Towards Key-Dependent Integral and Impossible Differential Distinguishers on 5-Round AES

Kai Hu[1,3], Tingting Cui[2], Chao Gao[4], and Meiqin Wang[1](✉)

[1] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan 250100, China
hukai@mail.sdu.edu.cn, mqwang@sdu.edu.cn

[2] School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310000, China
cuitingting@hdu.edu.cn

[3] Shandong Computer Science Center (National Supercomputer Center in Jinan),
Jinan 250100, China

[4] Affiliated Hospital of Shandong University of Traditional Chinese Medicine,
Jinan 250100, China
szygaochao@163.com

Abstract. Reduced-round AES has been a popular underlying primitive to design new cryptographic schemes and thus its security including distinguishing properties deserves more attention. At Crypto'16, a key-dependent integral distinguisher on 5-round AES was put forward, which opened up a new direction to take more insights into the distinguishing properties of AES. After that, two key-dependent impossible differential (ID) distinguishers on 5-round AES were proposed at FSE'16 and CT-RSA'18, respectively. It is strange that the current key-dependent integral distinguisher requires significantly higher complexities than the key-dependent ID distinguishers, even though they are constructed with the same property of MixColumns ($2^{128} \gg 2^{98.2}$). Proposers of the 5-round key-dependent distinguishers claimed that the corresponding integral and ID distinguishers can only work under chosen-ciphertext and chosen-plaintext settings, respectively, which is very different from the situations of traditional key-independent distinguishers.

In this paper, we first construct a novel key-dependent integral distinguisher on 5-round AES with 2^{96} chosen plaintexts, which is much better than the previous key-dependent integral distinguisher that requires the full codebook proposed at Crypto'16. Secondly, We show that both distinguishers are valid under either chosen-plaintext setting or chosen-ciphertext setting, which is different from the claims of previous cryptanalysis. However, under different settings, complexities of key-dependent integral distinguishers are very different while those of the key-dependent ID distinguishers are almost the same. We analyze the reasons for it.

Keywords: AES · Key-dependent · Integral · Impossible differential

C. Cid and M. J. Jacobson, Jr. (Eds.): SAC 2018, LNCS 11349, pp. 139–162, 2019.
https://doi.org/10.1007/978-3-030-10970-7_7

1 Introduction

1.1 Background

In symmetric-key cryptanalysis, one usually starts by identifying a distinguisher on the reduced-round target cipher and then proceeds with the key-recovery attack for more rounds. Besides the key recovery, the distinguishing property of some cryptographic schemes itself has been more and more important because many of new ciphers are designed based on well-studied schemes. Among these underlying primitives, reduced-round Advanced Encryption Standard (AES) [4] is a very popular choice. In one hand, the security of reduced-round AES has been analyzed a lot and in the other hand, processor manufactures provided single round instruction for AES, which much encourages researchers to rely on them for new designs. For example, the authentication encryption algorithm AEGIS [14] uses four rounds of AES in the state update functions and ELmd [5] suggests using some reduced-round including 5-round AES. Although the security of these schemes does not completely depend on the basic primitives, it is useful to understand them more deeply by studying the reduced-round AES.

Many distinguishers on reduced-round AES have been proposed and used to evaluate its security for different number of rounds. Traditional distinguishers can only cover four or less rounds [1,2,4,6,8,10]. At Crypto'16, Sun *et al.* proposed the first 5-round zero-correlation (ZC) linear hull and transformed it into a 5-round integral distinguisher. Then, with the statistical integral technique presented at FSE'16 [13], Cui *et al.* gave an attack on 5-round AES [3]. In [7,8], 5-round ID distinguishers were put forward by Grassi *et al.* In all, the 5-round ZC linear hull, integral, statistical integral and ID distinguishers are all key-dependent, which are valid only if the conditions of keys are satisfied. Later, the first key-independent 5-round distinguisher, named multiple-of-n distinguisher, was given in [9]. This distinguisher has a key-dependent variant based on the multiple-of-n property [7]. More recently, an interesting adaptive chosen-plaintext-ciphertext distinguisher Yoyo was proposed to mount a distinguishing attack [11] on reduced-round AES.

This paper focuses on the key-dependent distinguishers on 5-round AES. Key-dependent distinguishers can be regarded as "something in the middle" between secret-key distinguishers and key recovery attacks. Although the complexities of the key-dependent integral and ID distinguishers are higher than that of the multiple-of-n or Yoyo distinguisher, more insights for structural properties of AES such as the details of MixColumns (MC) matrix can be identified, which is based on the fact that all public key-dependent distinguishers on 5-round AES are based on the details of coefficients of this matrix.

Among key-dependent distinguishers on 5-round AES, there is a big gap between the complexities of the integral and ID distinguishers. Even with the same property (Property 1 which we will introduce in Sect. 2.3) of MC matrix, the integral distinguisher requires the whole codebook, while the ID distinguisher just needs $2^{98.2}$ chosen plaintexts. Moreover, it is claimed that the integral distinguisher proceeds only under chosen-ciphertext setting in [12] and the ID distinguishers work only under chosen-plaintext model in [7,8], because these two kinds of distinguishers are based or Property 1 or Property 2 of MC matrix (introduced in Sect. 2) but MC^{-1} matrix does not have such properties.

It is strange that the key-dependent integral and ID distinguishers can work only under specific scenarios, which is a limitation for key-dependent distinguishers. This paper investigates the principles behind the phenomenon and try to remove the limitations. The key-dependent integral distinguisher proposed at Crypto'16 requires the whole codebook and 2^{128} memory accesses. However, a distinguisher that requires the full codebook is usually thought as a trivial attack. Thus, we hope to reduce the complexities of the key-dependent integral distinguisher.

1.2 Contributions

The contributions of this paper are two-fold as follows:

Improved Key-Dependent Integral Distinguisher on 5-Round AES. Key-dependent integral distinguisher on 5-round AES [12] is derived by setting the constraints on the ciphertexts and requires the whole codebook. We construct a new integral distinguisher with only 2^{96} chosen plaintexts. Both our distinguisher and the one in [12] take advantage of the same property of MC matrix. In addition, our distinguisher works under the chosen-plaintext setting instead of the chosen-ciphertext setting. The complexities of chosen-plaintext and chosen-ciphertext key-dependent integral distinguishers are very different. We find that the reason lies on the addition of the last round key. Under chosen-ciphertext setting, we have to guess one byte of key information to achieve the attack while we avoid it under the chosen-plaintext setting.

Key-Dependent ID Distinguishers on 5-Round AES Under Chosen-Ciphertext Setting. We transform the chosen-plaintext key-dependent ID distinguishers into chosen-ciphertext ones, which extends the attacks presented in [7,8]. Both the distinguisher with $2^{98.2}$ chosen plaintexts in [8] and the one with $2^{76.4}$ chosen plaintexts in [7] can be transformed into new ID distinguishers with $2^{99.6}$ and $2^{76.5}$ chosen ciphertexts, respectively. The key-dependent ID distinguishers have slightly different complexities under different attacking scenarios. As the case for integral distinguishers, we analyze the influences of the key addition operation which the key-dependent ID distinguishers depend on.

The complexities of key-dependent integral and ID distinguishers under different models are listed in Table 1.

1.3 Outline of This Paper

In Sect. 2, some preliminaries are given. Then, we present new key-dependent integral distinguishers on 5-round AES in Sect. 3. In Sect. 4, we give the ID distinguishers on 5-round AES under chosen-ciphertext setting. At last, we conclude this paper in Sect. 5.

Table 1. Key-dependent integral and ID distinguishers on 5-round AES.

Distinguisher	Property of MC	Scenario	Data	Time (MA)	Reference
Integral	Property 1	CC	2^{128}	2^{128}	[12]
		CP	$\mathbf{2^{96}}$	$\mathbf{2^{96}}$	Sect. 3
ID	Property 1	CP	$2^{98.2}$	2^{107}	[8]
		CC	$\mathbf{2^{99.6}}$	$\mathbf{2^{103.6}}$	Sect. 4
ID	Property 2	CP	$2^{76.4}$	$2^{81.5}$	[7]
		CC	$\mathbf{2^{76.5}}$	$\mathbf{2^{80.5}}$	Sect. 4

– CP: Chosen-Plaintext CC: Chosen-Ciphertext MA: Memory Access

2 Preliminaries

2.1 Notations

To make the description clear and concise, we list some notations used in this paper as follows.

