Related-Differential Distinguishers on up to 7 Rounds of AES

Xueping Yan, Lin Tan(✉), and Wenfeng Qi

Information Engineering University, Zhengzhou, China
tanlin100@163.com

Abstract. Round-reduced variants of AES are widely used as building blocks in the design of cryptographic schemes. The study of non-random properties and distinguishers for round-reduced AES has always been an important research topic. The longest known secret-key distinguishers on AES cover 6 rounds. Related differences and related differentials were introduced by the designers of AES in 2009, but research in this direction remains limited. In this paper, we provide a new perspective on related differences through exchange and shift operations. Based on related differentials, we present new non-random properties and secret-key distinguishers for up to 7 rounds of AES. For 5-round AES, we present a new property with probability 2^{-22} by combining one-round byte-wise related differentials with the 4-round zero-difference property. Then we improve the secret-key distinguishers on 5-round AES in both the chosen plaintexts (CP) and adaptively chosen plaintexts (ACP) settings, achieving data/time complexities of $2^{27.2}/2^{28.05}$ and $2^{23.32}/2^{23.54}$, respectively. For 7-round AES, we identify the first non-random property by exploiting one-round exchanged diagonal related differentials and combining them with the 4-round related differentials given by Bardeh and Rijmen. Then, we propose the first secret-key distinguisher for 7-round AES with data complexity lower than the full codebook. For 6-round AES, using shifted diagonal related differentials, we present an alternative distinguisher that is dual to the exchange-attack distinguisher from ASIACRYPT 2019.

Keywords: AES · Non-random property · Secret-key distinguisher · Related differentials

1 Introduction

The Advanced Encryption Standard (AES) [15] is the most widely used block cipher and its security has been studied worldwide in the last twenty-five years. Round-reduced variants of AES are popular underlying components in the design of cryptographic schemes, such as Hound [22], WEM [13] and TNT-AES [1]. The security evaluation of round-reduced AES is an important problem. Many cryptanalysis techniques have been applied to round-reduced AES, such as integral [21], impossible differential [9,28], zero-correlation linear [10,27,32], subspace trail [25], mixture differential [3,24,26], meet-in-the-middle [17], yoyo [29,30], exchange [4,6], boomerang [8,20,33] and related differentials [5,16].

Identifying non-random properties of round-reduced AES to distinguish it from random permutations has always been an important research topic. Before 2016, both non-random properties and distinguishing attacks on AES covered at most 4 rounds, including integral [21], impossible differential [9] and zero-correlation linear [10]. Many researchers exploited the properties of the MixColumns matrix of AES to present key-dependent 5-round distinguishers in [23,27,32]. In EUROCRYPT 2017, Grassi et al. [26] proposed a new structural property for 5-round AES, called multiple-of-8 property. Based on this property, they presented the first secret-key distinguisher on 5-round AES. In [11], Boura et al. gave a general proof of the multiple-of-8 property for AES-like ciphers. In [6], Bardeh and Rønjom used the exchange attack to obtain an improved 5-round distinguisher with complexity of 2^{30}, which is the best known distinguisher on 5-round AES in the chosen plaintexts (CP) setting. In the adaptive setting, some 5-round distinguishers on AES were proposed using the techniques of exchange [4], yoyo [29,30], zero-difference [7] and boomerang [19,31].

In ASIACRYPT 2017, Rønjom et al. [30] presented the yoyo distinguishers for up to 6 rounds of AES in the adaptively chosen plaintexts and ciphertexts (ACPC) setting. In [29], the 6-round yoyo distinguisher was shown to be ineffective with the proposed data complexity. In ASIACRYPT 2019, Bardeh and Rønjom [6] proposed the exchange attack, and gave a distinguisher on 6-round AES in the CP setting with complexity of $2^{88.2}$. In [4], Bardeh gave an exchange-attack distinguisher on 6-round AES in the adaptively chosen ciphertexts (ACC) setting with complexity of 2^{84}. Bao et al. [2] gave a truncated differential distinguisher on 6-round AES in the CP setting. In EUROCRYPT 2023, Bariant and Leurent [8] proposed the truncated boomerang attack and gave a distinguisher on 6-round AES in the ACC setting. In ASIACRYPT 2024, Yan et al. [33] proposed the boomerang chain distinguisher on 6-round AES in the ACPC setting with complexity of $2^{76.57}$.

Motivation. Related differences and related differentials were proposed by the designers of AES in [16]. However, they have rarely been directly applied to attacks on AES except for the 7-round key-recovery attack given by Bardeh and Rijmen [5]. In fact, some recent cryptanalysis for AES, such as the exchange attack [4,6], yoyo tricks [29,30] and mixture differential [24], utilized the related differences with the zero-difference property. In [5], Bardeh and Rijmen estimated the probabilities of related differentials for 2 and 4 rounds of AES, and combined them with the 4-round zero-difference property to present some properties for 6 and 8 rounds of AES. It is worthwhile to further study the propagation probability of related differentials to explore new properties for AES.

Currently, the distinguishers on AES cover at most 6 rounds. Can 7-round AES be distinguished from a random permutation? This is a challenging problem in the academic research. Based on the observation of recent attacks on round-reduced AES, combined cryptanalysis may give better results, such as differential meet-in-the-middle [12], exchanged boomerang [31,33], and partial sums meet FFT [18]. Can related differentials be combined with other cryptanalysis techniques to improve the distinguishers on round-reduced AES?

Contributions. We provide a new insight on related differences from the perspectives of exchange and shift operations. For any related differences $\Delta x, \Delta x'$ and any state α, the pair $(\alpha + \Delta x', \alpha + \Delta x + \Delta x')$ can be obtained by exchanging or shifting some components of $(\alpha, \alpha + \Delta x)$, or by the mixed application of these two operations. By combining the related-differential cryptanalysis with the techniques of zero-difference, exchange and shift, we present new non-random properties for 5 to 7 rounds of AES. Based on these properties, we propose the first secret-key distinguisher on 7-round AES, improve the secret-key distinguishers on 5-round AES in both the CP and ACP settings, and present an alternative distinguisher on 6-round AES. These properties and distinguishers are independent of the details of the S-box, and therefore remain applicable even when the S-box is secret. The main results of secret-key distinguishers on round-reduced AES are listed in Table 1.

New non-random property and improved distinguishers for 5-round AES in both the CP and ACP settings. We present certain byte-wise related differentials over one-round AES, and combine them with the 4-round zero-difference property to present a new property for 5-round AES with probability 2^{-22}, while the probability is 2^{-32} for a random permutation. Based on the property, we improve the secret-key distinguishers on 5-round AES in both the CP setting and ACP setting, achieving data/time complexities of $2^{27.2}/2^{28.05}$ and $2^{23.32}/2^{23.54}$, respectively. We have verified experimentally the validity of these distinguishers.

The first non-random property and secret-key distinguisher for 7-round AES. We derive a formula for estimating the probability of exchanged diagonal related differentials over one-round AES. By combining certain one-round exchanged diagonal related differentials with 4-round related differentials given by Bardeh and Rijmen [5], we identify the first non-random property for 7-round AES. Based on the property, we propose the first secret-key distinguisher on 7-round AES with $2^{125.6}$ chosen plaintexts, extending the state of the art by one round.

An alternative distinguisher on 6-round AES. The exchange-attack distinguishers in [4,6] are actually based on the exchanged diagonal related differentials. Due to the relationship between the exchanged and shifted related differences, we utilize shifted diagonal related differentials to present an alternative distinguisher on 6-round AES with $2^{88.23}$ chosen plaintexts, which is dual to the 6-round exchange-attack distinguisher [6].

Organization. Sect. 2 gives some preliminaries. Sect. 3 provides a new insight on related differences from the perspectives of exchange and shift operations. In Sect. 4, we present a new property for 5-round AES, and improve the distinguishers on 5-round AES in both the CP and ACP settings. In Sect. 5, we present a non-random property and a distinguisher on 7-round AES. In Sect. 6, we give an alternative distinguisher on 6-round AES. The conclusion is given in Sect. 7. The code for all experiments in this paper is available at

https://github.com/XuepingYan/Distinguish-Round-Reduced-AES.

Table 1. Secret-key distinguishers on 5 to 7 rounds of AES

Technique	Rounds	Data[†]	Time[‡]	Memory	Succ.[*]	Reference
Multiple-of-8	5	2^{32} CP	$2^{35.6}$ M	2^{32}	100%	[26]
Exchange Attack	5	2^{30} CP	2^{30} E	2^{30}	63%	[6]
RD & ZD[*]	5	$2^{27.2}$ CP	$2^{28.05}$ E	$2^{15.6}$	63%	Subsect. 4.2
Yoyo	5	$2^{29.95}$ ACPC	$2^{29.95}$ E	-	55%	[29]
Yoyo	5	$2^{30.65}$ ACPC	$2^{30.65}$ E	-	81%	[29]
Exchange Attack	5	2^{39} ACC	2^{39} E	$2^{35.5}$	63%	[4]
Zero-Difference	5	$2^{27.2}$ ACC	$2^{27.2}$ E	$2^{12.2}$	58%	[7]
Retracing Boomerang	5	2^{31} ACC	2^{31} E	2^{31}	-	[19]
Exchanged Boomerang	5	$2^{27.1}$ ACC	$2^{27.1}$ E	$2^{12.58}$	80%	[31]
RD & ZD	5	$2^{23.32}$ ACP	$2^{23.54}$ E	2^{18}	63%	Subsect. 4.3
RD & ZD	5	$2^{24.07}$ ACP	$2^{24.29}$ E	2^{18}	81%	Subsect. 4.3
Truncated Boomerang	6	2^{87} ACC	2^{87} E	2^{64}	84%	[8]
Exchange Attack	6	2^{84} ACC	2^{84} E	2^{32}	63%	[4]
Boomerang Chain	6	$2^{76.57}$ ACPC	$2^{76.57}$ E	2^{32}	60%	[33]
Truncated Differential	6	$2^{89.4}$ CP	$2^{96.5}$ M	2^{33}	95%	[2]
Exchange Attack	6	$2^{88.2}$ CP	$2^{88.2}$ E	$2^{88.2}$	63%	[6]
RD & Shift	6	$2^{88.23}$ CP	$2^{89.1}$ E	$2^{88.23}$	63%	Sect. 6
RD & Exchange	7	$2^{125.6}$ CP	$2^{127.18}$ E	$2^{129.4}$	63%	Subsect. 5.2

[*] RD: Related Differentials, ZD: Zero-Difference, Succ.: Success Probability.
[†] CP: chosen plaintexts, ACC: adaptively chosen ciphertexts, ACP: adaptively chosen plaintexts, ACPC: adaptively chosen plaintexts and ciphertexts.
[‡] E: equivalent round-reduced AES encryptions, M: memory accesses. This paper regards one table insertion as one-round AES encryption, and [6] regards it as one S-box lookup, i.e., 1/16 of one-round AES encryption.

2 Preliminaries

2.1 AES and Notations

AES [15] is a Substitution-Permutation Network (SPN) cipher which has a 128-bit block and 128-bit, 192-bit or 256-bit keys. The 128-bit state of AES can be described as a 4×4 matrix over the finite field $\mathbb{F}_{2^8}$, and the order of bytes in the state matrix is shown in Figure 1. The round transformation of AES consists of the following four operations.

-*SubBytes* (SB) : applying the same 8-bit S-box to each byte of the state.

-*ShiftRows* (SR) : cyclic shift of the i-th row by i bytes to the left for $i = 0, 1, 2, 3$.

-*MixColumns* (MC) : multiplication of each column by an MDS matrix over $\mathbb{F}_{2^8}$.

-*AddRoundKey* (AK) : XORing the state with a 128-bit round key.

The number of rounds for the three versions of AES is 10, 12 and 14 respectively. Before the first round, an additional AK is applied to plaintext and in the last round the MC is omitted.

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Fig. 1. The order of bytes in the state matrix

Notations. Denote by $R = AK \circ MC \circ SR \circ SB$ one round of AES, and denote by R^t the t rounds of AES without MC in the last round, $t \geq 2$. Denote by $Col(i)$ the i-th column, and $X_{Col(i)}$ the i-th column of a state X, $0 \leq i \leq 3$. Denote by $SR(Col(i))$ the result of applying SR operation to the i-th column, and $X_{SR(Col(i))}$ the i-th inverse diagonal of a state X, $0 \leq i \leq 3$. Denote by $SR^{-1}(Col(i))$ the result of applying SR^{-1} operation to the i-th column, and $X_{SR^{-1}(Col(i))}$ the i-th diagonal of a state X, $0 \leq i \leq 3$. For a set $I \subseteq \{0, 1, 2, 3\}$, we use $Col(I), SR(Col(I))$ and $SR^{-1}(Col(I))$ to denote the columns, inverse diagonals and diagonals with indices in I, respectively. Denote by $|I|$ the cardinality of the set I. The notation $I_2 \subset I_1$ means that I_2 is a proper subset of I_1, that is, $I_2 \subseteq I_1$ and $I_2 \neq I_1$. For $I_2 \subset I_1$, denote by $I_1 \setminus I_2$ the set of all elements i, $i \in I_1$ and $i \notin I_2$.

2.2 Zero-Difference Property and Exchange Attack

In ASIACRYPT 2017, Rønjom et al. [30] proposed the zero-difference property for 4-round AES under the exchange operation, and presented yoyo cryptanalysis for up to 6 rounds of AES.

Definition 1 (Zero-difference pattern [30]). *For $\alpha = (\alpha_0, \alpha_1, ..., \alpha_{n-1}) \in \mathbb{F}_q^n$, define the zero-difference pattern of α by*

$$\nu(\alpha) = (z_0, z_1, ..., z_{n-1}),$$

which returns a binary vector in $\mathbb{F}_2^n$ where $z_i = 1$ indicates that α_i is zero or $z_i = 0$ otherwise, $i = 0, 1, ..., n-1$.

Definition 2 (Exchange [30]). *For a vector $v = (v_0, v_1, ..., v_{n-1}) \in \mathbb{F}_2^n$ and $\alpha = (\alpha_0, \alpha_1, ..., \alpha_{n-1}), \beta = (\beta_0, \beta_1, ..., \beta_{n-1}) \in \mathbb{F}_q^n$, define $\rho^v(\alpha, \beta) \in \mathbb{F}_q^n$ such that for $i = 0, 1, ..., n-1$,*

$$\rho^v(\alpha, \beta)_i = \begin{cases} \alpha_i & if\ v_i = 1, \\ \beta_i & if\ v_i = 0. \end{cases}$$

Then $(\rho^v(\alpha, \beta), \rho^v(\beta, \alpha))$ is a new pair formed by exchanging components between α and β according to v.

For AES, there exists the following 4-round zero-difference property. If (α, β) is a pair of inputs of AES, and $(\alpha', \beta') = (\rho^v(\alpha, \beta), \rho^v(\beta, \alpha))$ is formed by exchanging individual diagonals of (α, β) according to any vector $v \in \mathbb{F}_2^n$, then

$$R^2(\alpha) + R^2(\beta) + R^2(\alpha') + R^2(\beta') = 0,$$

and

$$\mu(R^4(\alpha) + R^4(\beta)) = \mu(R^4(\alpha') + R^4(\beta'))$$

hold with probability 1, where $\mu(\cdot) = \nu(SR^{-1}(\cdot))$ is the zero-difference pattern over inverse diagonals.

