\Pr[4 \to 1^+]$ and $\Pr[1 \to 1^+]$, and the resulting probability computations are not fully tight and rely on relatively intricate reasoning.

Bao et al. compute the probability of at least one passive inverse diagonal as $1 - \left(1 - P^4_{4,1^+}\right)^4 \approx 2^{-30} + 2^{-51.985}$ in [2]. This computation would be correct if the inverse diagonals (which simply refer to the bytes in a column at the end of the fourth round) were independent. However, the passiveness of a byte after the MC operation in a column is affected by the passiveness of other bytes. In fact, the probability that all the inverse diagonals are passive would be $P^{16}_{4,1^+}$ according to [2], but this case is not possible for two different plaintexts incorporated into a permutation. Moreover, the probability of exactly three given inverse diagonals being passive would be $P^{12}_{4,1^+}$. However, it is actually $P^4_{4,3}$ due to the property of the MC operation, which ensures that if three bytes in an active column are passive, then the remaining byte must be active. Similarly, the probability that exactly two given inverse diagonals are passive is $P^4_{4,2^+}$, rather than $P^8_{4,1^+}$. As a result, the correct probability of having at least one inverse diagonal at the end of the fifth round is

$$\Pr[1 \to 1^+] = 4P^4_{4,1^+} - 6P^4_{4,2^+} + 4P^4_{4,3^+}.$$

The actual probability is higher, with the ratio being $1 + 2^{-43.81}$.

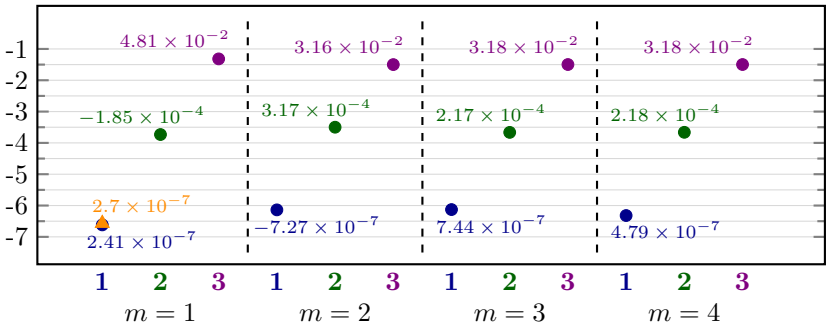
The computation of at least one passive inverse diagonal for $m = 4$ ($\Pr[4 \to 1^+]$) is also studied in [18]. Their approach considers the term $2^{-30} + 2^{-50.98}$, which corresponds to four times $2^{-32} + 2^{-52.98}$, i.e., $\chi(4 \to 1^+)$. This computation does not account for joint events where two or more inverse diagonals are simultaneously passive. As a result, the deviation from the more accurate probability is $2^{-57.75}$, corresponding to a relative difference of $1 - 2^{-27.75}$.

The orange triangles in Figure 6 show the results of [18, 2, 10]. The discrepancy between [18, 2] and our results is due to their simplified counting arguments, whereas the difference with [10] arises from the absence of an independence assumption across rounds. In particular, the small gap between [10] and our analysis indicates that the idealized model under our assumptions closely approximates the behavior in AES.

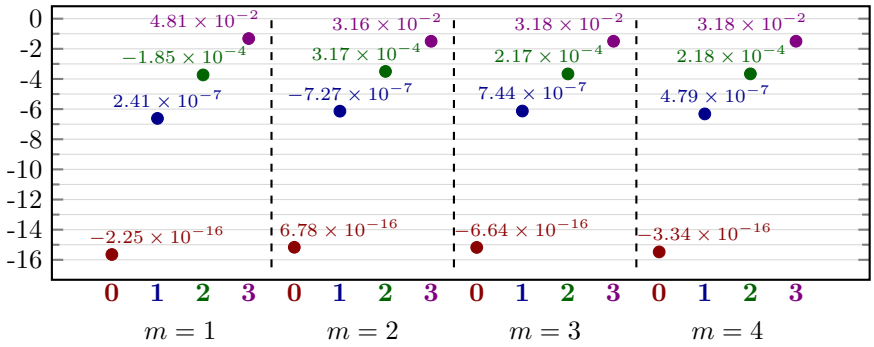
4.3 Checks related to Theorem 1

The statements in Theorem 1 can be partially verified using both independent results from the literature and our own computations.

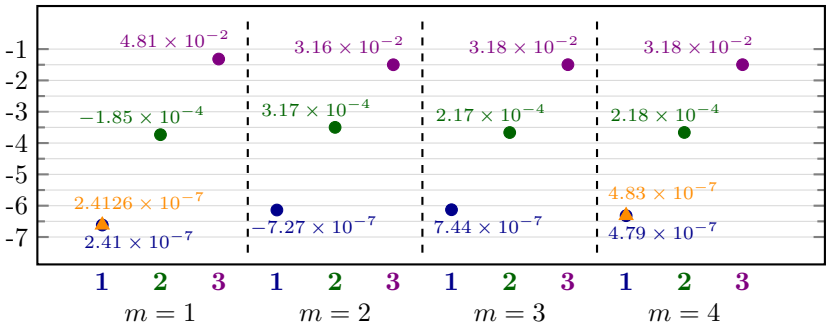
We compute the probability that all inverse diagonals are active after five rounds of encryption ($i = 0$), in part *(2)* of Theorem 1, given a plaintext with m active bytes in a diagonal. By subtracting this probability from the total, we obtain the probability that at least one inverse diagonal is passive, and we verify this value against the probability provided ($i = 1$) in part *(3)* of Theorem 1.



The first part of Theorem 1: $\chi(m \to i^+)$.



The second part of Theorem 1: $\Pr[m \to i]$.



The third part of Theorem 1: $\Pr[m \to i^+]$.

Fig. 6: Bias values for each (m, i) pair, defined as the deviation from 1 of the probability ratios obtained in Theorem 1 relative to the corresponding random permutation probabilities. The x-axis represents the values of m and i, while the y-axis shows the bias on a logarithmic scale. The cases for which $\chi(m \to 0^+) = \Pr[m \to 0^+] = 1$ are omitted from the first and third graphs. The ratios for $\Pr[4 \to 1^+]$ from Grassi and Rechberger [18], $\Pr[1 \to 1^+]$ from Bao et al. [2], and $\chi(1 \to 1^+)$ from Chang et al. [10] are shown in orange.

Secondly, in Lemma 3, we present a relation for arbitrary i and j between $\chi(m \to i^+)$ and $\Pr[m \to j]$ after 5 rounds, which depends only on the number of passive inverse diagonals. In parts *(1)* and *(2)* of Theorem 1, we state equalities for $\chi(m \to i^+)$ and $\Pr[m \to j]$, using the MC transition probabilities defined in Lemma 1. From these, we show that the relation in Lemma 3 also holds for $\chi(m \to i^+)$ and $\Pr[m \to j]$ given in parts *(1)* and *(2)* of Theorem 1, thereby verifying it.

Bao et al. [2] computed the probability that a specific inverse diagonal remains passive after five rounds by extending the integral distinguisher for a plaintext containing a single active byte. Using our approach, we compute the same probability in part *(1)* of Theorem 1, and the results are identical (see Proposition 1). Grassi and Rechberger [18] computed the expected value 2,147,484,685.6 for the number of plaintext pairs in which a specific inverse diagonal remains passive after five rounds (i.e., the case $i = 1$), starting from a set of 2^{32} plaintexts active on a single diagonal. In our notation, this overall probability can equivalently be computed as the weighted average of the probabilities corresponding to $m = 1, 2, 3$, or 4 active bytes.

Accordingly, using the probabilities $\chi(1 \to 1^+), \chi(2 \to 1^+), \chi(3 \to 1^+)$, and $\chi(4 \to 1^+)$ obtained from part *(1)* of Theorem 1, together with the numbers of plaintext pairs $4 \cdot 2^{31} \cdot (2^8 - 1)$, $6 \cdot 2^{31} \cdot (2^8 - 1)^2$, $4 \cdot 2^{31} \cdot (2^8 - 1)^3$, and $2^{31} \cdot (2^8 - 1)^4$ producible from 2^{32} plaintexts for $m = 1, 2, 3$, and 4, respectively, we obtain the expected value 2,147,484,685.59 by multiplying each probability by its corresponding number of pairs and summing the results.

The last part of Theorem 1 provides the probability that a ciphertext pair for 5-round AES contains at least one passive inverse diagonal ($i = 1$). Accordingly, the probability that all inverse diagonals are active (that is, $\Pr[m \to 0]$) is

$$\Pr[m \to 0] = 1 - \Pr[m \to 1^+].$$

In fact, if we write down $\Pr[m \to 0]$ using Part *(2)* of Theorem 1 and add it to the result in Part *(3)* of the same theorem, we obtain

$$\Pr[m \to 0] + \Pr[m \to 1^+] = \sum_{i=0}^{3} \Pr[m \to i].$$

On the other hand, note that

$$\sum_{i=0}^{3} \Pr[m \to i] = 1.$$

The computation of $\Pr[m \to 0]$ in two different ways can be regarded as a partial verification of the last two parts of Theorem 1.