- P: plaintext;
- C: ciphertext;
- K^r: round key of the r-th round and the whitening key is K^0;
- $X^{r,OP}$: the state after OP operation of the r-th round. e.g. $X^{4,MC}$ is the state after the MixColumns operation of the fourth round function, the state after the whitening key addition is denoted as $X^{0,AK}$;
- $X_{i,j}$, $i, j = 0, 1, 2, 3$: the byte in the i-th row and j-th column of the state X.
- OP_r: the OP operation of the r-th round, AK_0 means the AddRoundKey operation with the whitening key.

2.2 Description of AES

AES [4] is a 128-bit iterative block cipher that adopts substitution-permutation network (SPN). It has three versions according to the size of key, namely AES-128, -192 and -256, respectively, whose total rounds N_r are 10, 12 and 14 individually. The 128-bit internal state of AES can be regarded as a 4×4 matrix, each cell of which is an 8-bit value. All operations in AES are defined in the finite field $GF(2^8)$ whose irreducible polynomial is $m(x) = x^8 + x^4 + x^3 + x + 1$. Each round function $R(x) = AK \circ MC \circ SR \circ SB(x)$ has four components as follows.

- SubBytes (SB): A nonlinear bijective mapping $S : \mathbb{F}_2^8 \rightarrow \mathbb{F}_2^8$ on each byte of the state;
- ShiftRows (SR): Left rotate the i-th row by i bytes, where $i = 0, 1, 2, 3$;
- MixColumns (MC): Left multiply with an MDS matrix over the field $GF(2^8)$ on each column. The matrices used in the MC operation and its reverse operation MC^{-1} are

$$MC = \begin{bmatrix} 0x2 & 0x3 & 0x1 & 0x1 \\ 0x1 & 0x2 & 0x3 & 0x1 \\ 0x1 & 0x1 & 0x2 & 0x3 \\ 0x3 & 0x1 & 0x1 & 0x2 \end{bmatrix} \quad and \quad MC^{-1} = \begin{bmatrix} 0xe & 0xb & 0xd & 0x9 \\ 0x9 & 0xe & 0xb & 0xd \\ 0xd & 0x9 & 0xe & 0xb \\ 0xb & 0xd & 0x9 & 0xe \end{bmatrix};$$

– AddRoundKey (AK): XOR with a round key.

We can change the orders of MC and AK operations in some situations, i.e. $R(x) = MC \circ EAK \circ SR \circ SB(x)$, where $MC \circ EAK = AK \circ MC$. Note that there is a whitening key XORed with plaintext before the first round function and the MC operation in the last round is omitted.

For decryption process, N_r reverse rounds are applied to the ciphertext matrix. Each reverse round function applies four reverse operations: InvSubBytes(SB^{-1}), InvShiftRows(SR^{-1}), InvMixColumns(MC^{-1}) and InvAddRoundKey(AK^{-1}).

2.3 Previous Integral and ID Distinguishers on 5-Round AES

In this subsection, we recall the previous key-dependent integral and ID distinguishers on 5 rounds of AES [7,8,12]. The key techniques for these distinguishers are that they take advantage of the properties of MC matrix and manage to extend the known 4-round distinguishers one more round. We conclude the properties as follows.

Property 1. *The matrix of MC operation has two equal coefficients in each row or each column, i.e., the MC matrix of AES has two elements equal to 1 in each row or each column.*

Property 2. *The matrix of MC operation has two rows satisfying Eq. (1) or two columns satisfying Eq. (2).*

$$\begin{cases} MC[i_1, j] \oplus MC[i_1, k] \oplus MC[i_1, l] = 0, \\ MC[i_2, j] \oplus MC[i_2, k] \oplus MC[i_2, l] = 0. \end{cases} \tag{1}$$

$$\begin{cases} MC[j, i_1] \oplus MC[k, i_1] \oplus MC[l, i_1] = 0, \\ MC[j, i_2] \oplus MC[k, i_2] \oplus MC[l, i_2] = 0. \end{cases} \tag{2}$$

where $i_1 \neq i_2$, $j \neq k \neq l$, $0 \leq i_1, i_2, j, k, l \leq 3$.

Integral Distinguisher on 5-Round AES [12]**.** The 5-round integral distinguisher is transformed from a 5-round ZC linear hull based on Property 1 by setting a specific condition on ciphertexts. The ZC linear hull is illustrated in Proposition 1 and Fig. 4 in Appendix D.

Proposition 1. *Divide the whole ciphertext-plaintext space into* 2^8 *sets according to the value of* $C_{0,0} \oplus C_{1,3}$ *as*

$$V_\Delta = \{(C,P)|C_{0,0} \oplus C_{1,3} = \Delta, \Delta \in \mathbb{F}_2^8\}.$$

If the input mask Γ_{in} *on ciphertext and output mask* Γ_{out} *on plaintext are as follows,*

$$\Gamma_{in} = (\alpha_{i,j}), 0 \leqslant i,j \leqslant 3, \quad \alpha_{i,j} = \begin{cases} a, & \textit{if } (i,j) \in \{(0,0),(1,3)\}; \\ 0, & \textit{otherwise.} \end{cases}$$

$$\Gamma_{out} = (\beta_{i,j}), 0 \leqslant i,j \leqslant 3, \quad \beta_{i,j} = \begin{cases} \textit{nonzero}, & \textit{if } (i,j) = (0,0); \\ 0, & \textit{otherwise.} \end{cases}$$

where $a \in \mathbb{F}_2^8 \backslash \{0\}$.

Then $(\Gamma_{in} \rightarrow \Gamma_{out})$ *is a 5-round ZC linear hull when the ciphertexts are chosen from one specific set of* $V_\Delta, \Delta = K_{0,0}^5 \oplus K_{1,3}^5$.

Bogdanov *et al.* proposed a link between ZC linear hull and integral distinguisher in [2], which is summarized in Theorem 1.

Theorem 1 (From [2]). *Assume* $H : \mathbb{F}_2^s \times \mathbb{F}_2^t \rightarrow \mathbb{F}_2^u \times \mathbb{F}_2^v$ *is (part of) a cipher, without loss of generality, we can decompose the cipher and define the part cipher as*

$$H(x,y) = \begin{pmatrix} H_1(x,y) \\ H_2(x,y) \end{pmatrix}, H_1 : \mathbb{F}_2^s \times \mathbb{F}_2^t \rightarrow \mathbb{F}_2^u, H_2 : \mathbb{F}_2^s \times \mathbb{F}_2^t \rightarrow \mathbb{F}_2^v.$$

If we fix the t *bits of input value as* λ *and consider only* u *bits of the output value, we can construct another function* $T_\lambda(x) : \mathbb{F}_2^s \rightarrow \mathbb{F}_2^u$ *as follows*

$$T_\lambda(x) = H_1(x,\lambda).$$

When the input and output linear masks a *and* b *are independent, the approximation* $b \cdot H(x) \oplus a \cdot x$ *has correlation zero for any* $a = (a_1, 0)$ *and any* $b = (b_1, 0) \neq 0$ *(zero-correlation) if and only if the function* T_λ *is balanced for any* λ *(integral).*

With Theorem 1, one ZC linear hull on 5-round AES can be transformed into an integral distinguisher, which is shown in Proposition 2.

Proposition 2. *Divide the whole ciphertext-plaintext space into* 2^8 *sets*

$$V_\Delta = \{(C,P)|C_{0,0} \oplus C_{1,3} = \Delta, \Delta \in \mathbb{F}_2^8\}.$$

There is always one Δ *such that*

$$T_\Delta = \sum_{(C,P) \in V_\Delta} P = 0.$$

Note that this 5-round integral distinguisher requires the full codebook.

ID Distinguishers on 5-Round AES [7,8]**.** The first ID distinguisher on 5-round AES [8] is similar to the 5-round integral one [12]. It manages to extend the traditional 4-round impossible distinguisher one more round. This 5-round ID (see Fig. 5 in Appendix D) is summarized in Proposition 3.

Proposition 3. *For plaintexts in the sets*

$$V_{\Delta} = \{(P^l, C^l), l = 0, 1, 2, \cdots, 255 | P^l_{0,0} \oplus P^l_{1,1} = \Delta, \quad \forall l \quad \textit{and} \\ P^l_{i,j} = P^m_{i,j} \quad \forall (i,j) \notin \{(0,0), (1,1)\} \quad \textit{and} \quad l \neq m\},$$

there is always one Δ such that the difference of any two corresponding ciphertexts after 5-round AES encryption cannot be inactive in three reverse-diagonals at the same time.

This ID distinguisher requires $2^{98.2}$ chosen plaintexts with success rate 95%.

The second ID distinguisher based on Property 2 was proposed in [7], which requires $2^{76.4}$ chosen plaintexts. It is illustrated in Proposition 4 and shown in Fig. 6 in Appendix D.

