New Key Recovery Attack on Reduced-Round AES

Navid Ghaedi Bardeh[1] and Vincent Rijmen[2,3]

[1] Norwegian University of Science and Technology, Trondheim, Norway,
navid.ghaedibardeh@gmail.com
[2] imec-COSIC KU Leuven, Leuven, Belgium, firstname.lastname@esat.kuleuven.be
[3] University of Bergen, Bergen, Norway

Abstract. A new fundamental 4-round property against AES, called the zero-difference property, was introduced by Rønjom, Bardeh and Helleseth at Asiacrypt 2017. Our work characterizes it in a simple way by exploiting the notion of related differences which was introduced and well analyzed by AES designers. We then are interested in the way of extending the 4-round property by considering some further properties of related differences over the AES linear layer, generalizing the zero-difference property. This results in a new key recovery attack on 7-round AES which is the first attack on 7-round AES by exploiting the zero-difference property.

Keywords: SPN · AES · Secret-Key model · Zero-difference cryptanalysis · Related differences · Related differentials

1 Introduction

The Rijndael block cipher [DR98] has been designed in the late 1990's by Joan Daemen and Vincent Rijmen, and was chosen as the Advanced Encryption Standard (AES) by NIST in 2000. It is since then the most used and the most analysed symmetric primitive worldwide. There are three versions of AES, with different key sizes, and a different number of rounds: AES-128 with 10 rounds, AES-192 with 12 rounds, and AES-256 with 14 rounds. During the previous two decades, many different cryptanalytic techniques have been applied to AES. Up to now, the best attacks on AES-128 in the secret-key model cover seven rounds. Impossible differential attack [LP21] and meet-in-the-middle attack [DFJ13] are the two best-known attacks on AES-128.

A key recovery attack against a block cipher is generally based on the existence of a distinguishing property. A distinguishing property refers to a statistical or structural property of a cipher that a random permutation does not have, thus we can distinguish the cipher from a random permutation. For example, impossible differential attacks and meet-in-the-middle attacks on 7-round AES-128, exploit 4-round distinguishers.

Recently, in a series of works, new distinguishers for reduced-round AES appeared [GRR17, RBH17, Gra18, BR19b, BR19a, Bar19]. These distinguishers exhibit new and fundamental properties of the AES which result in new efficient key recovery attacks on 5-round AES. At Eurocrypt 2017, the authors of [GRR17] proposed the first key-independent 5-round distinguisher which requires 2^{32} chosen texts with a computational cost of $2^{35.6}$ look-ups into a memory of size 2^{36} bytes. They showed that by encrypting cosets of certain subspaces of the plaintext space the number of times the difference of ciphertext pairs lies in a particular subspace of the state space always is a multiple of 8, known as the multiple-of-8 property. However, this distinguisher could not be exploited directly for mounting a key-recovery attack because of the particular subspace used in the multiple-of-8 property.

This problem was solved in [Gra18] which results in a new key recovery attack on 5-round AES. Subsequent work [BDK+18], at Crypto 2018, improved on their result and proposed a key recovery attack on 5-round AES which requires 2^{24} chosen plaintexts and operations.

At Asiacrypt 2017, the authors of [RBH17] presented distinguishers for 3- to 6-round AES. The authors introduced a new deterministic 4-round property in AES, which states that sets of pairs of plaintexts that are equivalent by exchange of any subset of diagonals encrypts to a set of pairs of ciphertexts after four rounds that all have a difference of zero in exactly the same columns before the final linear layer, called zero-difference property. This deterministic property was extended to a probabilistic 5-round property in [BR19a]. By exploiting this 4-round distinguishing property, a new key recovery on 5-round AES was described in [RBH17]. At Eurocrypt 2020, the authors of [DKRS20] improved the key-recovery to the attack on 5-round AES to 2^9 adaptive chosen plaintexts and ciphertexts (ACCs) and 2^{23} encryptions, and proposed new attack on 5-round AES with 2^{15} ACCs and $2^{16.5}$ operations.

The aim of our paper is to present a key recovery attack against 7-round AES-128 based on the zero-difference property. We provide a general formulation of the zero-difference property which allows to combine the 4-round zero-difference property with related differentials (introduced in [DR09]). It then results in a new 7-round related differentials characteristic. We then present the first key-recovery attack on 7-round AES based on the zero-difference property.

1.1 Our contributions

This work generalizes the zero-difference property by providing new insights into it. It provides a simpler formulation and interpretation of the zero-difference property. For this, we recall the notion of *related differences* and *related differentials* which were introduced by Daemen and Rjimen in [DR09]. This notion provides a very simple formulation of the zero-difference property. In particular, we show that the zero-difference property works on larger sets of pairs of plaintexts than the one described in its original formulation [RBH17]. Most notably, we embed related differentials within the zero difference property for SPN's. We show here 2- and 4-round related differentials for AES, which result in extensions of the zero-difference property up to 8-round AES. We describe a new 7-round related differential characteristic for AES, which embeds 4-round related differentials. This permits to mount a key recovery attack on 7-round AES which data/time/memory complexities below $2^{110.2}$.

1.2 Overview of this paper and main result

Section 2 describes the AES and recalls the notion of related difference and differential. Section 3 presents the link between the notion of related difference and the zero-difference property, and it generalizes the zero-difference property. Section 4 presents related differentials trials for 2 and 4-round AES. It also explains how to extend the zero difference property to 6 and 8 rounds. Section 5 explains how to mount a key-recovery attack on 7-round AES based on the zero-difference property. For comparison, Table 1 summarizes the current best key-recovery attacks for 7 rounds of AES-128.

2 Preliminaries

2.1 AES

The *Advanced Encryption Standard* (AES) [AES01] is the most widely adopted block cipher in the world today. An AES internal state α is typically represented by a 4 by 4

Table 1: Current best cryptanalysis of 7-round AES-128 in the secret-key model.

Attack	Rounds	Data	Time	Memory	Ref.
Impossible Differential	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	[LDKK08]
Meet-in-the-Middle	7	2^{116}	2^{116}	2^{116}	[DKS10]
Impossible Differential	7	$2^{105.1}$	2^{113}	$2^{74.1}$	[BLNS18]
Impossible Differential	7	$2^{104.9}$	$2^{110.9}$	$2^{71.9}$	[LP21]
Zero-difference	7	$2^{110.2}$	$2^{110.2}$	$2^{110.2}$	**Section 5**
Meet-in-the-Middle	7	2^{97}	2^{99}	2^{98}	[DFJ13]

matrix of bytes

$$\begin{bmatrix} \alpha_0 & \alpha_4 & \alpha_8 & \alpha_{12} \\ \alpha_1 & \alpha_5 & \alpha_9 & \alpha_{13} \\ \alpha_2 & \alpha_6 & \alpha_{10} & \alpha_{14} \\ \alpha_3 & \alpha_7 & \alpha_{11} & \alpha_{15} \end{bmatrix},$$

where $\alpha_i \in \mathbb{F}_{2^8}$. AES-128 has 10 rounds where one full round of AES applies four operations to the state matrix:

- AddKey (AK) xors a 128-bit round-key to the state,
- SubBytes (SB) applies 16 identical Sboxes s, 8-bit to 8-bit, independently to each byte of the state,
- ShiftRows (SR) shifts the i-th row left by i positions,
- MixColumns (MC) applies a fixed linear transformation to each column.

In the last round, the MC operation is omitted. Also, an additional AK is applied to last internal state to produce the ciphertext. We denote by $R^t(x)$ the sequence of t full rounds of AES, including the last additional AK.

2.2 Related differentials

In [DR09], Daemen and Rijmen define a new type of difference called related differences. They studied the propagation of these differences through the AES linear layer. We call an element of $\mathbb{F}_q$ a word and a vector of words $\alpha = (\alpha_0, \alpha_1, ..., \alpha_{n-1}) \in \mathbb{F}_q^n$ a state. Then the related differences and differentials are defined in [DR09] as below:

Definition 1 (related differences [DR09])**.** A pair of differences $\Delta x, \Delta x' \in \mathbb{F}_q^n$ are *related differences* if and only if:

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

It is obvious that relation (1) holds iff at least one of Δx_i, $\Delta x'_i$ and $\Delta x_i \oplus \Delta x'_i$ equals zero for every value of i. For a state $\alpha \in \mathbb{F}_q^n$, we can define four distinct states, called a quartet, $(\alpha, \alpha \oplus \Delta x, \alpha \oplus \Delta x', \alpha \oplus \Delta x \oplus \Delta x')$ where the two differences Δx and $\Delta x'$ are related. The main important property of this quartet is that *the sets* $\{\alpha_i, \alpha_i \oplus \Delta x_i, \alpha_i \oplus \Delta x'_i, \alpha_i \oplus \Delta x_i \oplus \Delta x'_i\}$*, for every* i*, contain only two different elements.* As shown in [DR09], related differences can be combined into related differentials.

Definition 2 (related differentials [DR09])**.** Two differentials $(\Delta x, \Delta y)$ and $(\Delta x', \Delta y')$ for a linear map M are *related differentials* if and only if, $\Delta y = M(\Delta x)$, $\Delta y' = M(\Delta x')$, the differences Δx,$\Delta x'$ are related differences and the differences Δy, $\Delta y'$ are related differences.