We can further verify the first two parts of Theorem 1 using Lemma 3, which gives a relation between $\chi(m \to i^+)$ and $\Pr[m \to j]$ for arbitrary i and j. In parts *(1)* and *(2)* of Theorem 1, equalities for $\chi(m \to i^+)$ and $\Pr[m \to j]$ are stated using the MC transition probabilities defined in Lemma 1.

When the equalities from parts *(1)* and *(2)* of Theorem 1 are substituted into the equation of Lemma 3, the relation is verified. We consider the case $m = 2$ and $i = 2$

to make this equality explicit. From Lemma 3, we obtain

$$\Pr[2 \to 2] = 6 \cdot (\chi(2 \to 2^+) - 2 \cdot \chi(2 \to 3^+)).$$

From part *(1)* of Theorem 1, we have

$$\chi(2 \to 2^+) = P_{2,0} \cdot P^4_{4,2^+} + 4 \cdot P_{2,1} \cdot P^4_{3,2^+}, \quad \chi(2 \to 3^+) = P_{2,0} \cdot P^4_{4,3^+},$$

and from part *(2)* we obtain

$$\Pr[2 \to 2] = 6 \cdot P_{2,0} \cdot (P^4_{4,2^+} - 2 \cdot P^4_{4,3^+}) + 24 \cdot P_{2,1} \cdot P^4_{3,2^+}.$$

Substituting these expressions into the equation of Lemma 3 yields

$$6\big(P_{2,0}P^4_{4,2^+} + 4P_{2,1}P^4_{3,2^+} - 2P_{2,0}P^4_{4,3^+}\big) = 6P_{2,0}(P^4_{4,2^+} - 2P^4_{4,3^+}) + 24P_{2,1}P^4_{3,2^+}.$$

Similarly, the verification is easily seen to hold for all values of m and i. Lastly, we can easily verify part *(1)* of Theorem 1 for $i = 0$. This case corresponds to imposing no condition on the inverse diagonals of ciphertext pairs; hence, its probability is 1 by definition. In other words, $\chi(m \to 0^+) = 1$. Indeed,

$$\chi(m \to 0^+) = \sum_{\ell=0}^{m-1} \binom{4}{\ell} \cdot P_{m,\ell} \cdot P^4_{4-\ell,0^+},$$

by the first part of Theorem 1. This expression equals 1 since $P_{4-\ell,0^+} = 1$ for all ℓ, and summing the probabilities $P_{m,\ell}$ over all possibilities yields

$$\sum_{\ell=0}^{m-1} \binom{4}{\ell} \cdot P_{m,\ell} = 1.$$

5 Multiple active diagonals

We now consider the scenario in which a plaintext pair contains more than one active diagonal, a setting that has not been systematically explored in the literature. We further exploit one such truncated differential in our attacks, demonstrating the relevance of analyzing configurations with multiple active diagonals in the input.

All probability computations in this section are carried out under the standard independence assumptions described in Section 2.2, under which round-wise transition probabilities are combined multiplicatively.

To begin our generalization, in Theorem 2 we compute the probabilities that the corresponding ciphertext pair has three passive inverse diagonals and one active inverse diagonal, and that the passive bytes in the active inverse diagonal are distributed across the given j columns, when a plaintext pair consists of exactly the given i active diagonals, each containing exactly one active byte, for 5-round AES.

We show that these probabilities deviate from those expected under random permutations for $0 \leq j \leq 3$, and report in Figure 8 the deviation of their ratios from the corresponding random-permutation probabilities.

Additionally, we introduce our partitioning approach, which groups characteristics sharing the same input–output truncated differences according to the number of passive diagonals at the end of the second round. This partitioning is illustrated in Figure 7 for the case $i = 4$ and $j = 0$.

Theorem 3 generalizes Theorem 2. In Theorem 2, each active diagonal is restricted to contain exactly one active byte, whereas this restriction is removed in Theorem 3. The latter considers the more general setting in which a plaintext pair contains an arbitrary number of active diagonals in the input and a single passive inverse diagonal in the output. This result is derived from Theorem 1 by exploiting the symmetry between the AES encryption and decryption functions.

Theorem 4 addresses a related scenario in which one diagonal contains m_1 active bytes and another contains m_2 active bytes. Its proof is based on enumerating partitions of characteristics that share equal probabilities. Owing to this distinct proof technique, Theorem 4 also provides an independent consistency check for certain results of Theorem 3.

Theorem 2. *Consider a plaintext pair with i active diagonals, each containing exactly one active byte. The probability that the corresponding ciphertext pair for 5-round AES has three passive inverse diagonals and one active inverse diagonal, and that the passive bytes in the active inverse diagonal are distributed across the given j columns, is given by*

$$\sum_{\ell=0}^{\min\{i,4-j\}-1} 4 \cdot \binom{4}{\ell} \cdot P_{i,\ell}^{4} \cdot P_{4,3}^{4-\ell} \cdot P_{4-\ell,j}. \tag{6}$$

Proof. Assume a given plaintext pair has i active diagonals and each diagonal contains only one active byte. Then, there will be i active columns and each active column will contain only one active byte after the SR_1. We have four characteristics defined by the number of passive columns before MC_3. There can be 0, 1, 2, or 3 passive columns before MC_3. At the end of the first round, we have i fully active columns, each containing exactly i active bytes before MC_2.

In the first category ($\ell = 0$), the probability that all bytes remain active after MC_2 is $P_{i,0}^4$, obtained by applying Lemma 1 independently to each of the four columns.

At the end of the third round, only one diagonal remains active, thereby yielding one single active column before MC_4. The probability of this event is $4 \cdot P_{4,3}^4$ by Lemma 1.

Next, one fully active column results in j passive bytes in given positions with probability $P_{4,j}$ when $0 \leq j \leq 3$. The product of the above factors yields the $\ell = 0$ contribution in Equation 6.

Now, consider the categories with $\ell = 1, 2, 3$ passive columns before MC_3. The probability of having ℓ passive diagonals after MC_2 is $\binom{4}{\ell} \cdot P_{i,\ell}^4$. The probability that the $4 - \ell$ fully active columns yield only one active diagonal is $4 \cdot P_{4,3}^{4-\ell}$ by Lemma 1. This results in $4 - \ell$ active bytes in only one active column before MC_4, and this column yields j passive bytes in given positions with probability $P_{4-\ell,j}$, by Lemma 1 again. Additionally, due to the conditions $\ell < i$ and $j < 4 - \ell$, ℓ must be smaller than $\min\{i, 4 - j\}$. Multiplying these three probabilities and summing over

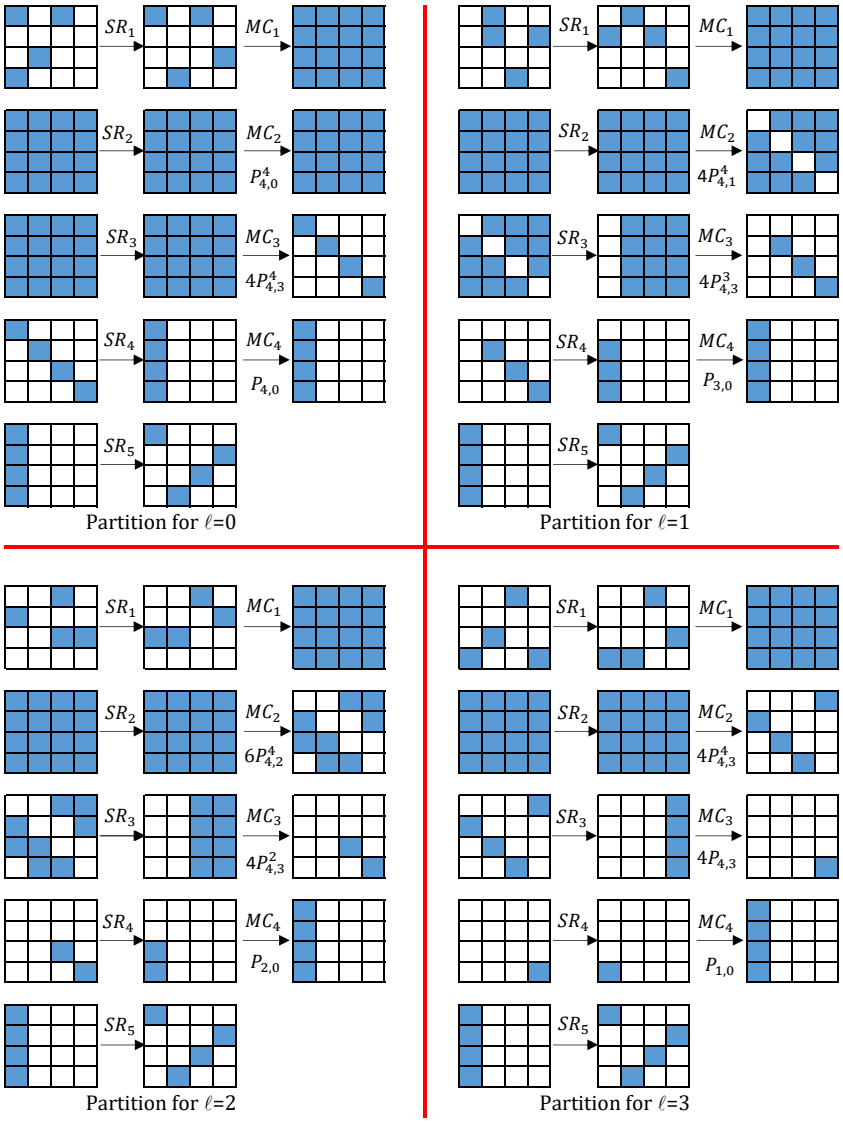


Fig. 7: Illustration of the four partitions of characteristics in Theorem 2 for $i = 4$ active diagonals in the plaintext and $j = 0$ passive byte in the active inverse diagonal of the ciphertext. Blue boxes indicate active states, and white boxes indicate passive states. The partitions correspond to the number ℓ of passive diagonals after MC_2, yielding 4, 16, 24, and 16 characteristics for $\ell = 0, 1, 2, 3$, respectively.