Proposition 4. *For plaintexts in the sets*

$$A_{(\Delta_1,\Delta_2)} = \{(P^l, C^l)\, l = 0, 1, \cdots, 255 |\ P^l_{0,0} \oplus P^l_{1,1} = \Delta_1 \quad \forall i, P^l_{0,0} \oplus P^l_{2,2} = \Delta_2 \quad \forall i \\ \textit{and} \quad P^l_{i,j} = P^m_{i,j} \quad \forall (i,j) \notin \{(0,0), (1,1), (2,2)\} \quad \textit{and} \quad l \neq m\}$$

there is always one tuple of (Δ_1, Δ_2) that the difference of ciphertexts after 5-round AES encryption cannot be inactive in two reverse-diagonals in the same time.

This distinguisher requires $2^{76.4}$ chosen plaintexts with success rate 95%.

3 Improved Integral Distinguishers on AES

The 5-round integral distinguisher based on Property 1 proposed in [12] requires the whole codebook, which will limit its contribution. However, we can improve this distinguisher by significantly reducing data and time complexities. In Sect. 3.1, we put forward an improved 5-round integral distinguisher based on Property 1 with 2^{96} chosen plaintexts, which is the longest integral distinguisher on AES as far as we know. In fact, our attack can be regarded as a chosen-plaintext counterpart of the distinguisher in [12]. Interestingly, the data complexities are very different between the two distinguishers. In Sect. 3.2, we discuss the reason why there is such a big gap between the data complexities. Originally, we plan to construct the key-dependent integral distinguisher based on Property 2 which was already used in building the key-dependent ID distinguisher, but we fail to do it. We discuss the reasons for it in Appendix A.

3.1 Improved Key-Dependent Integral Distinguisher on 5-Round AES

The 5-round integral distinguisher in [12] requires the whole codebook while the ID distinguisher in [8] needs only $2^{98.2}$ chosen plaintexts. Both distinguishers use Property 1 of MC matrix. There is a big gap for complexities between them. In this section, we will propose an improved integral distinguisher to eliminate or narrow this gap.

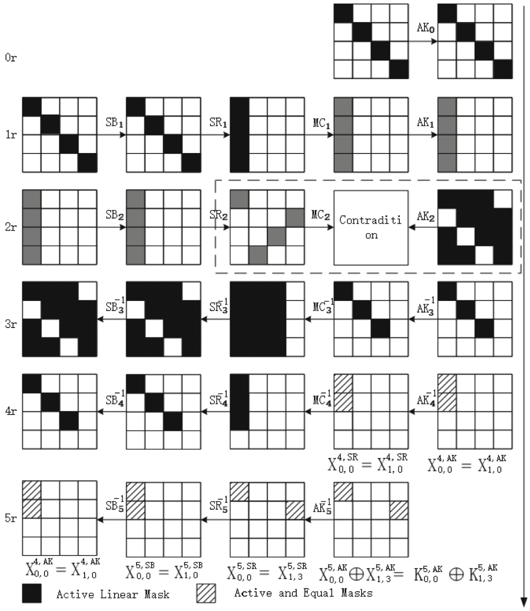

Fig. 1. 5-round ZC linear hull of AES.

In order to improve the 5-round integral distinguisher, we first construct a novel 4-round integral distinguisher on AES summarized in Lemma 1, which is transformed from a 4-round ZC linear hull shown in Fig. 1 (from Round 1 to Round 4), whose input mask Γ_{in} and output mask Γ_{out} are as follows.

$$\Gamma_{in} = (\alpha_{i,j}), 0 \leqslant i,j \leqslant 3, \quad \alpha_{i,j} = \begin{cases} nonzero & \text{if } (i,j) \in \{(0,0),(1,1),(2,2),(3,3)\}, \\ 0 & \text{otherwise} \end{cases}. \tag{3}$$

$$\Gamma_{out} = (\beta_{i,j}), 0 \leqslant i,j \leqslant 3, \quad \beta_{i,j} = \begin{cases} b & \text{if } (i,j) \in \{(0,0),(1,0)\}, \\ 0 & \text{otherwise} \end{cases}, b \in \mathbb{F}_2^8. \tag{4}$$

Lemma 1. *For 4-round AES with MC operation in the last round, if we take all 2^{96} plaintexts P by fixing $(P_{0,0}, P_{1,1}, P_{2,2}, P_{3,3})$ as constant, each value of $C_{0,0} \oplus C_{1,0} \in \mathbb{F}_2^8$ of ciphertexts appears 2^{88} times.*

Proof. As shown in Fig. 1, Γ_{in} and Γ_{out} (Eqs. (3) and (4)) are independent and lead to a ZC linear hull on 4 rounds of AES. According to Theorem 1,

- Γ_{in} can be denoted as $(a, 0)$, where a can be any value in $\mathbb{F}_2^{32}$;
- Γ_{out} can be denoted as $(b, b, 0)$, where b can be any value in $\mathbb{F}_2^8 \backslash \{0\}$.

Since it is required that Γ_{out} should be any value except 0, we proceed with some transformations on the output of 4-round AES in order to satisfy the conditions of Theorem 1.

Firstly, we can rewrite 4-round AES as a function H with two inputs and three outputs:

$$H(x, y) = (H_1(x, y), H_2(x, y), H_3(x, y)).$$

where $x = (P_{0,0}, P_{1,1}, P_{2,2}, P_{3,3})$, y is the concatenated value of other 12 bytes of plaintext, $(H_1(x, y), H_2(x, y)) = (C_{0,0}, C_{1,0})$ and $H_3(x, y)$ is the concatenated value of other 14 bytes.

We can produce a new function H' based on the function H with the same inputs:

$$H'(x, y) = (H_1(x, y) \oplus H_2(x, y), H_3(x, y)).$$

Then for the new function H', we derive that the linear approximation with $\Gamma_{in} = (a, 0)$ and $\Gamma_{out} = (b, 0)$ has correlation zero, where a can be any value in $\mathbb{F}_2^{32}$ and b can be any value in $\mathbb{F}_2^8 \backslash \{0\}$.

With Theorem 1, we can transform the ZC linear approximation on H' into an integral distinguisher, i.e. if we take all 2^{96} plaintexts P by fixing $(P_{0,0}, P_{1,1}, P_{2,2}, P_{3,3})$ as constant, the values of $H_1(x, y) \oplus H_2(x, y)$ are balanced, which means that each value of $C_{0,0} \oplus C_{1,0} \in \mathbb{F}_2^8$ of ciphertexts appears 2^{88} times. □

Based on Lemma 1, we can add one more round behind the 4-round integral distinguisher to deduce a 5-round integral distinguisher by the idea of Lemma 2 as follows.

Lemma 2. *For one-round AES without MC operation (i.e. $AK \circ SR \circ SB$), if we take N plaintexts P where N_1 plaintexts satisfy $P_{0,0} \oplus P_{1,0} = 0$, then there must be at least one $\delta \in \mathbb{F}_2^8$ such that the number of ciphertexts C satisfying $C_{0,0} \oplus C_{1,3} = \delta$ is exactly N_1 with probability 1.*

Proof. Due to the bijective mapping S-box S, we have

$$S(P_{0,0}) \oplus S(P_{1,0}) = \begin{cases} 0, & \text{if } P_{0,0} \oplus P_{1,0} = 0, \\ nonzero, & \text{if } P_{0,0} \oplus P_{1,0} \neq 0. \end{cases}$$

After SB operation, there are exactly N_1 values of $X^{1,SB}$ satisfying $X_{0,0}^{1,SB} \oplus X_{1,0}^{1,SB} = 0$, which leads $C_{0,0} \oplus C_{1,3} = K_{0,0}^1 \oplus K_{1,3}^1$ as well. Let $\delta = K_{0,0}^1 \oplus K_{1,3}^1$, thus $C_{0,0} \oplus C_{1,3} = \delta$ happens exactly N_1 times. □

With Lemmas 1 and 2, our new 5-round integral distinguisher on AES is summarized in Proposition 5.

Proposition 5. *Taking all 2^{96} plaintexts P by fixing $(P_{0,0}, P_{1,1}, P_{2,2}, P_{3,3})$ as constant, after 5-round AES encryption, there is at least one $\delta \in \mathbb{F}_2^8$ such that the number of ciphertexts satisfying $C_{0,0} \oplus C_{1,3} = \delta$ is exactly 2^{88}. Meanwhile, for any random permutation, the same event happens with probability only about $2^{-40.7}$.*

Proof. For 5-round AES, $X_{0,0}^{4,AK} \oplus X_{1,0}^{4,AK} = 0$ happens 2^{88} (out of 2^{96}) times according to Lemma 1. Then due to Lemma 2, $N = 2^{96}$ and $N_1 = 2^{88}$, so there is one δ such that $C_{0,0} \oplus C_{1,3} = \delta$ happens exactly 2^{88} times.

