New Impossible Differential Attacks on AES

Zheng Yuan[1,2] ⋆

[1] Beijing Electronic Science and Technology Institute, Beijing 100070,China
[2] Center for Advanced Study, Tsinghua University, Beijing 100084,China
yuanzheng@besti.edu.cn
zyuan@mail.tsinghua.edu.cn

Abstract. Some new near 5 rounds impossible differential properties of AES are first presented in this paper, in which active bytes of 1^{st} round or 5^{th} round are in different columns and in favor of extension. Additionally, we first propose the complexities expressions of an universal impossible differential attack, which can help us to rapidly search appropriate impossible differential paths. More importantly, our near 5 rounds impossible differential properties and complexities expressions lead to a series of new impossible differential attacks on 7 rounds AES-128, 7-9 rounds AES-192, and 8-12 rounds AES-256.
Keywords: AES, impossible differential properties, Impossible differential attacks.

1 Introduction

The Advanced Encryption Standard (AES)[8], designed by Joan Daemen and Vincent Rijmen, is a 128-bit block cipher with a variable key length(128, 192, and 256-bit keys are supported). Since adopted by NIST [13], AES has gradually become the most widely used block cipher. It has been widely used to protect secret data in both software and hardware applications, and to design other cryptographic primitives, for example, CBC-MAC and Alpha-MAC[17].

In the last ten years, AES has been subjected to very intensive cryptanalytic effort. There are some kinds of cryptanalysis on AES, including differential, linear, square, collision, impossible differential, related-key cryptanalyses, etc. In paper [8], it is proved that 4-round differential trails with a predicted prop ratio above 2^{-150} and 4-round linear trails with a correlation above 2^{-75} do not exist. What's more, it proved that there are no "square" attacks faster than exhaustive key search for 7 rounds or more of AES. In related-key attacks, the situation started to change from the spring of 2009, for Biryukov et al. found a series of keys recovery attacks on AES-256 and AES-192[3,4,5]. They, who first published attacks on the full AES-256 and AES-192 with time complexities of $2^{99.5}$ and 2^{176}, respectively[3], gave an attack on 9-round and 10-round AES-256 with practical

⋆ This work is supported by the Natural Science Foundation of Beijing (No.4102055), the Foundation of State Key Laboratory of Information Security (Institute of Software, Chinese Academy of Sciences)(No.01-01), and the Foundation of Key Laboratory of Information Security of BESTI(No.YZDJ0905)

complexities of 2^{32} and 2^{44}, respectively[5]. The security of AES against impossible differential attacks had been challenged in previous research[6,7,14,15,16]. Later, utilizing an almost same 4-round impossible differential property, an improved impossible differentials attacks on AES was presented[1,18]. Especially, the best results of AES-128 was proposed, which is attacking on 7-round AES-128 with $2^{115.5}$ data complexity and 2^{119} time complexity. In Paper [18], the better impossible differential attacks on 7-round AES-192 and 8-round AES-256 were also presented. The complexities of 7-round AES-192 were $2^{115.5}$ chosen plaintext (CP) pairs as well as 2^{119} time encrypting, and that of 8-round AES-256 were $2^{116.5}$ data complexity and $2^{247.5}$ time complexity. Recently, under the assumption that the (shifted) column with zero difference was fixed, the complexities in [1,16,18] were slightly improved by using a trivial sleight[11].

The main contributions of this paper are to present novel near 5 rounds impossible differential properties of AES and the complexities expressions of an universal impossible differential attack. In our new near 5 rounds impossible differential properties, the number of active bytes of the 1^{st} round or 5^{th} round can be 1,2 or 3, and the active bytes are in different columns and in favor of extension. In this paper, we sum up an universal impossible differential attack on AES and first give the formal expressions of their complexities, which can help us to rapidly search appropriate impossible differential paths. More importantly, utilize our near 5 rounds impossible differential properties and complexities expressions can obtain the best results of impossible differential attacks on AES-128/192/256. Table 2 shows some of our results of impossible differential attacks on AES-192/256, our result can be improved by lu's method.[11].

Up to now, the impossible differential attacks on 7-round AES-128 are the best known attacks. Besides impossible differential attacks, there exist two marginal attacks on 7-round AES-128[9,10] (ie., require nearly the entire codebook, or time complexity close to key exhaustive search), respectively using square attack and collision attack. In this paper, we add a new and non-marginal impossible differential attack on 7-round AES-128, as well as impossible differential attacks on more than 7-round AES-192 and more than 8-round AES-256. We summarize our results along with some previously known works in Table 1.

AES is an iterated block cipher, each iterated round applies four basic operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. Only MixColumn operation can change the number of active bytes, and the linear transformation of MixColumn has the characteristic: the sum of the number of active columns at its input and output is at least 5. Using this property and previous works[1,18], we find some new near 2.5-round difference trails with probability 1. Moreover, we first propose some near 5 rounds impossible differential properties. In these impossible differential properties, the number of active bytes of 1^{st} round and 5^{th} round can be 1,2 or 3, and active bytes are in different columns, so our impossible differential properties are easy to be extended.

The paper is organized as follows. In Section 2, we list the notations and Definitions used in this paper and give a brief description of the AES. Section 3 presents our universal impossible differential attacks methods. The impossible

differential properties of AES are described in Section 4. Some of our new impossible differential attacks on AES are presented in Section 5 and Section 6. Section 7 is our conclusions.

2 Backgrounds and Notations

In this section, we give a brief description of the AES, and define some notations.

2.1 A Brief Description of AES

AES is a 128-bit block cipher with square structure, and the length of secret key is 128 , 192 or 256 bits. A 128-bit data block of the AES is usually exhibited as an array of 4×4 bytes as shown in Fig. 1

The input plaintext block is passed through a iterated function, named encryp-

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

Fig. 1. 4×4 Byte coordinate of 128-bit AES data block

tion round function, 10 (respectively 12 or 14) times for 128-bit(respectively 192-bit or 256-bit) secret key. Each encryption round function consists of the four basic transformations in the following order:

- $SubBytes(SB)$: independently operate a non-linear byte substitution on each byte of the state using an 8×8 S-box.
- $ShiftRows(SR)$: cyclically shift left the bytes in the last three rows of the state with different numbers of bytes, i.e., one byte for the second row, two for the third row and three for the fourth row.
- $MixColumns(MC)$: multiply each column of the state with a fix matrix.
- $AddRoundKey(AK)$: an exclusive-or(XOR) of the data block with the round subkey.

Note that AK is applied before the first round and MC is excluded in the last round [8].

Similarly, the ciphertext block can be decrypted by decryption round functions, and each round functions is composed of the four basic inverse transformations: InvAddRoundKey(i.e. AddRoundKey), InvMixColumn, InvShiftRow, and InvSubByte.

There are two properties of inverse transformations: one is that the order of InvShiftRow and InvSubByte are indifferent, and the other is that the transformation sequence $AddRoundKey(S_i^r, K_r') \rightarrow InvMixColumn(S_{i+1}^r)$ can be

replaced by

$$InvMixColumn(S_i^r) \rightarrow AddRoundKey(S_{i+1}^r, {K'_r}^{-1}),$$

where ${K'_r}^{-1} = InvMixColumn(K'_r)$. So each decryption round function can be transformed into the following order:

- $InvSubBytes(SB^{-1})$: byte substitution is the inverse table of SubByte.
- $InvShiftRows(SR^{-1})$: only one difference from ShiftRows is shift right.
- $InvMixColumns(MC^{-1})$: a matrix multiplication with another different coefficients from MixColumns.
- $AddRoundKey(AK^{-1})$.