ℓ, we obtain the remaining cases of ℓ for Equation 6. Note that $\ell < i$ and $\ell < 4 - j$, since MC is an MDS matrix.

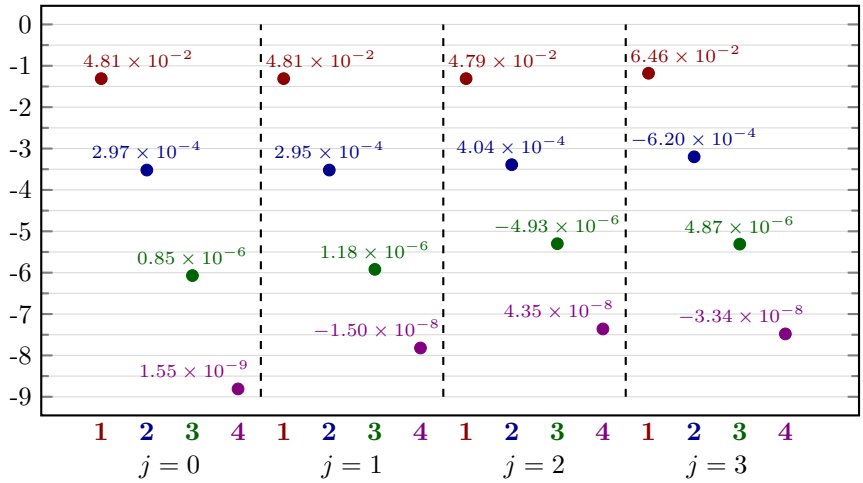


Fig. 8: Bias values for each (i, j) pair, defined as the deviation from 1 of the probability ratios obtained in Theorem 2, relative to the corresponding probabilities of a random permutation. The x- and y-axes are defined as in Figure 6. Smaller (more negative) values correspond to lower bias magnitudes.

Remark 2. There are $\min\{i, 4 - j\} - 1$ partitions of differential characteristics described in Theorem 2 for given i and j, which are depicted in Figure 7. The number of passive diagonals characterizes each partition in the second round (which we denote as ℓ), and any characteristic in a partition has an equal probability.

The probability given in Equation 6 differs from the corresponding probability for a random permutation. Figure 8 illustrates the deviation of the probability ratios derived from Theorem 2 relative to those for random permutations.

For a uniformly random permutation over 16 bytes, the probability that exactly three inverse diagonals are passive and one is active, with the passive bytes in the active inverse diagonal distributed over j specified columns, is given by

$$\frac{2^{-8j-94} \cdot (1 - 2^{-8})^{4-j}}{1 - 2^{-128}}.$$

This expression follows from the fact that each specified byte is active with probability $1 - 2^{-8}$, which yields a factor of $(1 - 2^{-8})^{4-j}$ for the $4 - j$ active bytes. The remaining $j + 12$ bytes are passive with probability $(2^{-8})^{j+12} = 2^{-8j-96}$. Moreover, there are four possible choices for the passive inverse diagonals. Finally, we

condition on the ciphertext pair containing at least one active byte by dividing by $1 - 2^{-128}$.

The expression in Equation 6 is evaluated for different values of i, and the resulting probabilities are illustrated in Figure 8. For $i = 1$, the biases are relatively large for all j. This follows from the fact that, for only one inverse diagonal to remain active after 5 rounds, the output of MC_3 must contain exactly one active diagonal. Hence, the active columns at the input of MC_3 must be fully active. When $i = 1$, the input of MC_3 is fully active with probability 1, yielding a larger bias than in the other cases. Since the overall biases are smaller than the expected probabilities, dividing the expected probabilities by the corresponding probabilities in the random permutation case and then subtracting the result from one further amplifies the effect, resulting in larger relative biases in cases such as $(i, j) = (1, 3)$ and $(i, j) = (4, 3)$.

This symmetry arises from the design of AES, where the decryption function can be expressed using the inverse transformations `InvSubBytes`, `InvShiftRows`, and `InvMixColumns` in a round structure analogous to that of encryption. In particular, the round operations can be rearranged to match the ordering in the encryption direction, with the final round omitting `MixColumns` in both cases. This design strategy yields closely related structural properties for encryption and decryption, allowing analogous probabilistic arguments to be applied in both directions [11].

We reinterpret Theorem 1 to obtain the corresponding probability in the reverse, i.e., decryption, direction of 5-round AES. By exploiting the structural symmetry between the encryption and decryption transformations of AES, we derive Theorem 3.

To the best of our knowledge, this structural symmetry has not previously been used to derive truncated differential probabilities with arbitrary input differences, as in Theorem 3. The resulting characteristics are directly exploited to construct the ciphertext-only attacks presented in Section 6.

Theorem 3. *Assume that given i diagonals of a plaintext pair for the 5-round AES are active and the other diagonals are passive. Then, the probability that the corresponding ciphertext pair for 5-round AES has given three passive inverse diagonals and one active inverse diagonal, with exactly m passive bytes in that active inverse diagonal, is given by*

$$\Pr[i \Rightarrow m] = \frac{\binom{4}{m} \sum_{\ell=0}^{\min\{4-m,i\}-1} \binom{4}{\ell} P_{4-m,\ell} \left(\sum_{j=0}^{i-\ell-1} \binom{i}{j} (-1)^j P^4_{4-\ell,(4-i+j)^+} \right)}{2^{32i+8m-32} \ (1-2^{-8})^{m-4} \ (1-2^{-32})^i}$$

for $1 \leq i \leq 4$ and $0 \leq m \leq 3$.

Proof. Let $i \in \{1, 2, 3, 4\}$ be fixed, and let i diagonals of the plaintext be specified. Assume that a plaintext pair is active exactly on these i diagonals and passive on the remaining ones.

From the second part of Theorem 1, we have shown that the probability $\Pr[(4 - m) \rightarrow (4 - i)]$, i.e., the probability that the corresponding ciphertext pair contains

exactly i active and $4-i$ passive inverse diagonals, is given by

$$\sum_{\ell=0}^{\min\{4-m,i\}-1} \binom{4}{\ell}\binom{4}{4-i} P_{4-m,\ell}\left(\sum_{j=0}^{i-\ell-1}\binom{i}{j}(-1)^j P^4_{4-\ell,(4-i+j)^+}\right).$$

Since this probability accounts for all $\binom{4}{4-i}$ possible choices of the $4-i$ passive inverse diagonals, the probability that a *fixed* set of $4-i$ inverse diagonals is passive is obtained by dividing by $\binom{4}{4-i}$.

We now compute $\Pr[m \Leftarrow i]$ using Bayes' theorem. Here, $\Pr[m \Leftarrow i]$ denotes the probability that the corresponding plaintext pair has exactly m passive bytes in a given active diagonal, conditioned on the event that the ciphertext pair has exactly i active inverse diagonals in the decryption direction (at specified positions).

By Bayes' theorem,

$$\Pr[m \Leftarrow i] = \frac{\Pr[(4-m) \to (4-i)] \cdot \Pr[m \text{ passive bytes in a fixed diagonal}]}{\binom{4}{4-i} \cdot \Pr[i \text{ active inverse diagonals at fixed positions}]}. \quad (7)$$

Here,

$$\Pr[m \text{ passive bytes in a fixed diagonal}] = \binom{4}{m} \cdot (1-2^{-8})^{4-m} \cdot 2^{-8(12+m)}$$

is the probability that a randomly chosen plaintext pair has exactly m passive bytes within a given diagonal, and

$$\Pr[i \text{ active inverse diagonals at fixed positions}] = (1-2^{-32})^i \cdot 2^{-32(4-i)}$$

is the probability that a randomly chosen ciphertext pair has exactly i active inverse diagonals at specified positions. Note that the fixed diagonal is active since the number of its passive bytes is less than 4: $0 \le m \le 3$.

Substituting these expressions into Equation (7) yields the desired formula for $\Pr[m \Leftarrow i]$.

Finally, by the symmetry between AES encryption and decryption, we have

$$\Pr[i \Rightarrow m] = \Pr[m \Leftarrow i].$$

This follows from the absence of the `MixColumns` operation in the final round of AES, together with the MDS property of the `InvMixColumns` transformation. Moreover, the inverse `SB` and inverse `ShiftRows` operations preserve the relevant structural properties, implying that Lemma 1 applies equally in the decryption direction.