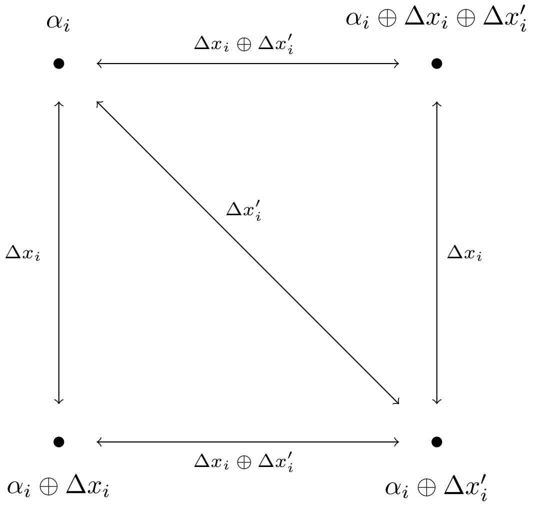
α_i
$\alpha_i \oplus \Delta x_i \oplus \Delta x'_i$
$\Delta x_i \oplus \Delta x'_i$
$\Delta x'_i$
Δx_i
Δx_i
$\Delta x_i \oplus \Delta x'_i$
$\alpha_i \oplus \Delta x_i$
$\alpha_i \oplus \Delta x'_i$

Figure 1: A schematic of the related differences and the associated quartet. The square collapses to a line or point depending on Δx_i and $\Delta x'_i$.

Moreover, it has been studied in [DR09] that AES MixColumns has some related differentials, where two related differences Δx and $\Delta x'$ are defined over $\mathbb{F}_{2^8}^4$. Four of them are listed in Table 2. The other related differentials can be derived from these four by means of rotation and/or multiplication by a scalar (see [DR09] for more details). In this paper we call them byte-related differences and differentials when they are defined over $\mathbb{F}_{2^8}^4$.

Table 2: The sets of byte-related differentials over AES MixColumns.

Δx	Δy	$\Delta x'$	$\Delta y'$	$\Delta x \oplus \Delta x'$	$\Delta y \oplus \Delta y'$
$[0,1,4,7]$	$[0,9,0,B]$	$[5,1,0,7]$	$[E,0,D,0]$	$[5,0,4,0]$	$[E,9,D,B]$
$[0,1,0,3]$	$[0,1,4,7]$	$[2,0,1,0]$	$[5,1,0,7]$	$[2,1,1,3]$	$[5,0,4,0]$
$[7,0,7,7]$	$[9,E,0,0]$	$[7,7,7,0]$	$[0,0,9,E]$	$[0,7,0,7]$	$[9,E,9,E]$
$[0,3,2,0]$	$[7,0,7,1]$	$[2,0,0,3]$	$[7,1,7,0]$	$[2,3,2,3]$	$[0,1,0,1]$

2.3 Zero-difference cryptanalysis

In [RBH17], a new fundamental property against 2 rounds of SPNs was introduced, called the zero-difference property. Consider an SPN where the round key is xored to state $\alpha \in \mathbb{F}_q^n$. The Sbox layer S can be seen as the concatenation of n independent Sboxes s over $\mathbb{F}_q$ and P denotes the linear layer. We recall here the main definitions and notations from [RBH17].

Definition 3 (The zero-difference pattern [RBH17])**.** Let $\alpha \in \mathbb{F}_q^n$ and define the *zero-difference pattern*

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

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

Through the paper we are interested in zero-difference patterns before the last linear layer. Thus, $\nu(\alpha)$ simply indicates the non-zero words of the state before the last linear layer.

Definition 4 ([RBH17]). For a vector $v \in \mathbb{F}_2^n$ and a pair of states $\alpha, \beta \in \mathbb{F}_q^n$ define a new state $\rho^v(\alpha, \beta) \in \mathbb{F}_q^n$ such that the i'th component is defined by

$$\rho^v(\alpha, \beta)_i = \alpha_i v_i \oplus \beta_i (v_i \oplus 1).$$

This is equivalent to

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

Notice that $(\alpha', \beta') = (\rho^v(\alpha, \beta), \rho^v(\beta, \alpha))$ is a new pair of states formed by exchanging individual words between α and β according to the binary coefficients of v. From the definition it can be seen that

$$\rho^v(\alpha, \beta) \oplus \rho^v(\beta, \alpha) = \alpha \oplus \beta. \tag{2}$$

Assume d is the number of common words between α and β, $\alpha_i = \beta_i$. Then, the number of possible unique pairs (α', β') generated this way is 2^{n-d-1} (including the original pair). Now, the following theorem shows a relation over 2-round SPN.

Theorem 1 ([RBH17]). *Let $\alpha, \beta \in \mathbb{F}_q^n$ and $\alpha' = \rho^v(\alpha, \beta)$, $\beta' = \rho^v(\beta, \alpha)$ for any $v \in \mathbb{F}_2^n$, then*

$$\nu(P \circ S \circ P \circ S(\alpha) \oplus P \circ S \circ P \circ S(\beta)) = \nu(P \circ S \circ P \circ S(\alpha') \oplus P \circ S \circ P \circ S(\beta')) \tag{3}$$

Theorem 1 states that sets of pairs of states that are equivalent by exchange of any subset of words encrypts to a set of pairs of states after 2-round SPN that all have a difference of (non-)zero in exactly the same words before the final linear layer. We call these pairs of states related pairs. In the next section, we will show that the set of related pairs is larger than the set considered here.

3 Generalize zero-difference cryptanalysis with related differences

The central notion of this work is to redefine the zero-difference property with the concept of related differences. This permits to generate more related pairs than the pairs mentioned in Subsection 2.3. Moreover, related differentials can be combined with zero-difference property exploiting this redefinition.

3.1 Generating more related pairs

Zero-difference cryptanalysis [RBH17,BR19a] works with a quartet $(\alpha, \beta, \rho^v(\alpha, \beta), \rho^v(\beta, \alpha))$, where $\alpha, \beta \in \mathbb{F}_q^n$. This quartet is very similar to the quartet defined by two related differences Δx and $\Delta x'$ in Subsection 2.2. More precisely, this quartet can be defined by two related differences Δx and $\Delta x'$ where the following condition holds:

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

Interestingly, this quartet has the same property that the quartet defined by related differences has:

> *The sets $\{\alpha_i, \alpha_i \oplus \Delta x_i, \alpha_i \oplus \Delta x'_i, \alpha_i \oplus \Delta x_i \oplus \Delta x'_i\}$, for every i, contain only two different elements.*

The only difference between these two quartets is the condition $\Delta x_i = 0$ was not considered in zero-difference property for generating new pairs of states. We will show that considering the condition $\Delta x_i = 0$ makes it possible to generate more number of related pairs, $\alpha = \alpha_0$ and $\alpha \oplus \Delta x = \alpha_1$, instead of 2^{n-d-1} pairs in the Definition 4. Let consider a quartet $(\alpha, \alpha \oplus \Delta x, \alpha \oplus \Delta x', \alpha \oplus \Delta x \oplus \Delta x')$. Since we can choose two related differences Δx and $\Delta x'$, if we choose $\Delta x_i = 0$ for some i, then there is exactly one value in those coordinates i of α and $\alpha \oplus \Delta x$, i.e. α_i. So we have freedom to choose a second value for those coordinates i, i.e. $\alpha_i \oplus \Delta x'_i$. In this way, when d words of Δx are zero, at most $(q^d - 1) \cdot 2^{n-d-1}$ pairs can be generated. Note that, if $\Delta x_i \neq 0$ for some i, then it means that we already chose the two values for those coordinates of α and $\alpha \oplus \Delta x$.[1]

In order to cover all related pairs, the trivial case is also considered when both Δx_i and $\Delta x'_i$ can equal zero for some coordinates i, which means that the four states have the common value in this coordinate. So we can state that the property of this quartet is that *the sets* $\{\alpha_i, \alpha_i \oplus \Delta x_i, \alpha_i \oplus \Delta x'_i, \alpha_i \oplus \Delta x_i \oplus \Delta x'_i\}$, *for every* i, *contain* at most *two different elements.*

As we have seen, the property of quartets defined by two related differences Δx and $\Delta x'$ is as the same as the ones exploit in zero-difference property. However, by exploiting the concept of related differences we can generate more related pairs. In the next subsection, we will show that quartets defined by related differences work in the zero-difference property as well.

3.2 Zero-difference cryptanalysis revisited

In Subsection 3.1, it is shown that more related quartets than the ones exploited in the zero-difference cryptanalysis can be defined by two related differences. Most notably, zero-difference cryptanalysis takes advantage of a property which can be also achieved by a quartet defined by two related differences. It then allows to redefine the main result of zero-difference cryptanalysis in [RBH17], Theorem 1, with the notion of related differences.

Theorem 2. *Let* $\alpha \in \mathbb{F}_q^n$ *and* $\Delta x, \Delta x' \in \mathbb{F}_q^n$ *be two related differences then*

$$\nu(F(\alpha) \oplus F(\alpha \oplus \Delta x)) = \nu(F(\alpha \oplus \Delta x') \oplus F(\alpha \oplus \Delta x \oplus \Delta x')) \tag{4}$$

where $F = P \circ S \circ P \circ S$*.*

Proof. Since the Sbox layer operates independently on individual words and the sets $\{\alpha_i, \alpha_i \oplus \Delta x_i, \alpha_i \oplus \Delta x'_i, \alpha_i \oplus \Delta x_i \oplus \Delta x'_i\}$, for every i, contain at most two different elements, we have

$$S(\alpha) \oplus S(\alpha \oplus \Delta x) \oplus S(\alpha \oplus \Delta x') \oplus S(\alpha \oplus \Delta x \oplus \Delta x') = 0.$$

It then follows that

$$P(S(\alpha)) \oplus P(S(\alpha \oplus \Delta x)) \oplus P(S(\alpha \oplus \Delta x')) \oplus P(S(\alpha \oplus \Delta x \oplus \Delta x')) = 0.$$

Since the Sbox layer operates independently on individual words and each S-box is a permutation, the (non-)zero words of each input difference map into (non-)zero words in the corresponding output difference

$$\nu(F(\alpha) \oplus F(\alpha \oplus \Delta x)) = \nu(F(\alpha \oplus \Delta x') \oplus F(\alpha \oplus \Delta x \oplus \Delta x')).$$

□

[1] In [Gra18], a similar technique was used to generate new pairs of texts.