Based on the 4-round zero-difference property, Bardeh and Rønjom [6] proposed the exchange attack on AES, and gave the best known distinguishers on 5 and 6 rounds of AES in the CP setting.

2.3 Related-Differential Cryptanalysis for AES

In [16], Daemen and Rijmen proposed the concepts of related differences and related differentials. In FSE 2023, Bardeh and Rijmen [5] estimated the probabilities of related differentials for 2 and 4 rounds of AES, combined them with the 4-round zero-difference property to present new properties for 6 and 8 rounds of AES, and gave a new key-recovery attack on 7-round AES. In this subsection, we recall the related definitions and results. This paper presents new properties and distinguishers for 5 to 7 rounds of AES based on related differentials.

Definition 3 (Related differences [16]). *Two differences* $\Delta x = (\Delta x_0, \Delta x_1, ..., \Delta x_{n-1})$, $\Delta x' = (\Delta x'_0, \Delta x'_1, ..., \Delta x'_{n-1}) \in \mathbb{F}_q^n$ *are related differences if and only if*

$$\Delta x_i \Delta x'_i (\Delta x_i + \Delta x'_i) = 0, \quad for \quad i = 0, 1, ..., n-1. \tag{1}$$

Any difference Δx is related to itself, and the all-zero difference is related to any difference $\Delta x'$. In this paper we exclude these two trivial cases. For AES, when the state is regarded as a vector in $\mathbb{F}_{2^8}^{16}$, and $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{16}$ satisfy Equation 1, then $\Delta x, \Delta x'$ are called **byte-wise related differences**. When the state of AES, Δx and $\Delta x'$ are regarded as vectors in $\mathbb{F}_{2^{32}}^4$ consisting of four columns (or diagonals), if Equation 1 holds, then $\Delta x, \Delta x'$ are called **column (or diagonal) related differences**.

For any state $\alpha \in \mathbb{F}_q^n$ and any related differences $\Delta x, \Delta x' \in \mathbb{F}_q^n$, we can obtain a quartet $(\alpha, \alpha + \Delta x, \alpha + \Delta x', \alpha + \Delta x + \Delta x')$. For each $i = 0, 1, ..., n-1$, the sets $\{\alpha_i, \alpha_i + \Delta x_i, \alpha_i + \Delta x'_i, \alpha_i + \Delta x_i + \Delta x'_i\}$ consist of two pairs of equal values. So, the related differences pass through the bijective S-box layer with probability 1 for SPN ciphers. In the related-differential cryptanalysis, we only need to consider the propagation of related differences through the linear layer.

Definition 4 (Related differentials [16]). *Let* $\Delta x, \Delta x'$ *be related differences, and* $\Delta y = M(\Delta x)$, $\Delta y' = M(\Delta x')$ *for a linear map* M. *If* $\Delta y, \Delta y'$ *are related differences, then* $\Delta x \to \Delta y$, $\Delta x' \to \Delta y'$ *are related differentials for* M.

For AES, if both the input differences $\Delta x, \Delta x'$ and the output differences $\Delta y, \Delta y'$ are byte-wise (or diagonal) related differences, then $\Delta x \to \Delta y$, $\Delta x' \to \Delta y'$ are called **byte-wise (or diagonal) related differentials**. In [5], Bardeh and Rijmen showed that the zero-difference property for 4-round AES holds with probability 1 for any quartet of plaintexts constructed by diagonal related differences. They also gave some properties for more rounds of AES by the probabilistic extension.

Theorem 1 ([5]). *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be diagonal related differences, then for any $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$,*

$$R^2(\alpha) + R^2(\alpha + \Delta x) + R^2(\alpha + \Delta x') + R^2(\alpha + \Delta x + \Delta x') = 0,$$

and

$$\mu(R^4(\alpha) + R^4(\alpha + \Delta x)) = \mu(R^4(\alpha + \Delta x') + R^4(\alpha + \Delta x + \Delta x'))$$

hold with probability 1, where $\mu(\cdot) = \nu(SR^{-1}(\cdot))$.

Lemma 1 ([5]). *If $\Delta x \to \Delta y$, $\Delta x' \to \Delta y'$ are related differentials of n-round AES with probability p, where Δy, $\Delta y'$ are diagonal related differences, then for any state $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$,*

$$R^{n+2}(\alpha) + R^{n+2}(\alpha + \Delta x) + R^{n+2}(\alpha + \Delta x') + R^{n+2}(\alpha + \Delta x + \Delta x') = 0,$$

and

$$\mu(R^{n+4}(\alpha) + R^{n+4}(\alpha + \Delta x)) = \mu(R^{n+4}(\alpha + \Delta x') + R^{n+4}(\alpha + \Delta x + \Delta x'))$$

hold with probability at least p, where $\mu(\cdot) = \nu(SR^{-1}(\cdot))$.

For 2-round AES, Bardeh and Rijmen [5] gave four diagonal related differentials, each of which holds with probability 2^{-96}. For 4-round AES, they gave eight diagonal related differentials, each of which holds with probability 2^{-192}. Based on these related differentials and Lemma 1, they presented the following properties.

Theorem 2 ([5]). *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be diagonal related differences, where all diagonals in Δx are nonzero and two non-consecutive diagonals in $\Delta x'$ are zero, then for any $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$,*

$$R^4(\alpha) + R^4(\alpha + \Delta x) + R^4(\alpha + \Delta x') + R^4(\alpha + \Delta x + \Delta x') = 0,$$

and

$$\mu(R^6(\alpha) + R^6(\alpha + \Delta x)) = \mu(R^6(\alpha + \Delta x') + R^6(\alpha + \Delta x + \Delta x'))$$

hold with probability at least 2^{-94}, where $\mu(\cdot) = \nu(SR^{-1}(\cdot))$.

Theorem 3 ([5]). *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be diagonal related differences, where all diagonals in Δx are nonzero and two non-consecutive diagonals in $\Delta x'$ are zero, then for any $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$,*

$$R^t(\alpha) + R^t(\alpha + \Delta x) + R^t(\alpha + \Delta x') + R^t(\alpha + \Delta x + \Delta x') = 0,$$

for $0 < t \leq 6$, and

$$\mu(R^8(\alpha) + R^8(\alpha + \Delta x)) = \mu(R^8(\alpha + \Delta x') + R^8(\alpha + \Delta x + \Delta x'))$$

hold with probability at least 2^{-189}, where $\mu(\cdot) = \nu(SR^{-1}(\cdot))$.

3 A New Insight on Related Differences

In this section, we provide a new insight on related differences from the perspectives of exchange and shift operations. For any related differences $\Delta x, \Delta x' \in \mathbb{F}_q^n$ and any state $\alpha \in \mathbb{F}_q^n$, we can construct the quartet $(\alpha, \alpha+\Delta x, \alpha+\Delta x', \alpha+\Delta x+\Delta x')$. Actually, the pair of states $(\alpha + \Delta x', \alpha + \Delta x + \Delta x')$ can be obtained by exchanging or shifting some components of $(\alpha, \alpha+\Delta x)$, or by the mixed application of these two operations. For any related differences $\Delta x, \Delta x' \in \mathbb{F}_q^n$, denote by I_1 and I_2 the sets of indices of nonzero components in Δx and $\Delta x'$ respectively, $I_1, I_2 \subseteq \{0, 1, 2, ..., n-1\}$. Without loss of generality, assume $|I_1| \geq |I_2|$.

In the case of $I_2 \subset I_1$, the pair of states $(\alpha + \Delta x', \alpha + \Delta x + \Delta x')$ can be obtained by exchanging the components of $(\alpha, \alpha + \Delta x)$ indexed by I_2. That is,

$$(\alpha + \Delta x')_i = \begin{cases} \alpha_i, & i \notin I_2, \\ (\alpha + \Delta x)_i, & i \in I_2, \end{cases}$$

$$(\alpha + \Delta x + \Delta x')_i = \begin{cases} (\alpha + \Delta x)_i, & i \notin I_2, \\ \alpha_i, & i \in I_2. \end{cases}$$

Definition 5. *Let $\Delta x, \Delta x' \in \mathbb{F}_q^n$ be related differences, and I_1 and I_2 be the sets of indices of nonzero components in Δx and $\Delta x'$ respectively, $I_1, I_2 \subseteq \{0, 1, 2, ..., n-1\}$, $|I_1| \geq |I_2|$. If $I_2 \subset I_1$, then Δx, $\Delta x'$ are called the exchanged related differences.*

For example, let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be diagonal related differences, $I_1 = \{0, 1, 2\}$, $I_2 = \{0\}$. That is,

$$\Delta x = \begin{bmatrix} \Delta x_0 & \Delta x_4 & \Delta x_8 & 0 \\ 0 & \Delta x_5 & \Delta x_9 & \Delta x_{13} \\ \Delta x_2 & 0 & \Delta x_{10} & \Delta x_{14} \\ \Delta x_3 & \Delta x_7 & 0 & \Delta x_{15} \end{bmatrix}, \qquad \Delta x' = \begin{bmatrix} \Delta x_0 & 0 & 0 & 0 \\ 0 & \Delta x_5 & 0 & 0 \\ 0 & 0 & \Delta x_{10} & 0 \\ 0 & 0 & 0 & \Delta x_{15} \end{bmatrix}.$$

For any state $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$, the quartet $(\alpha, \alpha+\Delta x, \alpha+\Delta x', \alpha+\Delta x+\Delta x')$ is shown in Figure 2. It can be seen that $(\alpha + \Delta x', \alpha + \Delta x + \Delta x')$ can be obtained by exchanging the 0-th diagonal of $(\alpha, \alpha + \Delta x)$. Thus, such $\Delta x, \Delta x'$ are exchanged diagonal related differences.

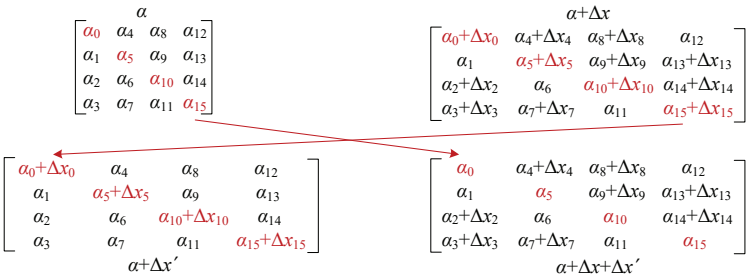


Fig. 2. An example of exchanged related differences

In the case of $I_1 \cap I_2 = \emptyset$, the pair of states $(\alpha + \Delta x', \alpha + \Delta x + \Delta x')$ can be obtained from $(\alpha, \alpha + \Delta x)$, shifting $(\alpha_i, (\alpha + \Delta x)_i)$ by the same values $\Delta x'_i$ only for $i \in I_2$.

Definition 6. *Let $\Delta x, \Delta x' \in \mathbb{F}_q^n$ be related differences, and I_1 and I_2 be the sets of indices of nonzero components in Δx and $\Delta x'$ respectively, $I_1, I_2 \subseteq \{0, 1, 2, ..., n-1\}$, $|I_1| \geq |I_2|$. If $I_1 \cap I_2 = \emptyset$, then Δx, $\Delta x'$ are called the shifted related differences.*

For example, let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be diagonal related differences, $I_1 = \{1, 2\}$, $I_2 = \{0\}$. That is,

$$\Delta x = \begin{bmatrix} 0 & \Delta x_4 & \Delta x_8 & 0 \\ 0 & 0 & \Delta x_9 & \Delta x_{13} \\ \Delta x_2 & 0 & 0 & \Delta x_{14} \\ \Delta x_3 & \Delta x_7 & 0 & 0 \end{bmatrix}, \qquad \Delta x' = \begin{bmatrix} \Delta x_0 & 0 & 0 & 0 \\ 0 & \Delta x_5 & 0 & 0 \\ 0 & 0 & \Delta x_{10} & 0 \\ 0 & 0 & 0 & \Delta x_{15} \end{bmatrix}.$$

Then for any state $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$, the quartet $(\alpha, \alpha + \Delta x, \alpha + \Delta x', \alpha + \Delta x + \Delta x')$ is shown in Figure 3. It can be seen that $(\alpha + \Delta x', \alpha + \Delta x + \Delta x')$ can be obtained by shifting the 0-th diagonals of α and $\alpha + \Delta x$ by the same value $\Delta x'_{SR^{-1}(Col(0))}$, keeping the difference in the 0-th diagonal still zero. Thus, such $\Delta x, \Delta x'$ are shifted diagonal related differences.

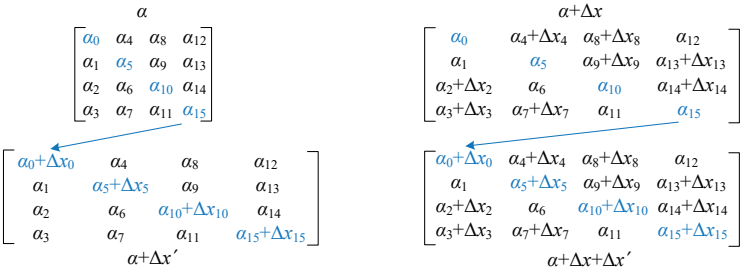


Fig. 3. An example of shifted related differences

Definition 7. *Let $\Delta x, \Delta x' \in \mathbb{F}_q^n$ be related differences, and I_1 and I_2 be the sets of indices of nonzero components in Δx and $\Delta x'$ respectively, $I_1, I_2 \subseteq \{0, 1, 2, ..., n-1\}$, $|I_1| \geq |I_2|$. If $I_2 \not\subseteq I_1$ and $I_1 \cap I_2 \neq \emptyset$, then Δx, $\Delta x'$ are called the mixed related differences.*

For the mixed related differences $\Delta x, \Delta x'$, the pair of states $(\alpha + \Delta x', \alpha + \Delta x + \Delta x')$ can be obtained by exchanging the i-th components of $(\alpha, \alpha + \Delta x)$ only for $i \in I_1 \cap I_2$, and shifting $(\alpha_j, (\alpha + \Delta x)_j)$ by the same values $\Delta x'_j$ only for $j \in I_2 \backslash (I_1 \cap I_2)$. For example, let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be diagonal related differences, $I_1 = \{0, 1\}$, $I_2 = \{0, 2\}$. That is,

$$\Delta x = \begin{bmatrix} \Delta x_0 & \Delta x_4 & 0 & 0 \\ 0 & \Delta x_5 & \Delta x_9 & 0 \\ 0 & 0 & \Delta x_{10} & \Delta x_{14} \\ \Delta x_3 & 0 & 0 & \Delta x_{15} \end{bmatrix}, \qquad \Delta x' = \begin{bmatrix} \Delta x_0 & 0 & \Delta x_8 & 0 \\ 0 & \Delta x_5 & 0 & \Delta x_{13} \\ \Delta x_2 & 0 & \Delta x_{10} & 0 \\ 0 & \Delta x_7 & 0 & \Delta x_{15} \end{bmatrix}.$$

Then for any state $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$, the quartet $(\alpha, \alpha + \Delta x, \alpha + \Delta x', \alpha + \Delta x + \Delta x')$ is shown in Figure 4. The pair of states $(\alpha + \Delta x', \alpha + \Delta x + \Delta x')$ can be obtained by exchanging the 0-th diagonal of $(\alpha, \alpha + \Delta x)$, and shifting the 2-nd diagonal of $(\alpha, \alpha + \Delta x)$ by the value $\Delta x'_{SR^{-1}(Col(2))}$.