Table 2 presents the ratios of the probabilities derived from Theorem 3 and those for random permutations. Theorem 3 is derived from Theorem 1. Similarly, we establish a related result for the case where a plaintext pair has two active diagonals, each containing a specified number of active bytes, as stated in Theorem 4. A noteworthy property of these results is that Theorem 4 can be used to verify Theorem 3 partially: the weighted average of the probabilities in Theorem 4 over all possible distributions of active bytes in the two diagonals yields the probability stated in Theorem 3.

i	$m=0$	$m=1$	$m=2$	$m=3$
1	1.031806538	1.031807802	1.031646620	1.048087204
2	1.000217970	1.000216687	1.000316814	0.999814986
3	$1+2^{-20.99}$	$1+2^{-20.35}$	$1-2^{-20.39}$	$1+2^{-21.98}$
4	$1-2^{-51.43}$	$1-2^{-50.67}$	$1+2^{-50.34}$	$1-2^{-52.01}$

Table 2: The ratios of the probabilities for different (i, m) values relative to a random permutation in Theorem 3.

Theorem 4. *Assume that a given plaintext pair for the 5-round AES encryption contains m_1 and m_2 active bytes in two diagonals, respectively, where $1 \leq m_1, m_2 \leq 4$. The probability that the corresponding ciphertext pair for 5-round AES has three passive inverse diagonals and one active inverse diagonal, and that the passive bytes in the active inverse diagonal are distributed across the given j columns, is given by*

$$\sum_{i_1=0}^{\alpha}\sum_{i_2=0}^{\beta}\sum_{t=0}^{\gamma} 4\binom{4}{t}\binom{4}{i_1}\binom{4-i_1}{i_2}\delta(t,i_1,i_2)P_{m_1,i_1}P_{m_2,i_2}P_{2,t}^{4-(i_1+i_2)}P_{4,3}^{4-t}P_{4-t,j}, \quad (8)$$

where $\alpha = \min\{3, m_1-1\}$, $\beta = \min\{4-i_1, m_2-1, 3\}$, $\gamma = \min\{2, 4-j\}-1$ and $\delta(t,i_1,i_2) = \left(\delta_{1-t}\,\delta_{i_1+i_2} + \delta_{1-(i_1+i_2)}\right)$.

Proof. Assume a given plaintext pair has m_1 and m_2 active bytes on any two diagonals, respectively. After SR_1, the MC_1 input has two columns containing m_1 and m_2 active bytes, respectively. Let the corresponding MC_1 output columns contain i_1 and i_2 passive bytes, and denote by t the number of passive diagonals on the output of MC_2. Since there are only two active columns at the output of MC_1, each column at the input of MC_2 can contain at most two active bytes; hence, by the branch number property, t can take only the values 0 or 1. Furthermore, if the corresponding ciphertext pair has one active inverse diagonal, where the passive bytes are distributed across the specific j columns, the $4-j$ active bytes must be located in a single column at the output of MC_4. Consequently, only one column is active on the input of MC_4 and on the output of MC_3; each active column contains exactly one active byte. By the branch number property, the active columns at the input of MC_3 therefore become fully active. As a result, the diagonals at MC_2 are either passive or fully active. Thus, every column in the input of MC_2 must be active, and every diagonal in the output of MC_1 must be active. Hence i_1+i_2 is bounded by 4, and the probability of MC_1 is $\binom{4}{i_1}\binom{4-i_1}{i_2}P_{m_1,i_1}P_{m_2,i_2}$.

After SR_2, the input of MC_1 contains one active byte in the i_1+i_2 columns and two active bytes in the remaining $4-(i_1+i_2)$ columns. Therefore, the probability of MC_2 is found to be $P_{2,t}^{4-(i_1+i_2)}$. The case $t=1$ in the output of MC_2 is stated to occur only when the input has two fully active inverse diagonals (i.e., $i_1+i_2=0$); in all other cases, the branch number property also forces $t=0$, and this is achieved by $\delta(t,i_1,i_2)$.

Finally, since the MC_2 output contains t passive and $4-t$ fully active diagonals, the MC_3 input has $4-t$ columns that are fully active. Hence, the probability of MC_3 is obtained as $4P_{4,3}^{4-t}$, and the probability that MC_4 has j passive bytes at the specific positions in the output is obtained as $P_{4-t,j}$.

Table 3 presents the ratios of the probabilities derived from Theorem 4 and those for random permutations.

(m_1, m_2)	$j=0$	$j=1$	$j=2$	$j=3$
$(1,1)$	1.000296695	1.000295332	1.000403601	0.999380157
$(1,2)$	1.000284748	1.000283426	1.000387547	0.999629982
$(1,3)$	1.000286335	1.000285012	1.000389174	0.999629026
$(1,4)$	1.000286319	1.000284996	1.000389158	0.999629030
$(2,2)$	1.000214442	1.000213159	1.000313208	0.999816419
$(2,3)$	1.000216222	1.000214939	1.000315027	0.999815699
$(2,4)$	1.000216205	1.000214923	1.000315010	0.999815702
$(3,3)$	1.000218003	1.000216720	1.000316848	0.999814980
$(3,4)$	1.000217987	1.000216703	1.000316831	0.999814983
$(4,4)$	1.000217970	1.000216687	1.000316814	0.999814985

Table 3: Ratios of probabilities for different (m_1, m_2, j) values relative to a random permutation, as in Theorem 4. We assume $m_1 \leq m_2$ without loss of generality, since MC transition probabilities are invariant under swapping m_1 and m_2.

5.1 Partial verifications of probabilities for multiple active diagonals

In this section, we verify the common input-output cases shared by the theorem pairs Theorem 1–Theorem 3, Theorem 2–Theorem 4, and Theorem 3–Theorem 4, respectively. We also re-verify, using a computer implementation[4], that these pairs of theorems yield the same results in the common cases.

Theorem 1 and Theorem 3 In Theorem 1, for $i=3$, we compute the probability that, for a given plaintext pair with m active bytes in one active diagonal, the corresponding ciphertext pair has three passive inverse diagonals and one active inverse diagonal. In Theorem 3, for $i=1$, given a plaintext pair with one active diagonal, we compute the probability that the corresponding ciphertext pair has the

[4] GitHub Code Repository

given three passive inverse diagonals and one active inverse diagonal, with exactly m passive bytes in the active inverse diagonal.

It should be noted that, in the first part of Theorem 1, the positions of the passive inverse diagonals in the ciphertext pair and the number of passive bytes in the active inverse diagonal are not specified, whereas in Theorem 3, the passive inverse diagonal positions are fixed, and the number of passive bytes is specified exactly. Therefore, for each value of m in Theorem 1, we normalize the corresponding probability by 4, apply the transition probability for the number of passive bytes in MC_4, and compute the weighted average over m. This yields the probability that the corresponding ciphertext byte is passive. Moreover, in Theorem 1, it can be easily seen that when there are exactly three passive inverse diagonals in the ciphertext pair, the active column in the input of MC_4 must be fully active.

Indeed, let $D(m) = \binom{4}{m} \cdot 2^{31} \cdot (2^8 - 1)^m$ denote the number of pairs that, for a given active diagonal, contain m active bytes and $4 - m$ passive bytes. The weighted average is computed as follows:

$$\sum_{m=1}^{4} \frac{D(m) \cdot \Pr[m \to 3] \cdot \binom{4}{j} \cdot P_{4,j}}{4 \cdot 2^{31} \cdot (2^{32} - 1)}. \tag{9}$$

If we incorporate the equalities of expressions $D(m)$, $\Pr[m \to 3]$ and $P_{4,j} = \frac{P_{4-j,0}}{(2^8-1)^j}$ into Equation 9, we get

$$\frac{\binom{4}{j} \cdot P_{4-j,0} \cdot P_{4,3+}^4}{(2^8 - 1)^j \cdot (1 - 2^{-8})^{-4} \cdot (1 - 2^{-32})}.$$

This expression is the same $\Pr[1 \Rightarrow j]$ obtained in Theorem 3 for each j.

Theorem 2 and Theorem 4 In both Theorem 2 and Theorem 4, we compute the probability that, after 5-round AES encryption of the corresponding plaintext pairs, the resulting ciphertext pairs have three passive inverse diagonals and one active inverse diagonal, and that the passive bytes in the active inverse diagonal are located in the given j columns. Therefore, the probabilities obtained for the common plaintext pair cases in these theorems are expected to coincide.

The common plaintext pair case for these theorems is the case in which the plaintext pair consists of two active diagonals, with one active byte in each diagonal. Therefore, for each value of $j = 0, 1, 2, 3$, the values obtained in Theorem 2 with $i = 2$ and in Theorem 4 with $m_1 = m_2 = 1$ are equal. If the relevant values are substituted into Theorem 4, the following expression is obtained,

$$\sum_{t=0}^{\min\{2,4-j\}-1} 4 \cdot \binom{4}{t} \cdot P_{2,t}^4 \cdot P_{4,3}^{4-t} \cdot P_{4-t,j}.$$

This expression is the same as the one obtained in Theorem 2 for $i = 2$ and for each j.

Theorem 3 and Theorem 4 We compute the probability that a ciphertext pair exhibits three passive and one active inverse diagonal under different input configurations (see Theorems 3 and 4). In Theorem 3, the active bytes within the inverse diagonal may occupy arbitrary positions, whereas in Theorem 4 they are constrained to specific column positions. This distinction leads to different combinatorial factors in the corresponding `MixColumns` transitions: a factor of $\binom{4}{m}$ in the former case and 4 in the latter.