Assume now that d words of Δx equal zero, then $\Delta x'$ can take $q^d - 1$ different values for those words, and there are $2^{(n-d)-1}$ choices for exchanging non-zero words, between α and $\alpha \oplus \Delta x$ (there are $n - d$ distinct words). So it means that there are $2^{(n-d)-1} \cdot (q^d - 1)$ different related pairs which all follow the relation (4). For typical 128-bit SPN based block ciphers, we have $q = 2^{32}$ and $n = 4$. As an example, by selecting $d = 2$, the total number of related pairs that are generated in this way is 2^{65}, including the original pair of texts.

The central advantage of redefining the zero-difference property with the concept of related differences, is to combine two techniques: related differentials and zero-difference cryptanalysis. In the next subsection, we discuss this in more details.

3.3 Embedding related differentials within zero-difference cryptanalysis

Now we are ready to combine the zero-difference property with related differentials for SPNs. Consider a t-round SPN which is divided into two parts: $E = F \circ G$. Thus G represents the first $t - 2$ rounds of the encryption operation, and F represents the final two rounds of the encryption operation. Assume that there are related differentials with probability pr over G:

$$\Delta x \xrightarrow{G} \Delta y,$$
$$\Delta x' \xrightarrow{G} \Delta y'.$$

Since differences Δy and $\Delta y'$ are related differences, we are allowed to combine it with the results of Theorem 2

$$\nu(F(\alpha) \oplus F(\alpha \oplus \Delta y)) = \nu(F(\alpha \oplus \Delta y') \oplus F(\alpha \oplus \Delta y \oplus \Delta y')).$$

We then have a zero-difference property over the t-round SPN with probability pr:

$$\nu(F \circ G(\alpha) \oplus F \circ G(\alpha \oplus \Delta x)) = \nu(F \circ G(\alpha \oplus \Delta x') \oplus F \circ G(\alpha \oplus \Delta x \oplus \Delta x')).$$

The existence of related differentials for an SPN relies on the details of its linear layer. In the case of AES-like ciphers, the linear layer is composed of the MixColumns and ShiftRows transformations. As studied in [DR09], there exist some MixColumns transformations without related differentials. However, there are some MixColumns transformations which have related differentials. So, in these cases, the combination mentioned here is not avoidable.

In the next section, we will show that there are related differentials for up to 4-round AES with certain probabilities. They result into extensions of the zero-difference property up to 8 rounds, using the generalization mentioned here.

4 Extensions of zero-difference property for reduced-round AES

In this section, we investigate how to extend the result of Theorem 2 to 6- and 8-round AES. For this, we look for related differentials over reduced-round AES. Let first reformulated the result of Theorem 2 for AES. Let $S = SB \circ AK \circ MC \circ SB$ and $P = SR \circ AK \circ MC \circ SR$ where S can be seen as the concatenation of four independent superboxes operating over $\mathbb{F}_{2^8}^4$. Then, four-round AES can be seen as

$$R^4 = AK \circ MC \circ SR \circ S \circ P \circ S \circ SR \circ AK.$$

This is a typical superbox representation of 4-round AES in the literature [DR09, Gil14, RBH17]. So the relation (4) also holds for the case of four-round AES where $F = R^4$ and

$\alpha, \Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$. We also assume $\Delta x, \Delta x'$ are (diagonal-) related differences if and only if

$$\Delta x_i \Delta x'_i(\Delta x_i \oplus \Delta x'_i) = 0, \text{ for } i = 0, 1, 2, 3,$$

where Δx_i and $\Delta x'_i$ indicate the diagonal i of the differences. It other words, the diagonals i in $\alpha_i, \alpha_i \oplus \Delta x_i, \alpha_i \oplus \Delta x'_i$ and $\alpha_i \oplus \Delta x_i \oplus \Delta x'_i$ take at most two values, for every i.

Our aim now is to find related differentials over reduced-round AES. The basic idea consists of choosing an input quartet $(\alpha, \alpha \oplus \Delta x, \alpha \oplus \Delta x', \alpha \oplus \Delta x \oplus \Delta x')$, where Δx and $\Delta x'$ are related differences, such that the corresponding output quartet $(R^t(\alpha), R^t(\alpha \oplus \Delta x), R^t(\alpha \oplus \Delta x'), R^t(\alpha \oplus \Delta x \oplus \Delta x'))$ for $t = 2, 4$, can be also defined by only two related differences

$$\Delta y = R^t(\alpha) \oplus R^t(\alpha \oplus \Delta x), \Delta y' = R^t(\alpha) \oplus R^t(\alpha \oplus \Delta x').$$

Then, the relation (4) will extend to 6-round and 8-round AES. To determine the essential role of MC in creating our results, we denote by now $R^4 = MC \circ G \circ MC \circ G$ where

$$G = SR \circ SB \circ AK \circ MC \circ SR \circ SB \circ AK.$$

G can also be seen as four parallel super-boxes operating on 4 bytes of the state independently (not four bytes placed in a column of state). This 4-round AES decomposition is a bit different from the decomposition of 4-round AES mentioned above. However, this 4-round AES decomposition will clearly show how the middle and last MC affect differences which forms a basis for our results. We have noticed that a careful combination of byte-related differentials sets from Table 2, provides related differentials over 2-round and 4-round AES.

4.1 2-round related differentials for AES

Let us now consider an input quartet $(\alpha, \alpha \oplus \Delta x, \alpha \oplus \Delta x', \alpha \oplus \Delta x \oplus \Delta x')$ where

$$\alpha = \begin{bmatrix} \alpha_0 & \alpha_4 & \alpha_8 & \alpha_{12} \\ \alpha_1 & \alpha_5 & \alpha_9 & \alpha_{13} \\ \alpha_2 & \alpha_6 & \alpha_{10} & \alpha_{14} \\ \alpha_3 & \alpha_7 & \alpha_{11} & \alpha_{15} \end{bmatrix}, \qquad \Delta x = \begin{bmatrix} \Delta x_0 & \Delta x_4 & \Delta x_8 & \Delta x_{12} \\ \Delta x_1 & \Delta x_5 & \Delta x_9 & \Delta x_{13} \\ \Delta x_2 & \Delta x_6 & \Delta x_{10} & \Delta x_{14} \\ \Delta x_3 & \Delta x_7 & \Delta x_{11} & \Delta x_{15} \end{bmatrix},$$

$$\Delta x' = \begin{bmatrix} \Delta x_0 & 0 & \Delta x_8 & 0 \\ 0 & \Delta x_5 & 0 & \Delta x_{13} \\ \Delta x_2 & 0 & \Delta x_{10} & 0 \\ 0 & \Delta x_7 & 0 & \Delta x_{15} \end{bmatrix}, \qquad \Delta x \oplus \Delta x' = \begin{bmatrix} 0 & \Delta x_4 & 0 & \Delta x_{12} \\ \Delta x_1 & 0 & \Delta x_9 & 0 \\ 0 & \Delta x_6 & 0 & \Delta x_{14} \\ \Delta x_3 & 0 & \Delta x_{11} & 0 \end{bmatrix},$$

and Δx and $\Delta x'$ are related differences. It is obvious from this quartet that two states $\alpha \oplus \Delta x'$ and $\alpha \oplus \Delta x \oplus \Delta x'$ are generated by exchanging diagonals 1 and 3 between α and $\alpha \oplus \Delta x$. Now assume that we have

$$G(\alpha) \oplus G(\alpha \oplus \Delta x) = \begin{bmatrix} 2\lambda_0 & 3\lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_0 & 2\lambda_1 & 3\lambda_2 & \lambda_3 \\ \lambda_0 & \lambda_1 & 2\lambda_2 & 3\lambda_3 \\ 3\lambda_0 & \lambda_1 & \lambda_2 & 2\lambda_3 \end{bmatrix}, \tag{5}$$

where $\lambda_i \in \mathbb{F}_{2^8}$. Since G acting independently on 32-bits of the state, the differences $G(\alpha) \oplus G(\alpha \oplus \Delta x')$ and $G(\alpha) \oplus G(\alpha \oplus \Delta x \oplus \Delta x')$ equal respectively

$$\begin{bmatrix} 2\lambda_0 & 0 & \lambda_2 & 0 \\ 0 & 2\lambda_1 & 0 & \lambda_3 \\ \lambda_0 & 0 & 2\lambda_2 & 0 \\ 0 & \lambda_1 & 0 & 2\lambda_3 \end{bmatrix}, \begin{bmatrix} 0 & 3\lambda_1 & 0 & \lambda_3 \\ \lambda_0 & 0 & 3\lambda_2 & 0 \\ 0 & \lambda_1 & 0 & 3\lambda_3 \\ 3\lambda_0 & 0 & \lambda_2 & 0 \end{bmatrix}. \tag{6}$$