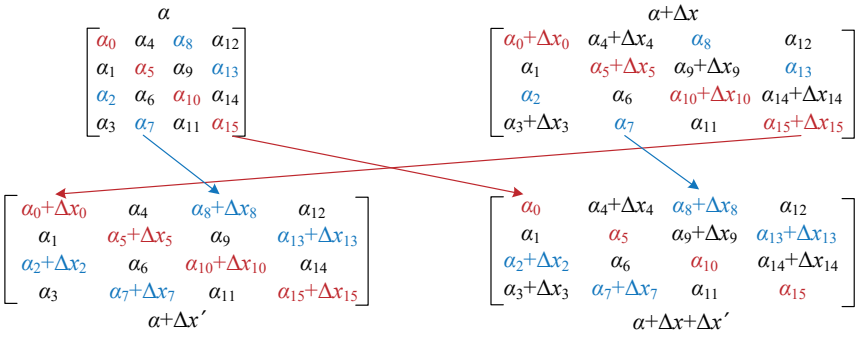


Fig. 4. An example of mixed related differences

Relationship between the exchanged and shifted related differences. As shown in Figure 5, if Δx, $\Delta x'$ are exchanged related differences, then $\Delta x'$, $\Delta x + \Delta x'$ are the shifted related differences. If Δx, $\Delta x'$ are shifted related differences, then both $\Delta x + \Delta x'$, Δx and $\Delta x + \Delta x'$, $\Delta x'$ are the exchanged related differences. If Δx, $\Delta x'$ are exchanged related differences, that is, $I_2 \subset I_1$, then $\Delta x + \Delta x'$ is nonzero only in $I_1 \setminus I_2$. Since $(I_1 \setminus I_2) \cap I_2 = \emptyset$, we have that $\Delta x'$, $\Delta x + \Delta x'$ are the shifted related differences. If Δx, $\Delta x'$ are shifted related differences, that is, $I_1 \cap I_2 = \emptyset$, then $\Delta x + \Delta x'$ is nonzero only in $I_1 \cup I_2$. So both $\Delta x + \Delta x'$, Δx and $\Delta x + \Delta x'$, $\Delta x'$ are the exchanged related differences.

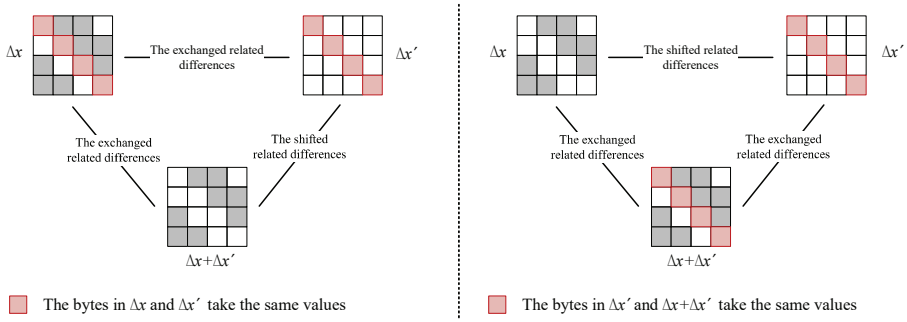


Fig. 5. Relationship between the exchanged and shifted related differences

4 New Property and Improved Distinguishers for 5-Round AES

In this section, we present certain byte-wise related differentials for one-round AES, and combine them with the 4-round zero-difference property in Theorem 1 to present a new property for 5-round AES. Then based on this property, we improve the distinguishers on 5-round AES in the chosen plaintexts setting and adaptively chosen plaintexts setting, respectively.

4.1 New Property for 5-Round AES

For the operation MC of AES as a function $z = MC(y)$ on $\mathbb{F}_{2^8}^4$, Daemen and Rijmen [16] gave all byte-wise related differentials. Four of them are listed in Table 2, and the others can be derived from these four by means of rotation and/or multiplication by a nonzero scalar. The following lemma gives the probability of certain byte-wise related differentials over one full round of AES.

Table 2. ([16]) Four byte-wise related differentials for MC

Δy	Δz	$\Delta y'$	$\Delta z'$	$\Delta y + \Delta y'$	$\Delta z + \Delta z'$
$[0,1,4,7]$	$[0,9,0,B]$	$[5,1,0,7]$	$[E,0,D,0]$	$[5,0,4,0]$	$[E,9,D,B]$
$[0,1,0,3]$	$[0,1,4,7]$	$[2,0,1,0]$	$[5,1,0,7]$	$[2,1,1,3]$	$[5,0,4,0]$
$[7,0,7,7]$	$[9,E,0,0]$	$[7,7,7,0]$	$[0,0,9,E]$	$[0,7,0,7]$	$[9,E,9,E]$
$[0,3,2,0]$	$[7,0,7,1]$	$[2,0,0,3]$	$[7,1,7,0]$	$[2,3,2,3]$	$[0,1,0,1]$

Lemma 2. *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be byte-wise related differences, where only the 0-th and 10-th bytes in Δx and the 5-th and 15-th bytes in $\Delta x'$ are nonzero. Let $\Delta z, \Delta z' \in \mathbb{F}_{2^8}^{4\times 4}$ be the corresponding output differences after one full round of AES. Then Δz, $\Delta z'$ are byte-wise related differences with probability 2^{-22}.*

Proof. Let $\Delta y, \Delta y'$ be the output differences of $\Delta x, \Delta x'$ after $SR \circ SB$. Then Δy is nonzero only in the 0-th and 2-nd bytes, and $\Delta y'$ is nonzero only in the 1-st and 3-rd bytes. It is obvious that Δy, $\Delta y'$ are byte-wise related differences. Note that $\Delta z = MC(\Delta y)$, and $\Delta z' = MC(\Delta y')$. From Table 2, Δz, $\Delta z'$ are byte-wise related differences if and only if $\Delta y_{Col(0)} = [2, 0, 1, 0]$ and $\Delta y'_{Col(0)} = [0, 1, 0, 3]$ or their rotation and/or multiplication by a nonzero scalar. All possible values of $\Delta y_{Col(0)}$ and $\Delta y'_{Col(0)}$ such that Δz, $\Delta z'$ are byte-wise related differences are listed in Table 3, where $\lambda \in \mathbb{F}_{2^8}^*$ can take any value. So the required probability is $4 \cdot (2^8 - 1) \cdot 2^{-32} \approx 2^{-22}$.

Table 3. All possible values of $\Delta y_{Col(0)}$ and $\Delta y'_{Col(0)}$ such that Δz, $\Delta z'$ are byte-wise related differences

$\Delta y_{Col(0)}$	$\Delta z_{Col(0)}$	$\Delta y'_{Col(0)}$	$\Delta z'_{Col(0)}$	$(\Delta y + \Delta y')_{Col(0)}$	$(\Delta z + \Delta z')_{Col(0)}$
$[2\lambda, 0, \lambda, 0]$	$[5\lambda, \lambda, 0, 7\lambda]$	$[0, \lambda, 0, 3\lambda]$	$[0, \lambda, 4\lambda, 7\lambda]$	$[2\lambda, \lambda, \lambda, 3\lambda]$	$[5\lambda, 0, 4\lambda, 0]$
$[\lambda, 0, 3\lambda, 0]$	$[\lambda, 4\lambda, 7\lambda, 0]$	$[0, \lambda, 0, 2\lambda]$	$[\lambda, 0, 7\lambda, 5\lambda]$	$[\lambda, \lambda, 3\lambda, 2\lambda]$	$[0, 4\lambda, 0, 5\lambda]$
$[\lambda, 0, 2\lambda, 0]$	$[0, 7\lambda, 5\lambda, \lambda]$	$[0, 3\lambda, 0, \lambda]$	$[4\lambda, 7\lambda, 0, \lambda]$	$[\lambda, 3\lambda, 2\lambda, \lambda]$	$[4\lambda, 0, 5\lambda, 0]$
$[3\lambda, 0, \lambda, 0]$	$[7\lambda, 0, \lambda, 4\lambda]$	$[0, 2\lambda, 0, \lambda]$	$[7\lambda, 5\lambda, \lambda, 0]$	$[3\lambda, 2\lambda, \lambda, \lambda]$	$[0, 5\lambda, 0, 4\lambda]$

By combining Lemma 2 with the 4-round zero-difference property, we have the following property for 5-round AES.

Theorem 4. *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be byte-wise related differences, where only the 0-th and 10-th bytes in Δx and the 5-th and 15-th bytes in $\Delta x'$ are nonzero. Then for any state $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$,*

$$R^3(\alpha) + R^3(\alpha + \Delta x) + R^3(\alpha + \Delta x') + R^3(\alpha + \Delta x + \Delta x') = 0,$$

and

$$\mu(R^5(\alpha) + R^5(\alpha + \Delta x)) = \mu(R^5(\alpha + \Delta x') + R^5(\alpha + \Delta x + \Delta x'))$$

hold with probability at least 2^{-22}, where $\mu(\cdot) = \nu(SR^{-1}(\cdot))$.

Proof. Let $\Delta z = R(\alpha) + R(\alpha + \Delta x)$, and $\Delta z' = R(\alpha) + R(\alpha + \Delta x')$. Note that Δz and $\Delta z'$ are nonzero only in the 0-th column, as shown in Figure 6. By Lemma 2, Δz, $\Delta z'$ are byte-wise related differences with probability 2^{-22}. So Δz, $\Delta z'$ are diagonal related differences with probability 2^{-22}. Then by Lemma 1, the theorem is proved.

Corollary 1. *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be byte-wise related differences, where only the 0-th and 10-th bytes in Δx and the 5-th and 15-th bytes in $\Delta x'$ are nonzero. For any state $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$, let $(C_0, C_1, C_2, C_3) = (R^5(\alpha), R^5(\alpha + \Delta x), R^5(\alpha + \Delta x'), R^5(\alpha + \Delta x + \Delta x'))$. If $C_0 + C_1$ is zero in the i-th inverse diagonal, then the probability that $C_2 + C_3$ is zero in the i-th inverse diagonal is at least 2^{-22}, $0 \le i \le 3$.*

By Corollary 1, we can distinguish 5-round AES, since the probability that $C_2 + C_3$ is zero in the same inverse diagonal as $C_0 + C_1$ is 2^{-32} for a random permutation.

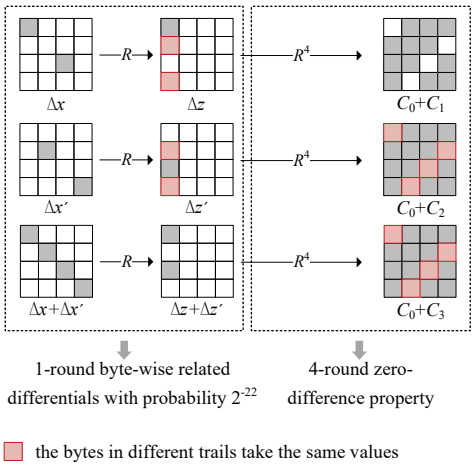


Fig. 6. Framework of distinguishers on 5-round AES

4.2 Improved Distinguisher on 5-Round AES in the Chosen Plaintexts Setting

Let Δx, $\Delta x'$ be byte-wise related differences as Corollary 1, where only the 0-th and 10-th bytes in Δx and the 5-th and 15-th bytes in $\Delta x'$ are nonzero. Randomly choose plaintexts $(P_0, P_1, P_2, P_3) = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$, and let $(C_0, C_1, C_2, C_3) = (R^5(P_0), R^5(P_1), R^5(P_2), R^5(P_3))$ be the corresponding ciphertexts. The probability that $C_0 + C_1$ is zero in one inverse diagonal is $4 \cdot 2^{-32} = 2^{-30}$. Then by Corollary 1, the probability that there exists one inverse diagonal $SR(Col(i))$, $0 \le i \le 3$, such that

$$(C_0 + C_1)_{SR(Col(i))} = (C_2 + C_3)_{SR(Col(i))} = 0$$

is $2^{-30} \cdot 2^{-22} = 2^{-52}$, while the probability is $4 \cdot 2^{-64} = 2^{-62}$ for a random permutation.

To generate 2^{52} desired quartets of plaintexts (P_0, P_1, P_2, P_3), we randomly choose two subsets $A_0, A_1 \subseteq \mathbb{F}_{2^8}^2$, each of size s. We construct s^2 plaintexts, where the 0-th and 10-th bytes take all possible elements in A_0, the 5-th and 15-th bytes take all possible elements in A_1, and the other bytes take any constants. Then the number of desired quartets (P_0, P_1, P_2, P_3) generated is $\frac{s^2(s-1)^2}{4}$. Taking $s = 2^{13.6}$, we can obtain 2^{52} desired quartets of plaintexts. Thus, the data complexity is $s^2 = 2^{27.2}$ chosen plaintexts.

The process of distinguishing 5-round AES in the chosen plaintexts setting is as follows, and the pseudocode is given in algorithm 1.

1. Choose randomly two subsets $A_0, A_1 \subseteq \mathbb{F}_{2^8}^2$, each of size $2^{13.6}$.

2. For each $\omega \in A_1$, construct $2^{13.6}$ plaintexts where the 0-th and 10-th bytes take all possible elements in A_0, the 5-th and 15-th bytes take ω, and the other

bytes take any constants. For each plaintext P, ask for the ciphertext C, and store P into four hash tables H_i, $0 \le i \le 3$, indexed by the i-th inverse diagonal of C, i.e., $C_{SR(Col(i))}$. Then for each table H_i, extract all pairs of plaintexts (P_0, P_1) with the same index and store them into the table T_i, $0 \le i \le 3$.

3. For each table T_i, $0 \le i \le 3$, check whether there exist two pairs (P_0, P_1) and (P_2, P_3) satisfying that both $P_0 + P_2$ and $P_1 + P_3$ are zero in the 0-th and 10-th bytes. If it holds, then output "It is 5-round AES". After all the above processes, if there is no output, then judge "It is a random permutation".