Consequently, for $i = 2$ in Theorem 3 and for each m, the probability given in Theorem 3, divided by $\binom{4}{m}$, is expected to be equal to the weighted average, divided by 4, over the j values corresponding to that m, and over all (m_1, m_2), of the probabilities stated in Theorem 4. Indeed, let $\Pr(m_1, m_2, j)$ denote the probability given by Equation 8, which is derived from Theorem 4, evaluated for the parameters (m_1, m_2) and j. The weighted average is computed as follows:

$$\frac{\sum_{m_1=1}^{4}\sum_{m_2=m_1}^{4}(2\cdot\delta_{m_2-m_1}+\delta_{m_1-m_2+1})\cdot D(m_1)\cdot D(m_2)\cdot P(m_1,m_2,j)}{(2^{31}\cdot(2^{32}-1))^2}.$$

Thus, for each value of m, $\dfrac{\Pr[2\Rightarrow m]}{\binom{4}{m}}$ equals the weighted average, divided by 4, calculated on the values of j corresponding to m and over all (m_1, m_2) of the probabilities $P(m_1, m_2, j)$.

6 Ciphertext-only attacks

We demonstrate the effectiveness of our new truncated differentials, particularly those starting with multiple active diagonals, by mounting a ciphertext-only attack on 6-round AES, and a distinguishing attack on 5-round AES.

Our ciphertext-only attacks are based on Theorem 3, which is derived by exploiting the structural symmetry of AES. In particular, the decryption function can be expressed in a form analogous to the encryption function [11]. This design feature ensures structural consistency between encryption and decryption.

In this work, we utilize this symmetry to define truncated differentials with arbitrary input differences, which in turn enables the construction of ciphertext-only attacks on 6-round AES.

The 6-round attack is illustrated in Figure 9. Moreover, Algorithm 1 details the procedure to mount the ciphertext-only key recovery attack on 6-round AES-128.

Under a uniform random model, i.e., in the idealized case where bytes are truly random, the collision probability of two independent bytes is 1/256 (approximately 0.39%). However, in the ciphertext-only setting, if we assume that plaintexts consist of natural English sentences encoded in ASCII, character frequencies are far from uniform, and the index of coincidence (IoC) yields a typical collision probability of about 6%–8% [9, 30]. In our analysis, we adopt the worst-case assumption for an attacker by taking the lower bound $6\% \approx 2^{-4.06}$.

Similarly, if we assume that plaintexts are generated uniformly over the 95 printable ASCII characters, each occurring with equal probability, then the probability that

a byte is passive is approximately $2^{-6.57}$. Consequently, under both the English-ASCII and the uniform-ASCII plaintext assumptions, the probability that exactly i $(1 \leq i \leq 4)$ diagonals are active in a plaintext pair changes (see Table 4).

i	Probability
1	$\frac{4(1-2^{-16.24})(2^{-4.06})^{12}}{1-2^{-64.9}} \approx 2^{-46.7}$
2	$\frac{6(1-2^{-16.24})^2(2^{-4.06})^{8}}{1-2^{-64.9}} \approx 2^{-29.9}$
3	$\frac{4(1-2^{-16.24})^3(2^{-4.06})^{4}}{1-2^{-64.9}} \approx 2^{-14.2}$
4	$\frac{(1-2^{-16.24})^4}{1-2^{-64.9}} \approx 1-2^{-14.2}$

English-ASCII plaintext assumption

i	Probability
1	$\frac{4(1-2^{-26.28})(2^{-6.57})^{12}}{1-2^{-105.1}} \approx 2^{-76.8}$
2	$\frac{6(1-2^{-26.28})^2(2^{-6.57})^{8}}{1-2^{-105.1}} \approx 2^{-50.0}$
3	$\frac{4(1-2^{-26.28})^3(2^{-6.57})^{4}}{1-2^{-105.1}} \approx 2^{-24.3}$
4	$\frac{(1-2^{-26.28})^4}{1-2^{-105.1}} \approx 1-2^{-24.3}$

Uniform-ASCII plaintext assumption

Table 4: Probabilities that a plaintext pair contains i active diagonals and $4-i$ passive diagonals under two plaintext models: natural English ASCII text and uniformly random ASCII text.

Our ciphertext-only attacks are instantiated on English-language plaintexts encoded in ASCII and on uniformly distributed ASCII plaintexts in order to provide concrete redundancy estimates and explicit complexity evaluations. More generally, the attacks rely on plaintext redundancy and a sufficiently high index of coincidence in the underlying byte distribution, and are therefore not inherently restricted to ASCII-based encodings. In particular, for English plaintexts consisting only of ASCII characters, UTF-8 encoding coincides with ASCII at the byte level, so the same redundancy assumptions and attack complexities apply directly. More broadly, similar distinguishing behavior is expected for plaintext sources exhibiting comparable statistical redundancy properties.

6.1 Ciphertext-only distinguishing attack on 5-round AES

Theorem 3 enables the construction of a ciphertext-only distinguisher for 5-round AES. By aggregating the probabilities $\Pr[i \Rightarrow 0]$ given in Theorem 3 under the English-ASCII plaintext model, we obtain the probability that a ciphertext pair of 5-round AES contains exactly four active bytes within a fixed inverse diagonal:

$$P_A = \frac{\sum_{i=1}^{4} \binom{4}{i} \Pr[i \Rightarrow 0] \cdot (1-2^{-16.24})^i \cdot (2^{-4.06})^{4(4-i)}}{1-2^{-64.9}} \approx 2^{-96.0226}, \tag{10}$$

where $1-2^{-64.9}$ denotes the probability that a plaintext pair contains at least one active diagonal. The expression is obtained by conditioning on this event, since

the two ciphertexts in each pair are distinct and thus the corresponding plaintext difference is non-zero. For a random permutation, the corresponding probability is

$$P_R = \frac{2^{-96} \cdot (1 - 2^{-8})^4}{1 - 2^{-128}}. \tag{11}$$

Hence, the resulting distinguishing gap is given by the ratio

$$\frac{P_A}{P_R} \approx 1 + 2^{-35.22}. \tag{12}$$

We mount a ciphertext-only distinguishing attack by using the above ratio ($P_A/P_R \approx 1 + 2^{-35.22}$). We adopt the approximation given in [29] to find the amount of data required to reach a 95% success rate. As defined in [29], α denotes the Type-I error probability (i.e., the probability of rejecting the AES output), while β denotes the Type-II error probability (i.e., the probability of accepting random data as AES output). We use the following equation:

$$N \approx \frac{3 \cdot \left(\sqrt{P_A \cdot \ln(1/\alpha)} + \sqrt{P_R \cdot \ln(2/\beta)}\right)^2}{(P_A - P_R)^2}. \tag{13}$$

Substituting $\alpha = \beta = 0.05$ yields $N \approx 2^{171.8}$. Accordingly, we use $2^{86.4}$ ciphertexts to generate $2^{171.8}$ ciphertext pairs. The threshold thd that satisfies the α and β constraints can be computed as

$$thd \;=\; N \cdot \big(P_A - P_R\big) \;-\; \sqrt{3 \cdot N \cdot P_A \cdot \ln(1/\alpha)}, \tag{14}$$

and, equivalently, from the random sampling bound as

$$thd \;=\; \sqrt{3 \cdot N \cdot P_R \cdot \ln(2/\beta)}. \tag{15}$$

For the chosen parameters, this yields $thd \approx 2^{39.6}$. The success probability of the distinguisher is computed as follows.

Let H_1: the output is produced by AES,
H_0: the output is produced by a random permutation, with equal priors $P(H_1) = P(H_0) = \frac{1}{2}$. Denote the distinguisher's decision by $D \in \{0, 1\}$ ($D = 1$ indicates AES). By the law of total probability, the overall success probability is

$$P_{\text{succ}} = P(D = 1 \mid H_1)\, P(H_1) + P(D = 0 \mid H_0)\, P(H_0).$$

Since $P(D = 1 \mid H_1) = 1 - \alpha$ and $P(D = 0 \mid H_0) = 1 - \beta$, we get

$$P_{\text{succ}} = \tfrac{1}{2}(1 - \alpha) + \tfrac{1}{2}(1 - \beta) = 1 - \frac{\alpha + \beta}{2}.$$

For $\alpha = \beta = 0.05$ this evaluates to

$$P_{\text{succ}} = 1 - \frac{0.05 + 0.05}{2} = 0.95.$$

As a result, we distinguish 5-round AES from a random permutation with a 95% success probability. The time complexity of the attack is $86.4 \cdot 2^{86.4} \approx 2^{92.8}$ memory accesses.

If we assume that plaintexts are generated uniformly over printable ASCII characters, then there are only 95 possible characters, each occurring with equal probability. In this case, the probability that a byte is passive is

$$\sum_{i=1}^{95} \left(\frac{1}{95}\right)^2 = \frac{1}{95} \approx 2^{-6.57}.$$

Under this assumption, we obtain that

$$P_A = \frac{\sum_{i=1}^{4} \binom{4}{i} \Pr[i \Rightarrow 0] \cdot (1 - 2^{-28.62})^i \cdot (2^{-6.57})^{4(4-i)}}{1 - 2^{-105.1}} \approx 2^{-96.02258625256}$$

and $P_A/P_R \approx 1 + 2^{-45.3}$. Substituting P_A, P_R, and $\alpha = \beta = 0.05$ into Equations 13 and 14 yields $N \approx 2^{191.9}$ and $thd \approx 2^{49.7}$, as in the English-ASCII plaintext assumption. Thus, we need $2^{96.5}$ ciphertexts to generate $2^{191.9}$ ciphertext pairs. Consequently, we distinguish 5-round AES from a random permutation with a 95% success probability, and the time complexity of the attack is $96.5 \cdot 2^{96.5} \approx 2^{103.1}$ memory accesses, under the assumption that plaintexts are generated uniformly over printable ASCII characters.

