A New Method for Impossible Differential Crypt-analysis of 8-Round AES-128

Ruihong Zhang
School of Computer, Huanggang normal University, Hubei 438000, P. R.China
*E-mail:18623582@qq.com

***Abstract*—Through profound study of the 3-round encryption characteristics of advanced encryption standard (AES), a new 3-round differential path with an existing probability to of 2-22 has been derived. Based on this path, a novel method was proposed for impossible differential cryptanalysis of 8-round AES-128. The analysis method requires 287 pairs of chosen plaintexts, about 299 words of memory and 296 encryption/decryption computations. According to the analysis process, it is found that the confusing level of the MixColumns transformation in AES algorithm is insufficient, which provides a theoretical basis to improve the AES security.**

***Index Terms*—advanced encryption standard, AES-128, impossible differential cryptanalysis, differential character**

I. INTRODUCTION

In the United States, Advanced Encryption Standard (AES) was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a five-year standardization process in which fifteen competing designs were presented and evaluated before it was selected as the most suitable[1]. It is available in many different encryption packages. Originally called Rijndael, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. Strictly speaking, AES is the name of the standard, and the algorithm described is a restricted variant of Rijndael. However, in practice the algorithm is also referred to as 'AES'. AES is based on a design principle known as a substitution-permutation network, which has a fixed block size of 128 bits and a key size of 128 (AES-128), 192 (AES-192), or 256 bits (AES-256).

Although AES can resist the traditional differential attack and linear attacks, due to the incompleteness of the linear diffusion layer, it can be attacked by kinds of new attacks these years, such as impossible differential attack[2], meet-in-the-middle attack[3], boomerang attack [4], rectangle attack [5], saturation attack[6], algebraic attack[7], structure collision attack [8], *etc*. Impossible differential cryptanalysis is a variant of differential cryptanalysis, which is an exceedingly uncomplicated and effective cryptanalysis method, and it has become a research focus to analyze AES with this method in recent years. The linear-layer-diffusion incompleteness of AES-192/AES-256 is more conspicuous compared with that of AES-128, resulting to less attention paid to AES-128[9][10].

In 2000, Biham and Keller presented an impossible differential cryptanalysis method for AES-128 for the first time, which demanded $2^{29.5}$ chosen plaintexts, about 2^{38} words of memory and 2^{31} 5-round encryptions, as shown in Table 1[11]. It was later improved in 2001 by Cheon *et al*. to apply to 6 rounds[12]. In 2006, Chen *et al.* presented a new method for impossible differential cryptanalysis of 6-round AES-128[13]. This was later improved in 2008 by Bahrak *et al.* to apply to 7 rounds[14], and further improved in 2010 by Mala *et al.*[15]. More detailed information of the above methods could be obtained in Table 1. It is not difficult to find there is a common ground among these methods: First, a 4-round impossible differential path is constructed based on a property of the MixColumns in AES algorithm. Then a possible differential path is added to the front and back ends of the impossible differential path. Finally, part of the initial keys are restored through the differential analysis method [11, 16, 17].

The meet-in-the-middle attack is another research focus for AES [3]. Demirci *et al*. have analyzed the internal structure of the AES encryption algorithm and presented the mapping properties of the 4-round AES encryption in 2009 [17]. They proposed a new meet-in-the-middle attack method for 7-round AES-128, which demanded 2^{80} chosen plaintexts, about 2^{122} words of memory and 2^{113} 7-round encryptions. Dunkelman *et al*. Have constructed a 4-round differential character for 8-round AES-128 and AES-256 in 2010 [18]. In this study, we have deduced a novel property of the 3-round AES encryption based on the above two works and further analyzed the 8-round AES-128 with the impossible differential cryptanalysis method, which is the highest round of AES-128 reported so far.

II. BACKGROUND KNOWLEDGE

The packet length of the AES encryption algorithm is 128 bits, which is in the form of a 4 × 4

column-major order matrix. The matrix can be regarded as a state table consisting of *Nb* column (*Nb* =4), and each column containing 32 bits. AES has a key size of 128 (AES-128), 192 (AES-192), or 256 (AES-256) bits [1]. The corresponding key data could be considered as a state table consisting of *Nk* column (*Nk* =4, 6, or 8), and each column containing 32 bits in the form of 4 bytes, respectively. AES requires different number of iterations for various key lengths. The number of iterations (*Nr*) for AES-128, AES-192 and AES-256 are 10, 12, and 14, respectively. The AES round function consists of the following four kinds of transformation [1]: a nonlinear S-box layer replace SubBytes(), a row-cycle left shift ShiftRows(), a linear transformation of column confusion MixColumns(), and a XOR operation of key addition AddRoundKey(). Except for a key addition operation before the first round and no column confusion operation at the last round, all other round functions of AES consist of a sequence of SubBytes, ShiftRows, MixColumns, and AddRoundKey.