$$\begin{bmatrix} \Delta x_0 & \Delta x_4 & \Delta x_8 & \Delta x_{12} \\ \Delta x_1 & \Delta x_5 & \Delta x_9 & \Delta x_{13} \\ \Delta x_2 & \Delta x_6 & \Delta x_{10} & \Delta x_{14} \\ \Delta x_3 & \Delta x_7 & \Delta x_{11} & \Delta x_{15} \end{bmatrix} \xrightarrow[-96]{G} \begin{bmatrix} 2\lambda_0 & 3\lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_0 & 2\lambda_1 & 3\lambda_2 & \lambda_3 \\ \lambda_0 & \lambda_1 & 2\lambda_2 & 3\lambda_3 \\ 3\lambda_0 & \lambda_1 & \lambda_2 & 2\lambda_3 \end{bmatrix} \xrightarrow[0]{MC} \begin{bmatrix} 5\lambda_0 & 0 & 4\lambda_2 & 0 \\ 0 & 5\lambda_1 & 0 & 4\lambda_3 \\ 4\lambda_0 & 0 & 5\lambda_2 & 0 \\ 0 & 4\lambda_1 & 0 & 5\lambda_3 \end{bmatrix}$$

$$\begin{bmatrix} \Delta x_0 & 0 & \Delta x_8 & 0 \\ 0 & \Delta x_5 & 0 & \Delta x_{13} \\ \Delta x_2 & 0 & \Delta x_{10} & 0 \\ 0 & \Delta x_7 & 0 & \Delta x_{15} \end{bmatrix} \xrightarrow[0]{G} \begin{bmatrix} 2\lambda_0 & 0 & \lambda_2 & 0 \\ 0 & 2\lambda_1 & 0 & \lambda_3 \\ \lambda_0 & 0 & 2\lambda_2 & 0 \\ 0 & \lambda_1 & 0 & 2\lambda_3 \end{bmatrix} \xrightarrow[0]{MC} \begin{bmatrix} 5\lambda_0 & 7\lambda_1 & 0 & \lambda_3 \\ \lambda_0 & 5\lambda_1 & 7\lambda_2 & 0 \\ 0 & \lambda_1 & 5\lambda_2 & 7\lambda_3 \\ 7\lambda_0 & 0 & \lambda_2 & 5\lambda_3 \end{bmatrix}$$

$$\begin{bmatrix} 0 & \Delta x_4 & 0 & \Delta x_{12} \\ \Delta x_1 & 0 & \Delta x_9 & 0 \\ 0 & \Delta x_6 & 0 & \Delta x_{14} \\ \Delta x_3 & 0 & \Delta x_{11} & 0 \end{bmatrix} \xrightarrow[0]{G} \begin{bmatrix} 0 & 3\lambda_1 & 0 & \lambda_3 \\ \lambda_0 & 0 & 3\lambda_2 & 0 \\ 0 & \lambda_1 & 0 & 3\lambda_3 \\ 3\lambda_0 & 0 & \lambda_2 & 0 \end{bmatrix} \xrightarrow[0]{MC} \begin{bmatrix} 0 & 7\lambda_1 & 4\lambda_2 & \lambda_3 \\ \lambda_0 & 0 & 7\lambda_2 & 4\lambda_3 \\ 4\lambda_0 & \lambda_1 & 0 & 7\lambda_3 \\ 7\lambda_0 & 4\lambda_1 & \lambda_2 & 0 \end{bmatrix}$$

Figure 2: 2-round related differential trails starting with Δx, $\Delta x'$ and $\Delta x \oplus \Delta x'$ respectively. The probability (binary logarithm) of each map is indicated under the corresponding arrow.

In other words, since two diagonals in each of input differences $\Delta x'$ and $\Delta x \oplus \Delta x'$ equal zero, it then causes that the two diagonals in the corresponding output differences equal zero (notice that G contains two SR operations). Therefore, MC maps these three differences (5) and (6) to a set of differences

$$\begin{bmatrix} 5\lambda_0 & 0 & 4\lambda_2 & 0 \\ 0 & 5\lambda_1 & 0 & 4\lambda_3 \\ 4\lambda_0 & 0 & 5\lambda_2 & 0 \\ 0 & 4\lambda_1 & 0 & 5\lambda_3 \end{bmatrix}, \begin{bmatrix} 5\lambda_0 & 7\lambda_1 & 0 & \lambda_3 \\ \lambda_0 & 5\lambda_1 & 7\lambda_2 & 0 \\ 0 & \lambda_1 & 5\lambda_2 & 7\lambda_3 \\ 7\lambda_0 & 0 & \lambda_2 & 5\lambda_3 \end{bmatrix}, \begin{bmatrix} 0 & 7\lambda_1 & 4\lambda_2 & \lambda_3 \\ \lambda_0 & 0 & 7\lambda_2 & 4\lambda_3 \\ 4\lambda_0 & \lambda_1 & 0 & 7\lambda_3 \\ 7\lambda_0 & 4\lambda_1 & \lambda_2 & 0 \end{bmatrix}, \tag{7}$$

which are related differences. Therefore,

$$\nu(R^6(\alpha) \oplus R^6(\alpha \oplus \Delta x)) = \nu(R^6(\alpha \oplus \Delta x') \oplus R^6(\alpha \oplus \Delta x \oplus \Delta x')).$$

We now need to evaluate the probability that, given an input random pair $(\alpha, \alpha \oplus \Delta x)$, the condition (5) holds. At random, this condition happens with probability $(2^{32}-1) \cdot 2^{-128} \approx 2^{-96}$, since there are $2^{32}-1$ values for $(\lambda_0, \lambda_1, \lambda_2, \lambda_3)$. Then, the differences (6) happen with probability one. This 2-round related differentials trail is depicted in Figure 2. We have also noticed that an identical rotation on all columns of the difference $G(\alpha) \oplus G(\alpha \oplus \Delta x)$, causes a new related differentials trail. There are three different possible cases for such rotations on $G(\alpha) \oplus G(\alpha \oplus \Delta x)$, i.e.

$$\begin{bmatrix} 3\lambda_0 & \lambda_1 & \lambda_2 & 2\lambda_3 \\ 2\lambda_0 & 3\lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_0 & 2\lambda_1 & 3\lambda_2 & \lambda_3 \\ \lambda_0 & \lambda_1 & 2\lambda_2 & 3\lambda_3 \end{bmatrix}, \begin{bmatrix} \lambda_0 & \lambda_1 & 2\lambda_2 & 3\lambda_3 \\ 3\lambda_0 & \lambda_1 & \lambda_2 & 2\lambda_3 \\ 2\lambda_0 & 3\lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_0 & 2\lambda_1 & 3\lambda_2 & \lambda_3 \end{bmatrix}, \begin{bmatrix} \lambda_0 & 2\lambda_1 & 3\lambda_2 & \lambda_3 \\ \lambda_0 & \lambda_1 & 2\lambda_2 & 3\lambda_3 \\ 3\lambda_0 & \lambda_1 & \lambda_2 & 2\lambda_3 \\ 2\lambda_0 & 3\lambda_1 & 2\lambda_2 & \lambda_3 \end{bmatrix}.$$

So there are four possible difference values for $G(\alpha) \oplus G(\alpha \oplus \Delta x)$. Then, such event happens with probability $4 \cdot 2^{-96} = 2^{-94}$ at random. We may summarize the result as follows.

Theorem 3. *Let $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$ and $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be two related differences, where all diagonals in Δx are non-zero and two non-consecutive diagonals in $\Delta x'$ are zero, then the relations*

$$R^4(\alpha) \oplus R^4(\alpha \oplus \Delta x) \oplus R^4(\alpha \oplus \Delta x') \oplus R^4(\alpha \oplus \Delta x \oplus \Delta x') = 0 \tag{8}$$

and

$$\nu(R^6(\alpha) \oplus R^6(\alpha \oplus \Delta x)) = \nu(R^6(\alpha \oplus \Delta x') \oplus R^6(\alpha \oplus \Delta x \oplus \Delta x')) \tag{9}$$

hold with probability 2^{-94}.

Proof. Assume that the input quartet $(\alpha, \alpha \oplus \Delta x, \alpha \oplus \Delta x', \alpha \oplus \Delta x \oplus \Delta x')$ conforms to differences (5) and (6) which happens with probability $4 \cdot 2^{-96} = 2^{-94}$, then the differences

$$\Delta y = R^2(\alpha) \oplus R^2(\alpha \oplus \Delta x), \Delta y' = R^2(\alpha) \oplus R^2(\alpha \oplus \Delta x')$$

are also related differences. The result then directly follows due to Theorem 2. □

More importantly, this 2-round related differentials can be extended to 4-round related differentials.