For a random permutation, the number N_δ of ciphertexts satisfying $C_{0,0} \oplus C_{1,3} = \delta$ for a fixed δ follows the binomial distribution

$$N_\delta \sim \mathcal{B}(2^{96}, 2^{-8}).$$

According to the Central Limit Theorem, the normal distribution can approximate the binomial distribution in this situation. Now

$$N_\delta \sim \mathcal{N}(2^{88}, 2^{96} \times 2^{-8} \times (1 - 2^{-8})).$$

Therefore, $p(N_\delta = 2^{88}) \approx 2^{-48.64}$. Because of 2^8 possible values for δ, the probability that there is at least one value for δ satisfying $N_\delta = 2^{88}$ is $1 - (1 - p(N_\delta = 2^{88}))^{2^8} \approx 2^{-40.7}$. □

The whole process of the integral distinguishing attack on 5-round AES is illustrated in Algorithm 1.

Algorithm 1. Improved 5-Round Integral Distinguisher on AES

```
Input: $2^{96}$ plaintexts $P^i$, $i = 0, 1, 2, \ldots, 2^{96} - 1$
Output: 5-Round AES or Random Permutation
Set one 8-bit vector counter $V[256]$ and initialize it as zero;
for Each $P^i$ of $2^{96}$ plaintexts do
    Query its ciphertext $C^i$ and calculate $\delta = C_{0,0}^i \oplus C_{1,3}^i$;
    Let $V[\delta] = V[\delta] + 1$;
for Each $\delta \in \mathbb{F}_2^8$ do
    if $V[\delta] = 2^{88}$ then
        return 5-Round AES;
return Random Permutation;
```

In Algorithm 1, the data complexity is 2^{96} chosen plaintexts and the time complexity is about 2^{96} memory accesses. Since we set a 2^8 vector counter, the memory requirements are 2^8 which can be ignored. The type-II error probability (the probability to wrongfully accept a random permutation as AES) is $2^{-40.7}$.

3.2 Gap for Complexities Between Chosen-Plaintext and Chosen-Ciphertext Integral Distinguishers

Interestingly, there exists a gap between the complexities of chosen-plaintext and chosen-ciphertext integral distinguishers although they are constructed from a same (or similar) ZC linear hull.

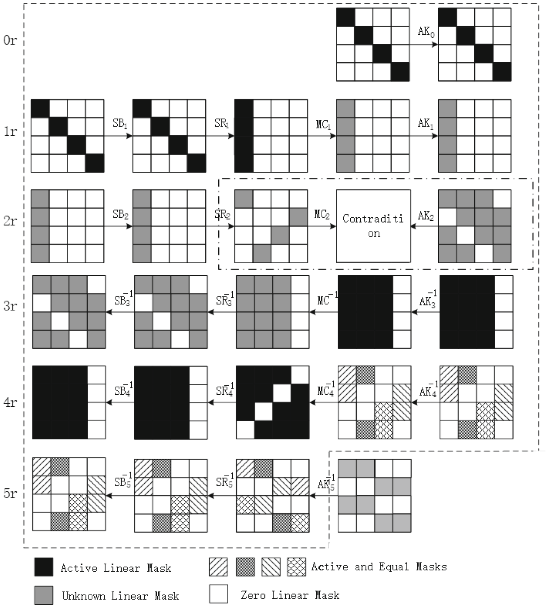

Fig. 2. 5-round integral distinguisher with(out) AK_5.

In the chosen-ciphertext integral distinguisher, we need to guess one byte of $K^5_{0,0} \oplus K^5_{1,3}$, which increases the complexities by a factor of 2^8. This inspires us that the AK operation which the integral distinguisher depends on, i.e. AK_5, influences the complexities. In this subsection, we investigate the influences of AK_5 on complexities by considering chosen-ciphertext and chosen-plaintext integral distinguishers on 5-round AES with and without AK_5, respectively. Notice that we use a general variant of the key-dependent integral distinguisher with four active masks on plaintext bytes (see Fig. 2).

Under Chosen-Ciphertext Setting. If we omit the operation AK_5 (the enclosure area by dotted line in Fig. 2) and decrypt from $X^{5,SR}$ in subspace $V_{X^{5,SR}}$ as follows to the plaintext P

$$V_{X^{5,SR}} = \{(X^{5,SR}, P) \mid X^{5,SR}_{0,0} = X^{5,SR}_{1,3}, X^{5,SR}_{0,1} = X^{5,SR}_{3,2}, X^{5,SR}_{2,0} = X^{5,SR}_{3,3}, \\ X^{5,SR}_{1,2} = X^{5,SR}_{2,1}, X^{5,SR}_{i,j} \in \mathbb{F}^8_2, 0 \leqslant i, j \leqslant 3\},$$

we can construct a chosen-ciphertext integral distinguisher whose corresponding plaintexts satisfy the balance property, i.e. each possible value of plaintext byte has the same number of occurrences. Since the size of $V_{X^{5,SR}}$ is 2^{96}, this integral distinguisher requires data complexity 2^{96} chosen ciphertexts.

If the operation AK_5 is included into the distinguisher (whole area in Fig. 2), we have to take a subspace of ciphertexts V_C which can produce $V_{X^{5,SR}}$ after the proceeding with the AK_5^{-1}. Thus the set V_C must be

$$V_C = \{(C,P) \mid C_{0,0} \oplus C_{1,3} = K^5_{0,0} \oplus K^5_{1,3}, C_{0,1} \oplus C_{3,2} = K^5_{0,1} \oplus K^5_{3,2},$$
$$C_{2,0} \oplus C_{3,3} = K^5_{2,0} \oplus K^5_{3,3}, C_{1,2} \oplus C_{2,1} = K^5_{1,2} \oplus K^5_{2,1}, C_{i,j} \in \mathbb{F}_2^8, 0 \leqslant i,j \leqslant 3\}.$$

However, the exact values of $K^5_{0,0} \oplus K^5_{1,3}$, $K^5_{0,1} \oplus K^5_{3,2}$, $K^5_{2,0} \oplus K^5_{3,3}$ and $K^5_{1,2} \oplus K^5_{2,1}$ are unknown, so we have to take the whole space of (C,P) and divide it into 2^{32} subspaces as follows:

$$V_{\Delta_0,\Delta_1,\Delta_2,\Delta_3} = \{(C,P) \mid C_{0,0} \oplus C_{1,3} = \Delta_0, C_{0,1} \oplus C_{3,2} = \Delta_1, C_{2,0} \oplus C_{3,3} = \Delta_2,$$
$$C_{1,2} \oplus C_{2,1} = \Delta_3, C_{i,j} \in \mathbb{F}_2^8, 0 \leqslant i,j \leqslant 3\},$$

with $\Delta_i \in \mathbb{F}_2^8, 0 \leqslant i \leqslant 3$.

There is always one tuple of $(\Delta_0, \Delta_1, \Delta_2, \Delta_3)$ equal to $(K^5_{0,0} \oplus K^5_{1,3}, K^5_{0,1} \oplus K^5_{3,2}, K^5_{2,0} \oplus K^5_{3,3}, K^5_{1,2} \oplus K^5_{2,1})$ and thus the data complexity becomes 2^{128} instead of 2^{96} chosen ciphertexts.

Under Chosen-Plaintext Setting. If we exclude AK_5 operation from 5-round AES and encrypt all 2^{96} possible plaintexts P to $X^{5,SR}$ by fixing $(P_{0,0}, P_{1,1}, P_{2,2}, P_{3,3})$ as constant. From Sect. 3.1, each of the following four events

1. $X^{5,SR}_{0,0} \oplus X^{5,SR}_{1,3} = 0$, 2. $X^{5,SR}_{0,1} \oplus X^{5,SR}_{3,2} = 0$,
3. $X^{5,SR}_{2,0} \oplus X^{5,SR}_{3,3} = 0$, 4. $X^{5,SR}_{1,2} \oplus X^{5,SR}_{2,1} = 0$,

occurs 2^{88} times with probability 1. We can distinguish AES from a random permutation with 2^{96} chosen plaintexts.

Again we take AK_5 operation into consideration, each of four events

1. $C_{0,0} \oplus C_{1,3} = K^5_{0,0} \oplus K^5_{1,3}$, 2. $C_{0,1} \oplus C_{3,2} = K^5_{0,1} \oplus K^5_{3,2}$,
3. $C_{2,0} \oplus C_{3,3} = K^5_{2,0} \oplus K^5_{3,3}$, 4. $C_{1,2} \oplus C_{2,1} = K^5_{1,2} \oplus K^5_{2,1}$,

occurs 2^{88} times with probability 1, respectively.