6.2 Ciphertext-only attack on 6-round AES

We introduce ciphertext-only attacks on 6-round AES under the English-ASCII plaintext assumption for all key sizes, and under the uniform-ASCII plaintext assumption for AES-192 and AES-256. The distinguisher starts from an arbitrary input pair and, after five rounds, results in a single active byte in a given inverse diagonal. By appending one additional round, we extend this construction to a 6-round encryption.

We compute a weighted sum over the indices i for $m = 3$, as described in Section 6.1, to evaluate the probability that a ciphertext pair of 5-round AES contains exactly one active byte in a fixed inverse diagonal under the English-ASCII plaintext assumption. The resulting expression is given by

$$\frac{\sum_{i=1}^{4} \binom{4}{i} \Pr[i \Rightarrow 3] \cdot (1 - 2^{-16.24})^i \cdot (2^{-4.06})^{4(4-i)}}{1 - 2^{-64.9}} \approx 2^{-118.006}.$$

On the other hand, for a random permutation, this probability is

$$\frac{4 \cdot 2^{-120} \cdot (1 - 2^{-8})}{(1 - 2^{-128})}.$$

It is known to the attacker that a ciphertext pair contains exactly one fully active inverse diagonal at positions $[0, 7, 10, 13]$. Therefore, when this pair is partially decrypted with the correct subkey $RK_6[0, 7, 10, 13]$, the probability that the resulting difference in ΔSR_5 consists of exactly one active byte is

$$P_A = \frac{2^{-118.006} \cdot (1 - 2^{-128})}{2^{-96} \cdot (1 - 2^{-8})^4},$$

since the event of having a single fully active inverse diagonal occurs with probability one whenever ΔSR_5 contains only one active byte.

For a wrong key, the corresponding conditional probability that ΔSR_5 has exactly one active byte is given by $4 \cdot P_{4,3}$ according to Lemma 1. Note that

$$P_R = 4 \cdot P_{4,3} = \frac{4 \cdot 2^{-120} \cdot (1 - 2^{-8})}{2^{-96} \cdot (1 - 2^{-8})^4}.$$

Comparing this probability under the correct key with the probability under a wrong key, we obtain a ratio of approximately $1 + 2^{-36.24}$.

We first compute the data complexity required to reach the target success probability and to discard the desired proportion of wrong keys. We then describe the attack procedure in detail.

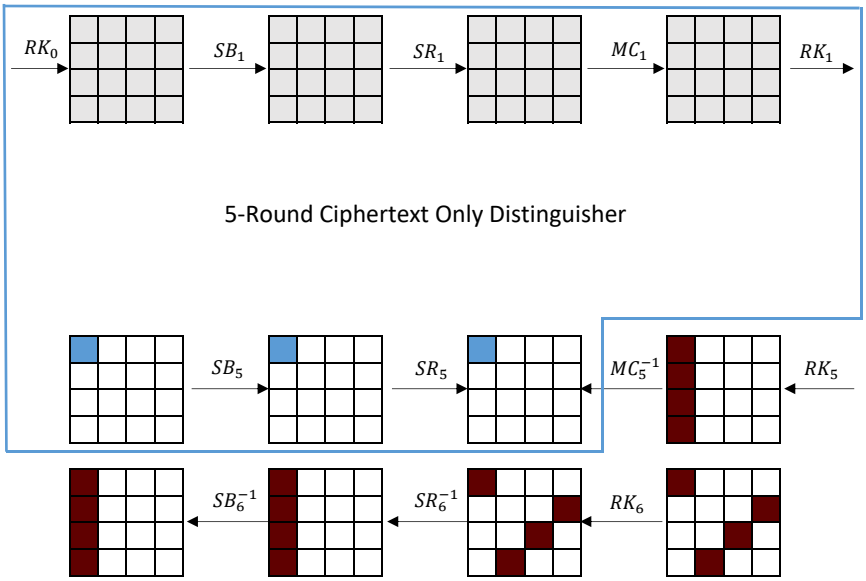


Fig. 9: Illustration of the 6-round ciphertext-only attack. Blue boxes denote active states of the distinguisher, maroon boxes denote active states in the last round appended to the distinguisher, white boxes denote passive states, and gray boxes denote unknown free bytes.

We set the attack's target success rate to 95% ($\alpha = 0.05$) and the Type-II error probability to $\beta = 2^{-32}$. Substituting P_A, P_R, α, and β into Equation 13 and Equation 14 directly yields $N \approx 2^{101.4}$ and $thd \approx 2^{42.8}$, as in Section 6.1. The probability that a ciphertext pair has exactly twelve passive bytes in specified positions is approximately 2^{-96}. Hence, the total number of pairs required is approximately $2^{101.4+96} = 2^{197.4}$.

Each key candidate is tested using $2^{101.4}$ pairs to count how many pairs satisfy the output difference of the distinguisher. Keys whose counts exceed the predetermined threshold are retained as candidates, while keys that do not exceed the threshold are discarded as wrong. Since the targeted subkey is 32 bits and the probability that a wrong key exceeds the threshold is 2^{-32}, all wrong candidates are eliminated with about 95% success over the 2^{32} possibilities. This leaves only the correct 32-bit subkey (see Step 3 for details).

The attack is described in the following step-by-step procedure.

1. There are $2^{197.4}$ ciphertext pairs, which are derived from $2^{99.2}$ ciphertexts. Discard pairs whose ciphertexts have a non-zero difference in bytes $[1, 2, 3, 4, 5, 6, 8, 9, 11, 12, 14, 15]$. Thus, approximately $2^{197.4} \cdot 2^{-96} = 2^{101.4}$ pairs remain after the filtering step (lines 2–7 of Algorithm 1), and these remaining pairs are added to the list A. The memory complexity of storing this list is approximately $2 \cdot 2^{101.4} \cdot 2^7 = 2^{109.4}$ bits, i.e., $2^{106.4}$ bytes.

2. We guess the 8-bit subkey $RK_6[0]$. Then, for each guess, we initialize an empty counter list B_i, where $1 \leq i \leq 2^{24}$, for each possible value of $RK_6[7, 10, 13]$ (line 9 of Algorithm 1). Then, with the guess fixed, for a ciphertext pair, we decrypt it through one round using this subkey. Next, we determine the 24-bit subkey $RK_6[7, 10, 13]$ by solving the three linear equations $\Delta MC_5^{-1}[1, 2, 3] = 0$ (lines 10–16 of Algorithm 1). As a result, the pair produces $2^{24} \cdot 2^{-22} = 2^2$ key candidates that satisfy the output difference of the distinguisher. We increment the counter B_i associated with each 2^2 subkey (line 14 of Algorithm 1) and repeat the process for each pair.

3. Finally, for each i, we check the counter B_i; if it exceeds the threshold, we record the key as a candidate together with the fixed 8-bit key; otherwise, it is discarded (lines 17-21 of Algorithm 1). We repeat this procedure for each guess of $RK_6[0]$.

The value *thd* defined above is the threshold for the difference between the expected values of P_A and P_R. Therefore, for the key $RK_6[7, 10, 13]$ the threshold is $thd + N \cdot P_R \approx 2^{42.8} + 2^{79.5}$. We generate 2^{24} counters and each counter has roughly 80 bits. Thus, the memory complexity of this operation is $2^{24} \cdot 80 \approx 2^{30.3}$ bits (i.e., $2^{27.3}$ bytes).

We have a total of 2^{32} candidate subkeys. The attack eliminates approximately all wrong keys with a success rate of approximately 95%; in that case, only the correct subkey remains (lines 18-22 of Algorithm 1).

In summary, for each of the $2^{101.4}$ pairs, 2^{10} subkeys satisfy the output difference of the distinguisher, resulting in $2^{101.4} \cdot 2^{10} = 2^{111.4}$ memory accesses, which is around $2^{108.4}$ encryptions. Moreover, we perform 2^{10} increment (addition) operations for each of the $2^{101.4}$ pairs, therefore, the complexity of this step is $2^{10} \cdot 2^{101.4} = 2^{111.4}$ additions. The overall time complexity of the attack is $2^{111.4}$ additions. The overall memory complexity is $2^{106.4}$ bytes, and the data complexity is $2^{99.2}$ ciphertexts. If we repeat the attack four times using the same ciphertext pairs and, in each run, choose the position of the active byte in the output of the 5-round distinguisher so that the positions lie in different columns, we recover the entire 128-bit key. Thus, the attack's overall time complexity is $2^{113.4}$ additions for AES-128.