$AddRoundKey(S^0, K_0)$ is used before the first round as well, and InvMixColumns is rejected in the last round.[8].

2.2 Notations and Definitions

P	:	a plaintext $P = (p_0, p_1, \ldots, p_{15})$.
C	:	a ciphertext $C = (c_0, c_1, \ldots, c_{15})$.
$\mathbb{P}$	:	a special set of four bytes position of an AES state. After SR operation, the four bytes must be in one column. Obviously, $\mathbb{P} = \{(0, 5, 10, 15), (4, 9, 14, 3), (8, 13, 2, 7), (12, 1, 6, 11)\}$.
$\mathbb{Q}$	:	as well as a special set of four bytes position of an AES state. After SR^{-1} operation, the four bytes must be in one column. $\mathbb{Q} = \{(0, 13, 10, 7), (4, 1, 14, 11), (8, 5, 2, 15), (12, 9, 6, 3)\}$.
b	:	the set of some bytes, $b = (b_1, \ldots, b_i)$, $0 < i \leq 4$. If b is a subset of any element of $\mathbb{P}$, we say that $b \in \mathbb{P}$.
$S(b_i)$	:	the output of s-box when input is byte b_i.
r	:	the iterated times of an encryption (or decryption)round function.
K^r	:	the r^{th} round's 128-bit encrypting subkey, $K^r = (k_0^r, k_1^r, \ldots, k_{15}^r)$.
K_j^r	:	part bytes of the r^{th} round's subkey, $K_j^r \in K^r$, $(0 < j < 15)$.
S_B^r	:	the output state of SB at the r^{th} encryption round.
$S_{B^{-1}}^r$	:	the output state of SB^{-1} at the r^{th} decryption round.
S_R^r	:	the output state of SR at the r^{th} encryption round.
S_C^r	:	the output state of MC at the r^{th} encryption round.
S_K^r	:	the output state of AK at the r^{th} encryption round.
t	:	the number of the structures.
Pr^r	:	the probability of the output of MC^{-1} of the r^{th} decrypting round.
Pr_d	:	the data complexity.
Pr_t	:	the time complexity.
d_e	:	the number of left message pairs before eliminating wrong subkey values by the part initialization key $K^0_{z_f^P}$.
z_k	:	the number of bytes for the guessed subkeys.
z_f^P	:	the number of active bytes for the chosen plaintexts.
z_f^C	:	the number of fixed bytes for the ciphertexts.
Δx	:	the XOR difference of x and x'.

3 Impossible Differential Attacks

Impossible differential attacks use differentials that hold with probability 0 (or non-existing differentials) to eliminate wrong key material and leave the right key candidate. The majority of impossible differential attacks on AES make use of the extremely similar algorithms, which is named as an universal impossible differential attack methods in the paper. Here, we describe the universal impossible differential attack method, and first deduce the formal expressions of their complexities evaluation. These formulae will help us to choose appropriate impossible differential paths quickly.

3.1 universal Impossible Differential Attacks and their Complexities

Assume that there is a r_0-round impossible differentials property, then extend r_1 rounds differentials and r_2 rounds differentials at the bottom and the top, respectively. We can get $r = r_0 + r_1 + r_2$ rounds AES. Without losing the generality, we only discuss $r_2 \leq 1$. Impossible differential attacks on the r-round AES can be summarized as follows:

1. Defined a structure as a set of $2^{8\times z_f^P}$ plaintexts, which have fixed values in all but z_f^P bytes. There are about $2^{16\times z_f^P-1}$ plaintexts pairs in such a structure.
2. Randomly take t structures, and encrypt all plaintexts pairs using r-round AES. Only choose the pairs whose ciphertexts pairs are same except z_f^C bytes in the appointed positions. The expected number of such pairs is $t \times 2^{16\times z_f^P-1-8\times z_f^C}$.
3. Guess some subkeys of last r_1 rounds, and suppose that z_k bytes be guessed. Decrypt the chosen pairs r_1 rounds using the guessed bytes ($K_{j_1}^{r_0+r_1+r_2}$, $K_{j_2}^{r_0+r_1+r_2-1}, \ldots, K_{j_3}^{r_0+r_2}$), $(j_1 + j_2 + j_3 = z_k)$. Only select pairs, at the output of MC^{-1} of the r_1^{th} round, whose differentials correspond to the output of the r_0-round impossible differentials property. If the probability of each decryption round is $Pr^{r_1}, Pr^{r_1-1}, \ldots, Pr^1$, respectively, the excepted number of remained pairs is $d_e = t \times 2^{16\times z_f^P-1-8\times z_f^C} \times Pr^{r_1} \times \ldots \times Pr^1$.
4. Eliminate wrong z_f^P bytes $K^0_{z_f^P} = (k^0_{a_1}, k^0_{a_2}, \ldots, k^0_{a_{z_f^P}}) \in K^0$,$(0 < a_1, a_2, \ldots, a_{z_f^P} < 16)$ by showing that the impossible differential property holds if these bytes are used in this step.
   (a) Precomputation:
      i. If $r_1 = 1$,, then for the state S^1_K, give all 2^m possible differences pairs (x, x_0), which meet the input of the r_0-round impossible differential property. For these pairs, perform orderly MC^{-1}, SR^{-1} and SB^{-1}, respectively, then obtain the output pairs $(S^1_{B^{-1}}, S'^1_{B^{-1}})$. Compute their difference $\Delta S^1_{B^{-1}}$. In all, there are $2^{8\times z_f^P}$ output difference values. On average, about $2^{m-8\times z_f^P}$ pairs (x, x_0) correspond to one value $\Delta S^1_{B^{-1}}$.

ii. If $r_1 = 0$, give all 2^m possible differences pairs (x, x_0), which meet the input of the r_0-round impossible differential property. In all, there are $2^{8\times z_f^P}$ difference values ΔS_K^0. On average, about $2^{m-8\times z_f^P}$ pairs (x, x_0) correspond to one value ΔS_K^0.

(b) Give a hash table H, which contain $\Delta S_{B^{-1}}^1$ and its corresponding values $S_{B^{-1}}^1$.

(c) For each remained pair in step 3, compute corresponding plaintext difference $P \oplus P' = (P \oplus K_{z_f^P}^0) \oplus (P' \oplus K_{z_f^P}^0) = \Delta S_{B^{-1}}^1$, check the hash table H, and obtain corresponding values $S_{B^{-1}}^1$.

(d) Initialize a list A, which contains all $2^{8\times z_f^P}$ possible values $K_{z_f^P}^0$. Compute a wrong value $K_{z_f^P}^{0'} = S_{B^{-1}}^1 \oplus P$, and eliminate it from A. At least one of $K_{z_f^P}^0$ is remained with probability $Pr_{K_{z_f^P}^0}^e = 2^{8\times z_f^P} \times (1 - \frac{2^{m-8\times z_f^P}}{2^{8\times z_f^P}})^{d_e}$.

(e) For all guessed z_k subkeys $(K_{j_1}^{r_0+r_1+r_2}, K_{j_2}^{r_0+r_1+r_2-1}, \ldots, K_{j_{r_1}}^{r_0+r_2})$, $(j_1 + j_2 + \ldots + j_{r_1} = z_k)$, the wrong value remains with probability

$$Pr_K^e = 2^{8\times(z_k+z_f^P)} \times (1 - \frac{2^{m-8\times z_f^P}}{2^{8\times z_f^P}})^{d_e} \approx 2^{8\times(z_k+z_f^P)} \times e^{-2^{-(16\times z_f^P - m)}d_e},$$

when Pr_K^e is very small, the false $K_{z_f^P}^0$ can be eliminated with very high probability. So if a value $K_{z_f^P}^0$ is remained, the guessed z_k-byte of subkeys are correct with high probability.