Algorithm 1: Distinguisher on 5-round AES in the CP setting

```
Choose randomly two subsets A_0, A_1 ⊆ F_{2^8}^2, each of size 2^{13.6}.
for each ω ∈ A_1 do
    Construct 2^{13.6} plaintexts where the 0-th and 10-th bytes take all
     possible elements in A_0, the 5-th and 15-th bytes take ω, and the
     other bytes take any constants.
    for each plaintext P do
        Ask for the ciphertext C, and store P into H_i indexed by
         C_{SR(Col(i))}, i = 0, 1, 2, 3.
    end
    for 0 ≤ i ≤ 3 do
        Extract all pairs of plaintexts (P_0, P_1) with the same index in H_i,
         and store (P_0, P_1) into T_i.
        Clear H_i.
    end
end
for 0 ≤ i ≤ 3 do
    for any two pairs (P_0, P_1) and (P_2, P_3) in T_i do
        Check whether both P_0 + P_2 and P_1 + P_3 are zero in the 0-th
         and 10-th bytes.
        if it holds then
            Return: It is 5-round AES.
        end
    end
end
Return: It is a random permutation.
```

Complexity analysis. The data complexity is $2^{27.2}$ chosen plaintexts. Step 2 needs to encrypt $2^{27.2}$ plaintexts and insert them into 4 tables H_i, $0 \le i \le 3$. The expected number of pairs (P_0, P_1) extracted from H_i, $0 \le i \le 3$, is $\binom{2^{13.6}}{2} \cdot 2^{13.6} \cdot 2^{-32} \approx 2^{7.8}$, so the complexity of extracting and storing these pairs is negligible. Referring to [3], we regard one table insertion as one-round AES encryption, then the time complexity of step 2 is about $2^{27.2} + 4 \cdot 2^{27.2}/5 \approx 2^{28.05}$ encryptions of 5-round AES. Step 3 needs to check $4 \cdot \binom{2^{7.8}}{2} \cdot 2 \approx 2^{17.59}$ equations, of which the complexity is negligible. Therefore, the overall time complexity is dominated by $2^{28.05}$ encryptions of 5-round AES. The memory complexity is

dominated by the 4 hash tables H_i, $0 \le i \le 3$, whose total size is $4 \times 2^{13.6} = 2^{15.6}$. For 5-round AES, the probability that there exists at least one required quartet among 2^{52} quartets is $1-(1-2^{-52})^{2^{52}} \approx 1-e^{-1} \approx 63\%$, so the success probability of the distinguisher is 63%. For a random permutation, the error probability that it is judged as 5-round AES is $1-(1-2^{-62})^{2^{52}} \approx 1-e^{-2^{-10}} \approx 2^{-10}$.

Comparison with previous work. The best previous distinguisher on 5-round AES in the CP setting [6] has data and time complexities of 2^{30} and a success probability of 63%. Our distinguisher reduces the data and time complexities by factors of about 7 and 4, respectively.

4.3 Improved Distinguisher on 5-Round AES in the Adaptively Chosen Plaintexts Setting

In the adaptively chosen plaintexts setting, the complexity of the distinguisher on 5-round AES can be reduced. First, we choose pairs of plaintexts $(P_0, P_1) = (P_0, P_0 + \Delta x)$, where Δx is nonzero only in the 0-th and 10-th bytes, and filter them to find (P_0, P_1) such that $R^5(P_0)+R^5(P_1)$ is zero in some inverse diagonal. Then shift (P_0, P_1) by all $(2^8-1)^2$ possible values of $\Delta x'$, which is nonzero only in the 5-th and 15-th bytes, to obtain new pairs of plaintexts $(P_2, P_3) = (P_0 + \Delta x', P_1 + \Delta x')$. By Corollary 1, for each pair (P_2, P_3) the probability that $R^5(P_2) + R^5(P_3)$ is zero in the same inverse diagonal as $R^5(P_0) + R^5(P_1)$ is 2^{-22}. For a random permutation, the probability is 2^{-32}. We choose 2^5 plaintext structures where the 0-th and 10-th bytes take all possible values and the other bytes take any constants. Then we can obtain $2^5 \cdot 2^{31} \cdot 2^{-30} = 2^6$ pairs (P_0, P_1) after the filter for ciphertext differences. By shifting (P_0, P_1) by all possible values of $\Delta x'$, there are $2^6 \cdot (2^8-1)^2 \approx 2^{22}$ pairs (P_2, P_3). Then there is one pair (P_2, P_3) such that $R^5(P_2) + R^5(P_3)$ is zero in the same inverse diagonal as $R^5(P_0)+R^5(P_1)$ on average. For a random permutation, the expected number of pairs (P_2, P_3) satisfying the above property is about 2^{-10}. Note that to obtain 2^5 plaintext structures, we randomly take 2^5 different constants in the three diagonals $SR^{-1}(Col(1,2,3))$.

The process of distinguishing 5-round AES in the adaptively chosen plaintexts setting is as follows, and the pseudocode is given in algorithm 2.

1. Choose 2^5 plaintext structures where the 0-th and 10-th bytes take all possible values and the other bytes take any constants.

2. For each plaintext structure, ask for the ciphertext C of each plaintext P, and store the plaintext P into four hash tables H_i, $0 \le i \le 3$, indexed by the i-th inverse diagonal of the ciphertext C, i.e., $C_{SR(Col(i))}$.

3. For each table H_i, $0 \le i \le 3$, extract all pairs of plaintexts (P_0, P_1) with the same index. For each pair (P_0, P_1), shift it by all $(2^8-1)^2$ possible values of $\Delta x'$ nonzero only in the 5-th and 15-th bytes to obtain pairs of plaintexts $(P_2, P_3) = (P_0 + \Delta x', P_1 + \Delta x')$, and ask for the corresponding ciphertexts (C_2, C_3). Check whether there exists one pair (C_2, C_3) such that $(C_2 + C_3)_{SR(Col(i))} = 0$. If it holds, then output "It is 5-round AES". After all the above processes, if there is no output, then judge "It is a random permutation".

Algorithm 2: Distinguisher on 5-round AES in the ACP setting

```
Choose 2^5 plaintext structures where the 0-th and 10-th bytes take all
 possible values and the other bytes take any constants.
for each plaintext structure do
    for each plaintext P do
        Ask for the ciphertext C, and store P into H_i indexed by
         C_{SR(Col(i))}, 0 ≤ i ≤ 3.
    end
    for 0 ≤ i ≤ 3 do
        Extract all pairs of plaintexts (P_0, P_1) with the same index in H_i.
        for each pair (P_0, P_1) do
            Construct (2^8 − 1)^2 pairs (P_2, P_3) = (P_0 + Δx', P_1 + Δx') for
             all possible Δx', and ask for the ciphertexts (C_2, C_3).
            for each (C_2, C_3) do
                Check whether (C_2 + C_3)_{SR(Col(i))} = 0.
                if it holds then
                    Return: It is 5-round AES.
                end
            end
        end
        Clear H_i.
    end
end
Return: It is a random permutation.
```

Complexity analysis. The distinguisher needs $2^5 \cdot 2^{16} = 2^{21}$ chosen plaintexts and $2 \cdot 2^{22} = 2^{23}$ adaptively chosen plaintexts, so the data complexity is $2^{23.32}$. Step 2 needs 2^{21} encryptions and $4 \cdot 2^{21}$ insertions into tables, which are equivalent to $2^{21} + 4 \cdot 2^{21}/5 \approx 2^{21.85}$ encryptions of 5-round AES. The time complexity of step 3 is dominated by the encryptions of 2^{23} adaptively chosen plaintexts. Therefore, the overall time complexity is about $2^{21.85} + 2^{23} \approx 2^{23.54}$. The memory complexity is dominated by the 4 hash tables H_i, $0 \le i \le 3$, whose total size is $4 \times 2^{16} = 2^{18}$. The attack succeeds if there exists one pair (P_2, P_3) satisfying $R^5(P_2) + R^5(P_3)$ is zero in the same inverse diagonal as $R^5(P_0) + R^5(P_1)$, the probability of which is $1 - (1 - 2^{-22})^{2^{22}} \approx 63\%$. The error probability that a random permutation is judged as 5-round AES is $1 - (1 - 2^{-32})^{2^{22}} \approx 2^{-10}$.

Comparison with previous work. In [31], Shin et al. proposed a 5-round distinguisher on AES in the adaptive setting with data and time complexities of $2^{27.1}$ and a success probability of 80%. To compare with this result, we increase the number of plaintext structures in step 1 from 2^5 to $2^{5.75}$, raising the success probability to $1 - (1 - 2^{-22})^{2^{22} \cdot 2^{0.75}} \approx 81\%$. The data complexity is $2^{0.75} \cdot 2^{23.32} = 2^{24.07}$, and the time complexity is $2^{0.75} \cdot 2^{23.54} = 2^{24.29}$. Our distinguisher is superior to [31].

4.4 Experimental Verification

We have mounted experiments to verify the validity of our distinguishers on 5-round AES. In the CP setting, we performed 1000 experiments for random keys and random subsets $A_0, A_1 \subseteq \mathbb{F}_{2^8}^2$. There are 614 results returning 5-round AES. The experimental success probability is 61.4%. In the ACP setting, we performed 2000 experiments for random keys and 2^5 random plaintext structures. There are 1266 results returning 5-round AES, then the experimental success probability is 63.3%. When the number of plaintext structures is increased to $2^{5.75}$, there are 1650 results returning 5-round AES. That is, the experimental success probability is increased to 82.5%. The programs are written in C++ including the Intel AES-NI instruction set. The computer has an Intel Core i7-9700 processor with 3.00 GHz and 32 GB RAM.

5 Non-Random Property and Distinguisher for 7-Round AES

In this section, we present the first property of 7-round AES that holds with a probability higher than that of a random permutation, when the quartets of plaintexts satisfy certain exchanged diagonal related differences. Based on this property, we give a distinguisher on 7-round AES with data complexity of $2^{125.6}$. It is the first secret-key distinguisher on 7-round AES with less data than the full codebook.

5.1 A Non-Random Property for 7-Round AES

In [5], Bardeh and Rijmen gave eight related differentials for 4 full rounds of AES, each with a probability of 2^{-192}. In fact, these eight related differentials are all exchanged diagonal related differentials with the same input differences. We revisit one of them, and present the other 7 related differentials in Appendix A. Readers are referred to [5] for more details.

Let $\Delta y, \Delta y'$ be the input related differences, and $\Delta z, \Delta z'$ be the output related differences after 4 full rounds of AES.

$$\Delta y = \begin{bmatrix} \Delta y_0 & \Delta y_4 & \Delta y_8 & \Delta y_{12} \\ \Delta y_1 & \Delta y_5 & \Delta y_9 & \Delta y_{13} \\ \Delta y_2 & \Delta y_6 & \Delta y_{10} & \Delta y_{14} \\ \Delta y_3 & \Delta y_7 & \Delta y_{11} & \Delta y_{15} \end{bmatrix} \longrightarrow \Delta z = \begin{bmatrix} E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \end{bmatrix},$$

$$\Delta y' = \begin{bmatrix} \Delta y_0 & 0 & \Delta y_8 & 0 \\ 0 & \Delta y_5 & 0 & \Delta y_{13} \\ \Delta y_2 & 0 & \Delta y_{10} & 0 \\ 0 & \Delta y_7 & 0 & \Delta y_{15} \end{bmatrix} \longrightarrow \Delta z' = \begin{bmatrix} E\lambda_0 & 0 & D\lambda_2 & 0 \\ 0 & D\lambda_1 & 0 & E\lambda_3 \\ D\lambda_0 & 0 & E\lambda_2 & 0 \\ 0 & E\lambda_1 & 0 & D\lambda_3 \end{bmatrix},$$

$$\Delta y + \Delta y' = \begin{bmatrix} 0 & \Delta y_4 & 0 & \Delta y_{12} \\ \Delta y_1 & 0 & \Delta y_9 & 0 \\ 0 & \Delta y_6 & 0 & \Delta y_{14} \\ \Delta y_3 & 0 & \Delta y_{11} & 0 \end{bmatrix} \longrightarrow \Delta z + \Delta z' = \begin{bmatrix} 0 & 9\lambda_1 & 0 & B\lambda_3 \\ 9\lambda_0 & 0 & B\lambda_2 & 0 \\ 0 & B\lambda_1 & 0 & 9\lambda_3 \\ B\lambda_0 & 0 & 9\lambda_2 & 0 \end{bmatrix}.$$

where all diagonals in Δy are nonzero, and $\lambda_i \in \mathbb{F}_{2^8}$, $i = 0, 1, 2, 3$, are not all zero. The other 7 related differentials can be derived from this one by applying the identical rotation on all columns of Δz and $\Delta z'$, and/or exchanging $\Delta z'$ with $\Delta z + \Delta z'$.

We notice that Δy, $\Delta y'$ are exchanged diagonal related differences, and Δz, $\Delta z'$ are also exchanged diagonal related differences. All diagonals of Δz are nonzero, and only two non-consecutive diagonals of $\Delta z'$ are nonzero. These eight exchanged diagonal related differentials will be combined with one-round exchanged diagonal related differentials to derive a non-random property for 7-round AES.

The following lemma gives a formula for the probability of exchanged diagonal related differentials over one full round of AES.

Lemma 3. *Let $I_1, I_2, J_1, J_2 \subseteq \{0, 1, 2, 3\}$ be four nonempty sets, and $I_2 \subset I_1$, $J_2 \subset J_1$. Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be exchanged diagonal related differences and nonzero only in $SR^{-1}(Col(I_1))$ and $SR^{-1}(Col(I_2))$ respectively. Let $\Delta y, \Delta y' \in \mathbb{F}_{2^8}^{4\times 4}$ be the corresponding output differences after one full round of AES. Then the probability that $\Delta y, \Delta y'$ are exchanged diagonal related differences and nonzero only in $SR^{-1}(Col(J_1))$ and $SR^{-1}(Col(J_2))$ respectively, is*

$$P(|I_1|, |I_2|, |J_1|, |J_2|) = (2^{-8})^{|I_1|\cdot(4-|J_1|+|J_2|)+|I_2|\cdot(|J_1|-2|J_2|)}. \tag{2}$$

Proof. Since $\Delta x, \Delta x'$ are diagonal related differences and the related differences pass through the S-box layer with probability 1, after one-round AES Δy, $\Delta y'$ are column related differences and nonzero only in $Col(I_1)$ and $Col(I_2)$ respectively, as shown in Figure 7. Because $I_2 \subset I_1$, we have $\Delta y_{Col(I_2)} = \Delta y'_{Col(I_2)}$ by the definition of related differences. To prove this lemma, we need to consider the event that Δy is nonzero only in $SR^{-1}(Col(J_1))$, $\Delta y'$ is nonzero only in $SR^{-1}(Col(J_2))$, and $\Delta y_{SR^{-1}(Col(J_2))} = \Delta y'_{SR^{-1}(Col(J_2))}$.

To ensure that Δy is nonzero only in $SR^{-1}(Col(J_1))$, we just need the bytes of Δy in $Col(I_1) \cap SR^{-1}(Col(\{0, 1, 2, 3\} \setminus J_1))$ to be zero, of which the number is

$$|Col(I_1) \cap SR^{-1}(Col(\{0, 1, 2, 3\} \setminus J_1))| = |I_1| \cdot (4 - |J_1|).$$

Since $\Delta y_{Col(I_2)} = \Delta y'_{Col(I_2)}$, the bytes of $\Delta y'$ in $Col(I_2) \cap SR^{-1}(Col(\{0, 1, 2, 3\} \setminus J_1))$ are zero. To ensure that $\Delta y'$ is nonzero only in $SR^{-1}(Col(J_2))$, we just need the bytes of $\Delta y'$ in $Col(I_2) \cap SR^{-1}(Col(J_1 \setminus J_2))$ to be zero, of which the number is

$$|Col(I_2) \cap SR^{-1}(Col(J_1 \setminus J_2))| = |I_2| \cdot (|J_1| - |J_2|).$$

To ensure that $\Delta y_{SR^{-1}(Col(J_2))} = \Delta y'_{SR^{-1}(Col(J_2))}$, we need the bytes of Δy in $Col(I_1 \setminus I_2) \cap SR^{-1}(Col(J_2))$ to be zero, of which the number is

$$|Col(I_1 \setminus I_2) \cap SR^{-1}(Col(J_2))| = (|I_1| - |I_2|) \cdot |J_2|.$$

In total, the number of bytes in Δy and $\Delta y'$ that need to be zero is

$$\begin{aligned} &|I_1| \cdot (4 - |J_1|) + |I_2| \cdot (|J_1| - |J_2|) + (|I_1| - |I_2|) \cdot |J_2| \\ =&|I_1| \cdot (4 - |J_1| + |J_2|) + |I_2| \cdot (|J_1| - 2|J_2|). \end{aligned}$$

Thus, the probability of the event is $P(|I_1|, |I_2|, |J_1|, |J_2|)$.