Algorithm 1: Ciphertext-only Attack on 6-Round AES (English-ASCII)

Require: $2^{99.2}$ ciphertexts
Ensure: Correct 32-bit subkey $RK_6[0, 7, 10, 13]$

Initialize empty lists A and K
for each ciphertext pair (C_m, C_n), where $1 \leq m < n$, generated from the $2^{99.2}$ ciphertexts **do**
    if $\Delta(C_m[t], C_n[t]) = 0$ for all $t \notin S$ and $\Delta(C_m[t], C_n[t]) \neq 0$ for all $t \in S$, where $S = \{0, 7, 10, 13\}$ **then**
        Add (C_m, C_n) to the list A
    end if
end for
for each 8-bit guess for $RK_6[0]$ **do**
    Initialize an empty counter list B_i for each possible value of $RK_6[7, 10, 13]$, where $1 \leq i \leq 2^{24}$
    for each ciphertext pair (C_m, C_n) in A **do**
        Compute $\Delta SB_6^{-1}[1, 2, 3]$ through $\Delta MC_5^{-1}[1, 2, 3] = 0$
        if $SB_{out}^{in}(\Delta SB_6^{-1}[1, 2, 3], \Delta SB_6) \neq \emptyset$ **then**
            Determine subkeys for $RK_6[7, 10, 13]$
            Increment the counter B_i associated with each subkey
        end if
    end for
    for each $i \in \{1, \ldots, 2^{24}\}$, where i indexes one candidate value of $RK_6[7, 10, 13]$ **do**
        if counter of $B_i > 2^{79.5} + 2^{42.8}$ **then**
            Add 32-bit subkey $(RK_6[0, 7, 10, 13])$ to K
        end if
    end for
end for
return list K

If we assume that plaintexts are generated uniformly over printable ASCII characters, the probability that a ciphertext pair of 5-round AES contains one active byte in one given inverse diagonal,

$$\frac{\sum_{i=1}^{4} \binom{4}{i} \Pr[i \Rightarrow 3] \cdot (1 - 2^{-28.62})^i \cdot (2^{-6.57})^{4(4-i)}}{1 - 2^{-105}} \approx 2^{-118.00564656314}.$$

If we calculate P_A and P_R as in the English-ASCII plaintext assumption, we obtain

$$P_A / P_R \approx 1 + 2^{-46.3}.$$

Substituting P_A, P_R, $\alpha = 0.05$, and $\beta = 2^{-32}$ into Equations 13 and 14 yields $N \approx 2^{121.6}$ and $thd \approx 2^{52.8}$. Hence, the total number of pairs required is approximately $2^{121.6+96} = 2^{217.6}$.

This allows us to recover the 128-bit subkey RK_6. Under the uniform-ASCII plaintext assumption, the time complexity of the attack is $2^{133.6}$ additions, the memory complexity is $2^{126.6}$ bytes, and the data complexity is $2^{109.3}$ ciphertexts.

For AES-128, the time complexity exceeds that of exhaustive search, and thus the attack is not competitive in this setting. Consequently, under the uniform-ASCII assumption, the attack is applicable only to AES-192 and AES-256.

For AES-192, we guess the 64-bit $RK_5[8, 9, 10, 11, 12, 13, 14, 15]$ and combine each candidate with the recovered 128-bit RK_6. Then, we can decrypt a given ciphertext and check whether the resulting plaintext is generated uniformly over printable ASCII characters for each candidate key to recover the main key. However, when this ciphertext is decrypted with a wrong key, there is a risk of obtaining a plaintext that satisfies the assumption. We know that the probability that a byte of the resulting plaintext satisfies the assumption is $95/256 \approx 2^{-1.43}$. Thus, the probability that the plaintext satisfies the assumption is

$$(2^{-1.43})^{16} \approx 2^{-22.9}.$$

As a result, the unicity distance is approximately $64/22.9 \approx 2.79$ blocks. Therefore, three independent ciphertexts are sufficient to determine whether a given 192-bit candidate key is correct with high confidence. In practice, using 3–4 ciphertexts provides a comfortable safety margin.

We then perform an exhaustive search to recover the master key using four ciphertexts. The time complexity of this step is $4 \cdot 2^{64} \approx 2^{66}$ encryptions and is not dominant in the overall attack.

Consequently, for the attack on 6-round AES-192, the overall time complexity is $2^{133.6}$ additions, the memory complexity is $2^{126.6}$ bytes, and the data complexity is $2^{109.3}$ ciphertexts.

For AES-256, we first guess the 128-bit subkey RK_5 and combine each candidate with the recovered 128-bit subkey RK_6. The resulting unicity distance is approximately $128/22.9 \approx 5.59$ blocks, which implies that 7–8 ciphertexts are sufficient to recover the correct key with high confidence. Based on this, we perform an exhaustive search over the master key using the available 8 ciphertexts. The time complexity of this procedure is approximately $8 \cdot 2^{128} \approx 2^{131}$ encryptions. Consequently, for the attack on 6-round AES-256, the overall time complexity is 2^{131} encryptions, the memory complexity is $2^{126.6}$ bytes, and the data complexity is $2^{109.3}$ ciphertexts.

The probability that the plaintext obtained by decrypting a given ciphertext under a randomly chosen key corresponds to natural English text encoded in ASCII is lower than the probability that it consists of characters uniformly distributed over the printable ASCII alphabet. Consequently, the unicity distance computed under the English-ASCII plaintext assumption is smaller than that computed under the uniform-ASCII plaintext assumption. Therefore, the number of ciphertexts required for an exhaustive search under the uniform-ASCII assumption is sufficient to recover the correct key with high confidence under the English-ASCII assumption as well.

As a result, under the English-ASCII plaintext assumption, we guess the 64-bit $RK_5[8, 9, 10, 11, 12, 13, 14, 15]$ for AES-192 and the 128-bit RK_5 for AES-256 and

combine each candidate with the recovered 128-bit RK_6, to perform two brute-force attacks to recover the master key using 4 and 8 ciphertexts for AES-192 and AES-256, respectively. Thus, for AES-192, the time complexity of exhaustive search is $4 \cdot 2^{64} \approx 2^{66}$ encryptions; however, the overall time complexity is $2^{113.4}$ additions. For AES-256, the time complexity of exhaustive search is $8 \cdot 2^{128} \approx 2^{131}$ encryptions, and this term dominates the overall time complexity. For both attacks, the memory complexity is $2^{106.4}$ bytes and the data complexity is $2^{99.2}$ ciphertexts.

Remark 3. We also show that the proposed attack can be converted to a chosen-plaintext setting. For example, for $i = 2$, the corresponding distinguisher considers two active diagonals in the input and results, after five rounds, in a single active byte in a specified inverse diagonal. By appending one additional round, this construction naturally extends to a 6-round encryption.

If we compute P_A and P_R in the same manner as in the ciphertext-only attack, we obtain

$$P_A = \frac{\Pr[2 \Rightarrow 3] \cdot (1 - 2^{-128})}{2^{-96} \cdot (1 - 2^{-8})^4},$$

and

$$P_R = \frac{4 \cdot 2^{-120} \cdot (1 - 2^{-8})}{2^{-96} \cdot (1 - 2^{-8})^4}.$$

Setting $\alpha = 0.05$ and $\beta = 2^{-32}$ in Equation 13 together with the values of P_A and P_R yields $N \approx 2^{53.7}$, and therefore the total required number of pairs is approximately $2^{53.7+96} = 2^{149.7}$.

To generate this number of pairs efficiently, we use structures, where a structure denotes a set of plaintexts in which the active diagonal takes all possible values while the remaining bytes are fixed. We require approximately $2^{22.7}$ such structures, corresponding to a total of $2^{86.7}$ chosen plaintexts, since each structure provides about 2^{127} usable pairs after excluding pairs containing three passive diagonals.

The remaining steps of the attack are the same as in the ciphertext-only attack given in Algorithm 1; only the number of pairs used is different. As a result, for AES-128, the time complexity of this attack is $2^{65.7}$ additions, the memory complexity is $2^{58.7}$ bytes, and the data complexity is $2^{86.7}$ chosen plaintexts.

For AES-192 and AES-256, the fifth-round key can be recovered with significantly lower complexity by peeling off one round from the 6-round construction. For instance, the integral attack of [11] recovers the fifth-round equivalent subkey with a total complexity of approximately 2^{38} encryptions. The master key can then be recovered efficiently from two consecutive round subkeys through inversion of the AES key schedule.

7 Conclusion and future work

In this work, we introduce a systematic analytical framework for computing truncated differential probabilities in 5-round AES. Our approach unifies and extends prior analyses by providing a more general treatment of truncated differentials and enabling the derivation of distinguishers that are not readily captured by statistical or subspace-based techniques.

Using this framework, we compute truncated differential probabilities for an arbitrary number of active bytes within a plaintext diagonal under three ciphertext conditions: exactly i passive inverse diagonals ($\Pr[m \to i]$), i specified passive inverse diagonals ($\chi(m \to i^+)$), and at least i passive inverse diagonals ($\Pr[m \to i^+]$). This yields 48 distinct configurations, substantially extending the small number of previously known cases in the literature, which were limited to comparatively restricted parameter settings. We further extend the analysis to multiple active diagonals and, to the best of our knowledge, provide the first systematic treatment of truncated differentials involving multiple active diagonals in AES.

To ensure correctness, we validate our results through independent implementations, exhaustive recomputation, and consistency checks against known special cases. As an application, we derive the first ciphertext-only distinguishing attack on 5-round AES and the first ciphertext-only key-recovery attack on 6-round AES across all key sizes under standard plaintext assumptions.