A. SYMBOLS

AES operates on a 4×4 column-major order matrix of bytes. For actual convenience, we can label the elements in the matrix as 0, 1, …, 15 from top (left) to bottom (right). Another labeling method is in terms of line/row coordinates (both of the line and row are labeled as 1, 2, 3, 4, respectively). (P, P') and (C, C') stand for the input plaintext and output ciphertext. $C^{(k)}$ indicates the k round output, m_{ij} represents the byte in line *i* and row *j* of the input, $c_{ij}^{(k)}$ means the byte in line *i* and row *j* of the *k*-round output. $\Delta SR_{ij}^{(k)}$ represents the byte in line *i* and row *j* of the *k*-round line-shift transformation. SB, SR, MC, AR stand for SubBytes, ShiftRows, MixColumns, and AddRoundKey, respectively. SB^{-1}, SR^{-1}, MC^{-1}, AR^{-1} represent their inverse operation, respectively.

B. MIXCOLUMNS OF AES

MixColumns is the mixed transformation for status rows, which can be expressed in the form of a matrix multiplication:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

where $[a_0\ a_1\ a_2\ a_3]^T$ and $[b_0\ b_1\ b_2\ b_3]^T$ represent the input and output row of MixColumns, respectively.

Property 1: If the output row of MixColumns satisfies the differential $[\gamma\ 0\ 0\ 0]^T$, the input row will satisfy the differential $[0E\gamma\ 09\gamma\ 0D\gamma\ 0B\gamma]^T$, and vice verse.

It can be proved as follows:

According to the MixColumns matrix, one can achieve:

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}^{-1} \times \begin{bmatrix} \gamma \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \times \begin{bmatrix} \gamma \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0E\gamma \\ 09\gamma \\ 0D\gamma \\ 0B\gamma \end{bmatrix}$$

where 01, 02, 03, 0*E*, 0*B*, 0*D*, 09 are in hexadecimal. There are 4 kinds of situations that the output differential contains only one active byte, and a non-zero input differential leads to a non-zero output differential, therefore, the probability that 3 bytes of the output differential equal 0 is 2^{-22} $\{4\times(2^8-1)/2^{32}\approx 2^{-22}\}$. This property can be proved vice verse.

III. A NEW 3-ROUND DIFFERENTIALL PATH

An important distinguisher for 4-round AES has been proposed in Ref.[17]. In that differentiator, when only the first byte of input is not fixed (the rest are fixed) after 4 rounds of encryptions, $c_{11}^{(4)}$ can be expressed with 25 byte-variables. A new 4-round differential property is proposed later in Ref.[18]. In this differential property, when only the first byte of input is not fixed (the rest are fixed) after 4 encryptions, and when only ΔC_{11}^4 of the output differential is active byte (others are fixed), there would be 2^{32} output differentials at most after the first round encryption. Based on the above two properties, we have deduced a new 3-round distinguisher and a novel 3-round differential path.

A. A NEW DISTINGUISHER FOR 3-ROUND AES

First, construct an input plaintext which meets $m_{11}=m_{21}=m_{31}=m_{41}=x$, $(0\le x\le 255)$, then do AddRoundKey operation with initial keys as shown below:

$x+k_{11}^{(0)}$	$m_{12}+k_{12}^{(0)}$	$m_{13}+k_{13}^{(0)}$	$m_{14}+k_{14}^{(0)}$
$x+k_{12}^{(0)}$	$m_{22}+k_{22}^{(0)}$	$m_{23}+k_{23}^{(0)}$	$m_{24}+k_{24}^{(0)}$
$x+k_{13}^{(0)}$	$m_{32}+k_{32}^{(0)}$	$m_{33}+k_{33}^{(0)}$	$m_{34}+k_{34}^{(0)}$
$x+k_{14}^{(0)}$	$m_{42}+k_{42}^{(0)}$	$m_{43}+k_{43}^{(0)}$	$m_{44}+k_{44}^{(0)}$

Figure 1. The construction of the plaintext structural diagram

With a fixed m_{ij} in "Fig. 1," various input differentials can be constructed by changing the x value in Figure 1. With a fixed input differential, various input pairs can be constructed by changing m_{ij}.