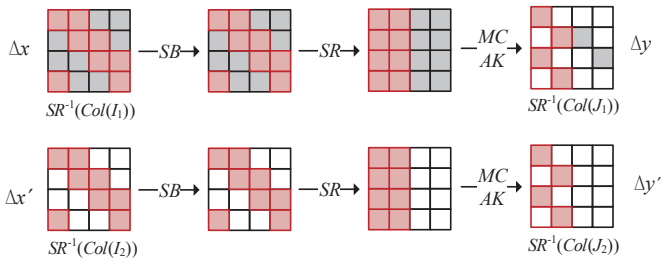


Fig. 7. An example of Lemma 3 with $I_1 = \{0, 1, 2, 3\}, I_2 = \{0, 1\}, J_1 = \{0, 1, 2\}, J_2 = \{0, 2\}$

Experimental simulation of Lemma 3. For the cases of $I_1 = \{0, 1, 2, 3\}$, $I_2 = \{0\}$ or $\{0, 1\}$, $J_1 = \{0, 1, 2, 3\}$, $J_2 = \{0, 2\}$ or $\{1, 3\}$ in Lemma 3, we performed simulation on small-scale AES in [14], as shown in Table 4. The theoretical probability is 2^{-32} for each case on small-scale AES. We randomly choose $50 \cdot 2^{32}$ samples for each case. The experimental probabilities match the theoretical estimations.

Table 4. The simulation results of Lemma 3 on small-scale AES

I_1	I_2	J_1	J_2	Theoretical Prob.	Experimental Prob.
$\{0, 1, 2, 3\}$	$\{0\}$	$\{0, 1, 2, 3\}$	$\{0, 2\}$	2^{-32}	2^{-32}
			$\{1, 3\}$	2^{-32}	$2^{-32.03}$
$\{0, 1, 2, 3\}$	$\{0, 1\}$	$\{0, 1, 2, 3\}$	$\{0, 2\}$	2^{-32}	$2^{-31.97}$
			$\{1, 3\}$	2^{-32}	$2^{-32.03}$

If $J_1 = \{0, 1, 2, 3\}$, $J_2 = \{0, 2\}$ or $J_2 = \{1, 3\}$ in Lemma 3, then Δy is nonzero in all diagonals, and $\Delta y'$ is nonzero only in two non-consecutive diagonals. Then $\Delta y, \Delta y'$ meet the input differences of those eight diagonal related differentials for 4 full rounds of AES in [5]. By combining these two one-round exchanged diagonal related differentials with eight 4-round exchanged diagonal related differentials and extending two rounds, we give a non-random property for 7-round AES in the following theorem.

Theorem 5. *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be exchanged diagonal related differences, where all diagonals in Δx are nonzero, and only one or two diagonals in $\Delta x'$ are nonzero. For any state $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$, let $(C_0, C_1, C_2, C_3) = (R^7(\alpha), R^7(\alpha + \Delta x), R^7(\alpha + \Delta x'), R^7(\alpha + \Delta x + \Delta x'))$. Then the probability that (C_2, C_3) can be obtained by exchanging two non-consecutive inverse diagonals of (C_0, C_1) is at least 2^{-252}.*

Proof. Denote by Δy, $\Delta y'$ the output differences of Δx, $\Delta x'$ after one full round, and denote by Δz, $\Delta z'$ the output differences after five full rounds, as shown in Figure 8.

Firstly, we calculate the probability that Δy, $\Delta y'$ are exchanged diagonal related differences, where all diagonals in Δy are nonzero, and only two non-consecutive diagonals in $\Delta y'$ are nonzero. From Lemma 3, we have $|I_1| = 4$, $|I_2| = 1$ or 2, $|J_1| = 4$, $|J_2| = 2$. By Equation 2, we have $P(4,1,4,2) = 2^{-64}$ and $P(4,2,4,2) = 2^{-64}$. Since J_2 can be $\{0,2\}$ or $\{1,3\}$, the probability is $2 \cdot 2^{-64} = 2^{-63}$.

For the two cases of $J_2 = \{0,2\}$ and $J_2 = \{1,3\}$, the related differences $\Delta y, \Delta y'$ meet the input of eight diagonal related differentials for 4-round AES given in [5]. By combining one-round exchanged diagonal related differentials with 4-round exchanged diagonal related differentials, with probability at least $2^{-63} \cdot 8 \cdot 2^{-192} = 2^{-252}$, we have that Δz, $\Delta z'$ are exchanged diagonal related differences, all diagonals in Δz are nonzero and only two non-consecutive diagonals in $\Delta z'$ are nonzero.

The final 2-round AES can be seen as four parallel super S-boxes, of which the input is the i-th diagonal and the output is the i-th inverse diagonal, $i = 0,1,2,3$. If Δz, $\Delta z'$ are exchanged diagonal related differences, and $\Delta z'$ is nonzero only in two non-consecutive diagonals, then (C_2, C_3) can be obtained by exchanging two non-consecutive inverse diagonals of (C_0, C_1). Then the theorem is proved.

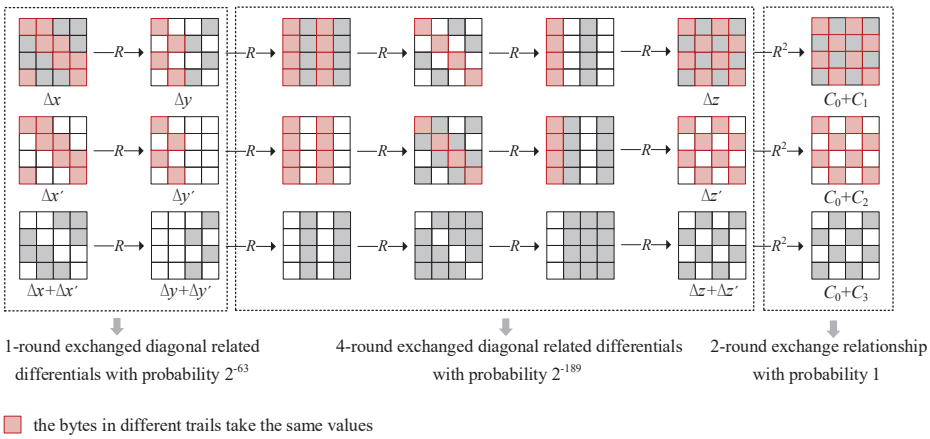


Fig. 8. Framework of 7-round distinguisher

For a random permutation, the probability that (C_2, C_3) can be obtained by exchanging two non-consecutive inverse diagonals of (C_0, C_1) is $2^{-256} \cdot 2 = 2^{-255}$. Utilizing the property in Theorem 5, we can give a distinguisher on 7-round AES.

5.2 A Secret-Key Distinguisher on 7-Round AES

We adopt the same techniques to collect data and construct pairs as the 6-round exchange-attack distinguisher in [6].

Choose plaintexts. To distinguish 7-round AES by Theorem 5, we need 2^{252} quartets of plaintexts $(P_0, P_1, P_2, P_3) = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$,

where Δx, $\Delta x'$ are exchanged diagonal related differences, all diagonals in Δx are nonzero and only one or two diagonals in $\Delta x'$ are nonzero. We randomly choose four subsets $A_0, A_1, A_2, A_3 \subseteq \mathbb{F}_{2^8}^4$, each of size s, and generate s^4 plaintexts where the i-th diagonal takes all possible elements in A_i, $i = 0, 1, 2, 3$. Then we can obtain $\frac{s^4(s-1)^4}{2}$ pairs of plaintexts (P_0, P_1) such that all diagonals of $\Delta x = P_0 + P_1$ are nonzero.

For the case of $\Delta x'$ with only one nonzero diagonal, we have 4 different pairs $(P_2, P_3) = (P_0 + \Delta x', P_1 + \Delta x')$ derived from (P_0, P_1). For the case of $\Delta x'$ with two nonzero diagonals, we have $\frac{1}{2} \cdot \binom{4}{2} = 3$ different pairs $(P_2, P_3) = (P_0 + \Delta x', P_1 + \Delta x')$ derived from (P_0, P_1). Thus, for each pair (P_0, P_1), we can obtain 7 quartets of plaintexts (P_0, P_1, P_2, P_3) satisfying the condition of Theorem 5. So, in total we can obtain $\frac{s^4(s-1)^4}{2} \cdot 7 \cdot \frac{1}{2} = \frac{7s^4(s-1)^4}{4}$ desired quartets of plaintexts.

Taking $s = 2^{31.4}$, we have $\frac{7s^4(s-1)^4}{4} \approx 2^{252}$. Thus, the data complexity is $s^4 = 2^{125.6}$ chosen plaintexts.

Construct pairs of plaintext-ciphertext pairs. For the quartets of plaintexts $(P_0,\ P_1,\ P_2, P_3) = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$, denote the ciphertexts $C_i = R^7(P_i)$, $i = 0, 1, 2, 3$. If (C_2, C_3) can be obtained by exchanging the k-th and $(k + 2)$-th inverse diagonals of (C_0, C_1), then both $C_0 + C_2$ and $C_1 + C_3$ are zero in the $(k+1)$-th and $(k+3)_{\mathrm{mod}\,4}$-th inverse diagonals, $k = 0$ or 1. Before generating quartets, we construct all pairs of plaintext-ciphertext pairs $((P, C), (P', C'))$ such that $P + P' = \Delta x'$ is nonzero only in one or two diagonals, and $C + C'$ is zero in the $(k + 1)$-th and $(k + 3)_{\mathrm{mod}\,4}$-th inverse diagonals, $k = 0$ or 1.

Case of $\Delta x'$ with one nonzero diagonal. Assume the i-th diagonal of $\Delta x'$ is nonzero, $i = 0, 1, 2, 3$. For each plaintext-ciphertext pair (P, C), store it in 8 tables $L_{i,k}$, $i = 0, 1, 2, 3$, $k = 0, 1$, respectively. The index of $L_{i,k}$ is the concatenation of the values of P in diagonals $\{0, 1, 2, 3\} \setminus \{i\}$ and the values of C in inverse diagonals $\{k + 1, (k + 3)_{\mathrm{mod}\,4}\}$, i.e., $P_{SR^{-1}(Col(\{0,1,2,3\}\setminus\{i\}))} \| C_{SR(Col(k+1,(k+3)_{\mathrm{mod}\,4}))}$. Then any two pairs (P, C) and (P', C') with the same index in $L_{i,k}$ can form a desired pair of plaintext-ciphertext pairs $((P, C), (P', C'))$. For each table $L_{i,k}$, we extract all such pairs $((P, C), (P', C'))$ and store (C, C') in a new table $T_{i,k}$ indexed by $P_{SR^{-1}(Col(i))} \| P'_{SR^{-1}(Col(i))}$, $i = 0, 1, 2, 3$, $k = 0, 1$.

Case of $\Delta x'$ with two nonzero diagonals. Assume the 0-th and m-th diagonals of $\Delta x'$ are nonzero, $m = 1, 2, 3$. For each plaintext-ciphertext pair (P, C), store it in 6 tables $L'_{m,k}$, $m = 1, 2, 3$, $k = 0, 1$, respectively, indexed by the concatenation $P_{SR^{-1}(Col(\{1,2,3\}\setminus\{m\}))} \| C_{SR(Col(k+1,(k+3)_{\mathrm{mod}\,4}))}$. Then any two pairs (P, C) and (P', C') with the same index in $L'_{m,k}$ can form a desired pair of plaintext-ciphertext pairs $((P, C), (P', C'))$. For each table $L'_{m,k}$, we extract all such pairs $((P, C), (P', C'))$ and store (C, C') in a new table $T'_{m,k}$ indexed by $P_{SR^{-1}(Col(0,m))} \| P'_{SR^{-1}(Col(0,m))}$, $m = 1, 2, 3$, $k = 0, 1$.

Generate quartets and find right quartets. For each of 14 tables $T_{i,k}$ and $T'_{m,k}$, $i = 0,\ 1,\ 2,\ 3$, $m = 1, 2, 3$, $k = 0, 1$, we generate quartets of ciphertexts

(C_0, C_1, C_2, C_3) by the following two approaches, and check whether (C_2, C_3) can be obtained by exchanging the k-th and $(k+2)$-th inverse diagonals of (C_0, C_1).

Approach I: In each table, any two pairs (C, C') and $(\bar{C}, \bar{C}')$ with the same index can form a quartet of ciphertexts $(C_0, C_1, C_2, C_3) = (C, \bar{C}', C', \bar{C})$, since their plaintexts $(P, \bar{P}', P', \bar{P}) = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$ satisfy the condition of Theorem 5. That is, Δx, $\Delta x'$ are exchanged diagonal related differences, all diagonals of Δx are nonzero and only one or two diagonals of $\Delta x'$ are nonzero. For each quartet of ciphertexts, we check whether $(C', \bar{C})$ can be obtained by exchanging the k-th and $(k+2)$-th inverse diagonals of $(C, \bar{C}')$. Since $C' + C$ and $\bar{C} + \bar{C}'$ are zero in the $(k+1)$-th and $(k+3)_{\mathrm{mod}\,4}$-th inverse diagonals, we only need to check whether $C_{SR(Col(k,k+2))} = \bar{C}_{SR(Col(k,k+2))}$ and $\bar{C}'_{SR(Col(k,k+2))} = C'_{SR(Col(k,k+2))}$. If the two equations hold, then $(C, \bar{C}', C', \bar{C})$ is a right quartet.

Approach II: In each table, any pair (C, C') indexed by $a\|b$ and any pair $(\bar{C}, \bar{C}')$ indexed by $b\|a$ can form a quartet of ciphertexts $(C_0, C_1, C_2, C_3) = (C, \bar{C}, C', \bar{C}')$, where a and b are the two halves of the indices. Their plaintexts $(P, \bar{P}, P', \bar{P}') = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$ satisfy the condition of Theorem 5. For each quartet of ciphertexts, we check whether $(C', \bar{C}')$ can be obtained by exchanging the k-th and $(k+2)$-th inverse diagonals of $(C, \bar{C})$. Since $C' + C$ and $\bar{C}' + \bar{C}$ are zero in the $(k+1)$-th and $(k+3)_{\mathrm{mod}\,4}$-th inverse diagonals, we only need to check whether $C_{SR(Col(k,k+2))} = \bar{C}'_{SR(Col(k,k+2))}$ and $\bar{C}_{SR(Col(k,k+2))} = C'_{SR(Col(k,k+2))}$. If the two equations hold, then $(C, \bar{C}, C', \bar{C}')$ is a right quartet.