Though we do not know any information about the secret key, we can predict there is always one tuple of $(\Delta'_0, \Delta'_1, \Delta'_2, \Delta'_3)$ ensuring each of the four experiences

1. $C_{0,0} \oplus C_{1,3} = \Delta'_0$, 2. $C_{0,1} \oplus C_{3,2} = \Delta'_1$,
3. $C_{2,0} \oplus C_{3,3} = \Delta'_2$, 4. $C_{1,2} \oplus C_{2,1} = \Delta'_3$,

to occur 2^{88} times (when $(\Delta'_0, \Delta'_1, \Delta'_2, \Delta'_3)$ are just the four XOR values of K_5). Yet any one event occurs with probability about $2^{-40.7}$ for a random permutation. So 2^{96} chosen plaintexts are enough to proceed this distinguishing attack.

At last, we summarize the reasons resulting in the gap from two cases between chosen-plaintext and chosen-ciphertext integral distinguishers. If AK_5 is omitted, the data complexities of the two distinguishers under both settings are the same. If AK_5 is included, the chosen-ciphertext integral distinguisher has to take the whole codebook while the chosen-plaintext integral distinguisher does not increase the data complexity. To make it more clear, we compare the data complexities of them in Table 2.

Table 2. Data complexities of integral distinguishers with(out) AK_5.

Setting	Target	Data complexity	Time (MA)
CC	5-round AES without AK_5	2^{96}	2^{96}
	5-round AES with AK_5	2^{128}	2^{128}
CP	5-round AES without AK_5	2^{96}	2^{96}
	5-round AES with AK_5	2^{96}	2^{96}

– CC: Chosen-Ciphertext CP: Chosen-Plaintext MA: Memory Access

4 ID Distinguishers on 5-Round AES Under Chosen-Ciphertext Setting

Until now there have been two key-dependent ID distinguishers on 5-round AES in [7,8] by utilizing the Property 1 and 2 of MC matrix respectively. In this section we put forward two ID distinguishers on 5-round AES under chosen-ciphertext model in Sects. 4.1 and 4.2 respectively, which are transformed from the ones under chosen-plaintext setting. Their data complexities are $2^{99.6}$ and $2^{76.5}$ chosen ciphertexts, which are slightly different from those of the original ones with $2^{98.2}$ and $2^{76.4}$ chosen plaintexts, respectively. We analyze the reasons in Appendix C.

4.1 ID Distinguisher on 5-Round AES Based on Property 1 of MC

In this subsection, we first propose 16 key-dependent IDs for 5-round AES shown in Proposition 6 and we list one of them in Fig. 5. With these IDs, a distinguisher under chosen-ciphertext model is put forward with data complexity $2^{99.6}$ chosen ciphertexts.

Proposition 6. *If the difference of ciphertext pair (C^1, C^2) is nonzero at the four bytes $(C_{0,3}, C_{1,2}, C_{2,1}, C_{3,0})$ and zero at other 12 bytes, after 5-round AES decryption, the corresponding plaintext pair (P^1, P^2) never satisfies each of the following 16 cases:*

$$P^1_{s,t} \oplus P^1_{s+1,t+1} = P^2_{s,t} \oplus P^2_{s+1,t+1} = K^0_{s,t} \oplus K^0_{s+1,t+1},$$
$$P^1_{l,m} \oplus P^2_{l,m} = 0, (l,m) \neq (s,t), (s+1,t+1),$$

where $0 \leqslant s,t \leqslant 3$.[1]

Proof. Proof by contradiction. Assume that there is one ciphertext pair (C^1, C^2) leading to such plaintext pair (P^1, P^2). From the forward direction, since there exists one (s,t) such that (P^1, P^2) satisfies $P^1_{s,t} \oplus P^1_{s+1,t+1} = P^2_{s,t} \oplus P^2_{s+1,t+1} = K^0_{s,t} \oplus K^0_{s+1,t+1}$, we have $\Delta X^{1,SB}_{s,t} = \Delta X^{1,SB}_{s+1,t+1}$. Due to the Property 1 of MC matrix, there are only three nonzero bytes of difference $\Delta X^{1,MC}$ in one column, which leads to at least one zero byte on each column of $\Delta X^{3,SR}$. From the backward direction, (C^1, C^2) results in at most one nonzero byte for each column of $\Delta X^{3,MC}$. Since the branch number of MC matrix is 5, each column of $\Delta X^{3,MC}$ has at least two zero bytes. This yields a contradiction and shows that they are IDs. □

Taking $(s,t) = (0,0)$ as an example, we illustrate Proposition 6 in Fig. 5. Actually, the value of $K^0_{s,t} \oplus K^0_{s+1,t+1}$ is secret, so we cannot directly check whether $P^1_{s,t} \oplus P^1_{s+1,t+1} = P^2_{s,t} \oplus P^2_{s+1,t+1} = K^0_{s,t} \oplus \ K^0_{s+1,t+1}$ or not. In the following, we will define good pair to further identify if there exist solutions for $K^0_{s,t} \oplus K^0_{s+1,t+1}$ by using the ID characteristic.

Definition 1 (Good Pair). *One pair* (P^1, P^2) *is a good pair related to* (s,t) *if it satisfies the following conditions:*

$$P^1_{s,t} \oplus P^1_{s+1,t+1} = P^2_{s,t} \oplus P^2_{s+1,t+1},$$
$$P^1_{l,m} \oplus P^2_{l,m} = 0, (l,m) \neq (s,t), (s+1,t+1),$$

where (s,t), $0 \leqslant s,t \leqslant 3$.

No matter how many ciphertext pairs as the form in Proposition 6 we take, for each (s,t) there always exists one value $\delta_{s,t} \in \mathbb{F}_2^8$ that $P^1_{s,t} \oplus P^1_{s+1,t+1} = P^2_{s,t} \oplus P^2_{s+1,t+1} = \delta_{s,t} = K^0_{s,t} \oplus \ K^0_{s+1,t+1}$ never happens for each good pair.

According to the fact above, we put forward an ID distinguishing attack on 5-round AES under chosen-ciphertext model, see Algorithm 2. For each of 16 (s,t), $0 \leq s,t, \leq 3$, we take N_s structures of ciphertexts that each one includes 2^{32} ciphertexts by traversing all values of bytes $(C_{0,3}, C_{1,2}, C_{2,1}, C_{3,0})$ and fixing other bytes as constant, to find all good pairs and record their $P^1_{s,t} \oplus P^1_{s+1,t+1}$ in a vector counter $V_{s,t}$. For 5-round AES, there is always a value δ_{st} never happening in $V_{s,t}$ for each (s,t). The probability that there is always a value $\delta_{s,t}$ never happening in $V_{s,t}$ for each (s,t) for a random permutation is calculated in Proposition 7.

Proposition 7. *For a random permutation, for each of 16* (s,t), $0 \leq s,t \leq 3$, *the probability that there always exists at least one value* $\delta_{s,t} = P^1_{s,t} \oplus P^1_{s+1,t+1}$ *never appearing for any one of* N *random good pairs is* $2^{128} \times (1 - 2^{-8})^{16N}$.

[1] The addition used in subscripts of the equations are actually addition modulo 4. For example, when $t = 3$, $t + 1 = 0$.

Proof. For a random permutation and any given value of (s, t), the event that there is at least one value for $\delta_{s,t} = P^1_{s,t} \oplus P^1_{s+1,t+1}$ never occurring for any one of N random good pairs happens with the following probability

$$p_{s,t} = 2^8 \times (1 - 2^{-8})^N,$$

then the probability that this event happens for all 16 values of (s, t) is $p^{16}_{s,t} = 2^{128} \times (1 - 2^{-8})^{16N}$. □

Algorithm 2. 5-Round ID Distinguisher under Chosen-Ciphertext Model Based on Property 1

```
   Input: $N_s$ structures of ciphertexts and corresponding plaintexts
   Output: 5-Round AES or Random Permutation
1  for Each $s \in \{0,1,2,3\}$ do
2      for Each $t \in \{0,1,2,3\}$ do
3          Initialize 256 indicators $V[256]$ as false;
4          for Each one of $N_s$ structures do
               // Each structure includes $2^{32}$ ciphertexts.
5              Initialize a table $T[2^{32}]$;
6              Query the corresponding $2^{32}$ plaintexts and put them into $T$;
7              Sort $T$ according to the value of 14 bytes except the $(s,t)$-th and
               $(s+1,t+1)$-th bytes;
8              Traverse all items of $T$ and find adjacent plaintexts to combine good
               pairs;
               // About $N = N_s \times 2^{63} \times 2^{-120}$ good pairs are found.
9              for Each $(P^1, P^2)$ of $N$ good pairs do
10                 Let $V[P^1_{s,t} \oplus P^1_{s+1,t+1}]$ = true;
11         if all 256 indicators are true then
12             return Random Permutation;
13 return 5-Round AES;
```