Theorem 1: Assuming the input (P, P') meets the constructed plaintext as shown in Figure, the

differentials of output bytes $\Delta C_{ii}^{(2)}$ (i=1, 2, 3, 4) can be expressed with 20 one-byte constants after two rounds of encryptions, respectively, and $\Delta C_{11}^{(3)}$ can be expressed with 24 one-byte parameter after three rounds of encryptions.

Theorem 1 can be demonstrated as follows:

After a round of encryption

$$C_{11}^{(1)} = 2S(x + k_{11}^{(0)}) + 3S(m_{22} + k_{22}^{(0)}) + S(m_{33} + k_{33}^{(0)}) + S(m_{44} + k_{44}^{(0)}) + k_{11}^{(1)}$$
$$= 2S(x + k_{11}^{(0)}) + c_1$$

Similarly, it can be deduced that:

$$C_{22}^{(1)} = S(x + k_{41}^{(0)}) + c_2,$$
$$C_{33}^{(1)} = 2S(x + k_{31}^{(0)}) + c_3,$$
$$C_{44}^{(1)} = S(x + k_{21}^{(0)}) + c_4.$$

By further developing, it is achieved as follows:

$$C_{11}^{(2)} = 2S(2S(x + k_{11}^{(0)}) + c_1) + 3S(S(x + k_{41}^{(0)}) + c_2) + S(2S(x + k_{31}^{(0)}) + c_3) + S(S(x + k_{21}^{(0)}) + c_4) + k_{11}^{(2)};$$
$$C_{22}^{(2)} = S(S(x + k_{41}^{(0)}) + c_5) + 2S(3S(x + k_{31}^{(0)}) + c_6) + 3S(S(x + k_{21}^{(0)}) + c_7) + S(3S(x + k_{11}^{(0)}) + c_8) + k_{22}^{(2)};$$
$$C_{33}^{(2)} = S(S(x + k_{31}^{(0)}) + c_9) + S(2S(x + k_{21}^{(0)}) + c_{10}) + 2S(S(x + k_{11}^{(0)}) + c_{11}) + 3S(2S(x + k_{41}^{(0)}) + c_{12}) + k_{33}^{(2)};$$
$$C_{44}^{(2)} = 3S(3S(x + k_{21}^{(0)}) + c_{13}) + S(S(x + k_{11}^{(0)}) + c_{14}) + S(3S(x + k_{41}^{(0)}) + c_{15}) + 2S(S(x + k_{31}^{(0)}) + c_{16}) + k_{44}^{(2)};$$

Various input differentials can be achieved by changing the x value, after two rounds of encryptions, the corresponding differentials $\Delta C_{ii}^{(2)}$ (i=1, 2, 3, 4) could be expressed as follows:

$$\Delta C_{11}^{(2)} = 2S(2S(x + k_{11}^{(0)}) + c_1) + 2S(2S(x' + k_{11}^{(0)}) + c_1) + 3S(S(x + k_{41}^{(0)}) + c_2) + 3S(S(x' + k_{41}^{(0)}) + c_2) +$$
$$S(2S(x + k_{31}^{(0)}) + c_3) + S(2S(x' + k_{31}^{(0)}) + c_3) + S(S(x + k_{21}^{(0)}) + c_4) + S(S(x + k_{21}^{(0)}) + c_4) \quad (1),$$
$$\Delta C_{22}^{(2)} = S(S(x + k_{41}^{(0)}) + c_5) + S(S(x' + k_{41}^{(0)}) + c_5) + 2S(3S(x + k_{31}^{(0)}) + c_6) + 2S(3S(x' + k_{31}^{(0)}) + c_6) +$$
$$3S(S(x + k_{21}^{(0)}) + c_7) + 3S(S(x'' + k_{21}^{(0)}) + c_7) + S(3S(x + k_{11}^{(0)}) + c_8) + S(3S(x' + k_{11}^{(0)}) + c_8) \quad (2),$$
$$\Delta C_{33}^{(2)} = S(S(x + k_{31}^{(0)}) + c_9) + S(S(x' + k_{31}^{(0)}) + c_9) + S(2S(x + k_{21}^{(0)}) + c_{10}) + S(2S(x' + k_{21}^{(0)}) + c_{10}) +$$
$$2S(S(x + k_{11}^{(0)}) + c_{11}) + 2S(S(x' + k_{11}^{(0)}) + c_{11}) + 3S(2S(x + k_{41}^{(0)}) + c_{12}) + 3S(2S(x' + k_{41}^{(0)}) + c_{12}) \quad (3),$$
$$\Delta C_{44}^{(2)} = 3S(3S(x + k_{21}^{(0)}) + c_{13}) + 3S(3S(x' + k_{21}^{(0)}) + c_{13}) + S(S(x + k_{11}^{(0)}) + c_{14}) + S(S(x' + k_{11}^{(0)}) + c_{14})$$
$$+ S(3S(x + k_{41}^{(0)}) + c_{15}) + S(3S(x' + k_{41}^{(0)}) + c_{15}) + 2S(S(x + k_{31}^{(0)}) + c_{16}) + 2S(S(x' + k_{31}^{(0)}) + c_{16}) \quad (4).$$