Overall, our framework establishes a general foundation for truncated differential analysis in AES and, more broadly, in SPN ciphers. We focus on 5-round AES as the setting in which the resulting truncated differential structure remains sufficiently constrained to allow exact enumeration, while still exhibiting non-negligible biases that can be effectively exploited in attacks.

The independence assumption across rounds is commonly used in the literature, although it does not hold exactly for AES. Chang et al. [10] compute the probability that a given inverse diagonal is passive under the condition that the input contains only one active byte (i.e., $\chi(1 \to 1^+)$), without relying on an independence assumption. They further validate their results experimentally on mini-AES. As shown in Figure 6, their estimate of $\chi(1 \to 1^+)$ is very close to ours. The resulting difference is negligible and does not significantly affect the attack complexity estimates. Similar observations are reported by Grassi et al. [19] and Bao et al. [2], who also conduct experiments on mini-AES and conclude that the impact of independence assumptions is negligible.

What distinguishes our work is not a claim to have removed the independence assumption, but rather the observation that even under this standard heuristic, probability computations for 5-round AES involving multiple active diagonals or multiple passive inverse diagonals become substantially more complex than previously studied configurations. The required combinatorial enumeration exceeds the scope of earlier methods. The investigation of independence properties and their quantitative effect on AES-based probabilistic models constitutes a separate line of research, with several foundational studies providing partial theoretical support for such heuristic assumptions. In particular, Liu et al. [24] analyze independence properties of AES under independent round keys and show that approximate pairwise independence emerges for sufficiently many rounds.

Our contribution is to introduce a systematic analytical framework that makes these computations tractable under the same heuristic assumptions commonly used in the literature. Even if future work removes the independence assumption entirely, our results would still provide a useful baseline within the current modeling framework. The techniques we introduce, including partitioning into equivalence classes, exact MDS transition probabilities, and systematic inclusion–exclusion, would also remain applicable.

The methodology is not restricted to 5 rounds and can potentially be extended under additional structural or probabilistic relaxations. Our analysis covers configurations involving either a single active diagonal in the plaintext with arbitrary passive inverse diagonals in the ciphertext, or multiple active diagonals in the plaintext with a single passive inverse diagonal in the ciphertext. The remaining setting involving multiple active diagonals in the plaintext together with multiple passive inverse diagonals in the ciphertext for 5-round AES remains open. Another natural direction is the investigation of 6-round AES under relaxed plaintext assumptions. More broadly, the framework may also be applicable to other SPN-based designs, particularly AES-like ciphers whose diffusion layers rely on MDS or almost-MDS matrices. One example of such an extension is provided in [1] through truncated differential analysis of the Midori cipher.

Acknowledgements We thank Subhadeep Banik and Eik List for carefully reviewing an earlier draft of this paper and for their valuable feedback, and Kağan Kurşungöz for his insightful comments.

Funding This work is partially supported by TUBITAK 1001 Project under grant number 124F270.

References

[1] Can Balıkçı and Orhun Kara. Two Complementary Truncated Differential Attacks on Midori-64. *International Journal of Information Security Science*, 15(1):25–47, 2026.

[2] Zhenzhen Bao, Jian Guo, and Eik List. Extended Truncated-Differential Distinguishers on Round-reduced AES. *IACR Trans. Symmetric Cryptol.*, 2020(3):197–261, 2020.

[3] Navid Ghaedi Bardeh and Vincent Rijmen. New Key-Recovery Attack on Reduced-Round AES. *IACR Trans. Symmetric Cryptol.*, 2022(2):43–62, 2022.

[4] Navid Ghaedi Bardeh and Sondre Rønjom. The Exchange Attack: How to Distinguish Six Rounds of AES with 2ˆ88.2 Chosen Plaintexts. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III*, volume 11923 of *Lecture Notes in Computer Science*, pages 347–370, Berlin, Heidelberg, 2019. Springer.

[5] Augustin Bariant and Gaëtan Leurent. Truncated Boomerang Attacks and Application to AES-Based Ciphers. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV*, volume 14007 of *Lecture Notes in Computer Science*, pages 3–35, Cham, 2023. Springer.

[6] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. *J. Cryptol.*, 18(4):291–311, 2005.

[7] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21, Berlin, Heidelberg, 1990. Springer.

[8] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique Cryptanalysis of the Full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 344–371, Berlin, Heidelberg, 2011. Springer.

[9] Derek C Brown. A Cryptanalysis of The Autokey Cipher Tsing The Index of Coincidence. In *Proceedings of the 2018 ACM Southeast Conference*, pages 1–8, 2018.

[10] Chengcheng Chang, Meiqin Wang, Ling Sun, and Wei Wang. Improved Truncated Differential Distinguishers of AES with Concrete S-Box. In Takanori

Isobe and Santanu Sarkar, editors, *Progress in Cryptology - INDOCRYPT 2022 - 23rd International Conference on Cryptology in India, Kolkata, India, December 11-14, 2022, Proceedings*, Lecture Notes in Computer Science, pages 422–445. Springer, 2022.

[11] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, Berlin, Heidelberg, 2002.

[12] Hüseyin Demirci and Ali Aydin Selçuk. A Meet-in-the-Middle Attack on 8-Round AES. In Kaisa Nyberg, editor, *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 116–126, Heidelberg, Germany, 2008. Springer.

[13] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 371–387, Berlin, Heidelberg, 2013. Springer.

[14] Victor Dolgov, Victor Ruzhentsev. Towards Provable Security of Rijndael-like SPN Ciphers Against Differential Attacks. *Tatra Mt. Math. Publ*, 53:189–199, 2012.

[15] Morris Dworkin, Elaine Barker, James Nechvatal, James Foti, Lawrence Bassham, E. Roback, and James Dray. Advanced Encryption Standard (AES), 2001-11-26 2001.

[16] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David A. Wagner, and Doug Whiting. Improved Cryptanalysis of Rijndael. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 213–230, Heidelberg, Germany, 2000. Springer.

[17] Lorenzo Grassi. Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES. *IACR Trans. Symmetric Cryptol.*, 2018(2):133–160, 2018.

[18] Lorenzo Grassi and Christian Rechberger. Truncated Differential Properties of the Diagonal Set of Inputs for 5-Round AES. In Khoa Nguyen, Guomin Yang, Fuchun Guo, and Willy Susilo, editors, *Information Security and Privacy - 27th Australasian Conference, ACISP 2022, Wollongong, NSW, Australia, November 28-30, 2022, Proceedings*, volume 13494 of *Lecture Notes in Computer Science*, pages 24–45, Cham, 2022. Springer.

[19] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace trail cryptanalysis and its applications to AES. *IACR Trans. Symmetric Cryptol.*, 2016(2):192–225, 2016.

[20] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A New Structural-Differential Property of 5-Round AES. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *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*, volume 10211 of *Lecture Notes in Computer Science*, pages 289–317, 2017.

[21] Lorenzo Grassi and Markus Schofnegger. Mixture Integral Attacks on Reduced-Round AES with a Known/Secret S-Box. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 312–331, Berlin, Heidelberg, 2020. Springer.

[22] Lars R. Knudsen. Truncated and Higher Order Differentials. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211, Berlin, Heidelberg, 1994. Springer.

[23] Susan K. Langford and Martin E. Hellman. Differential-Linear Cryptanalysis. In Yvo Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 17–25, Berlin, Heidelberg, 1994. Springer.

[24] Tianren Liu, Stefano Tessaro, and Vinod Vaikuntanathan. The t-wise independence of substitution-permutation networks. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part IV*, Lecture Notes in Computer Science, pages 454–483. Springer, 2021.

[25] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New Impossible Differential Attacks on AES. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *Progress in Cryptology - INDOCRYPT 2008, 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. Proceedings*, volume 5365 of *Lecture Notes in Computer Science*, pages 279–293, Berlin, Heidelberg, 2008. Springer.

[26] Sandip Kumar Mondal, Mostafizar Rahman, Santanu Sarkar, and Avishek Adhikari. Revisiting Yoyo Tricks on AES. *IACR Trans. Symmetric Cryptol.*, 2023(4):28–57, 2023.

[27] Sondre Rønjom. A Short Note on a Weight Probability Distribution Related to SPNs. *Cryptology ePrint Archive*, 2019.

[28] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo Tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 217–243, Berlin, Heidelberg, 2017. Springer.

[29] Subhabrata Samajder and Palash Sarkar. Rigorous Upper Bounds on Data Complexities of Block Cipher Cryptanalysis. *J. Math. Cryptol.*, 11(3):147–175, 2017.

[30] Ganapathi Sivagurunathan and T Purusothaman. Reduction of Key Search Space of Vigenere Cipher Using Particle Swarm Optimization. *Journal of computer science*, 7(11):1633, 2011.

[31] David A. Wagner. The Boomerang Attack. In Lars R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170, Berlin, Heidelberg, 1999. Springer.

[32] Xueping Yan, Lin Tan, Hong Xu, and Wen-Feng Qi. The Boomerang Chain Distinguishers: New Record for 6-Round AES. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part VII*, volume 15490 of *Lecture Notes in Computer Science*, pages 301–329, Cham, 2024. Springer.