According to paper[1], let $Pr_K^e \approx 2^{-19}$, the number of chosen structures

$$t = \frac{2^{\frac{log_{10}^{(19+8\times(z_k+z_f^P))\times log_e^2}}{log_{10}^2} + 1 + 8\times z_f^C - m}}{Pr^{r_1} \times Pr^{r_1-1} \ldots Pr^1}. \quad (1)$$

Complexity Evaluation. Let $Pr^{r_1} = 2^{-pr_{r_1}}$, $Pr^{r_1-1} = 2^{-pr_{r_1-1}}, \ldots,$ $Pr^1 = 2^{-pr_1}$, the date complexity is

$$Pr_d = 2^{z_f^P} \times t = 2^{\frac{log_{10}^{(19+8\times(z_k+z_f^P))\times log_e^2}}{log_{10}^2} + 1 + 8\times(z_f^C + z_f^P) - m + pr_{r_1} + pr_{r_1-1} + \cdots}. \quad (2)$$

The time complexity Pr_t is changed according to the impossible differential paths. Here we can give a reference.

If having two nonzero differences bytes in the last round of impossible differential property, such as Type 1, then $Pr_t \leq 2^{\frac{log_{10}^{(19+8\times(z_k+z_f^P))\times log_e^2}}{log_{10}^2} + 8\times z_k + 16\times z_f^P - m + 31}$;

If having 3 nonzero differences bytes in the last round of impossible differential property, such as Type 2, then $Pr_t \leq 2^{\frac{log_{10}^{(19+8\times(z_k+z_f^P))\times log_e^2}}{log_{10}^2} + 8\times z_k + 16\times z_f^P - m + 33}$.

4 Some Important Properties of AES

Some new near 2.5-round difference paths of AES are given in this section, which result in a series of novel near 5-round impossible differential properties of AES. The advantage of the near 5-round impossible differential properties is easier to be extended.

4.1 Near 2.5-round Difference Paths of AES

We propose some new near 2.5-round differential trails. Combining these near 2.5-round differential trails with other $2-3$ rounds differential trails [2,8], some novel 5-round impossible differential properties of AES will be exhibited, subsequently.

Fact1: Given a plaintext pair (P, P') whose all bytes are fixed except two bytes

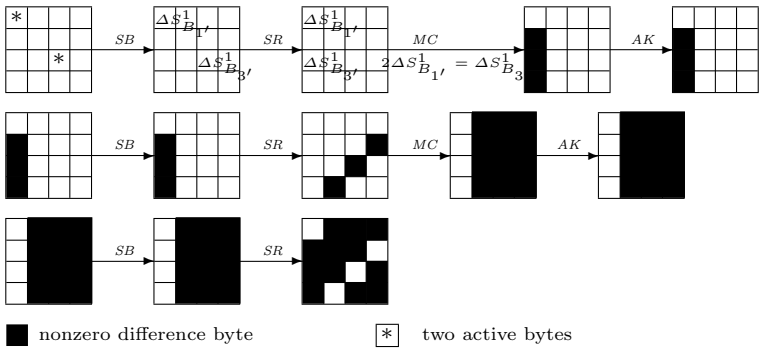

Fig. 2. Near 2.5-round differential path with two difference bytes in $(b_1, b_3) \in P$

$(b_i, b_j) \in \mathbb{P}, (1 \le i, j \le 4)$. After the SB operation of the 1^{st} round, if differences $(\Delta S^1_{B_{i'}}, \Delta S^1_{B_{j'}})$=$(S(b_i) \oplus S(b'_i), S(b_j) \oplus S(b'_j))$ satisfy some special conditions, then at the output of MC of the 2^{rd} round, it holds with probability 1 that one column is fixed with four zero difference bytes, and each of the other three columns is active with four nonzero difference bytes. Especially, once the condition is determinate, so is the site of the fixed column. There is no differences propagation until the output of SR of the 3^{rd} round.

Assume that $i = 1, j = 3$, $(b_1, b_3) \in \mathbb{P}$, there are four cases as follows:

Case 1: If $2\Delta S^1_{B_{1'}} = \Delta S^1_{B_{3'}}$, only the column 0 is fixed with probability 1. See Fig 2.

Case 2: If it is satisfied that $\Delta S^1_{B_{1'}} = 3\Delta S^1_{B_{3'}}$, then only the column 1 is fixed with probability 1.

Case 3: If $\Delta S^1_{B_{1'}} = 2\Delta S^1_{B_{3'}}$, only the column 2 is fixed with probability 1..

Case 4: If $3\Delta S^1_{B_{1'}} = \Delta S^1_{B_{3'}}$, only the column 3 is fixed with probability 1.

Proof. The proof of Fact 1 is obvious. $(b_i, b_j) \in P$, according to the definition in Section 2.2, their output differences of SR of 1^{st} round are in one column. For example, in Fig.2, differences of MC of 1^{st} round can be computed by

$$\begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \cdot \begin{pmatrix} \Delta S^1_{B_{1'}} \\ 0 \\ \Delta S^1_{B_{3'}} \\ 0 \end{pmatrix}$$

if $2\Delta S^1_{B_{1'}} = \Delta S^1_{B_{3'}}$, then $2\Delta S^1_{B_{1'}} \oplus 3{\cdot}0 \oplus \Delta S^1_{B_{3'}} \oplus 1{\cdot}0 = 0$. It holds with probability 1 that the 1^{st} byte difference is zero. The zero difference byte deduces four zero difference bytes in column 0 at the output of MC of the 2^{nd} round. Only MC operation produces difference propagate, so there is no differences propagation until the output of SR of the 3^{rd} round.

The proofs of other cases are similar. □

Remark 1: In the paper, the black boxes refer to nonzero difference (active) bytes while the white boxes denote the equal(fixed) bytes.
Remark 2: Assume that $i = 1, j = 2$, $(b_1, b_2) \in \mathbb{P}$, then there are another four cases, i.e., if $2\Delta S^1_{B_{1'}} = 3\Delta S^1_{B_{2'}}$, the columns 0 is fixed with probability 1; if $\Delta S^1_{B_{1'}} = 2\Delta S^1_{B_{2'}}$, the columns 1 is fixed with probability 1 ; if $\Delta S^1_{B_{1'}} = \Delta S^1_{B_{2'}}$, the columns 2 is fixed with probability 1 ; if $3\Delta S^1_{B_{1'}} = \Delta S^1_{B_{2'}}$, the columns 3 is fixed with probability 1.
Remark3: The number of the elements of set $\mathbb{P}$ is 4, and each element has 4 positions, so $4 \times C_4^2 = 24$; one $(b_i, b_j) \in \mathbb{P}$ produces 4 near 2.5-round differential paths. In all, there is 96 near 2.5-round differential paths in Fact 1.