where $c_1\ c_2 \cdots c_{16}$ and $k_{11}^{(0)}\ k_{21}^{(0)}\ k_{31}^{(0)}\ k_{41}^{(0)}$ are one-byte constants, respectively. $S0$ is the nonlinear S-box transformation in AES. Therefore, $\Delta C_{11}^{(2)}$ can be expressed with the $S0$ transformation of 8-byte constants $k_{11}^{(0)}$、$k_{21}^{(0)}$、$k_{31}^{(0)}$、$k_{41}^{(0)}$、c_1、c_2、c_3、c_4. Similarly, $\Delta C_{ii}^{(2)}$ (i=2, 3, 4)can be conveyed with a 8-byte constant, respectively. According to Equations (1-4), $\Delta C_{ii}^{(2)}$ (i=1, 2, 3, 4) can be conveyed with a 24-byte constant, respectively. Moreover, the equation $\Delta C_{11}^{(3)} = 2S(C_{11}^{(2)}) + 3S(C_{22}^{(2)}) + S(C_{33}^{(2)}) + S(C_{44}^{(2)})$ is confirmed, thus $\Delta C_{11}^{(3)}$ can be expressed with a 24-byte constant.

B. A NOVEL 3-ROUND DIFFERENTIAL PATH

The important distinguisher for 4-round AES proposed in Ref.[17] has been employed to analyze 7-round AES-192 and AES-256 successfully. Based on this and by taking advantage of the new distinguisher for 3-round AES proposed in last chapter, a novel 3-round differential path can be constructed, which could be employed to analyze 8-round AES-128. The concrete differential path is as follows:

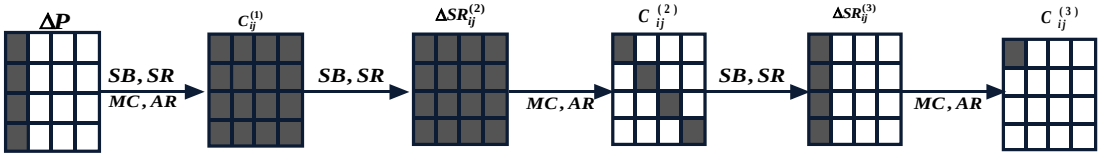

Figure 2. A novel 3-round differential path

The value of $\Delta C_{11}^{(3)}$ in Figure 2 is the one given in Theorem 1, and the value of $\Delta SR_{mn}^{(3)}$ can be expressed with the following equation:

$$\Delta SR_{mn}^{(3)} = \begin{bmatrix} 0E\Delta C_{11}^{(3)} & 0 & 0 & 0 \\ 0B\Delta C_{11}^{(3)} & 0 & 0 & 0 \\ 0D\Delta C_{11}^{(3)} & 0 & 0 & 0 \\ 09\,\Delta C_{11}^{(3)} & 0 & 0 & 0 \end{bmatrix} \quad (5)$$

where $\Delta C_{ii}^{(2)}$ (i=1, 2, 3, 4) meet the equations as

follows:

$$SB(C_{11}^{i(2)}) \oplus SB(C_{11}^{j(2)}) = \Delta SR_{11}^{(3)}$$
$$SB(C_{22}^{i(2)}) \oplus SB(C_{22}^{j(2)}) = \Delta SR_{21}^{(3)}$$
$$SB(C_{33}^{i(2)}) \oplus SB(C_{33}^{j(2)}) = \Delta SR_{31}^{(3)}$$
$$SB(C_{44}^{i(2)}) \oplus SB(C_{4}^{j(2)}) = \Delta SR_{41}^{(3)}$$