By setting the type-II error probability as 5%, it means that the success rate is 95%, then, $N \approx 2^{10.6}$ good pairs are required for each $(s, t), 0 \leq s, t \leq 3$. Since the probability to find a good pair from random ones is 2^{-120}, we have $N_s = 2^{67.6}$ by using $N_s \times 2^{63} \times 2^{-120} = N$. As a result, the data complexity is $2^{99.6}$ chosen ciphertexts. From Algorithm 2, Step 6 needs $16 \times N_s \times 2^{32} = 2^{103.6}$ memory accesses. Since the time to sort a table of size 2^n is $O(2^n log(2^n))$, Step 7 needs about $16 \times N_s 2^{32} log(2^{32})$. Then the time complexities of Step 8 and Steps 9–10 are $16 \times N_s \times 2^{32} = 2^{103.6}$ and $16 \times N_s \times N = 2^{82.2}$ memory accesses, respectively. Totally, the time complexity is about $2^{103.6}$ memory accesses. The memory requirements are 2^{32} to construct table T.

4.2 ID Distinguisher on 5-Round AES Based on Property 2 of MC

Similar to the method of constructing ID distinguisher on 5-round AES under chosen-ciphertext model in Sect. 4.1, we also can get an ID distinguisher under chosen-ciphertext model by using Property 2 of MC matrix transformed from the distinguisher in [7], see Proposition 8.

Proposition 8. *If the difference of ciphertext pair (C^1, C^2) is nonzero at the eight bytes $(C_{0,3}, C_{1,2}, C_{2,1}, C_{3,0}, C_{0,2}, C_{1,2}, C_{2,0}, C_{3,3})$ and zero at other 8 bytes, after 5-round AES decryption, the corresponding plaintext pair (P^1, P^2) never satisfies any one of the following 16 cases:*

$$\begin{aligned}&P^1_{s,t} \oplus P^1_{s+1,t+1} = P^2_{s,t} \oplus P^2_{s+1,t+1} = K^0_{s,t} \oplus K^0_{s+1,t+1},\\&P^1_{s,t} \oplus P^1_{s+2,t+2} = P^2_{s,t} \oplus P^2_{s+2,t+2} = K^0_{s,t} \oplus K^0_{s+2,t+2},\\&P^1_{l,m} \oplus P^2_{l,m} = 0, (l,m) \neq (s,t), (s+1,t+1), (s+2,t+2),\end{aligned}$$

where $0 \leqslant s, t \leqslant 3$.

However, for a random permutation, under each (s,t), the probability that there always exists a tuple $(\delta^1_{s,t}, \delta^2_{s,t})$ that $\delta^1_{s,t} = P^1_{s,t} \oplus P^1_{s+1,t+1}$ and $\delta^2_{s,t} = P^1_{s,t} \oplus P^1_{s+2,t+2}$ never appearing for any one of N random good pairs is $2^{256} \times (1 - 2^{-16})^{16N}$.

We omit the proof here due to its similarity to the distinguisher in Sect. 4.1. The distinguisher is illustrated in Algorithm 3 which is in Appendix B. The data and time complexities are $2^{76.5}$ chosen-ciphertexts and $2^{80.5}$ memory accesses, respectively. The type-II error probability is 5%.

5 Conclusions

In this paper, we study key-dependent integral and ID distinguishers on 5-round AES. A new key-dependent integral distinguisher is constructed with 2^{96} chosen plaintexts, which is more efficient than the previous one that requires the full codebook. Under different settings, the complexities of key-dependent integral distinguishers have a significant gap while those of the key-dependent ID distinguishers are almost the same. We analyze the principles behind the phenomena. If the AK operation which the key-dependent distinguishers depend on is positioned in the end of the distinguishers, the data complexities of integral and ID distinguishers will be almost unchanged no matter whether we consider or not the AK operations. Otherwise, the data complexities will increase significantly when we contain the AK operations in 5-round AES.

Acknowledgement. The authors thank the anonymous SAC 2018 reviewers for careful reading and many helpful comments. This work is supported by National Natural Science Foundation of China (Grant No. 61572293), Key Science Technology Project of Shandong Province (Grant No. 2015GGX101046), and Chinese Major Program of National Cryptography Development Foundation (Grant No. MMJJ2017012).

A Property 2 and Key-Dependent Integral Distinguisher

In [7], Grassi *et al.* took advantage of Property 2 to build a more efficient ID distinguisher requiring $2^{76.4}$ chosen plaintexts. A question arises: Can we build an integral distinguisher based on Property 2?

Recall the key-dependent ID distinguisher based on Property 2, once the differences of $X_{0,0}^{1,SR}$, $X_{1,0}^{1,SR}$ and $X_{2,0}^{1,SR}$ are identical, differences on $X_{0,0}^{1,MC}$ and $X_{1,0}^{1,MC}$ will be zero with probability 1 (As described in Sect. 2.3). Therefore, in order to construct a key-dependent integral distinguisher with the similar technique we have to enforce the mask on $X^{4,MC}$ to statisfy following condition:

$$\begin{aligned} &\Gamma_{X^{4,MC}} = \Gamma_{X^{4,AK}} = \beta_{i,j}, 0 \leqslant i,j \leqslant 3, \\ &\beta_{i,j} \begin{cases} b \in F_2^8 \backslash \{0\} & \text{if}(i,j) = \in \{(0,0),(1,0),(2,0)\}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

For the purpose of extending the ZC linear hull one more round, we should carefully select the masks of $\Gamma_{X^{5,SB}}$ and make sure the correlation of $\Gamma_{X^{5,SB}} \rightarrow \Gamma_{X^{4,AK}}$ is 1, i.e. the equation

$$b \cdot (X_{0,0}^{4,AK} \oplus X_{0,0}^{4,AK} \oplus X_{0,0}^{4,AK}) = \Gamma_{X^{5,SB}} \cdot X^{5,SB}$$

always holds for any $X^{5,SB}$. Unfortunately, we cannot find any set of $X^{5,SB}$ or value of $\Gamma_{5,SB}$ to ensure it because of the non-linear property of SB.

B Algorithm of 5-Round ID Distinguisher Under Chosen-Ciphertext Model Based on Property 2

The Algorithm 3 shows the process that we transfer the chosen-plaintext ID distinguisher based on Property 2 into a chosen-ciphertext one.

C Gap Between Complexities of Chosen-Plaintext and Chosen-Ciphertext ID Distinguishers

Although the key-dependent integral distinguishers on 5-round AES have different data complexities under chosen-plaintext and chosen-ciphertext models, the complexity of key-dependent chosen-ciphertext ID distinguisher is slightly different from that of the chosen-plaintext one.

Similar to the key-dependent integral distinguishers, we will consider the influences of AK_0 operation, which the key-dependent ID distinguishers depend on. In this subsection, we only take the key-dependent ID distinguisher based on Property 1 for example. Situations are similar for the distinguihser based on Property 2. Notice that here we use a general ID characteristic with more active plaintext bytes (see Fig. 3) to make our analysis more convincing.

Algorithm 3. 5-Round ID Distinguisher under Chosen-Ciphertext Model Based on Property 2

```
Input: $N_s$ structures of ciphertexts and corresponding plaintexts
Output: 5-Round AES or Random Permutation
for Each $s \in \{0,1,2,3\}$ do
    for Each $t \in \{0,1,2,3\}$ do
        Initialize $2^{16}$ indicators $V[2^{16}]$ as false;
        for Each one of $N_s$ structures do
            // Each structure includes $2^{64}$ ciphertexts.
            Initialize a table $T[2^{64}]$;
            Query the corresponding $2^{64}$ plaintexts and put them into $T$ ;
            Sort $T$ according to the value of 13 bytes except bytes $(s,t)$ and
              $(s+1,t+1)$ and $(s+2,s+2)$;
            Traverse all items of $T$ and find adjacent plaintexts to combine find
              good pairs;
            // About $N = N_s \times 2^{127} \times 2^{-120}$ good pairs are found.
            for Each $(P^1, P^2)$ of $N$ good pairs do
                Let $V[P^1_{s,t} \oplus P^1_{s+1,t+1}]$ = true;
        if all $2^{16}$ indicators are true then
            return Random Permutation;
return 5-Round AES;
```

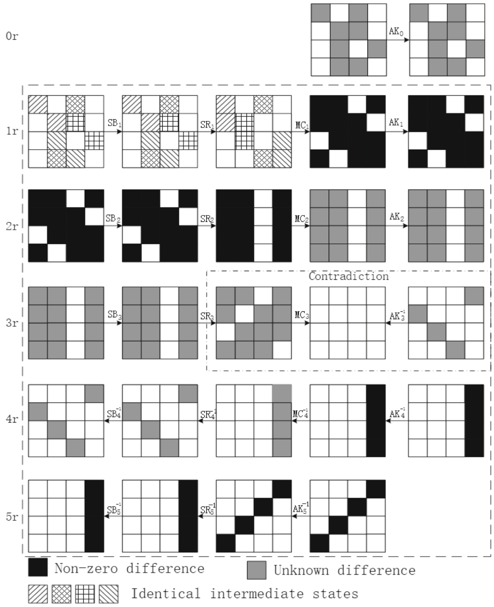

Fig. 3. 5-round impossible distinguisher with(out) AK_5.