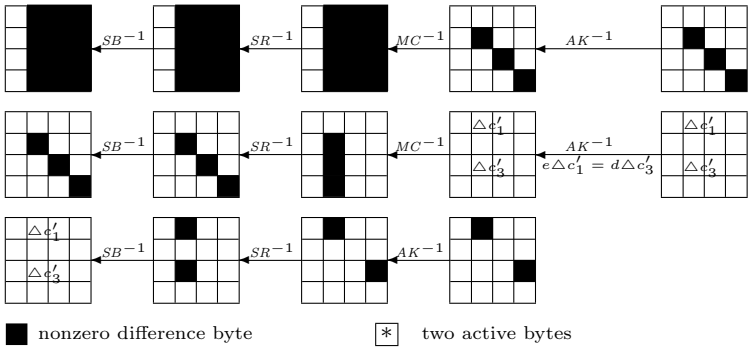

Fig. 3. Near 2.5-Round differential path with two difference bytes in $(c_1, c_3) \in Q$

Fact 2: Given a ciphertext pair (C, C') whose all bytes are fixed except two bytes $(c_i, c_j) \in \mathbb{Q}, (1 \le i, j \le 4)$. After the output of SB^{-1} of the 1^{st} round, if the two nonzero differences $(\Delta S^1_{B^{-1}_{i'}}, \Delta S^1_{B^{-1}_{j'}}) = (S^{-1}(c_i) \oplus S^{-1}(c'_i), S^{-1}(c_j) \oplus S^{-1}(c'_j))$

satisfy some special conditions, then at the output of MC^{-1} of the 2^{rd} round, it holds with probability 1 that one column is fixed with four zero difference bytes, and each of other three columns are active with four nonzero difference bytes. Especially, once the condition is confirmed, so does the site of the fixed columns. There is no differences propagation until the output of SR^{-1} of the 3^{rd} round. Assume that two active bytes be $(c_1, c_3) \in \mathbb{Q}$, Then at the output of MC^{-1} of the 2^{rd} round, it holds with probability 1 that one column is fixed and the other three columns are active. There are four cases as follows:
Case 1: If $e \cdot \Delta S^1_{B^{-1}_{1'}} = d \cdot \Delta S^1_{B^{-1}_{3'}}$, only the column 0 is fixed. let $\Delta S^1_{B^{-1}_{1'}} = \Delta c'_1$, $\Delta S^1_{B^{-1}_{3'}} = \Delta c'_3$, Fig. 3 shows its near 2.5-round decrypting differential path.
Case 2: If $9 \cdot \Delta S^1_{B^{-1}_{1'}} = b \cdot \Delta S^1_{B^{-1}_{3'}}$, the column 1 is fixed .
Case 3: If $d \cdot \Delta S^1_{B^{-1}_{1'}} = e \cdot \Delta S^1_{B^{-1}_{3'}}$, the column 2 is fixed.
Case 4: If $b \cdot \Delta S^1_{B^{-1}_{1'}} = 9 \cdot \Delta S^1_{B^{-1}_{3'}}$, then the column 3 is fixed.

Proof. The proof of Fact 2 is similar to that of Fact 1. For example Fig.3, we only need to make $e \cdot \Delta S^1_{B^{-1}_{1'}} \oplus b \cdot 0 \oplus d \cdot \Delta S^1_{B^{-1}_{3'}} \oplus 9 \cdot 0 = 0$ replace $2 \cdot \Delta S^1_{B_{1'}} \oplus 3 \cdot 0 \oplus 1 \cdot \Delta S^1_{B_{3'}} \oplus 1 \cdot 0 = 0$ in Fig.2. □

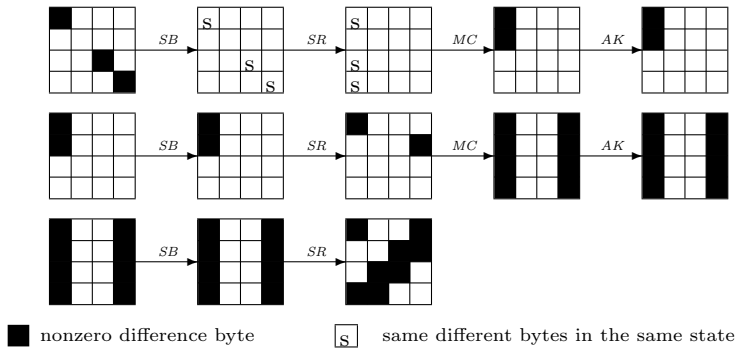

Fig. 4. near 2.5-Round Differential Path with Three Active Bytes

Fact 3: Given a plaintext pair (M, M') whose all bytes are fixed except three bytes $(b_i, b_j, b_k) \in \mathbb{P}, (1 \le i, j, k \le 4)$. After the output of SB of the 1^{st} round, if $\Delta S^1_{B_{i'}} = \Delta S^1_{B_{j'}} = \Delta S^1_{B_{k'}}$, then at the output of MC of the 2^{rd} round, it is satisfied with probability 1 that two columns are fixed and the other two columns are active . Especially, once the sites of three difference bytes $(b'_i, b'_j, b'_k) \in \mathbb{P}$ are determinate, so are the sites of two fixed columns. There is no differences propagation until the output of SR of the 3^{rd} round. For example, if the three active bytes are in position (0,10,15), the near 2.5-round differential path can be

seen in Fig.4.

Proof. Let $\Delta S^1_{B_{i'}} = \Delta S^1_{B_{j'}} = \Delta S^1_{B_{k'}} = \gamma$. The difference bytes are in one column at the output of the 1^{st} SR operation, as shown in Fig.4, the output difference of MC of the 1^{st} round in column 0 can be computed as follows:

$$\begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \cdot \begin{pmatrix} \gamma \\ 0 \\ \gamma \\ \gamma \end{pmatrix} = \begin{pmatrix} \gamma \\ \gamma \\ 0 \\ 0 \end{pmatrix}$$

If zero difference byte multiplies coefficient 01, we have $02 \cdot \gamma \oplus 03 \cdot \gamma \oplus 01 \cdot \gamma = 0$. In coefficient matrix, each row has two coefficients 01, which means two zero differences bytes in one column. After MC operation of the 2^{nd} round, in all, there are eight nonzero differences bytes in two columns. Only MC operation can produce difference propagation, so there is no differences propagation until the output of SR of the 3^{rd} round. □

Fact 4: Given a ciphertext pair (C, C') whose all bytes are fixed except three bytes $(c_i, c_j, c_k) \in \mathbb{Q}, (1 \leq i, j, k \leq 4)$. After the output of SB^{-1} of the 1^{st} round, if $(\Delta S^1_{B^{-1}_{i'}}, \Delta S^1_{B^{-1}_{j'}}, \Delta S^1_{B^{-1}_{k'}})$ satisfy some special conditions, then at the output of MC^{-1} of the 2^{rd} round, at least one column is fixed with probability 1. Especially, once the condition is determined, so do the number and the sites of fixed columns. There is no differences propagation until the output of SR^{-1} of the 3^{rd} round.

Assume that $i = 1, j = 3, k = 4$, and three active bytes are $(c_1, c_3, c_4) \in \mathbb{Q}$. At the output of MC^{-1} of the 2^{rd} round, if we want at least one column fixed with probability 1, there are four cases. The details are as follows:
Case 1: If $e \cdot \Delta S^1_{B^{-1}_{1'}} = d \cdot \Delta S^1_{B^{-1}_{3'}} \oplus 9 \cdot \Delta S^1_{B^{-1}_{4'}}$, then at least the column 0 is fixed. Among all $(2^8 - 1)^3 \approx 2^{24}$ values $(\Delta S^1_{B^{-1}_{1'}}, \Delta S^1_{B^{-1}_{3'}}, \Delta S^1_{B^{-1}_{4'}})$, about $(2^8 - 1) \cdot (2^8 - 2) \approx 2^{16}$ values fulfil the condition 1, so the probability is 2^{-8}.
Case 2: If $9 \cdot \Delta S^1_{B^{-1}_{1'}} = b \cdot \Delta S^1_{B^{-1}_{3'}} \oplus d \cdot \Delta S^1_{B^{-1}_{4'}}$, then at least the column 1 is fixed. Similarly, about 2^{16} values hold the condition 2.
Case 3: If $d \cdot \Delta S^1_{B^{-1}_{1'}} = e \cdot \Delta S^1_{B^{-1}_{3'}} \oplus b \cdot \Delta S^1_{B^{-1}_{4'}}$, at least the column 2 is fixed, 2^{16} values meet this condition.
Case 4: If $b \cdot \Delta S^1_{B^{-1}_{1'}} = 9 \cdot \Delta S^1_{B^{-1}_{3'}} \oplus e \cdot \Delta S^1_{B^{-1}_{4'}}$, then at least the column 3 is fixed. 2^{16} values satisfy the condition 4.