4.2 4-round related differentials for AES

Suppose now that the differences (7) map to the following differences through G, respectively:

$$\begin{bmatrix} 5\gamma_0 & 0 & 4\gamma_2 & 0 \\ 0 & 4\gamma_1 & 0 & 5\gamma_3 \\ 4\gamma_0 & 0 & 5\gamma_2 & 0 \\ 0 & 5\gamma_1 & 0 & 4\gamma_3 \end{bmatrix}, \begin{bmatrix} 5\gamma_0 & \gamma_1 & 0 & 7\gamma_3 \\ \gamma_0 & 0 & 7\gamma_2 & 5\gamma_3 \\ 0 & 7\gamma_1 & 5\gamma_2 & \gamma_3 \\ 7\gamma_0 & 5\gamma_1 & \gamma_2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \gamma_1 & 4\gamma_2 & 7\gamma_3 \\ \gamma_0 & 4\gamma_1 & 7\gamma_2 & 0 \\ 4\gamma_0 & 7\gamma_1 & 0 & 7\gamma_3 \\ 7\gamma_0 & 0 & \gamma_2 & 4\gamma_3 \end{bmatrix}, \tag{10}$$

where $\gamma_i \in \mathbb{F}_{2^8}$. Then MC maps these three differences to a new set of differences, respectively:

$$\begin{bmatrix} E\gamma_0 & 9\gamma_1 & D\gamma_2 & B\gamma_3 \\ 9\gamma_0 & D\gamma_1 & B\gamma_2 & E\gamma_3 \\ D\gamma_0 & B\gamma_1 & E\gamma_2 & 9\gamma_3 \\ B\gamma_0 & E\gamma_1 & 9\gamma_2 & D\gamma_3 \end{bmatrix}, \begin{bmatrix} E\gamma_0 & 0 & D\gamma_2 & 0 \\ 0 & D\gamma_1 & 0 & E\gamma_3 \\ D\gamma_0 & 0 & E\gamma_2 & 0 \\ 0 & E\gamma_1 & 0 & D\gamma_3 \end{bmatrix}, \begin{bmatrix} 0 & 9\gamma_1 & 0 & B\gamma_3 \\ 9\gamma_0 & 0 & B\gamma_2 & 0 \\ 0 & B\gamma_1 & 0 & 9\gamma_3 \\ B\gamma_0 & 0 & 9\gamma_2 & 0 \end{bmatrix}, \tag{11}$$

which are again related differences. It is worth noting that this 4-round differential is iterative (depicted in Figure 3). Unfortunately, the probability of this differential is very low. The probability that the difference

$$\begin{bmatrix} 5\gamma_0 & 0 & 4\gamma_2 & 0 \\ 0 & 4\gamma_1 & 0 & 5\gamma_3 \\ 4\gamma_0 & 0 & 5\gamma_2 & 0 \\ 0 & 5\gamma_1 & 0 & 4\gamma_3 \end{bmatrix}$$

$$\xrightarrow[-96]{G}\begin{bmatrix}2\lambda_0 & 3\lambda_1 & \lambda_2 & \lambda_3\\ \lambda_0 & 2\lambda_1 & 3\lambda_2 & \lambda_3\\ \lambda_0 & \lambda_1 & 2\lambda_2 & 3\lambda_3\\ 3\lambda_0 & \lambda_1 & \lambda_2 & 2\lambda_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}5\lambda_0 & 0 & 4\lambda_2 & 0\\ 0 & 5\lambda_1 & 0 & 4\lambda_3\\ 4\lambda_0 & 0 & 5\lambda_2 & 0\\ 0 & 4\lambda_1 & 0 & 5\lambda_3\end{bmatrix}\xrightarrow[-32]{G}\begin{bmatrix}5\gamma_0 & 0 & 4\gamma_2 & 0\\ 0 & 4\gamma_1 & 0 & 5\gamma_3\\ 4\gamma_0 & 0 & 5\gamma_2 & 0\\ 0 & 5\gamma_1 & 0 & 4\gamma_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}E\gamma_0 & 9\gamma_1 & D\gamma_2 & B\gamma_3\\ 9\gamma_0 & D\gamma_1 & B\gamma_2 & E\gamma_3\\ D\gamma_0 & B\gamma_1 & E\gamma_2 & 9\gamma_3\\ B\gamma_0 & E\gamma_1 & 9\gamma_2 & D\gamma_3\end{bmatrix}$$

$$\xrightarrow[0]{G}\begin{bmatrix}2\lambda_0 & 0 & \lambda_2 & 0\\ 0 & 2\lambda_1 & 0 & \lambda_3\\ \lambda_0 & 0 & 2\lambda_2 & 0\\ 0 & \lambda_1 & 0 & 2\lambda_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}5\lambda_0 & 7\lambda_1 & 0 & \lambda_3\\ \lambda_0 & 5\lambda_1 & 7\lambda_2 & 0\\ 0 & \lambda_1 & 5\lambda_2 & 7\lambda_3\\ 7\lambda_0 & 0 & \lambda_2 & 5\lambda_3\end{bmatrix}\xrightarrow[-64]{G}\begin{bmatrix}5\gamma_0 & \gamma_1 & 0 & 7\gamma_3\\ \gamma_0 & 0 & 7\gamma_2 & 5\gamma_3\\ 0 & 7\gamma_1 & 5\gamma_2 & \gamma_3\\ 7\gamma_0 & 5\gamma_1 & \gamma_2 & 0\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}E\gamma_0 & 0 & D\gamma_2 & 0\\ 0 & D\gamma_1 & 0 & E\gamma_3\\ D\gamma_0 & 0 & E\gamma_2 & 0\\ 0 & E\gamma_1 & 0 & D\gamma_3\end{bmatrix}$$

$$\xrightarrow[0]{G}\begin{bmatrix}0 & 3\lambda_1 & 0 & \lambda_3\\ \lambda_0 & 0 & 3\lambda_2 & 0\\ 0 & \lambda_1 & 0 & 3\lambda_3\\ 3\lambda_0 & 0 & \lambda_2 & 0\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}0 & 7\lambda_1 & 4\lambda_2 & \lambda_3\\ \lambda_0 & 0 & 7\lambda_2 & 4\lambda_3\\ 4\lambda_0 & \lambda_1 & 0 & 7\lambda_3\\ 7\lambda_0 & 4\lambda_1 & \lambda_2 & 0\end{bmatrix}\xrightarrow[0]{G}\begin{bmatrix}0 & \gamma_1 & 4\gamma_2 & 7\gamma_3\\ \gamma_0 & 4\gamma_1 & 7\gamma_2 & 0\\ 4\gamma_0 & 7\gamma_1 & 0 & \gamma_3\\ 7\gamma_0 & 0 & \gamma_2 & 4\gamma_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}0 & 9\gamma_1 & 0 & B\gamma_3\\ 9\gamma_0 & 0 & B\gamma_2 & 0\\ 0 & B\gamma_1 & 0 & 9\gamma_3\\ B\gamma_0 & 0 & 9\gamma_2 & 0\end{bmatrix}$$

Figure 3: 4-round related differential trails starting with Δx, $\Delta x'$ and $\Delta x \oplus \Delta x'$ respectively. The probability (binary logarithm) of each map is indicated under the corresponding arrow.

happens is $(2^{32}-1)\cdot 2^{-64} \approx 2^{-32}$, since there are $2^{32}-1$ values for $(\gamma_0, \gamma_1, \gamma_2, \gamma_3)$. And, the difference

$$\begin{bmatrix}5\gamma_0 & \gamma_1 & 0 & 7\gamma_3\\ \gamma_0 & 0 & 7\gamma_2 & 5\gamma_3\\ 0 & 7\gamma_1 & 5\gamma_2 & \gamma_3\\ 7\gamma_0 & 5\gamma_1 & \gamma_2 & 0\end{bmatrix}$$

happens with probability 2^{-64} (notice that the output difference of the first superbox is already determined). The probability of 4-round related differentials trail is $2^{-32}\cdot 2^{-64}\cdot 2^{-96} = 2^{-192}$. Also, another set of related differences, by exchanging the positions of $5\gamma_i$ and $4\gamma_i$, and $7\gamma_i$ and γ_i in the related differences set (10), works here. And, there are four sets of related differences for (5). Therefore, in total, there are eight 4-round related differentials trails so the probability of this event is $4\cdot 2\cdot 2^{-192} = 2^{-189}$ which makes that the iteration of this related differentials has a too low probability. However, it provides relations up to 6 rounds

$$R^t(\alpha)\oplus R^t(\alpha\oplus\Delta x)\oplus R^t(\alpha\oplus\Delta x')\oplus R^t(\alpha\oplus\Delta x\oplus\Delta x') = 0, \tag{12}$$

for $0 < t \leq 6$, since all differences are related differences every two rounds. We may summarize the results as follows.

Theorem 4. *Let $\alpha \in \mathbb{F}_{2^8}^{4\times 4}$ and $\Delta x, \Delta x' \in \mathbb{F}_{2^8}^{4\times 4}$ be two related differences, where all diagonals in Δx are non-zero and two non-consecutive diagonals in $\Delta x'$ are zero, then the relations*

$$R^t(\alpha)\oplus R^t(\alpha\oplus\Delta x)\oplus R^t(\alpha\oplus\Delta x')\oplus R^t(\alpha\oplus\Delta x\oplus\Delta x') = 0, \tag{13}$$

for $0 < t \leq 6$, and

$$\nu(R^8(\alpha)\oplus R^8(\alpha\oplus\Delta x)) = \nu(R^8(\alpha\oplus\Delta x')\oplus R^8(\alpha\oplus\Delta x\oplus\Delta x')) \tag{14}$$

hold with probability 2^{-189}.

Proof. Assume that the input quartet $(\alpha, \alpha \oplus \Delta x, \alpha \oplus \Delta x', \alpha \oplus \Delta x \oplus \Delta x')$ conforms the 4-round differential depicted in Figure 3 which happens with probability 2^{-189}. Since the input differences, and state differences at the end of round 2 and 4 are related differences, from Theorem 2, we have

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

for $0 < t \leq 6$. Also, since the differences

$$\Delta y = R^4(\alpha) \oplus R^4(\alpha \oplus \Delta x), \Delta y' = R^4(\alpha) \oplus R^4(\alpha \oplus \Delta x'),$$

are also related differences, due to Theorem 2 we have

$$\nu(R^8(\alpha) \oplus R^8(\alpha \oplus \Delta x)) = \nu(R^8(\alpha \oplus \Delta x') \oplus R^8(\alpha \oplus \Delta x \oplus \Delta x'))$$

□

There is another 4-round related differentials trail, provided in Appendix A. In the next section, we show that the results of Theorem 4 can be used to attack 7-round AES.