Under Chosen-Plaintext Setting. If AK_0 operation is excluded from the 5-round AES (the enclosure area by dotted line in Fig. 3), we encrypt a pair of $(X^{0,AK}, \bar{X}^{0,AK})$ satisfying

- *Condition 1*:

$$\hat{X}^{0,AK}_{0,0} = \hat{X}^{0,AK}_{1,1}, \hat{X}^{0,AK}_{1,2} = \hat{X}^{0,AK}_{2,3},$$
$$\hat{X}^{0,AK}_{0,2} = \hat{X}^{0,AK}_{3,1}, \hat{X}^{0,AK}_{0,3} = \hat{X}^{0,AK}_{3,2},$$

  where $\hat{X}$ represents X or $\bar{X}$;
- *Condition 2*:

$$X^{0,AK}_{j,k} = \bar{X}^{0,AK}_{j,k},$$

  where $(j,k) \neq (0,0),(1,1),(1,2),(2,3),(0,2),(3,1),(0,3),(3,2),$

It is impossible that the corresponding ciphertext pair of $(C, \bar{C})$ has the active differences in only one reverse-diagonal. Yet for a random permutation, such pair appears with probability $4 \times 2^{-96} = 2^{-94}$. Given 2^{N_1} pairs of $(X^{0,AK}, \bar{X}^{0,AK})$, the probability p_1 that we identify a random permutation as 5-round AES without AK_0 is

$$p_1 = 1 - (1 - 2^{-94})^{2^{N_1}} = 1 - e^{-2^{N_1 - 94}}.$$

If we set $p_1 \geqslant 95\%$, then $N_1 \geqslant 95.6$.

All the $X^{0,AK}$ satisfying *Condition 1* and *2* compose a structure whose size is 2^{32}. Each structure can produce 2^{63} pairs. To construct $2^{95.6}$ pairs, we need to take $2^{95.6-63}$ different structures. Therefore, the total data complexity is $2^{95.6-63+32} = 2^{64.6}$ chosen plaintexts. To check the specific ciphertext pairs, we insert each ciphertext into a hash table indexed by four bytes in one diagonal and test whether there are two different ciphertexts in the same row of the hash table. Therefore, the time complexity of this attack is $2^{64.6}$ memory accesses.

If the AK_0 operation is taken into consideration, we will encrypt a pair of plaintexts $(P, \bar{P})$ and expect that the difference of corresponding $(C, \bar{C})$ would never be active in only one reverse-diagonal. To ensure it, $(P, \bar{P})$ should satisfy Eqs. (5) and (6):

$$\begin{aligned} \hat{P}_{0,0} \oplus \hat{P}_{1,1} = K^0_{0,0} \oplus K^0_{1,1}, \hat{P}_{1,2} \oplus \hat{P}_{2,3} = K^0_{1,2} \oplus K^0_{2,3}, \\ \hat{P}_{0,2} \oplus \hat{P}_{3,1} = K^0_{0,2} \oplus K^0_{3,1}, \hat{P}_{0,3} \oplus \hat{P}_{3,2} = K^0_{0,3} \oplus K^0_{3,2}, \end{aligned} \tag{5}$$

where $\hat{P}$ represents P or $\bar{P}$.

$$P^1_{j,k} = P^2_{j,k}, (j,k) \neq (0,0),(1,1),(1,2),(2,3),(0,2),(3,1),(0,3),(3,2). \tag{6}$$

However, the XOR values of K^0 involved in Eq. (5) are unknown. We traverse 2^{32} possible values to ensure that the right XOR values of key are contained. For each XOR value in our traversing process, we fix other eight bytes of plaintexts involved in Eq. (6) as constant. Then we get 2^{32} structures of plaintexts.

For 5-round AES, structures with the right XOR values, i.e. the four XOR values are equal to the XOR values of a key described in Eq. (5), will never produce ciphertext pairs which have active differences in only one reverse-diagonal, but the structures with the wrong XOR values will do. However, for a random permutation, there will be at least one pair of ciphertexts with active bytes in only one diagonal if we take enough structures for each of 2^{32} XOR values.

The key point of the distinguisher is that we take enough pairs and make sure that we can get ciphertext pairs with active bytes in only one diagonal for each XOR value, if the target is a random permutation. If the probability that we get such a pair for one XOR value is p_1', the probability that we get such pairs for all the 2^{32} XOR values is $(p_1')^{2^{-32}}$.

If we set the probability that we can identify a random permutation as a random permutation at least 95%, we get $p_1' \geqslant (0.95)^{2^{-32}}$.

Given $2^{N_1'}$ pairs from structures one certain XOR value, p_1' can be calculated as follows

$$p_1' = 1 - (1 - 2^{-94})^{2^{N_1'}} = 1 - e^{-2^{N_1'-94}}.$$

Since $p_1' \geqslant (95\%)^{2^{-32}}$, we get $N_1' \geqslant 98.7$.

One structure produces 2^{63} pairs, so we need $2^{98.7-63} = 2^{35.7}$ structures, i.e. $2^{35.7+32} = 2^{67.7}$ chosen plaintexts for each XOR values. We have 2^{32} possible XOR values, so the total complexity is $2^{67.7+32} = 2^{99.7}$ chosen plaintexts. For each XOR value, we encrypt plaintexts and insert the corresponding ciphertexts into a hash table indexed by the four bytes in one diagonal and then check whether there are two ciphertexts in the same row of the hash table. Thus the time complexity is $2^{99.7}$ memory accesses.

Under Chosen-Ciphertext Setting. If AK_0 operation is excluded and we decrypt a pair of ciphertexts $(C, \bar{C})$ with active bytes in only one diagonal to $(X^{0,AK}, \bar{X}^{0,AK})$. For 5-round AES without AK_0, the pair $(X^{0,AK}, \bar{X}^{0,AK})$ will never satisfy *Condition 1* and *2* at the same time while for a random permutation, such pair appears with probability 2^{-128} (2^{-64} for the probability to satisfy *Condition 1* and 2^{-64} for *Condition 2*).

In order to distinguish 5-round AES without AK_0 from a random permutation, we use 2^{N_2} ciphertext pairs, thus the probability p_2 that there will be at least a pair of $(X^{0,AK}, \bar{X}^{0,AK})$ satisfying *Condition 1* and *2* for a random permutation is:

$$p_2 = 1 - (1 - 2^{-94})^{2^{N_2}} = 1 - e^{-2^{N_2-94}}.$$

Setting $p_2 \geqslant 95\%$ we will get $N_2 \geqslant 129.6$.

We fix 12 bytes of three diagonals as constants and take all possible values for other four bytes to compose a structure. Each structure provides 2^{63} pairs with 2^{32} ciphertexts. Thus we need $2^{129.6-63} = 2^{66.6}$ structures and the total data complexity is $2^{66.6+32} = 2^{98.6}$. We decrypt ciphertexts and insert the $X^{0,AK}$

satisfying *Condition 1* into a hash table indexed by eight bytes involved in *Condition 2* and then check whether there are two texts in the same row of the hash table. Thus the time complexity is $2^{98.6}$ memory access.

If AK_0 operation is contained and we decrypt a pair of ciphertexts $(C, \bar{C})$ with active differences in only one diagonal to get corresponding plaintext pair $(P, \bar{P})$, the intermediate state $(X^{0,AK}, \bar{X}^{0,AK})$ will never satisfy *Condition 1* and *2*, thus $(P, \bar{P})$ cannot satisfy Eqs. (5) and (6), neither.

Since we do not know the key information involved in the Eq. (5), we have to collect good pairs and test whether each possible XOR value will occur as described in Sect. 4.1. Given $2^{N_2'}$ ciphertext pairs, we expect to collect $2^{N_2'-96}$ good pairs. The probability p_2' that all the possible XOR values will occur is

$$p_2' = 1 - 2^{32} \times (1 - 2^{-32})^{2^{N_2'-96}}$$

Setting $p_2' \geqslant 95\%$ we can get $N_2' \geqslant 132.7$.