For 7-round AES, we can find one right quartet on average, while for a random permutation the expected number of right quartets is $2^{-255} \cdot 2^{252} = 2^{-3}$.

The process of distinguishing 7-round AES. The pseudocode of 7-round distinguisher is given in algorithm 3, and the process is as follows.

1. Choose randomly four subsets $A_0, A_1, A_2, A_3 \subseteq \mathbb{F}_{2^8}^4$, each of size $2^{31.4}$, and construct $2^{125.6}$ plaintexts where the i-th diagonal takes all possible elements in A_i, $i = 0, 1, 2, 3$.

2. For each plaintext P, ask for its ciphertext C. For $i = 0, 1, 2, 3$ and $k = 0, 1$, store $P\|C$ into the table $L_{i,k}$ indexed by $P_{SR^{-1}(Col(\{0,1,2,3\}\setminus\{i\}))}\| C_{SR(Col(k+1,(k+3)_{\mathrm{mod}\,4}))}$. For $m = 1, 2, 3$ and $k = 0, 1$, store $P\|C$ into the table $L'_{m,k}$ indexed by $P_{SR^{-1}(Col(\{1,2,3\}\setminus\{m\}))}\|C_{SR(Col(k+1,(k+3)_{\mathrm{mod}\,4}))}$.

3. For each table $L_{i,k}$, $i = 0, 1, 2, 3$, $k = 0, 1$, extract all pairs $(P\|C,\ P'\|C')$ with the same index, and store (C, C') in a new table $T_{i,k}$ indexed by $P_{SR^{-1}(Col(i))}$ $\|P'_{SR^{-1}(Col(i))}$. For each table $L'_{m,k}$, $m = 1, 2, 3$, $k = 0, 1$, extract all pairs $(P\|C, P'\|C')$ with the same index, and store (C, C') in a new table $T'_{m,k}$ indexed by $P_{SR^{-1}(Col(0,m))}\|P'_{SR^{-1}(Col(0,m))}$.

4. For each of 14 tables $T_{i,k}$ and $T'_{m,k}$, $i = 0, 1, 2, 3$, $m = 1, 2, 3$, $k = 0, 1$, check whether there exist (C, C') and $(\bar{C},\ \bar{C}')$ with the same index such that $C_{SR(Col(k,k+2))} = \bar{C}_{SR(Col(k,k+2))}$ and $\bar{C}'_{SR(Col(k,k+2))} = C'_{SR(Col(k,k+2))}$. If there exist such pairs, then output "It is 7-round AES". Otherwise, check whether there exist (C, C') indexed by $a\|b$ and $(\bar{C}, \bar{C}')$ indexed by $b\|a$ such that $C_{SR(Col(k,k+2))} = \bar{C}'_{SR(Col(k,k+2))}$ and $\bar{C}_{SR(Col(k,k+2))} = C'_{SR(Col(k,k+2))}$. If there

exist such pairs, then output "It is 7-round AES". After all the above processes, if there is no output, then judge "It is a random permutation".

Complexity analysis. The data complexity is $2^{125.6}$ chosen plaintexts. In the following we analyze the time complexity. In step 2, we need to encrypt $2^{125.6}$ plaintexts and store the plaintext-ciphertext pairs into 14 tables $L_{i,k}$ and $L'_{m,k}$, $i = 0, 1, 2, 3$, $m = 1, 2, 3$, $k = 0, 1$. Referring to [3], we regard one table insertion as one-round AES encryption, then the time complexity of step 2 is $2^{125.6} + 14 \cdot 2^{125.6}/7 \approx 2^{127.18}$ encryptions of 7-round AES.

In step 3, for each table $L_{i,k}$, $i = 0, 1, 2, 3$, $k = 0, 1$, the expected number of indices $P_{SR^{-1}(Col(\{0,1,2,3\}\setminus\{i\}))} \| C_{SR(Col(k+1,(k+3)_{\mathrm{mod}\,4}))}$ is $2^{31.4\times 3} \cdot 2^{64} = 2^{158.2}$, so the number of pairs $(P\|C, P'\|C')$ extracted is about $\binom{2^{125.6}}{2} \cdot 2^{-158.2} \approx 2^{92}$. For each table $L'_{m,k}$, $m = 1, 2, 3$, $k = 0, 1$, the number of indices $P_{SR^{-1}(Col(\{1,2,3\}\setminus\{m\}))} \| C_{SR(Col(k+1,(k+3)_{\mathrm{mod}\,4}))}$ is $2^{31.4\times 2} \cdot 2^{64} = 2^{126.8}$, so the number of pairs $(P\|C, P'\|C')$ extracted is about $\binom{2^{125.6}}{2} \cdot 2^{-126.8} = 2^{123.4}$. Then the time complexity of step 3 is about $8 \cdot 2^{92} + 6 \cdot 2^{123.4} \approx 2^{125.98}$ table lookups and insertions, which is equivalent to $2^{125.98} \cdot 2/7 \approx 2^{124.17}$ encryptions.

In step 4, for each table $T_{i,k}$, $i = 0, 1, 2, 3$, $k = 0, 1$, the number of indices $P_{SR^{-1}(Col(i))} \| P'_{SR^{-1}(Col(i))}$ is $2^{31.4\times 2} = 2^{62.8}$. For each index of $T_{i,k}$, there are $2^{92} \cdot 2^{-62.8} = 2^{29.2}$ pairs on average. Then, the number of quartets that need to be checked is about $2^{62.8} \cdot \binom{2^{29.2}}{2} + 2^{61.8} \cdot 2^{29.2\times 2} \approx 2^{121.2}$ for each $T_{i,k}$. For each table $T'_{m,k}$, $m = 1, 2, 3$, $k = 0, 1$, the number of indices $P_{SR^{-1}(Col(0,m))} \| P'_{SR^{-1}(Col(0,m))}$ is $2^{31.4\times 4} = 2^{125.6}$. For each index of $T'_{m,k}$, the expected number of collisions (C, C') and $(\bar{C}, \bar{C}')$ is $\binom{2^{123.4}}{2} \cdot 2^{-125.6\times 2} \approx 2^{-5.4}$. Then, the number of quartets that need to be checked is about $2^{-5.4} \cdot 2^{125.6} \cdot 2 = 2^{121.2}$ for each $T'_{m,k}$. The time complexity of step 4 is about $14 \cdot 2^{121.2} \cdot 2/7 \approx 2^{123.2}$ encryptions. Therefore, the overall time complexity is dominated by step 2 of $2^{127.18}$ encryptions of 7-round AES.

The memory complexity is dominated by the 14 tables $L_{i,k}$ and $L'_{m,k}$ constructed in step 2, $i = 0, 1, 2, 3$, $m = 1, 2, 3$, $k = 0, 1$. In fact, for each table $L_{i,k}$, $i = 0, 1, 2, 3$, $k = 0, 1$, we only need to store $P_{SR^{-1}(Col(i))} \| C_{SR(Col(k,k+2))}$ instead of the whole $P\|C$. Similarly, for each table $L'_{m,k}$, $m = 1, 2, 3$, $k = 0, 1$, we only need to store $P_{SR^{-1}(Col(0,m))} \| C_{SR(Col(k,k+2))}$ instead of the whole $P\|C$. This does not affect the operations of steps 3 and 4. Therefore, the overall memory complexity is about $14 \times 2^{125.6} \approx 2^{129.41}$. We note that the memory complexity can be reduced to $2^{126.6}$ by constructing and processing the 14 tables one by one, at the cost of increasing $14 \cdot 2^{125.6}$ memory accesses to the plaintext-ciphertext table.

For 7-round AES, the probability that there exists at least one right quartet among 2^{252} quartets is $1 - (1 - 2^{-252})^{2^{252}} \approx 63\%$, so the success probability of the distinguisher is 63%. For a random permutation, the error probability that it is judged as 7-round AES is $1 - (1 - 2^{-255})^{2^{252}} \approx 2^{-3.09}$.

Algorithm 3: Distinguisher on 7-round AES

Choose randomly four subsets $A_0, A_1, A_2, A_3 \subseteq \mathbb{F}_{2^8}^4$, each of size $2^{31.4}$.
Construct $2^{125.6}$ plaintexts where the i-th diagonal takes all possible elements in A_i, $i = 0, 1, 2, 3$.
for *each plaintext* P **do**
  Ask for its ciphertext C.
  Store $P\|C$ into eight tables $L_{i,k}$ indexed by $P_{SR^{-1}(Col(\{0,1,2,3\}\setminus\{i\}))}\| C_{SR(Col(k+1,(k+3)_{\bmod 4}))}$, $i = 0, 1, 2, 3$, $k = 0, 1$.
  Store $P\|C$ into six tables $L'_{m,k}$ indexed by $P_{SR^{-1}(Col(\{1,2,3\}\setminus\{m\}))}\| C_{SR(Col(k+1,(k+3)_{\bmod 4}))}$, $m = 1, 2, 3$, $k = 0, 1$.
end
for $i = 0, 1, 2, 3$ *and* $k = 0, 1$ **do**
  Extract all pairs $(P\|C, P'\|C')$ with the same index in $L_{i,k}$.
  Store (C, C') in $T_{i,k}$ indexed by $P_{SR^{-1}(Col(i))}\|P'_{SR^{-1}(Col(i))}$.
end
for $m = 1, 2, 3$ *and* $k = 0, 1$ **do**
  Extract all pairs $(P\|C, P'\|C')$ with the same index in $L'_{m,k}$.
  Store (C, C') in $T'_{m,k}$ indexed by $P_{SR^{-1}(Col(0,m))}\|P'_{SR^{-1}(Col(0,m))}$.
end
for *each of* 14 *tables* $T_{i,k}$ *and* $T'_{m,k}$, $i = 0, 1, 2, 3$, $m = 1, 2, 3$, $k = 0, 1$ **do**
  for *any two pairs* (C, C') *and* $(\bar{C}, \bar{C}')$ *with the same index* **do**
    Check whether the equations $C_{SR(Col(k,k+2))} = \bar{C}_{SR(Col(k,k+2))}$ and $\bar{C}'_{SR(Col(k,k+2))} = C'_{SR(Col(k,k+2))}$ hold.
    if *the two equations hold* **then**
      Return: It is 7-round AES.
    end
  end
  for *any pair* (C, C') *indexed by* $a\|b$ *and any pair* $(\bar{C}, \bar{C}')$ *indexed by* $b\|a$ **do**
    Check whether the equations $C_{SR(Col(k,k+2))} = \bar{C}'_{SR(Col(k,k+2))}$ and $\bar{C}_{SR(Col(k,k+2))} = C'_{SR(Col(k,k+2))}$ hold.
    if *the two equations hold* **then**
      Return: It is 7-round AES.
    end
  end
end
Return: It is a random permutation.

On the complexity of table insertion. Currently, there is no unified standard in the literature for the equivalent cost of one table insertion. In the exchange-attack distinguisher on 6-round AES [6], one table insertion was equivalent to one

S-box lookup, i.e., 1/16 of one-round AES encryption, so its time complexity was dominated by the encryptions of plaintexts. If we adopt the same equivalence as in [6], the time complexity of our attack will also be dominated by $2^{125.6}$ encryptions of plaintexts. However, we adopt a more conservative equivalence as in [3], which regards one table insertion as one-round AES encryption. We also conducted 100 experiments to compare the cost of table insertion with that of one-round AES encryption. In each experiment, we measured the cost of inserting 2^{32} AES states into a table and that of applying one-round AES encryption to these states. The average costs were 10.8 seconds for table insertions, 14.3 seconds for one-round encryptions using AES-NI instructions, and 56.4 seconds for one-round encryptions using the source code of AES from the OpenSSL 3.6.0 library. Our computer has an Intel Xeon W-2255 processor with 3.70 GHz and 128 GB RAM.

6 An Alternative Distinguisher on 6-Round AES

In [6], Bardeh and Rønjom proposed the exchange attack to distinguish 6-round AES with $2^{88.2}$ chosen plaintexts. In [4], Bardeh used the exchange attack to give a distinguisher on 6-round AES in the adaptive setting. The exchange-attack distinguishers in [4,6] actually utilize the one-round exchanged related differentials. In Sect. 3, we presented the relationship between exchanged and shifted related differences. Therefore, there exist dual distinguishers to the exchange-attack distinguishers. Utilizing shifted diagonal related differentials, we present some dual results to the exchange attack in [6], and present an alternative distinguisher on 6-round AES in the chosen plaintexts setting.

Lemma 4. *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be shifted diagonal related differences and nonzero only in two diagonals and one diagonal respectively. Let $\Delta y, \Delta y' \in \mathbb{F}_{2^8}^{4\times 4}$ be the corresponding output differences after one full round of AES. Then the probability that Δy, $\Delta y'$ are shifted diagonal related differences is 2^{-38}.*

Proof. From Figure 5, $\Delta y, \Delta y'$ are shifted diagonal related differences if and only if $\Delta y + \Delta y'$, Δy are exchanged diagonal related differences. Note that $\Delta x + \Delta x'$, Δx are exchanged diagonal related differences, and $\Delta x + \Delta x'$ is nonzero in three diagonals. By Lemma 3, the probability that $\Delta y + \Delta y'$, Δy are exchanged diagonal related differences is

$$\sum_{\substack{J_1 \subseteq \{0,1,2,3\} \\ J_2 \subset J_1, |J_2| \geq 1}} P(3, 2, |J_1|, |J_2|) \approx 2^{-38}.$$

Then the lemma is proved.

Theorem 6. *Let $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be shifted diagonal related differences and nonzero only in two diagonals and one diagonal respectively. For any state $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$, let $(C_0, C_1, C_2, C_3) = (R^6(\alpha), R^6(\alpha+\Delta x), R^6(\alpha+\Delta x'), R^6(\alpha+\Delta x+\Delta x'))$. If $C_0 + C_3$ is zero in three inverse diagonals, then the probability that $C_1 + C_2$ is zero in three inverse diagonals is at least 2^{-82}.*

Proof. Let $\Delta y = R(\alpha)+R(\alpha+\Delta x)$, $\Delta y' = R(\alpha)+R(\alpha+\Delta x')$, and $(z_0, z_1, z_2, z_3) = (R^5(\alpha),\ R^5(\alpha+\Delta x),\ R^5(\alpha+\Delta x'),\ R^5(\alpha+\Delta x+\Delta x'))$, as shown in Figure 9. By Lemma 4, the probability that Δy, $\Delta y'$ are shifted diagonal related differences is 2^{-38}. If Δy, $\Delta y'$ are diagonal related differences, then $\Delta y+\Delta y'$, Δy are also diagonal related differences. Thus, the probability that $\Delta y+\Delta y'$, Δy are diagonal related differences is 2^{-38}. Then by Lemma 1, the probability that

$$\mu(z_0+z_3) = \mu(z_1+z_2) \tag{3}$$

is at least 2^{-38}, where $\mu(\cdot) = \nu(SR^{-1}(\cdot))$. If C_0+C_3 is zero in three inverse diagonals, then z_0+z_3 has only one nonzero byte with probability 2^{-22}. Then by Equation 3, $SR^{-1}(z_1+z_2)$ has only one nonzero column. So, the probability that z_1+z_2 has only one nonzero byte is at least $2^{-38}\cdot 2^{-22}\cdot 2^{-22} = 2^{-82}$. Thus, the probability that C_1+C_2 is zero in three inverse diagonals is at least 2^{-82}.