5 New key-recovery attack for 7 round of AES-128

In this section, we present a 7-round key-recovery attack for AES-128, which follows from a straight-forward extension of relation (13). Let an input quartet $(P_0, P_0 \oplus \Delta x, P_0 \oplus \Delta x', P_0 \oplus \Delta x \oplus \Delta x')$ be generated by two related differences Δx and $\Delta x'$ where P_0 is a random plaintext and all diagonals in Δx are non-zero and two non-consecutive diagonals in $\Delta x'$ are zero. Let (C_0, C_1, C_2, C_3) be the corresponding ciphertexts after 7-round AES. Assume now this input quartet $(P_0, P_0 \oplus \Delta x, P_0 \oplus \Delta x', P_0 \oplus \Delta x \oplus \Delta x')$ conforms the differential characteristics depicted in Figure 4, which embeds the previous 4-round related differentials characteristic in the first four rounds. From Theorem 4, with probability 2^{-189}, we have

$$R^6(P_0) \oplus R^6(P_0 \oplus \Delta x) \oplus R^6(P_0 \oplus \Delta x') \oplus R^6(P_0 \oplus \Delta x \oplus \Delta x') = 0. \tag{15}$$

Assume the following additional condition holds

$$\nu(R^7(P_0) \oplus R^7(P_0 \oplus \Delta x')) = \nu(R^7(P_0 \oplus \Delta x) \oplus R^7(P_0 \oplus \Delta x \oplus \Delta x')), \tag{16}$$

where $wt(\nu(R^7(P_0) \oplus R^7(P_0 \oplus \Delta x')) = 2$. In other words, it means that $SR^{-1} \circ MC^{-1}(C_0 \oplus C_2)$ is zero in two columns and that $SR^{-1} \circ MC^{-1}(C_1 \oplus C_3)$ is zero in exactly the same columns. The goal of this attack is to find candidates for this quartet by filtering output quartets exploiting the condition (16). Then, for each of candidates the condition (15) will be partially checked to recover some bytes of last-round key. And, by guessing the rest of bytes of last-round key, it will be checked that the quartet conforms the 7-round differential characteristics.

We first need to evaluate the probability that the condition (16) holds. Since two diagonals in the difference $R^4(P_0) \oplus R^4(P_0 \oplus \Delta x')$ are non-zero, see (11). Then, in order to satisfy (16), two diagonals in the difference $R^5(P_0) \oplus R^5(P_0 \oplus \Delta x')$ should be zero which means that four bytes in this difference should be zero. Therefore, two columns in the difference $R^6(P_0) \oplus R^6(P_0 \oplus \Delta x')$ equal zero. Also, from (15), we know that

$$R^6(P_0) \oplus R^6(P_0 \oplus \Delta x') = R^6(P_0 \oplus \Delta x) \oplus R^6(P_0 \oplus \Delta x \oplus \Delta x').$$

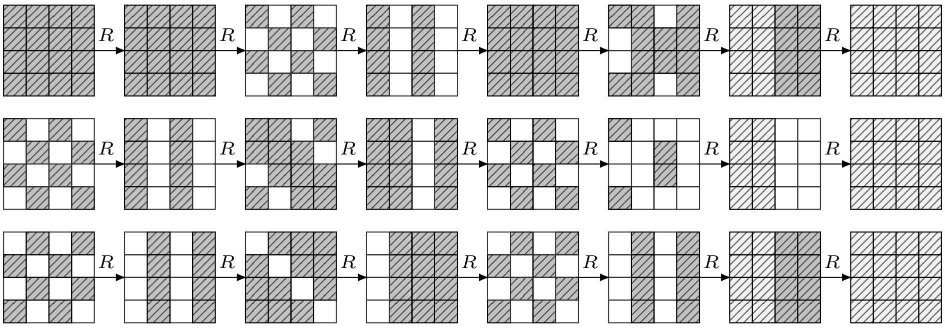

Figure 4: 7-round differential trails starting with Δx,$\Delta x'$ and $\Delta x \oplus \Delta x'$ respectively. A white cell indicates that the state difference is zero for that bytes. Both darker and lighter line pattern cell indicate that the state difference is non-zero in the cell while darker one also indicates the value of difference in a cell equal to the value of one of other two differences in the same cell.

It then means that two columns in the difference $R^6(P_0 \oplus \Delta x) \oplus R^6(P_0 \oplus \Delta x \oplus \Delta x')$ equal zero. Equivalently, two columns in the difference $R^6(P_0) \oplus R^6(P_0 \oplus \Delta x)$ equal the two corresponding columns in the difference $R^6(P_0) \oplus R^6(P_0 \oplus \Delta x \oplus \Delta x')$.

Therefore, the condition $wt(\nu(R^7(P_0) \oplus R^7(P_0 \oplus \Delta x')) = 2$ happens when any two diagonals in this difference $R^5(P_0) \oplus R^5(P_0 \oplus \Delta x')$ are zero, i.e four bytes are zero. This happens with probability $\binom{4}{2} \cdot 2^{-4 \cdot 8} \approx 2^{-29.4}$, $\binom{4}{2}$ possible cases that two diagonals are zero. So, in total, an input quartet $(P_0, P_0 \oplus \Delta x, P_0 \oplus \Delta x', P_0 \oplus \Delta x \oplus \Delta x')$ satisfies the two conditions (15) and (16) with probability $2^{-189} \cdot 2^{-29.4} = 2^{-218.4}$. On the other hand, for a random output quartet (C_0, C_1, C_2, C_3), the probability that $SR^{-1} \circ MC^{-1}(C_0 \oplus C_2)$ is zero in two columns, eight bytes, is $\binom{4}{2} \cdot 2^{-8 \cdot 8} \approx 2^{-61.4}$, $\binom{4}{2}$ possible cases that two columns are zero. And, the probability that $SR^{-1} \circ MC^{-1}(C_1 \oplus C_3)$ is zero in the exact same columns as $SR^{-1} \circ MC^{-1}(C_0 \oplus C_2)$ is 2^{-64}. Therefore, the probability that such random output quartet satisfies the condition (16) is $2^{-61.4} \cdot 2^{-64} = 2^{-125.4}$.

5.1 Data collection

To generate one input quartet $(P_0, P_0 \oplus \Delta x, P_0 \oplus \Delta x', P_0 \oplus \Delta x \oplus \Delta x')$ conforming the 7-round characteristic where P_0 is a random plaintext and all diagonals in Δx are non-zero and two non-consecutive diagonals in $\Delta x'$ are zero, we pick two random subsets A_0 and A_1 of $\mathbb{F}_{2^8}^8$, each of size m. Then we generate all m^2 possible plaintexts from these two sets where the first and third diagonals take the possible elements from the set A_0 and the second and last diagonals take the possible elements from the set A_1. Note that, from each set, we can generate $\binom{m}{2}$ unique combinations of pairs. Then the number of unique quartets generated from this set, $A = A_0 \oplus A_1$, is $\binom{m}{2} \cdot \binom{m}{2}$ (see [BR19a, Theorem 2] for more details, assume there are only two sets). If we set $m = 2^{55.1}$, we can prepare $2^{109.2} \cdot 2^{109.2} = 2^{218.4}$ such quartets. The expected number of quartets conforming the 7-round characteristic of Figure 4 equals one.

5.2 Search for double collisions

Among $2^{218.4}$ quartets, the expected number of quartets satisfying the condition (16) is given by

$$2^{218.4-125.4} = 2^{93}.$$

We can find them, using hash tables as follows. We know that both pairs $(P_0, P_0 \oplus \Delta x')$ and $(P_0 \oplus \Delta x, P_0 \oplus \Delta x \oplus \Delta x')$, which should satisfy the condition (16), are differed in $\Delta x'$

$$P_0 \oplus (P_0 \oplus \Delta x') = \Delta x' = (P_0 \oplus \Delta x) \oplus (P_0 \oplus \Delta x \oplus \Delta x'). \tag{17}$$

We also know that the set of plaintexts A is formed by spanning the first and third diagonals with the possible elements from A_0 and the rest of diagonals with elements from A_1. In order to find two pairs that satisfy the condition (16), we first search for plaintext pairs, which differ in $\Delta x'$, such that their corresponding ciphertext pairs differ in two columns before the last linear layer. Since we can generate $2^{109.2}$ combinations of pairs from A_0 and there are $2^{55.1}$ elements in A_1, the expected number of remaining pairs equals $2^{55.1} \cdot 2^{109.2-64} = 2^{100.3}$. Therefore, it requires $2^{110.2}$ table look ups in the ciphertexts table, using a hash table.

We now want to generate pairs of pairs (quartets) from $2^{100.3}$ remaining pairs such that they satisfy the condition (16). Notice that not all possible pairs of pairs, $2^{199.6}$ quartets, are our desired input quartets. In other words, we are interested in pairs of pairs which satisfy (17). Also, notice that the plaintexts $P_0 \oplus \Delta x'$ and $P_0 \oplus \Delta x \oplus \Delta x'$ are generated by exchanging two diagonals between P_0 and $P_0 \oplus \Delta x$. Thus, in order to filter these undesired input quartets, we insert $2^{100.3}$ remaining pairs in a hash table indexed by $\Delta x'$, i,e. $2^{109.2}$ possible combinations of pairs from A_0. So, we find quartets which satisfy the conditions (16) and (17) simultaneously. It is expected that $2^{199.6-109.2} = 2^{90.4}$ input quartets are found. And, by repeating this for all possible cases where two columns in the difference $R^7(P_0) \oplus R^7(P_0 \oplus \Delta x')$ are zero, $\binom{4}{2} = 6$ cases, we find $6 \cdot 2^{90.4} = 2^{93}$ quartets which satisfy the condition (16) and (17). This part requires $6 \cdot 2 \cdot 2^{100.3}$ table look ups in the ciphertexts table.