Since one structure provides 2^{32} ciphertexts and 2^{63} pairs, we need $2^{132.7-63} = 2^{69.7}$ structures and totally $2^{69.7+32} = 2^{101.7}$ chosen ciphertexts. When proceeding the attack, we decrypt ciphertexts and insert the corresponding plaintexts satisfying *Condition 1* into a hash table indexed by other eight bytes, and check whether there are two plaintexts in the same row. Therefore the time complexity is $2^{101.7}$ memory accesses. The complexity is very similar with the distinguisher without AK_0.

We analyze the reason why the chosen-plaintext and chosen-ciphertext ID distinguishers have a similar data complexity. Without AK_0 operation, the chosen-plaintext distinguisher requires $2^{64.6}$ chosen plaintexts while the chosen-ciphertext distinguisher needs $2^{98.6}$ chosen ciphertexts. However, when we take the AK_0 operation into consideration, the data complexity increases significantly under chosen-plaintext setting while it remains almost unchanged under chosen-ciphertext setting. To make it clear, we list the complexities of these distinguishers in Table 3.

Table 3. Data complexities of 5-round ID distinguishers with(out) AK_0.

Setting	Target	Data complexity	Time (MA)
CP	5-round AES without AK_0	$2^{64.6}$	$2^{64.6}$
	5-round AES with AK_0	$2^{96.7}$	$2^{101.7}$
CC	5-round AES without AK_0	$2^{98.6}$	$2^{98.6}$
	5-round AES with AK_0	$2^{101.7}$	$2^{101.7}$

– CC: Chosen-Ciphertext CP: Chosen-Plaintext MA: Memory Access

D Figures of the Distinguisher Introduced in Sect. 2

See Figs. 4, 5, and 6.

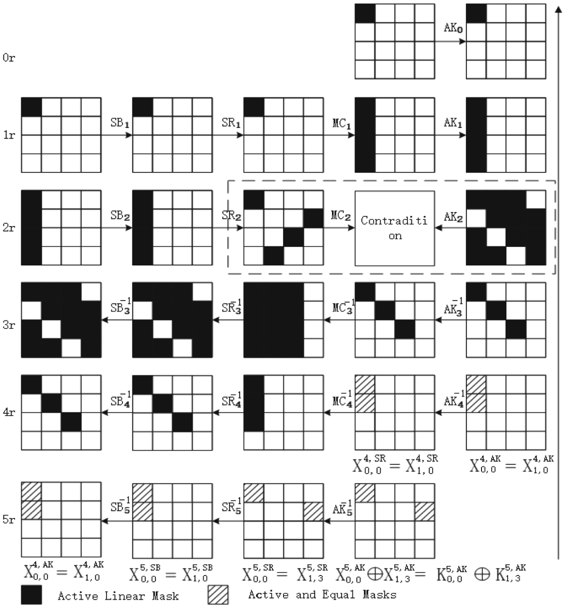
0r
AK0
1r
SB1
SR1
MC1
AK1
2r
SB2
SR2
MC2
Contradition
AK2
3r
SB3^-1
SR3^-1
MC3^-1
AK3^-1
4r
SB4^-1
SR4^-1
MC4^-1
AK4^-1
X^{4,SR}_{0,0} = X^{4,SR}_{1,0}
X^{4,AK}_{0,0} = X^{4,AK}_{1,0}
5r
SB5^-1
SR5^-1
AK5^-1
X^{4,AK}_{0,0} = X^{4,AK}_{1,0}
X^{5,SB}_{0,0} = X^{5,SB}_{1,0}
X^{5,SR}_{0,0} = X^{5,SR}_{1,3}
X^{5,AK}_{0,0} ⊕ X^{5,AK}_{1,3} = K^{5,AK}_{0,0} ⊕ K^{5,AK}_{1,3}
Active Linear Mask
Active and Equal Masks

Fig. 4. ZC linear hull of 5-round AES [12].

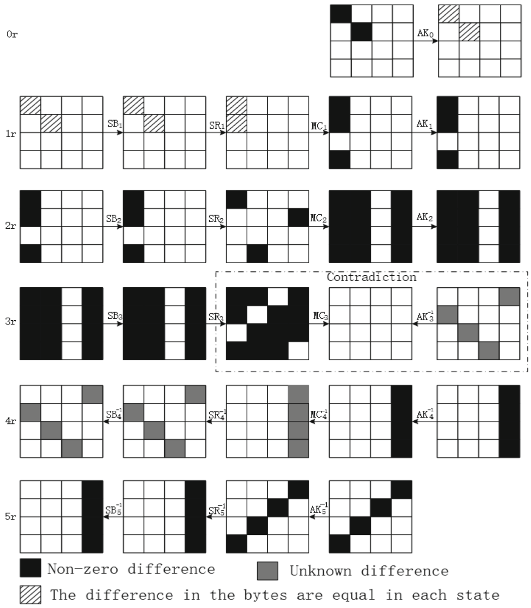

Fig. 5. ID of 5-round AES based on Property 1 [8].

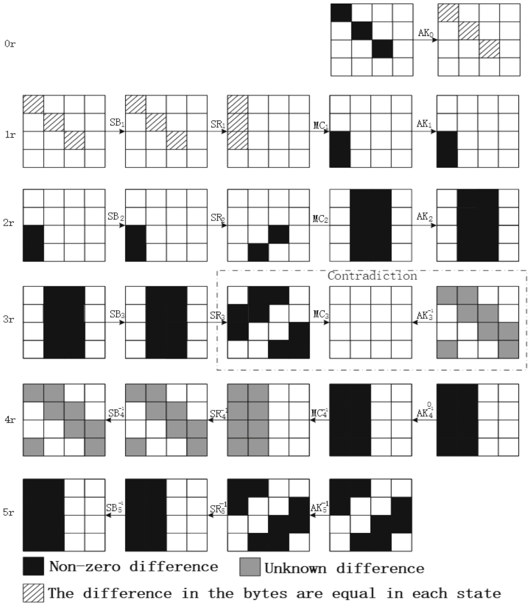

Fig. 6. ID of 5-round AES based on Property 2 [7].

References

1. Biham, E., Keller, N.: Cryptanalysis of reduced variants of Rijndael. In: 3rd AES Conference, vol. 230 (2000)
2. Bogdanov, A., Leander, G., Nyberg, K., Wang, M.: Integral and multidimensional linear distinguishers with correlation zero. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 244–261. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_16
3. Cui, T., Sun, L., Chen, H., Wang, M.: Statistical integral distinguisher with multi-structure and its application on AES. In: Pieprzyk, J., Suriadi, S. (eds.) ACISP 2017. LNCS, vol. 10342, pp. 402–420. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60055-0_21
4. Daemen, J., Rijmen, V.: The Design of Rijndael: AES-The Advanced Encryption Standard. ISC. Springer Science & Business Media, Heidelberg (2013). https://doi.org/10.1007/978-3-662-04722-4
5. Datta, N., Nandi, M.: ELmD v2.0 (2015). Submission to the caesar competition
6. Gilbert, H., Minier, M.: A collision attack on 7 rounds of Rijndael. In: AES Candidate Conference, pp. 230–241 (2000)
7. Grassi, L.: MixColumns properties and attacks on (round-reduced) AES with a single secret S-Box. In: Smart, N.P. (ed.) CT-RSA 2018. LNCS, vol. 10808, pp. 243–263. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76953-0_13
8. Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to AES. IACR Trans. Symmetric Cryptol. **2016**(2), 192–225 (2016)

9. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round AES. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 289–317. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_10
10. Lu, J., Dunkelman, O., Keller, N., Kim, J.: New impossible differential attacks on AES. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 279–293. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89754-5_22
11. Rønjom, S., Bardeh, N.G., Helleseth, T.: Yoyo tricks with AES. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10624, pp. 217–243. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70694-8_8
12. Sun, B., Liu, M., Guo, J., Qu, L., Rijmen, V.: New insights on AES-like SPN ciphers. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 605–624. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4_22
13. Wang, M., Cui, T., Chen, H., Sun, L., Wen, L., Bogdanov, A.: Integrals go statistical: cryptanalysis of full skipjack variants. IACR Cryptology ePrint Archive 2016:178 (2016)
14. Wu, H., Preneel, B.: AEGIS: a fast authenticated encryption algorithm. In: Lange, T., Lauter, K., Lisoněk, P. (eds.) SAC 2013. LNCS, vol. 8282, pp. 185–201. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43414-7_10