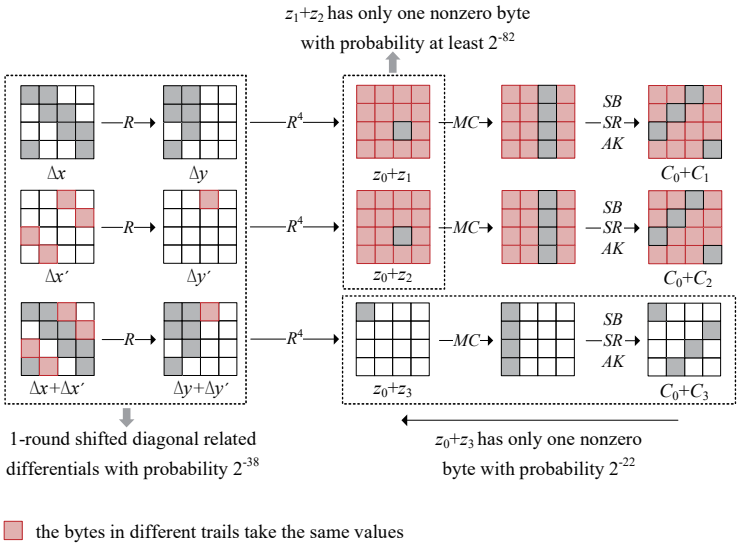


Fig. 9. Framework of 6-round distinguisher

Let Δx, $\Delta x'$ be shifted diagonal related differences as Theorem 6. Randomly choose plaintexts $(P_0, P_1, P_2, P_3) = (P_0, P_0+\Delta x, P_0+\Delta x', P_0+\Delta x+\Delta x')$, and let $(C_0, C_1, C_2, C_3) = (R^6(P_0), R^6(P_1), R^6(P_2), R^6(P_3))$ be the corresponding ciphertexts. The probability that C_0+C_3 is zero in three inverse diagonals is $4\cdot 2^{-96} = 2^{-94}$. Then the probability that both C_0+C_3 and C_1+C_2 are zero in three inverse diagonals is $2^{-94}\cdot 2^{-82} = 2^{-176}$, while it is $2^{-94}\cdot 2^{-94} = 2^{-188}$ for a random permutation.

To generate 2^{176} desired quartets of plaintexts (P_0, P_1, P_2, P_3), we randomly choose three subsets $A_0, A_1, A_2 \subseteq \mathbb{F}_{2^8}^4$, each of size s, and construct s^3 plaintexts where the i-th diagonal takes all possible elements in A_i, $i = 0, 1, 2$, and the other

bytes take any constants. Then we can obtain $3 \cdot s \cdot \frac{s^2(s-1)^2}{2}$ pairs of plaintexts (P_0, P_1) such that $\Delta x = P_0 + P_1$ is nonzero only in two diagonals. For each pair (P_0, P_1), we can obtain $s-1$ pairs $(P_2, P_3) = (P_0 + \Delta x', P_1 + \Delta x')$ by shifting the other active diagonal. Totally, we can get $3 \cdot s \cdot \frac{s^2(s-1)^2}{2} \cdot \frac{s-1}{2} = \frac{3s^3(s-1)^3}{4}$ quartets (P_0, P_1, P_2, P_3). Taking $s = 2^{29.41}$, we have $\frac{3s^3(s-1)^3}{4} \approx 2^{176}$. Thus, the data complexity is $s^3 = 2^{88.23}$ chosen plaintexts.

The process of distinguishing 6-round AES is as follows.

1. Choose randomly three subsets $A_0, A_1, A_2 \subseteq \mathbb{F}_{2^8}^4$, each of size $2^{29.41}$. Construct $2^{88.23}$ plaintexts where the i-th diagonal takes all possible elements in A_i, $i = 0, 1, 2$, and the other bytes take any constants.

2. For the k-th plaintext P, $0 \leq k \leq 2^{88.23} - 1$, store P in the table T indexed by k. Ask for the ciphertext C, and store k into four hash tables H_j, $0 \leq j \leq 3$, indexed by $C_{SR(Col(\{0,1,2,3\}\setminus\{j\}))}$.

3. For each table H_j, $0 \leq j \leq 3$, extract all pairs (k, k') with the same index, obtain the corresponding plaintext pairs (P, P') from the table T, and store (P, P') in the table L indexed by $P + P'$.

4. For any two pairs (P, P') and $(\bar{P}, \bar{P}')$ with the same index in L, check whether the set $\{P_{SR^{-1}(Col(i))}, \bar{P}_{SR^{-1}(Col(i))}, \bar{P}'_{SR^{-1}(Col(i))}, P'_{SR^{-1}(Col(i))}\}$ consists of two pairs of equal values for each $0 \leq i \leq 2$. If there exist (P, P') and $(\bar{P}, \bar{P}')$ satisfying the condition, then output "It is 6-round AES". After all the above processes, if there is no output, then judge "It is a random permutation".

Complexity analysis. The data complexity is $2^{88.23}$. Step 2 needs $2^{88.23}$ encryptions of plaintexts and $5 \cdot 2^{88.23}$ insertions into tables, which are equivalent to $2^{88.23} + 5 \cdot 2^{88.23}/6 \approx 2^{89.1}$ encryptions of 6-round AES. In step 3, the expected number of pairs (P, P') is $4 \cdot \binom{2^{88.23}}{2} \cdot 2^{-96} \approx 2^{81.46}$, so the time complexity of step 3 is negligible compared to step 2. In step 4, the expected number of quartets that need to be checked is $\binom{2^{81.46}}{2} \cdot 2^{-96} \approx 2^{65.92}$, so the time complexity of step 4 is negligible. Therefore, the overall time complexity is $2^{89.1}$ encryptions of 6-round AES. The memory complexity is dominated by the table T, which stores $2^{88.23}$ plaintexts. The success probability of the distinguisher is $1 - (1 - 2^{-176})^{2^{176}} \approx 63\%$, and the error probability that a random permutation is judged as 6-round AES is $1 - (1 - 2^{-188})^{2^{176}} \approx 2^{-12}$.

Note that if we round the complexities to one decimal place and regard one table insertion as one S-box lookup, as in the 6-round exchange-attack distinguisher [6], then the data, time, and memory complexities of our distinguisher are all $2^{88.2}$, identical to those reported in [6].

7 Conclusion

This paper studies the non-random properties and distinguishers for 5 to 7 rounds of AES based on related differentials. We provide a new insight on related differences from the perspectives of exchange and shift operations. We present certain byte-wise related differentials over one-round AES, and combine them

with the 4-round zero-difference property to present a new non-random property for 5-round AES. Based on the property, we improve the distinguishers on 5-round AES in both the CP and ACP settings. We present a formula for estimating the probability of the exchanged diagonal related differentials over one-round AES, combine them with the 4-round related differentials given by Bardeh and Rijmen, and extend two rounds to present the first non-random property for 7-round AES. Based on the property, we give the first secret-key distinguisher on 7-round AES with data complexity of $2^{125.6}$, which is lower than the full codebook. Utilizing shifted diagonal related differentials, we present an alternative distinguisher on 6-round AES, dual to the 6-round exchange-attack distinguisher. This paper shows the potential of the related-differential cryptanalysis. There are two interesting directions for future work. One is to explore our distinguishers to do key-recovery attacks on round-reduced AES. The other is to study whether other cryptanalysis techniques can be combined with related differentials to further improve the distinguishers.

Acknowledgments. This work was supported by the National Natural Science Foundation of China under Grant No. 62672511 and by the Natural Science Foundation of Henan under Grant No. 252300420396.

A Related Differentials for 4 Full Rounds of AES in [5]

Four full rounds of AES can be written as

$$AK \circ MC \circ G \circ MC \circ G,$$

where $G = SR \circ SB \circ AK \circ MC \circ SR \circ SB \circ AK$. In [5], Bardeh and Rijmen gave eight diagonal related differentials for 4 full rounds of AES, each with a probability of 2^{-192}. For one of them, the trails of diagonal related differentials over the first 2 rounds are as follows.

$$\underset{\Delta y}{\begin{bmatrix} \Delta y_0 & \Delta y_4 & \Delta y_8 & \Delta y_{12} \\ \Delta y_1 & \Delta y_5 & \Delta y_9 & \Delta y_{13} \\ \Delta y_2 & \Delta y_6 & \Delta y_{10} & \Delta y_{14} \\ \Delta y_3 & \Delta y_7 & \Delta y_{11} & \Delta y_{15} \end{bmatrix}} \xrightarrow{G} \begin{bmatrix} 2\gamma_0 & 3\gamma_1 & \gamma_2 & \gamma_3 \\ \gamma_0 & 2\gamma_1 & 3\gamma_2 & \gamma_3 \\ \gamma_0 & \gamma_1 & 2\gamma_2 & 3\gamma_3 \\ 3\gamma_0 & \gamma_1 & \gamma_2 & 2\gamma_3 \end{bmatrix} \xrightarrow{MC} \begin{bmatrix} 5\gamma_0 & 0 & 4\gamma_2 & 0 \\ 0 & 5\gamma_1 & 0 & 4\gamma_3 \\ 4\gamma_0 & 0 & 5\gamma_2 & 0 \\ 0 & 4\gamma_1 & 0 & 5\gamma_3 \end{bmatrix}, \quad (4)$$

$$\underset{\Delta y'}{\begin{bmatrix} \Delta y_0 & 0 & \Delta y_8 & 0 \\ 0 & \Delta y_5 & 0 & \Delta y_{13} \\ \Delta y_2 & 0 & \Delta y_{10} & 0 \\ 0 & \Delta y_7 & 0 & \Delta y_{15} \end{bmatrix}} \xrightarrow{G} \begin{bmatrix} 2\gamma_0 & 0 & \gamma_2 & 0 \\ 0 & 2\gamma_1 & 0 & \gamma_3 \\ \gamma_0 & 0 & 2\gamma_2 & 0 \\ 0 & \gamma_1 & 0 & 2\gamma_3 \end{bmatrix} \xrightarrow{MC} \begin{bmatrix} 5\gamma_0 & 7\gamma_1 & 0 & \gamma_3 \\ \gamma_0 & 5\gamma_1 & 7\gamma_2 & 0 \\ 0 & \gamma_1 & 5\gamma_2 & 7\gamma_3 \\ 7\gamma_0 & 0 & \gamma_2 & 5\gamma_3 \end{bmatrix}, \quad (5)$$

$$\begin{bmatrix} 0 & \Delta y_4 & 0 & \Delta y_{12} \\ \Delta y_1 & 0 & \Delta y_9 & 0 \\ 0 & \Delta y_6 & 0 & \Delta y_{14} \\ \Delta y_3 & 0 & \Delta y_{11} & 0 \end{bmatrix} \xrightarrow{G} \begin{bmatrix} 0 & 3\gamma_1 & 0 & \gamma_3 \\ \gamma_0 & 0 & 3\gamma_2 & 0 \\ 0 & \gamma_1 & 0 & 3\gamma_3 \\ 3\gamma_0 & 0 & \gamma_2 & 0 \end{bmatrix} \xrightarrow{MC} \begin{bmatrix} 0 & 7\gamma_1 & 4\gamma_2 & \gamma_3 \\ \gamma_0 & 0 & 7\gamma_2 & 4\gamma_3 \\ 4\gamma_0 & \gamma_1 & 0 & 7\gamma_3 \\ 7\gamma_0 & 4\gamma_1 & \gamma_2 & 0 \end{bmatrix}, \quad (6)$$
$$\Delta y + \Delta y'$$

where all diagonals in Δy are nonzero, and $\gamma_i \in \mathbb{F}_{2^8}$, $i = 0, 1, 2, 3$, are not all zero. The probability of the differential trail in (4) is $2^{-128} \cdot (2^8 - 1)^4 \approx 2^{-96}$. Since G can be seen as operating on four diagonals in parallel, if the differential trail in (4) holds, then the differential trails in (5) and (6) hold. Thus, the probability of the diagonal related differentials over the first 2 rounds is 2^{-96}.

For the last two rounds, the trails of diagonal related differentials are as follows.

$$\begin{bmatrix} 5\gamma_0 & 0 & 4\gamma_2 & 0 \\ 0 & 5\gamma_1 & 0 & 4\gamma_3 \\ 4\gamma_0 & 0 & 5\gamma_2 & 0 \\ 0 & 4\gamma_1 & 0 & 5\gamma_3 \end{bmatrix} \xrightarrow{G} \begin{bmatrix} 5\lambda_0 & 0 & 5\lambda_2 & 0 \\ 0 & 4\lambda_1 & 0 & 5\lambda_3 \\ 4\lambda_0 & 0 & 4\lambda_2 & 0 \\ 0 & 5\lambda_1 & 0 & 4\lambda_3 \end{bmatrix} \xrightarrow[AK]{MC} \begin{bmatrix} E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \end{bmatrix}, \quad (7)$$
$$\Delta z$$

$$\begin{bmatrix} 5\gamma_0 & 7\gamma_1 & 0 & \gamma_3 \\ \gamma_0 & 5\gamma_1 & 7\gamma_2 & 0 \\ 0 & \gamma_1 & 5\gamma_2 & 7\gamma_3 \\ 7\gamma_0 & 0 & \gamma_2 & 5\gamma_3 \end{bmatrix} \xrightarrow{G} \begin{bmatrix} 5\lambda_0 & \lambda_1 & 0 & 7\lambda_3 \\ \lambda_0 & 0 & 7\lambda_2 & 5\lambda_3 \\ 0 & 7\lambda_1 & 5\lambda_2 & \lambda_3 \\ 7\lambda_0 & 5\lambda_1 & \lambda_2 & 0 \end{bmatrix} \xrightarrow[AK]{MC} \begin{bmatrix} E\lambda_0 & 0 & D\lambda_2 & 0 \\ 0 & D\lambda_1 & 0 & E\lambda_3 \\ D\lambda_0 & 0 & E\lambda_2 & 0 \\ 0 & E\lambda_1 & 0 & D\lambda_3 \end{bmatrix}, \quad (8)$$
$$\Delta z'$$

$$\begin{bmatrix} 0 & 7\gamma_1 & 4\gamma_2 & \gamma_3 \\ \gamma_0 & 0 & 7\gamma_2 & 4\gamma_3 \\ 4\gamma_0 & \gamma_1 & 0 & 7\gamma_3 \\ 7\gamma_0 & 4\gamma_1 & \gamma_2 & 0 \end{bmatrix} \xrightarrow{G} \begin{bmatrix} 0 & \lambda_1 & 4\lambda_2 & 7\lambda_3 \\ \lambda_0 & 4\lambda_1 & 7\lambda_2 & 0 \\ 4\lambda_0 & 7\lambda_1 & 0 & \lambda_3 \\ 7\lambda_0 & 0 & \lambda_2 & 4\lambda_3 \end{bmatrix} \xrightarrow[AK]{MC} \begin{bmatrix} 0 & 9\lambda_1 & 0 & B\lambda_3 \\ 9\lambda_0 & 0 & B\lambda_2 & 0 \\ 0 & B\lambda_1 & 0 & 9\lambda_3 \\ B\lambda_0 & 0 & 9\lambda_2 & 0 \end{bmatrix}, \quad (9)$$
$$\Delta z + \Delta z'$$

where $\lambda_i \in \mathbb{F}_{2^8}$, $i = 0, 1, 2, 3$, are not all zero. Similarly, the probability is 2^{-96}. Thus, the probability of the 4-round diagonal related differentials is 2^{-192}.