5.3 Retrieving key candidates

We now check partially the condition (15) for each remaining quartet. W.l.o.g., we assume that the first two columns of $R^6(P_0) \oplus R^6(P_0 \oplus \Delta x')$ are non-zero and the last two columns equal zero, which we already checked for the condition (16). Now we should check that

$$R^6(P_0) \oplus R^6(P_0 \oplus \Delta x) \oplus R^6(P_0 \oplus \Delta x') \oplus R^6(P_0 \oplus \Delta x \oplus \Delta x') = 0,$$

considering only the first two columns of each state. Let us denote the last-round key by k_7. We assume that the last SR and MC, and AK are swapped. It then means that an equivalent round-key $u_7 = SR^{-1}(MC^{-1}(k_7))$ is xored with data before the last SR and MC. For each (C_0, C_1, C_2, C_3), assuming that we already applied $SR^{-1} \circ MC^{-1}$ to all ciphertexts, we guess byte i of u_7^i and check

$$s^{-1}(C_0^i \oplus u_7^i) \oplus s^{-1}(C_1^i \oplus u_7^i) \oplus s^{-1}(C_2^i \oplus u_7^i) \oplus s^{-1}(C_3^i \oplus u_7^i) = 0, \tag{18}$$

for $i = \{0, 1, 2, ..., 7\}$ (all bytes placed in the first two columns) where s^{-1} is the inverse of the AES Sbox and C_j^i denotes byte i of C_j. We then expect that there is a key candidate for 8 bytes of u_7, for each quartet. Now we check that each of the first and second diagonal in the differences $R^5(P_0) \oplus R^5(P_0 \oplus \Delta x')$ and $R^5(P_0) \oplus R^5(P_0 \oplus \Delta x \oplus \Delta x')$ contains only two active bytes since we computed the first two columns of the differences $R^6(P_0) \oplus R^6(P_0 \oplus \Delta x')$ and $R^6(P_0) \oplus R^6(P_0 \oplus \Delta x \oplus \Delta x')$. This is a 64-bit filtering, 32-bit filtering by checking the condition on each difference $R^5(P_0) \oplus R^5(P_0 \oplus \Delta x')$ and $R^5(P_0) \oplus R^5(P_0 \oplus \Delta x \oplus \Delta x')$. Then, the expected number of quartets satisfying this condition equals $2^{93-32-32} = 2^{29}$.

In the first step, for each remaining quartet, it requires four table look ups in s^{-1} for each key candidates, u_7^i. We check eight bytes of u_7 so this step needs $4 \cdot 8 \cdot 2^8$ table look ups in s^{-1}. In the second step, after eight bytes of u_7^i are computed, we need to decrypt partially the first two diagonals of $R^{-2}(C_i)$ for all four ciphertexts in the quartet. So this step requires $4 \cdot 8$ table look ups in s^{-1}. Therefore, these two steps can be done by

$$2^{93}(4 \cdot 8 \cdot 2^8 + 4 \cdot 8) \approx 2^{106}$$

table look ups in s^{-1}. The rest of bytes of u_7 are recovered with an exhaustive search for 2^{29} quartets, which takes $2^{29} \cdot 2^{64} = 2^{93}$ 7-round encryption. Therefore, the data complexity of the attack is $2^{110.2}$ chosen plaintexts, the memory complexity is $2^{110.2}$ 128-bit blocks, and the time complexity is dominated by encrypting the plaintexts. And, this attack is independent of the AES key-schedule since only last round-key is recovered during the attack.

References

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST), FIPS PUB 197, U.S. Department of Commerce, November 2001.

[Bar19] Navid Ghaedi Bardeh. 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.

[BDK+18] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved key recovery attacks on reduced-round AES with practical data and memory complexities. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 185–212. Springer, Heidelberg, August 2018.

[BLNS18] Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder. Making the impossible possible. *Journal of Cryptology*, 31(1):101–133, January 2018.

[BR19a] Navid Ghaedi Bardeh and Sondre Rønjom. The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 347–370. Springer, Heidelberg, December 2019.

[BR19b] Navid Ghaedi Bardeh and Sondre Rønjom. Practical attacks on reduced-round AES. In Johannes Buchmann, Abderrahmane Nitaj, and Tajje eddine Rachidi, editors, *AFRICACRYPT 19*, volume 11627 of *LNCS*, pages 297–310. Springer, Heidelberg, July 2019.

[DFJ13] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved key recovery attacks on reduced-round AES in the single-key setting. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 371–387. Springer, Heidelberg, May 2013.

[DKRS20] Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. The retracing boomerang attack. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 280–309. Springer, Heidelberg, May 2020.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 158–176. Springer, Heidelberg, December 2010.

[DR98] Joan Daemen and Vincent Rijmen. The block cipher rijndael. In Jean-Jacques Quisquater and Bruce Schneier, editors, *Smart Card Research and Applications, This International Conference, CARDIS '98, Louvain-la-Neuve, Belgium, September 14-16, 1998, Proceedings*, volume 1820 of *Lecture Notes in Computer Science*, pages 277–284. Springer, 1998.

[DR09] Joan Daemen and Vincent Rijmen. New criteria for linear maps in aes-like ciphers. *Cryptogr. Commun.*, 1(1):47–69, 2009.

[Gil14] Henri Gilbert. A simplified representation of AES. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 200–222. Springer, Heidelberg, December 2014.

[Gra18] Lorenzo Grassi. Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced AES. *IACR Trans. Symm. Cryptol.*, 2018(2):133–160, 2018.

[GRR17] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A new structural-differential property of 5-round AES. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 289–317. Springer, Heidelberg, April / May 2017.

[LDKK08] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New impossible differential attacks on AES. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT 2008*, volume 5365 of *LNCS*, pages 279–293. Springer, Heidelberg, December 2008.

[LP21] Gaëtan Leurent and Clara Pernot. New representations of the AES key schedule. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 54–84. Springer, Heidelberg, October 2021.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 217–243. Springer, Heidelberg, December 2017.

A Related differentials on reduced-round AES

A.1 3-round related differentials

Let us now consider an input quartet $(\alpha, \alpha \oplus \Delta x, \alpha \oplus \Delta x', \alpha \oplus \Delta x \oplus \Delta x')$

$$\alpha = \begin{bmatrix} \alpha_0 & 0 & 0 & 0 \\ 0 & \alpha_5 & 0 & 0 \\ 0 & 0 & \alpha_{10} & 0 \\ 0 & 0 & 0 & \alpha_{15} \end{bmatrix}, \qquad \Delta x = \begin{bmatrix} \Delta x_0 & 0 & 0 & 0 \\ 0 & \Delta x_5 & 0 & 0 \\ 0 & 0 & \Delta x_{10} & 0 \\ 0 & 0 & 0 & \Delta x_{15} \end{bmatrix},$$

$$\Delta x' = \begin{bmatrix} \Delta x_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \Delta x_{10} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad \Delta x \oplus \Delta x' = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \Delta x_5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \Delta x_{15} \end{bmatrix},$$

where Δx and $\Delta x'$ are related differences. This quartet conforms the differential characteristics depicted in Figure 5 with probability of $4 \cdot 2 \cdot 2^{-24} \cdot 2^{-96} = 2^{-117}$.

$$\xrightarrow[-24]{F}\begin{bmatrix}2\lambda_0 & 0 & 0 & 0\\ \lambda_0 & 0 & 0 & 0\\ \lambda_0 & 0 & 0 & 0\\ 3\lambda_0 & 0 & 0 & 0\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}5\lambda_0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 4\lambda_0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}\xrightarrow[-32]{G}\begin{bmatrix}5\gamma_0 & 0 & 4\gamma_2 & 0\\ 0 & 4\gamma_1 & 0 & 5\gamma_3\\ 4\gamma_0 & 0 & 5\gamma_2 & 0\\ 0 & 5\gamma_1 & 0 & 4\gamma_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}E\gamma_0 & 9\gamma_1 & D\gamma_2 & B\gamma_3\\ 9\gamma_0 & D\gamma_1 & B\gamma_2 & E\gamma_3\\ D\gamma_0 & B\gamma_1 & E\gamma_2 & 9\gamma_3\\ B\gamma_0 & E\gamma_1 & 9\gamma_2 & D\gamma_3\end{bmatrix}$$

$$\xrightarrow[0]{F}\begin{bmatrix}2\lambda_0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ \lambda_0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}5\lambda_0 & 0 & 0 & 0\\ \lambda_0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 7\lambda_0 & 0 & 0 & 0\end{bmatrix}\xrightarrow[-64]{G}\begin{bmatrix}5\gamma_0 & \gamma_1 & 0 & 7\gamma_3\\ \gamma_0 & 0 & 7\gamma_2 & 5\gamma_3\\ 0 & 7\gamma_1 & 5\gamma_2 & \gamma_3\\ 7\gamma_0 & 5\gamma_1 & \gamma_2 & 0\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}E\gamma_0 & 0 & D\gamma_2 & 0\\ 0 & D\gamma_1 & 0 & E\gamma_3\\ D\gamma_0 & 0 & E\gamma_2 & 0\\ 0 & E\gamma_1 & 0 & D\gamma_3\end{bmatrix}$$

$$\xrightarrow[0]{F}\begin{bmatrix}0 & 0 & 0 & 0\\ \lambda_0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 3\lambda_0 & 0 & 0 & 0\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}0 & 0 & 0 & 0\\ \lambda_0 & 0 & 0 & 0\\ 4\lambda_0 & 0 & 0 & 0\\ 7\lambda_0 & 0 & 0 & 0\end{bmatrix}\xrightarrow[0]{G}\begin{bmatrix}0 & \gamma_1 & 4\gamma_2 & 7\gamma_3\\ \gamma_0 & 4\gamma_1 & 7\gamma_2 & 0\\ 4\gamma_0 & 7\gamma_1 & 0 & \gamma_3\\ 7\gamma_0 & 0 & \gamma_2 & 4\gamma_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}0 & 9\gamma_1 & 0 & B\gamma_3\\ 9\gamma_0 & 0 & B\gamma_2 & 0\\ 0 & B\gamma_1 & 0 & 9\gamma_3\\ B\gamma_0 & 0 & 9\gamma_2 & 0\end{bmatrix}$$

Figure 5: 3-round related differential trails starting with Δx, $\Delta x'$ and $\Delta x \oplus \Delta x'$ respectively. The probability (binary logarithm) of each map is indicated under the corresponding arrow. Function F is $SR \circ SB$.