Proof. The proof of Fact 4 is similar to that of Fact 1 and Fact 3. □

4.2 Near 5-round impossible differential property of AES

In this section, we present three kinds near 5-round impossible differential properties of AES. By reversing the two parts of the difference paths or by changing

positions of difference bytes, it is easy to obtain new impossible differential properties, Here we no longer describe the details.

Type 1: If messages pairs (M, M') satisfy Fact 1 or Fact 2, they have near 5-round impossible differential property illustrated in Fig.5.

Type 2: If messages pairs (M, M') satisfy Fact 3 or Fact 4, they hold near

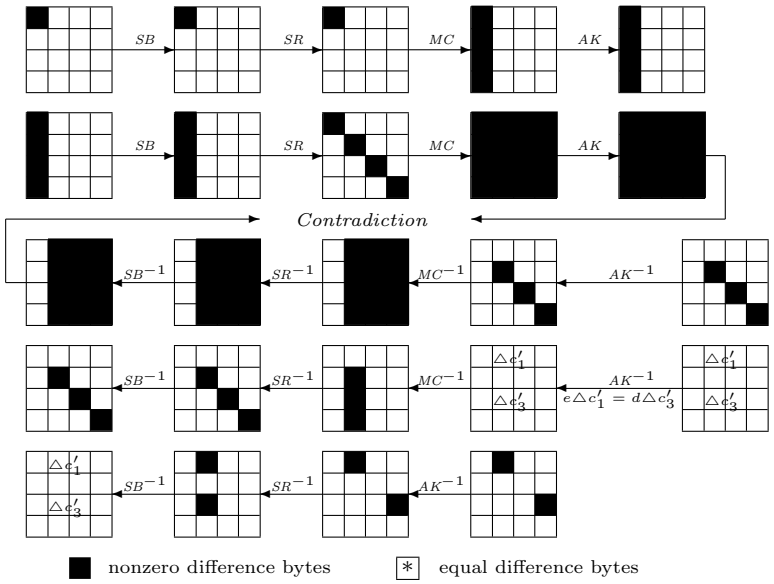

Fig. 5. Type 1: Near 5-Round impossible differential property of AES

5-round impossible differential property, which is shown in Fig.6.

Type 3: If messages pairs (M, M') satisfy Fact 2 and Fact 3, they possess of near 5-round impossible differential property like Fig.7.

Using the three kinds of new impossible differential properties of AES described above, we can give some new impossible differential attacks on 7-round AES-128/192. Furthermore, we can first give some new impossible differential attacks on 8-round or more of AES-192/256.

5 New impossible differential attack on 7-round AES

According to the three kinds of new impossible differential properties of AES described in Section 4, we present a new impossible differential attack on 7-round AES-128, as well as 7-round AES-192.

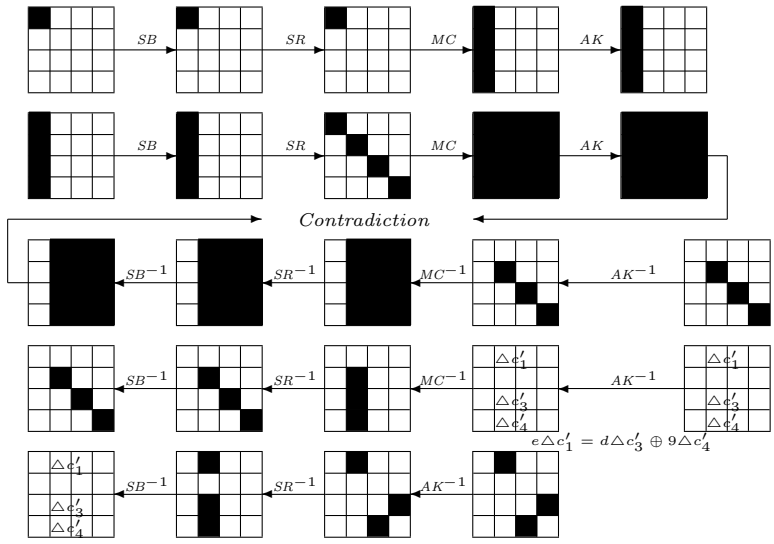

Fig. 6. Type 2: Near 5-Round impossible differential property of AES

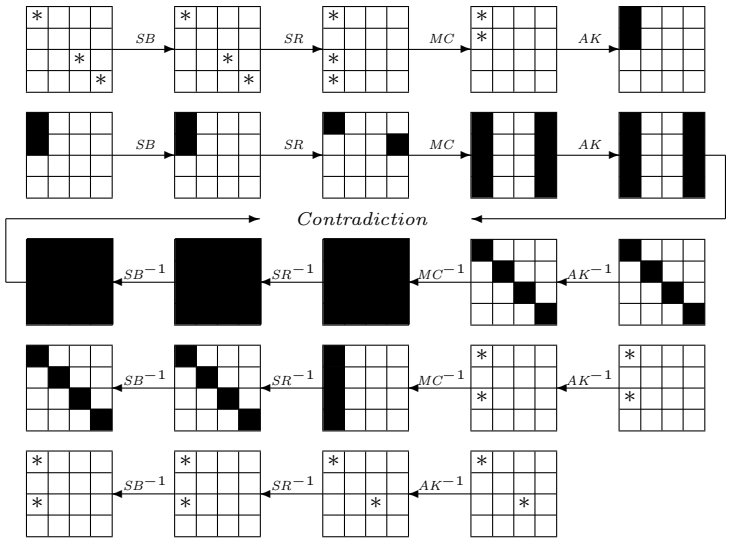

Fig. 7. Type 3: one of near 5-round impossible differential property of AES

5.1 New impossible differential attack on 7-round AES-128

ATTACK 1: For Fig.8, the impossible differential attack is as follows:

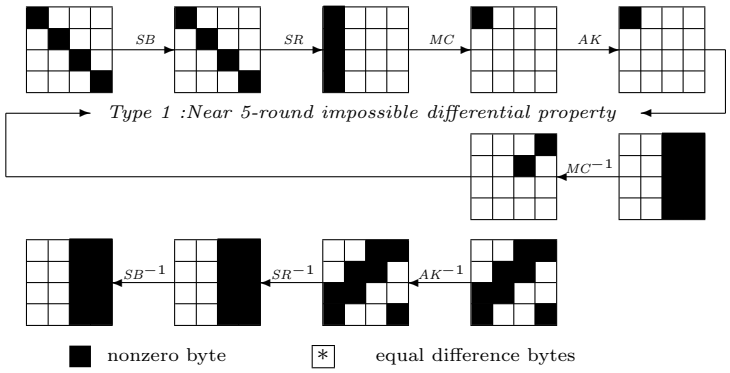

Fig. 8. Attack 1: Impossible differential attack on 7-round of AES

1. Define a structure T, whose all bytes are fixed except four bytes in position $(0, 5, 10, 15)$, there are $C_{32}^2 \approx 2^{63}$ plaintexts pairs in such a structure.
2. Randomly choose t structures with plaintexts pairs(P, P'), and encrypt these plaintexts pairs by 7-round AES. Only filtrate the pairs whose ciphertexts pairs (C, C') are same except eight bytes in positions $(2, 3, 5, 6, 8, 9, 12, 15)$. $2^{63} \times 2^{-64}t = 2^{-1}t$ pairs are excepted in this step.
3. Guess four bytes $K_1^7 = (k_2^7, k_5^7, k_8^7, k_{15}^7) \in K^7$, and partially decrypt the remained pairs (C, C') one round using K_1^7. Only select the pairs whose output of MC^{-1} are zero difference except byte in position 9. The excepted number of the pairs is $2^{-1} \times 2^{-24}t = 2^{-25}t$ in this step.
4. Guess another four bytes $K_2^7 = (k_3^7, k_6^7, k_9^7, k_{12}^7) \in K^7$, partially decrypt the remained pairs (C, C') one round using K_2^7. Only choose the pairs whose output of MC^{-1} are zero difference except byte in position 12.
   Compute two subkey bytes $k_9^6 = k_9^7 \oplus k_5^7$ and $k_{12}^6 = k_{12}^7 \oplus k_8^7$,
   For the remained $2^{-25} \times 2^{-24}t = 2^{-49}t$ pairs, check if *Fact 2* is satisfied. In this case, the probability of *Fact 2* is 2^{-6}. Finally, the excepted number of pairs is $d_e = 2^{-49} \times 2^{-6}t = 2^{-55}t$ in this step.
5. Eliminate wrong four bytes $K_1^0 = (k_0^0, k_5^0, k_{10}^0, k_{15}^0) \in K^0$ by impossible differential property in this step.
   (a) Precomputation: For the state s_K^1, given all 2^{42} possible differences pairs (x, x'), which only have one nonzero difference byte in column 0. For these pairs, perform orderly MC^{-1}, SR^{-1} and SB^{-1}, respectively, and obtain the output pairs $(s_{B^{-1}}^1, s_{B^{-1}}'^1)$. Computer their difference $\Delta s_{B^{-1}}^1$.

In all, there are 2^{32} output difference values. On average, there are about 2^{10} pairs (x, x') corresponding to one value $\Delta s^1_{B^{-1}}$.

(b) Give a hash table H, which contain $\Delta s^1_{B^{-1}}$ and its corresponding values $s^1_{B^{-1}}$.

(c) For remained pairs in step 4, compute corresponding plaintext difference $P \oplus P' = (P \oplus K^0_1) \oplus (P' \oplus K^0_1) = \Delta s^1_{B^{-1}}$, check table H, and obtain corresponding values $s^1_{B^{-1}}$.

(d) Given a table A containing all 2^{32} values K^0_1. Compute wrong values $K^0_1 = s^1_{B^{-1}} \oplus P$, and eliminate them from A. If at least one value is remained, the probability is $Pr^e_{K^0_1} = 2^{32} \times (1 - \frac{2^{10}}{2^{32}})^{d_e} \approx 2^{32} \times e^{-2^{-22}d_e}$.

(e) For all guessed key K^7_1 and K^7_2, the wrong value (K^0_1, K^7_1, K^7_2) remains with probability $Pr^e_{K^7} = 2^{64+32} \times e^{-2^{-22}d_e}$. If select $d_e = 2^{28.32}$, then $Pr^e_{K^7}$ is very small, i.e. $Pr^e_{K^7} = 2^{96} \times e^{-2^{-22}d_e} \approx 2^{-19}$, thus, the false K^0_1 can be eliminated with very high probability. Hence if remains a value K^0_1, the guessed 8-byte of K^7 can be regarded as correct.

Complexity Evaluation. The date complexity is $2^{32}t = 2^{87}d_e = 2^{115.32}$ chosen plaintexts. Step 3 requires about $2 \times 2^{32} \times 2^{82.32} = 2^{115.32}$ one round operation, Step 4 requires about $2 \times 2^{64} \times 2^{58.32} = 2^{123.32}$ two round operation, Step 5 requires about $2^{28.32} \times 2^{10} \times 2^{64} = 2^{102.32}$ memory access to A. Thus, the overall time complexity of the attack is about $\frac{2^{115.32}+2^{123.32}/2+2^{102.32}}{7} \approx 2^{120}$ 7-round AES encryption operations, and the required memory is about 2^{45} bytes.

5.2 New impossible differential attack on 7-round AES-192

ATTACK 2: See Fig.9, the impossible differential attack is as follow:

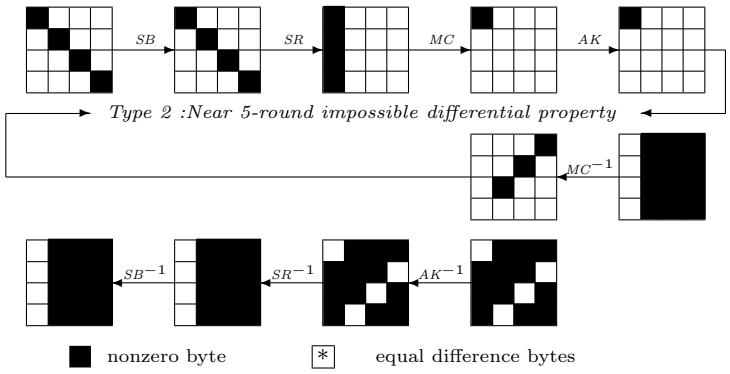

Fig. 9. Attack 2: Impossible differential attack on 7-round of AES

1. Define the same structure T as **ATTACK 1** above.
2. Randomly choose t structures, encrypt all plaintexts pairs using 7-round of AES-192, sieve the pairs whose ciphertexts pairs are different but 4-byte in positions $(0, 7, 10, 13)$, $2^{63} \times 2^{-32}t = 2^{31}t$ pairs are excepted in this step.
3. Guess bytes $K_1^7 = (k_1^7, k_4^7, k_{11}^7, k_{14}^7) \in K^7$, $K_2^7 = (k_2^7, k_5^7, k_8^7, k_{15}^7) \in K^7$, and $K_3^7 = (k_3^7, k_6^7, k_9^7, k_{12}^7) \in K^7$, respectively.
   For the chosen pairs, partly decrypt one round using K_1^7, K_2^7, and K_3^7, respectively, only choose the pairs whose output of MC^{-1} are same except three bytes $(b_1, b_2, b_3) \in \mathbb{P}$(See definition in Section 2.2). The excepted number of the pairs is $2^{31} \times (2^{-24})^3 t = 2^{-41}t$ in this step.
4. Compute relevant three subkey bytes $k_6^6 = k_2^7 \oplus k_6^7$, $k_9^6 = k_9^7 \oplus k_5^7$ and $k_{12}^6 = k_{12}^7 \oplus k_8^7$. For remained pairs in step 3, select the pairs which hold Fact 4, the probability is $\frac{(2^8-1)\times(2^8-2)}{(2^8-1)^3} \approx 2^{-8}$, the number of remained pairs is $d_e = 2^{-41} \times 2^{-8}t = 2^{-49}t$ in this step.
5. Eliminate wrong four bytes $K_1^0 = (k_0^0, k_5^0, k_{10}^0, k_{15}^0) \in K^0$ by displaying that the impossible differential property holds if the wrong values K_1^0 are used. Refer to Step 5 in **ATTACK** 1.
   Let $d_e = 28.67$, then $t = 77.67$. At least, one 32-bit key K_1^0 is remained with probability $Pr^e_{K_1^0} = 2^{32} \times (1 - \frac{2^{10}}{2^{32}})^{d_e} \approx 2^{32} \times e^{-2^{-22}d_e}$. For all guessed 12-byte of K^7, the wrong value $(K_1^0, K_1^7, K_2^7, K_3^7)$ remains with probability $Pr^e_{K^7} = 2^{96} \times 2^{32} \times (1 - \frac{2^{10}}{2^{32}})^{d_e} \approx 2^{128} \times e^{-2^{-22}d_e} = 2^{-19}$. so if a value K_1^0 is remained, the guessed 8-byte of K^7 will be correct with high probability.
   Complexity Evaluation. The date complexity of attack is $2^{32}t = 2^{109.67}$. Step 3 requires about $2 \times 2^{32} \times 2^{31+77.67} + 2 \times 2^{64} \times 2^{84.67} + 2^{96} \times 2^{60.67} = 2^{141.67} + 2^{149.67} + 2^{156.67} \approx 2^{156.67}$ one round operation, and Step 5 requires about $2^{28.67} \times 2^{10} \times 2^{64} = 2^{102.67}$ memory access to A. Thus, the overall time complexity of the attack is about $\frac{2^{156.67}+2^{102.67}}{7} \approx 2^{154}$ 7-round AES encryption operations, and the required memory is about 2^{45} bytes.