The other 7 related differentials can be derived from this one by applying the identical rotation on all columns of Δz and $\Delta z'$, and/or exchanging $\Delta z'$ with $\Delta z + \Delta z'$. All of the 8 diagonal related differentials are listed in Table 5.

References

1. Bao, Z., Guo, C., Guo, J., Song, L.: TNT: How to tweak a block cipher. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, Part II. Lecture Notes in Computer Science, vol. 12106, pp. 641–673. Springer, Cham, Switzerland, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45724-2_22
2. Bao, Z., Guo, J., List, E.: Extended truncated-differential distinguishers on round-reduced AES. IACR Transactions on Symmetric Cryptology **2020**(3), 197–261 (2020). https://doi.org/10.13154/tosc.v2020.i3.197-261

Table 5. Eight diagonal related differentials for 4-round AES in [5]

The input differences	$\Delta y = \begin{bmatrix} \Delta y_0 & \Delta y_4 & \Delta y_8 & \Delta y_{12} \\ \Delta y_1 & \Delta y_5 & \Delta y_9 & \Delta y_{13} \\ \Delta y_2 & \Delta y_6 & \Delta y_{10} & \Delta y_{14} \\ \Delta y_3 & \Delta y_7 & \Delta y_{11} & \Delta y_{15} \end{bmatrix}$	, $\Delta y' = \begin{bmatrix} \Delta y_0 & 0 & \Delta y_8 & 0 \\ 0 & \Delta y_5 & 0 & \Delta y_{13} \\ \Delta y_2 & 0 & \Delta y_{10} & 0 \\ 0 & \Delta y_7 & 0 & \Delta y_{15} \end{bmatrix}$
The output differences	1. $\Delta z = \begin{bmatrix} E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \end{bmatrix}$	, $\Delta z' = \begin{bmatrix} E\lambda_0 & 0 & D\lambda_2 & 0 \\ 0 & D\lambda_1 & 0 & E\lambda_3 \\ D\lambda_0 & 0 & E\lambda_2 & 0 \\ 0 & E\lambda_1 & 0 & D\lambda_3 \end{bmatrix}$
	2. $\Delta z = \begin{bmatrix} 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \\ E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \end{bmatrix}$	, $\Delta z' = \begin{bmatrix} 0 & D\lambda_1 & 0 & E\lambda_3 \\ D\lambda_0 & 0 & E\lambda_2 & 0 \\ 0 & E\lambda_1 & 0 & D\lambda_3 \\ E\lambda_0 & 0 & D\lambda_2 & 0 \end{bmatrix}$
	3. $\Delta z = \begin{bmatrix} D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \\ E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \end{bmatrix}$	, $\Delta z' = \begin{bmatrix} D\lambda_0 & 0 & E\lambda_2 & 0 \\ 0 & E\lambda_1 & 0 & D\lambda_3 \\ E\lambda_0 & 0 & D\lambda_2 & 0 \\ 0 & D\lambda_1 & 0 & E\lambda_3 \end{bmatrix}$
	4. $\Delta z = \begin{bmatrix} B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \\ E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \end{bmatrix}$	, $\Delta z' = \begin{bmatrix} 0 & E\lambda_1 & 0 & D\lambda_3 \\ E\lambda_0 & 0 & D\lambda_2 & 0 \\ 0 & D\lambda_1 & 0 & E\lambda_3 \\ D\lambda_0 & 0 & E\lambda_2 & 0 \end{bmatrix}$
	5. $\Delta z = \begin{bmatrix} D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \\ E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \end{bmatrix}$	, $\Delta z' = \begin{bmatrix} 0 & B\lambda_1 & 0 & 9\lambda_3 \\ B\lambda_0 & 0 & 9\lambda_2 & 0 \\ 0 & 9\lambda_1 & 0 & B\lambda_3 \\ 9\lambda_0 & 0 & B\lambda_2 & 0 \end{bmatrix}$
	6. $\Delta z = \begin{bmatrix} B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \\ E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \end{bmatrix}$	, $\Delta z' = \begin{bmatrix} B\lambda_0 & 0 & 9\lambda_2 & 0 \\ 0 & 9\lambda_1 & 0 & B\lambda_3 \\ 9\lambda_0 & 0 & B\lambda_2 & 0 \\ 0 & B\lambda_1 & 0 & 9\lambda_3 \end{bmatrix}$
	7. $\Delta z = \begin{bmatrix} E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \end{bmatrix}$	, $\Delta z' = \begin{bmatrix} 0 & 9\lambda_1 & 0 & B\lambda_3 \\ 9\lambda_0 & 0 & B\lambda_2 & 0 \\ 0 & B\lambda_1 & 0 & 9\lambda_3 \\ B\lambda_0 & 0 & 9\lambda_2 & 0 \end{bmatrix}$
	8. $\Delta z = \begin{bmatrix} 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3 \\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3 \\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3 \\ E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3 \end{bmatrix}$	, $\Delta z' = \begin{bmatrix} 9\lambda_0 & 0 & B\lambda_2 & 0 \\ 0 & B\lambda_1 & 0 & 9\lambda_3 \\ B\lambda_0 & 0 & 9\lambda_2 & 0 \\ 0 & 9\lambda_1 & 0 & B\lambda_3 \end{bmatrix}$

3. Bar-On, A., Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: Improved key recovery attacks on reduced-round AES with practical data and memory complexities. Journal of Cryptology **33**(3), 1003–1043 (Jul 2020). https://doi.org/10.1007/s00145-019-09336-w
4. Bardeh, N.G.: A key-independent distinguisher for 6-round AES in an adaptive setting. Cryptology ePrint Archive, Report 2019/945 (2019), https://eprint.iacr.org/2019/945
5. Bardeh, N.G., Rijmen, V.: New key-recovery attack on reduced-round AES. IACR Transactions on Symmetric Cryptology **2022**(2), 43–62 (2022). https://doi.org/10.46586/tosc.v2022.i2.43-62
6. Bardeh, N.G., Rønjom, S.: The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019, Part III. Lecture Notes in Computer Science, vol. 11923, pp. 347–370. Springer, Cham, Switzerland, Kobe, Japan (Dec 8–12, 2019). https://doi.org/10.1007/978-3-030-34618-8_12
7. Bardeh, N.G., Rønjom, S.: Practical attacks on reduced-round AES. In: Buchmann, J., Nitaj, A., eddine Rachidi, T. (eds.) AFRICACRYPT 19: 11th International Conference on Cryptology in Africa. Lecture Notes in Computer Science, vol. 11627, pp. 297–310. Springer, Cham, Switzerland, Rabat, Morocco (Jul 9–11, 2019). https://doi.org/10.1007/978-3-030-23696-0_15
8. Bariant, A., Leurent, G.: Truncated boomerang attacks and application to AES-based ciphers. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part IV. Lecture Notes in Computer Science, vol. 14007, pp. 3–35. Springer, Cham, Switzerland, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30634-1_1
9. Biham, E., Keller, N.: Cryptanalysis of reduced variants of Rijndael (2000), in third AES Conference
10. Bogdanov, A., Rijmen, V.: Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Designs, Codes and Cryptography **70**, 369–383 (Mar 2014). https://doi.org/10.1007/s10623-012-9697-z
11. Boura, C., Canteaut, A., Coggia, D.: A general proof framework for recent AES distinguishers. IACR Transactions on Symmetric Cryptology **2019**(1), 170–191 (2019). https://doi.org/10.13154/tosc.v2019.i1.170-191
12. Boura, C., David, N., Derbez, P., Leander, G., Naya-Plasencia, M.: Differential meet-in-the-middle cryptanalysis. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023, Part III. Lecture Notes in Computer Science, vol. 14083, pp. 240–272. Springer, Cham, Switzerland, Santa Barbara, CA, USA (Aug 20–24, 2023). https://doi.org/10.1007/978-3-031-38548-3_9
13. Cho, J., Choi, K.Y., Dinur, I., Dunkelman, O., Keller, N., Moon, D., Veidberg, A.: WEM: A new family of white-box block ciphers based on the Even-Mansour construction. In: Handschuh, H. (ed.) Topics in Cryptology – CT-RSA 2017. Lecture Notes in Computer Science, vol. 10159, pp. 293–308. Springer, Cham, Switzerland, San Francisco, CA, USA (Feb 14–17, 2017). https://doi.org/10.1007/978-3-319-52153-4_17
14. Cid, C., Murphy, S., Robshaw, M.J.B.: Small scale variants of the AES. In: Gilbert, H., Handschuh, H. (eds.) Fast Software Encryption – FSE 2005. Lecture Notes in Computer Science, vol. 3557, pp. 145–162. Springer Berlin Heidelberg, Germany, Paris, France (Feb 21–23, 2005). https://doi.org/10.1007/11502760_10
15. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography, Springer (2002). https://doi.org/10.1007/978-3-662-04722-4

16. Daemen, J., Rijmen, V.: New criteria for linear maps in AES-like ciphers. Cryptography and Communications **2009**(1), 47–69 (2009). https://doi.org/10.1007/s12095-008-0003-x
17. Derbez, P., Fouque, P.A., Jean, J.: Improved key recovery attacks on reduced-round AES in the single-key setting. In: Johansson, T., Nguyen, P.Q. (eds.) Advances in Cryptology – EUROCRYPT 2013. Lecture Notes in Computer Science, vol. 7881, pp. 371–387. Springer Berlin Heidelberg, Germany, Athens, Greece (May 26–30, 2013). https://doi.org/10.1007/978-3-642-38348-9_23
18. Dunkelman, O., Ghosh, S., Keller, N., Leurent, G., Marmor, A., Mollimard, V.: Partial sums meet FFT: Improved attack on 6-round AES. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 128–157. Springer, Cham, Switzerland, Zurich, Switzerland (May 26–30, 2024). https://doi.org/10.1007/978-3-031-58716-0_5
19. Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: The retracing boomerang attack. Cryptology ePrint Archive, Report 2019/1154 (2019), https://eprint.iacr.org/2019/1154
20. Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: The retracing boomerang attack. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12105, pp. 280–309. Springer, Cham, Switzerland, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45721-1_11
21. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.: Improved cryptanalysis of Rijndael. In: Schneier, B. (ed.) Fast Software Encryption – FSE 2000. Lecture Notes in Computer Science, vol. 1978, pp. 213–230. Springer Berlin Heidelberg, Germany, New York, NY, USA (Apr 10–12, 2001). https://doi.org/10.1007/3-540-44706-7_15
22. Fouque, P.A., Karpman, P., Kirchner, P., Minaud, B.: Efficient and provable white-box primitives. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology – ASIACRYPT 2016, Part I. Lecture Notes in Computer Science, vol. 10031, pp. 159–188. Springer Berlin Heidelberg, Germany, Hanoi, Vietnam (Dec 4–8, 2016). https://doi.org/10.1007/978-3-662-53887-6_6
23. Grassi, L.: MixColumns properties and attacks on (round-reduced) AES with a single secret S-box. In: Smart, N.P. (ed.) Topics in Cryptology – CT-RSA 2018. Lecture Notes in Computer Science, vol. 10808, pp. 243–263. Springer, Cham, Switzerland, San Francisco, CA, USA (Apr 16–20, 2018). https://doi.org/10.1007/978-3-319-76953-0_13
24. Grassi, L.: Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced AES. IACR Transactions on Symmetric Cryptology **2018**(2), 133–160 (2018). https://doi.org/10.13154/tosc.v2018.i2.133-160
25. Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to AES. IACR Transactions on Symmetric Cryptology **2016**(2), 192–225 (2016). https://doi.org/10.13154/tosc.v2016.i2.192-225, https://tosc.iacr.org/index.php/ToSC/article/view/571
26. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round AES. In: Coron, J.S., Nielsen, J.B. (eds.) Advances in Cryptology – EUROCRYPT 2017, Part II. Lecture Notes in Computer Science, vol. 10211, pp. 289–317. Springer, Cham, Switzerland, Paris, France (Apr 30 – May 4, 2017). https://doi.org/10.1007/978-3-319-56614-6_10
27. Hu, K., Cui, T., Gao, C., Wang, M.: Towards key-dependent integral and impossible differential distinguishers on 5-round AES. In: Cid, C., Jacobson, Jr.,

M.J. (eds.) SAC 2018: 25th Annual International Workshop on Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 11349, pp. 139–162. Springer, Cham, Switzerland, Calgary, AB, Canada (Aug 15–17, 2019). https://doi.org/10.1007/978-3-030-10970-7_7
28. Leurent, G., Pernot, C.: New representations of the AES key schedule. In: Canteaut, A., Standaert, F.X. (eds.) Advances in Cryptology – EUROCRYPT 2021, Part I. Lecture Notes in Computer Science, vol. 12696, pp. 54–84. Springer, Cham, Switzerland, Zagreb, Croatia (Oct 17–21, 2021). https://doi.org/10.1007/978-3-030-77870-5_3
29. Mondal, S.K., Rahman, M., Sarkar, S., Adhikari, A.: Revisiting yoyo tricks on AES. IACR Transactions on Symmetric Cryptology **2023**(4), 28–57 (2023). https://doi.org/10.46586/tosc.v2023.i4.28-57
30. Rønjom, S., Bardeh, N.G., Helleseth, T.: Yoyo tricks with AES. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017, Part I. Lecture Notes in Computer Science, vol. 10624, pp. 217–243. Springer, Cham, Switzerland, Hong Kong, China (Dec 3–7, 2017). https://doi.org/10.1007/978-3-319-70694-8_8
31. Shin, H., Kim, S., Lee, D., Hong, D., Sung, J., Hong, S.: New exchanged boomerang distinguishers for 5-round AES. Cryptology ePrint Archive, Report 2025/248 (2025), https://eprint.iacr.org/2025/248
32. Sun, B., Liu, M., Guo, J., Qu, L., Rijmen, V.: New insights on AES-like SPN ciphers. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016, Part I. Lecture Notes in Computer Science, vol. 9814, pp. 605–624. Springer Berlin Heidelberg, Germany, Santa Barbara, CA, USA (Aug 14–18, 2016). https://doi.org/10.1007/978-3-662-53018-4_22
33. Yan, X., Tan, L., Xu, H., Qi, W.F.: The boomerang chain distinguishers: New record for 6-round AES. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024, Part VII. Lecture Notes in Computer Science, vol. 15490, pp. 301–329. Springer, Singapore, Singapore, Kolkata, India (Dec 9–13, 2024). https://doi.org/10.1007/978-981-96-0941-3_10