A.2 4-round related differentials

Let us now consider an input quartet $(\alpha, \alpha \oplus \Delta x, \alpha \oplus \Delta x', \alpha \oplus \Delta x \oplus \Delta x')$

$$\alpha = \begin{bmatrix}\alpha_0 & \alpha_4 & \alpha_8 & \alpha_{12}\\ \alpha_1 & \alpha_5 & \alpha_9 & \alpha_{13}\\ \alpha_2 & \alpha_6 & \alpha_{10} & \alpha_{14}\\ \alpha_3 & \alpha_7 & \alpha_{11} & \alpha_{15}\end{bmatrix}, \qquad \Delta x = \begin{bmatrix}\Delta x_0 & 0 & \Delta x_8 & 0\\ 0 & \Delta x_5 & 0 & \Delta x_{13}\\ \Delta x_2 & 0 & \Delta x_{10} & 0\\ 0 & \Delta x_7 & 0 & \Delta x_{15}\end{bmatrix},$$

$$\Delta x' = \begin{bmatrix}\Delta x_0 & \Delta x_4 & 0 & \Delta x_{12}\\ \Delta x_1 & \Delta x_5 & \Delta x_9 & 0\\ 0 & \Delta x_6 & \Delta x_{10} & \Delta x_{14}\\ \Delta x_3 & 0 & \Delta x_{11} & \Delta x_{15}\end{bmatrix}, \qquad \Delta x \oplus \Delta x' = \begin{bmatrix}0 & \Delta x_4 & \Delta x_8 & \Delta x_{12}\\ \Delta x_1 & 0 & \Delta x_9 & \Delta x_{13}\\ \Delta x_2 & \Delta x_6 & 0 & \Delta x_{14}\\ \Delta x_3 & \Delta x_7 & \Delta x_{11} & 0\end{bmatrix},$$

where Δx and $\Delta x'$ are related differences. This quartet conforms the the differential characteristics depicted in Figure 6 with probability of 2^{-189}.

B 6-round distinguisher for AES

Theorem 3 in Section 3 can be used directly to set up a straightforward 6-round chosen-plaintext distinguisher for AES. Consider an input quartet $(P_0, P_0 \oplus \Delta x, P_0 \oplus \Delta x', P_0 \oplus \Delta x \oplus \Delta x')$ generated by two related differences Δx and $\Delta x'$ where P_0 is a random plaintext and all diagonals in Δx are non-zero and two non-consecutive diagonals in $\Delta x'$ are zero. And, let this input quartet map to (C_0, C_1, C_2, C_3) after 6-round AES encryption. By Theorem 3, with probability 2^{-94} we have

$$\nu(R^6(P_0) \oplus R^6(P_0 \oplus \Delta x')) = \nu(R^6(P_0 \oplus \Delta x) \oplus R^6(P_0 \oplus \Delta x \oplus \Delta x')). \qquad (19)$$

$$\xrightarrow[-32]{G}\begin{bmatrix}5\lambda_0 & 0 & 4\lambda_2 & 0\\ 0 & 4\lambda_1 & 0 & 5\lambda_3\\ 4\lambda_0 & 0 & 5\lambda_2 & 0\\ 0 & 5\lambda_1 & 0 & 4\lambda_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}E\lambda_0 & 9\lambda_1 & D\lambda_2 & B\lambda_3\\ 9\lambda_0 & D\lambda_1 & B\lambda_2 & E\lambda_3\\ D\lambda_0 & B\lambda_1 & E\lambda_2 & 9\lambda_3\\ B\lambda_0 & E\lambda_1 & 9\lambda_2 & D\lambda_3\end{bmatrix}\xrightarrow[-96]{G}\begin{bmatrix}2\gamma_0 & 3\gamma_1 & \gamma_2 & \gamma_3\\ \gamma_0 & 2\gamma_1 & 3\gamma_2 & \gamma_3\\ \gamma_0 & \gamma_1 & 2\gamma_2 & 3\gamma_3\\ 3\gamma_0 & \gamma_1 & \gamma_2 & 2\gamma_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}5\gamma_0 & 0 & 4\gamma_2 & 0\\ 0 & 5\gamma_1 & 0 & 4\gamma_3\\ 4\gamma_0 & 0 & 5\gamma_2 & 0\\ 0 & 4\gamma_1 & 0 & 5\gamma_3\end{bmatrix}$$

$$\xrightarrow[-64]{G}\begin{bmatrix}5\lambda_0 & \lambda_1 & 0 & 7\lambda_3\\ \lambda_0 & 0 & 7\lambda_2 & 5\lambda_3\\ 0 & 7\lambda_1 & 5\lambda_2 & \lambda_3\\ 7\lambda_0 & 5\lambda_1 & \lambda_2 & 0\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}E\lambda_0 & 0 & D\lambda_2 & 0\\ 0 & D\lambda_1 & 0 & E\lambda_3\\ D\lambda_0 & 0 & E\lambda_2 & 0\\ 0 & E\lambda_1 & 0 & D\lambda_3\end{bmatrix}\xrightarrow[0]{G}\begin{bmatrix}2\gamma_0 & 0 & \gamma_2 & 0\\ 0 & 2\gamma_1 & 0 & \gamma_3\\ \gamma_0 & 0 & 2\gamma_2 & 0\\ 0 & \gamma_1 & 0 & 2\gamma_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}5\gamma_0 & 7\gamma_1 & 0 & \gamma_3\\ \gamma_0 & 5\gamma_1 & 7\gamma_2 & 0\\ 0 & \gamma_1 & 5\gamma_2 & 7\gamma_3\\ 7\gamma_0 & 0 & \gamma_2 & 5\gamma_3\end{bmatrix}$$

$$\xrightarrow[0]{G}\begin{bmatrix}0 & \lambda_1 & 4\lambda_2 & 7\lambda_3\\ \lambda_0 & 4\lambda_1 & 7\lambda_2 & 0\\ 4\lambda_0 & 7\lambda_1 & 0 & \lambda_3\\ 7\lambda_0 & 0 & \lambda_2 & 4\lambda_3\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}0 & 9\lambda_1 & 0 & B\lambda_3\\ 9\lambda_0 & 0 & B\lambda_2 & 0\\ 0 & B\lambda_1 & 0 & 9\lambda_3\\ B\lambda_0 & 0 & 9\lambda_2 & 0\end{bmatrix}\xrightarrow[0]{G}\begin{bmatrix}0 & 3\gamma_1 & 0 & \gamma_3\\ \gamma_0 & 0 & 3\gamma_2 & 0\\ 0 & \gamma_1 & 0 & 3\gamma_3\\ 3\gamma_0 & 0 & \gamma_2 & 0\end{bmatrix}\xrightarrow[0]{MC}\begin{bmatrix}0 & 7\gamma_1 & 4\gamma_2 & \gamma_3\\ \gamma_0 & 0 & 7\gamma_2 & 4\gamma_3\\ 4\gamma_0 & \gamma_1 & 0 & 7\gamma_3\\ 7\gamma_0 & 4\gamma_1 & \gamma_2 & 0\end{bmatrix}$$

Figure 6: 4-round related differentials trails starting with Δx, $\Delta x'$ and $\Delta x \oplus \Delta x'$ respectively. The probability (binary logarithm) of each map is indicated under the corresponding arrow.

Now assume the following condition is given by

$$wt(\nu(R^6(P_0) \oplus R^6(P_0 \oplus \Delta x)) = 3 \tag{20}$$

It then means that $SR^{-1} \circ MC^{-1}(C_0 \oplus C_1)$ is zero in three columns and that $SR^{-1} \circ MC^{-1}(C_2 \oplus C_3)$ is zero in exactly the same columns. This condition happens with probability $4 \cdot 2^{-96} = 2^{-94}$. So, in total, (C_0, C_1, C_2, C_3) follows (20) and (19) with probability $2^{-94} \cdot 2^{-94} = 2^{-188}$. In the random case, however, the probability that a ciphertext quartet satisfies the conditions (20) and (19) simultaneously is $2^{-94} \cdot 2^{-96} = 2^{-190}$.

Similar to data collection in Subsection 5.1, we set $m = 2^{47.5}$ and we prepare 2^{188} different input quartets. For the AES case, the expected number of quartets that satisfy the conditions (20) and (19) equals one, while, at random, the expected number of quartets equals $2^{188-190} = 2^{-2}$. Thus, the data complexity of the 6-rounds distinguisher is $m^2 = 2^{95}$ chosen plaintexts.