6 New impossible differential attack on 8 round or More of AES

From the three kinds of new impossible differential properties of AES described in Section 4, we can obtain many of new impossible differential attacks on 8-round or more of AES-192/256. Here, we only simply introduce one, the results of some others attacks refer to Table 2.
Note: the complexities in Table 2 can been slightly improved by Lu's methods[11].

6.1 New impossible differential attack on 8 round of AES-192

ATTACK 3: See Fig.10, the process of impossible differential attack on AES-192 is as follows:

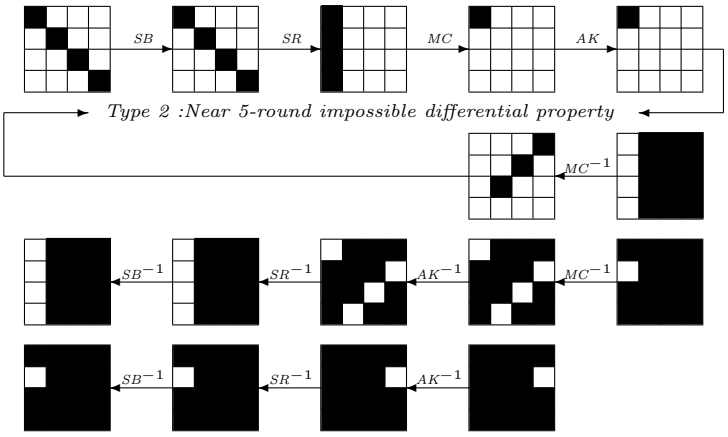

Fig. 10. Attack 3: Impossible differential attack on 8-round of AES

1. For t chosen structures, encrypt all plaintexts pairs using 8-round of AES. Choose the pairs, whose ciphertexts are different except z_f^C-byte, $2^{63} \times 2^{-8\times z_f^C} t = 2^{63-8z_f^C} t$ pairs are excepted in this step.
2. In all, guess z_k bytes of (K_i^8, K_j^7, K_k^6). Decrypt the chosen pairs two rounds using guessed bytes of (K_i^8, K_j^7, K_k^6). Only choose the pairs whose output of MC^{-1} of the 1^{st} round are different except four bytes $(0, 7, 10, 13)$, and whose output of MC^{-1} of the 2^{nd} hold Fact 4. The excepted number of pairs is $2^{-(41+8z_f^C)}t = d_e$ in this step.
3. Eliminate wrong four bytes $K_4^0 = (k_0^0, k_5^0, k_{10}^0, k_{15}^0) \in K^0$ using the same method as ATTACK 1. Similarly, the probability of remaining wrong K_4^0 is $Pr_{K^0}^e = 2^{32} \times (1 - \frac{2^{10}}{2^{32}})^{d_e} = 2^{32} \times e^{-(2^{-22}d_e)}$.
   If $d_e = 2^{28.5}$, then $e^{-(2^{-22}d_e)} \approx 2^{-131}$, and the wrong value (K_4^0, K_i^7, K_j^8) remains with probability $2^{8\times z_f^C} \times Pr_{K^0}^e \approx 2^{-19}$. So if a value K_4^0 is remained, the guessed w-byte will be correct with high probability.
   Complexity Evaluation. From Section 3, The date complexity $Pr_d = 2^{73+8\times z_f^C} d_e$. If $d_e = 2^{28.5}$, then $Pr_d < 2^{128}$ only and if only $z_f^C < 3.3$. Refer to Table 2 for the date complexity and time complexity .

6.2 New impossible differential attack on more than 8-round AES-192/256

Using our near 5-round impossible differential properties and complexities expressions of an universal impossible differential attacks methods, we can have some new impossible differential attacks on 8-9 rounds AES-192/256 and 10-12 rounds AES-256, Table 2 shows some results. Because of the limited space, we don't discuss them.

Intuitively, impossible differential attacks on 10-round AES-192 and 12 or 13 rounds AES-256 can be achieved by our complexities expressions and near 5-round impossible differential properties.
Note: the complexities of Table 2 can been slightly improved.

7 Conclusion

we first propose some near 5 rounds impossible differential properties. In our properties, the number of active bytes of 1^{st} round and 5^{th} round can be 1,2 or 3, and the active bytes are in different columns, so our impossible differential properties are easy to be extended. Additionally,we first propose the complexities expressions of an universal impossible differential attack, which can help us to rapidly search appropriate impossible differential paths. Utilizing our near 5-round impossible differential properties and complexities expressions, we can give a series of new impossible differential attacks on 8-9 rounds AES-192/256 and 10-11 rounds AES-256 in Table 2. Intuitively, the complexities of Table 2 can been slightly improved, and impossible differential attacks on 10 rounds AES-192 and 12-13 rounds AES-256 can been obtained by our methods.

References

1. B. Bahrak, M. Reza Aref. Impossible Differential Attack on Seven-Round AES-128, IET Information Security journal, Vol. 2, Number 2, pp. 28-32, IET, 2008.
2. E. Biham, N. Keller, Cryptanalysis of reduced variants of Rijndael, 3rd AES Conference, 2000, submitted for publication.
3. A. Biryukov and D. Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. in M.Matsui(Ed.): Asiacrypt 2009, LNCS 5912, PP.1-18,2009.
4. A. Biryukov, D. Khovratovich, and I. Nikolić. Distinguisher and related-key attack on the full AES-256. In S.Halevi (Ed.): CRYPTO 2009, LNCS 5677, pp.231-249, 2009.
5. A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir. Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds. available at http://eprint.iacr.org/2009/374.pdf.
6. E. Biham, N. Keller. Cryptanalysis of Reduced Variants of Rijndael. in Official public comment for Round 2 of the AES development effort (2000), available at http://csrc.nist.gov/encryption/aes/round2/conf3/aes3papers.html
7. J.H. Cheon, M. Kim, K. Kim, J.-Y. Lee, S. Kang. Improved Impossible Differential Cryptanalysis of Rijndael and Crypton. In: K.-c. Kim(ed.): Proc. 3rd International Conference on Information Security and Cryptology (ICISC 2001). LNCS 2288, Springer-Verlag, Berlin, pp. 39-49, 2001.
8. J. Daemen, V. Rijmen, AES Proposal : Rijndae. The First Advanced Encryption Standard Candidate Conference. NIST AES Proposal, 1998.
9. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, D. Whiting. Improved cryptanalysis of Rijndael. In: B. Schneier(ed.) FSE 2000. LNCS 1978, pp. 213-230. Springer, Heidelberg,2001.
10. H. Gilbert, M. Minier. A collision attack on 7 rounds of Rijndael. In: The Third Advanced Encryption Standard Candidate Conference, pp. 230-241 (April 2000), see http://www.nist.gov/aes.