Each value of $\Delta SR_{mn}^{(2)}$ can be conveyed with Equation (6)

$$\Delta SR_{mn}^{(2)} = \begin{bmatrix} 0E\Delta C_{11}^2 & 09\Delta C_{22}^2 & 0D\Delta C_{33}^2 & 0B\Delta C_{44}^2 \\ 0B\Delta C_{11}^2 & 0E\Delta C_{22}^2 & 09\Delta C_{33}^2 & 0D\Delta C_{44}^2 \\ 0D\Delta C_{11}^2 & 0B\Delta C_{22}^2 & 0E\Delta C_{33}^2 & 09\Delta C_{44}^2 \\ 09\Delta C_{11}^2 & 0D\Delta C_{22}^2 & 0B\Delta C_{33}^2 & 0E\Delta C_{44}^2 \end{bmatrix} \quad (6)$$

Theorem 2: Construct the plaintexts (P^i, P^j) with each of them meeting the structure as shown in "Fig. 1," if the input differentials meet the structure in "Fig. 1," the output differentials agree with the structure in "Fig. 2," after 3 rounds of encryptions, and there are 2^{74} existent plaintexts.

Theorem 2 can be demonstrated as follows:

Since c_1、$c_2 \cdots c_{16}$ are employed to expressed $\Delta C_{11}^{(3)}$, their values decide the number of the plaintexts constructed. With the $k_{ii}^{(0)}$(i=1, 2, 3, 4)、$k_{11}^{(1)}$ fixed, a value of c_1 can be determined by m_{22}, m_{33}, m_{44}, and there are 2^{16} probable values of c_1. Similarly, c_2, c_3, c_4 can be determined by (m_{12}, m_{23}, m_{34}), (m_{13}, m_{24}, m_{42}), (m_{14}, m_{32}, m_{43}), respectively, and the number of each of their probable values is 2^{16}。Therefore, a group of (c_1, c_2, c_3, c_4), (c_5, c_6, c_7, c_8), (c_9, c_{10}, c_{11}, c_{12}), or (c_{13}, c_{14}, c_{15}, c_{16}) consists of 2^{64} groups of various (m_{22}, m_{33}, m_{44}, m_{12}, m_{23}, m_{34}, m_{13}, m_{24}, m_{42}, m_{14}, m_{32}, m_{43}), respectively. The value of $\Delta C_{ii}^{(2)}$ (i=1, 2, 3, 4) can be determined by c_i. If $\Delta C_{11}^{(2)} \neq 0$ and $\Delta C_{i1}^{(2)} = 0$ (i=2,3,4), there are 2^{10} ($2^{32-22}=2^{10}$) groups of qualified (c_1, c_2, c_3, c_4) according to Property 1. Similarly, the probable differential numbers of $\Delta C_{ii}^{(2)}$ (i=2, 3, 4) and $\Delta C_{11}^{(3)}$ are 2^{10} and 2^{18}, respectively. Considering the existence of repeatability, there are 2^{10} groups of c_i (i=1, 2, 3, 4) existing at most. Therefore, if the output differentials meet the structure in "Fig. 2," there are 2^{74} ($2^{64+10}=2^{74}$) probable existing plaintexts, which is consistent with the conclusion of Theorem 1.

IV. IMPOSSIBLE DIFFERENTIAL CRYTANALYSIS OF 8-ROUND AES-128

Herein we are proposing a novel method for impossible differential cryptanalysis of 8-round AES-128. This method is based on the 4-round impossible differential path as shown in Figure 3, by adding a 3-round possible differential path before it and adding a 1-round possible differential path after it, a new 8-round impossible differential path could be constructed. This method demands 2^{96} encryptions.

The existing probability of the 3-round differential path is 2^{-22}. The attack process can be divided into 11 steps as shown below:

A. THE ATTACK PROCESS

Step 1: Construct the input plaintexts (P^i, P^j) meeting Figure 1. With m_{jk} fixed in Figure 1, about 2^8(2^8-1≈2^8) input differentials can be constructed by changing the value of x_i, 2^{104} ($2^{96+8}=2^{104}$) input pairs can be constructed by changing m_{jk}. Choose a pair of input differential and change m_{jk}, calculate the values of ci (i=1, 2, …, 15, 16) and store them in the linear table L_1 according to Theorem 1 and 2. Figure out $\Delta C_{ii}^{(2)}$(i=1, 2, 3, 4) and the according values of $k_{ii}^{(2)}$(i=1, 2, 3, 4), then store them in the linear table L_2. Calculate the value of $\Delta SR_{mn}^{(2)}$, which has a corresponding relationship with $k_{ii}^{(2)}$(i=1, 2, 3, 4), and store it in the linear table L_3.