11. J. Lu, O. Dunkelman, N. Keller, and J. Kim. New Impossible Differential Attacks on AES. In D.R. Chowdhury et al.(Eds.):INDOCRYPT 2008, LNCS 5365, pp. 279-293, 2008.
12. National Institute of Standards and Technology (NIST), Draft FIPS for the AES, 2001.
13. NIST,FIPS 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES),Nov.26, 2001.
14. R.C.-W. Phan, M.U. Siddiqi. Generalised impossible Differentials of Advanced Encryption standard, Electronics Letters 37 (14), pp. 896-898, 2001.
15. R.C.-W. Phan, Classes of impossible Differentials of Advanced Encryption standard, Electronics Letters 38 (11), pp. 508-510, 2002.
16. R.C.-W. Phan. Impossible Differential Cryptanalysis of 7-round Advanced Encryption Standard (AES). Information Processing Letters 91(1), pp.33-38, 2004.
17. Z. YUAN, W. Wang, K. Jia,G. Xu,X. Wang. New Birthday Attacks on Some MACs Based on Block Ciphers. In: Shai Halevi: Advances in Cryptology -CRYPTO 2009, LNCS 5677, Springer-Verlag, Berlin Heidelberg, New York, pp. 209-230, 2009.
18. W. Zhang, W. Wu, and D. Feng. New Results on Impossible Differential Cryptanalysis of Reduced AES. In K.-H. Nam and G. Rhee (Eds.): ICISC 2007, LNCS 4817, pp. 239-250, 2007.

Appendix A:

Table 1. Comparison of Some Previous Attacks with Our New Attacks

Key Size	Source	Number of Round	Data Complexity(CP)	Time Complexity	Attack . Type .
AES-128	Ref.[1,18]	7	$2^{115.5}$	2^{119}	Imp.Diff.
	Ref.[11]	7	$2^{112.2}$	$2^{117.2}$	Imp.Diff.
AES-192	Ref.[16]	7	2^{92}	$2^{186.2}$	Imp.Diff.
	Ref.[18]	7	$2^{115.5}$	2^{119}	Imp.Diff.
	Ref.[11]	7	$2^{113.8}$	$2^{118.8}MA$	Imp.Diff.
	Ref.[18]	7	2^{92}	2^{162}	Imp.Diff.
	Ref.[11]	7	$2^{91.2}$	$2^{139.2}$MA	Imp.Diff.
AES-256	Ref.[16]	7	$2^{92.5}$	$2^{250.5}$	Imp.Diff.
	Ref.[11]	7	2^{92}	2^{163}MA	Imp.Diff.
	Ref.[18]	7	$2^{115.5}$	2^{119}	Imp.Diff.
	Ref.[11]	7	$2^{113.8}$	$2^{118.8}MA$	Imp.Diff.
	Ref.[18]	8	$2^{116.5}$	$2^{247.5}$	Imp.Diff.
	Ref.[11]	8	$2^{111.1}$	$2^{227.8}MA$	Imp.Diff.
	Ref.[11]	8	$2^{89.1}$	$2^{229.7}MA$	Imp.Diff.
AES-128	Ref.[9]	7	2^{128}–2^{119}	2^{120}	Square.
	Ref.[10]	7	2^{32}	$\approx 2^{128}$	Collision.
AES-192	Ref.[9]	8	2^{128}–2^{119}	2^{188}	Related Key.
	Ref.[3]	12	2^{123}	2^{176}	Related Key.
AES-256	Ref.[5]	8	$2^{26.5}$–2^{31}	$2^{26.5}$–2^{31}	Related Key.
	Ref.[5]	9	2^{32}–2^{39}	2^{32}–2^{38}	Related Key.
	Ref.[5]	10	2^{45},2^{49}	2^{44},2^{48}	Related Key.
	Ref.[4,3]	14	$2^{99.5}$,2^{131}	$2^{99.5}$,2^{131}	Related Key.
AES-128	This Paper	7	$2^{115.32}$	$2^{119.32}$	Imp.Diff.
AES-192	This Paper	7	$2^{109.67}$	$2^{154.67}$	Imp.Diff.
	This Paper	8	$2^{102.3}$	$2^{166.3}$	Imp.Diff.
	This Paper	9	$2^{115.89}$	$2^{180.89}$	Imp.Diff.
	This Paper	9	$2^{125.89}$	$2^{150.89}$	Imp.Diff.
AES-256	This Paper	11	$2^{122.4}$	$< 2^{254.4}$	Imp.Diff.

Appendix B:

Table 2. Our Impossible Differential Attacks on 8 Rounds or More of AES

Key Size	r	z_f^P	z_f^C	z_k	Pr^1	Pr^2	Pr^3	Pr^4	Pr^5		Pr_d	Pr_t . .
AES-192	8	4	1	19	2^{-54}	2^{-60}					$2^{120.14}$	$2^{165.14}$
	8	4	3	19	2^{-80}	2^{-24}					$2^{126.14}$	$2^{155.14}$
	8	4	2	20	2^{-80}	2^{-24}					$2^{118.19}$	$2^{174.19}$
	8	4	1	21	2^{-80}	2^{-24}					$2^{109.89}$	$2^{182.89}$
	8	4	0	20	2^{-54}	2^{-60}					$2^{112.19}$	$2^{173.19}$
	8	4	0	22	2^{-80}	2^{-24}					$2^{102.3}$	$2^{166.3}$
AES-192	9	4	1	15	2^{-54}	2^{-60}	2^{-60}				$2^{125.89}$	$2^{150.89}$
	9	4	1	23	2^{-54}	2^{-60}					$2^{120.35}$	$2^{185.35}$
	9	4	2	22	2^{-80}	2^{-24}	2^{-6}				$2^{124.30}$	$2^{173.30}$
	9	4	1	15	2^{-80}	2^{-24}	2^{-6}				$2^{115.89}$	$2^{180.89}$
	9	4	1	15	2^{-80}	2^{-24}	2^{-12}				$2^{121.89}$	$2^{186.89}$
	9	4	1	22	2^{-80}	2^{-24}	2^{-15}				$2^{125.30}$	$2^{181.30}$
AES-256	10	4	0	24	2^{-80}	2^{-24}	2^{-12}	2^{-6}			$2^{120.4}$	$< 2^{254.4}$
	10	2	0	25	2^{-80}	2^{-24}	2^{-12}	2^{-6}			$2^{122.4}$	$< 2^{248.4}$
	10	2	0	25	2^{-80}	2^{-24}	2^{-6}	2^{-6}			$2^{116.35}$	$< 2^{248.35}$
	10	4	0	24	2^{-80}	2^{-24}	2^{-6}	2^{-6}			$2^{114.4}$	$< 2^{254.4}$
	10	3	0	24	2^{-80}	2^{-24}	2^{-6}	2^{-6}			$2^{116.4}$	$< 2^{248.4}$
	11	2	0	26	2^{-80}	2^{-24}	2^{-6}	2^{-6}	2^{-6}		$2^{122.4}$	$< 2^{254.4}$
perhaps	12	2	0	26	2^{-80}	2^{-24}	2^{-6}	2^{-6}	2^{-6}	0	$2^{122.4}$	$< 2^{254.4}$