Step 2: Construct the input plaintexts (P^i, P^j) meeting "Fig. 1." With x_i fixed in "Fig. 1," 2^{96} input pairs can be constructed by changing the value of m_{jk}. Choose 2^{87} plaintexts out of them to be carried out 8 rounds of encryptions, resulting to 2^{87} ciphertexts.

Step 3. Select the ciphertexts which meet the situation that the differentials equal zero at the 5th, 7th, 12nd and 14th byte, 2^{55} ($2^{87-32}=2^{55}$) corresponding ciphertexts can be obtained.

Step 4. Surmise the corresponding keys $k0^{(8)}$, $k13^{(8)}$, $k10^{(8)}$, $k7^{(8)}$ of the Byte 0, 13, 10, 7 of the 8th-round ciphertexts, do the inverse operation of S-box $S^{-1}(C0^{(8)} \oplus k0^{(8)})$, $S^{-1}(C13^{(8)} \oplus k13^{(8)})$, $S^{-1}(C10^{(8)} \oplus k10^{(8)})$, $S^{-1}(C7^{(8)} \oplus k7^{(8)})$, and carry out the inverse operation MC^{-1} of MixColumns for the achieved results, select the ciphertexts whose intermediate states before the 7th MixColumns have the characteristic that only the Byte 0 equals zero (other bytes are non-zero), there are 2^{47} ($2^{55-8}=2^{47}$) possible ciphertexts.

Step 5. Surmise the corresponding keys $k4^{(8)}$, $k1^{(8)}$, $k14^{(8)}$, $k11^{(8)}$ of the Byte 4, 1, 14, 11 of the 8th-round ciphertexts, and do the inverse operation of S-box $S^{-1}(C4^{(8)} \oplus k4^{(8)})$, $S^{-1}(C1^{(8)} \oplus k1^{(8)})$, $S^{-1}(C14^{(8)} \oplus k14^{(8)})$, $S^{-1}(C11^{(8)} \oplus k11^{(8)})$, carry out the inverse operation MC^{-1} of MixColumns for the achieved results, select the ciphertexts whose intermediate states before the 7th

MixColumns have the characteristic that only the Byte 7 equals zero (other bytes are non-zero), there are 2^{39} ($2^{47-8}=2^{39}$) possible ciphertexts .

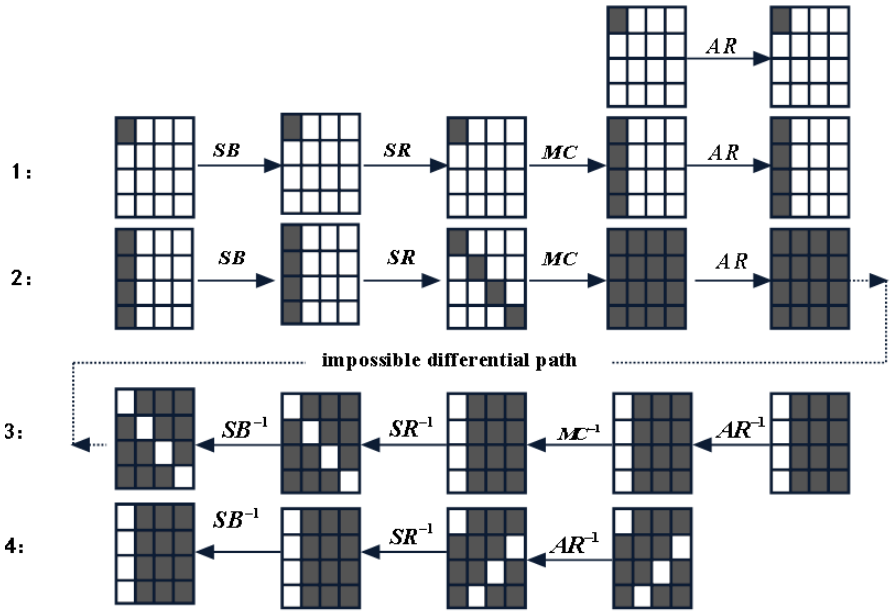

Figure 3. 4-round impossible differential path of AES

The concrete process of this attack method for AES-128 is shown in "Fig. 4."

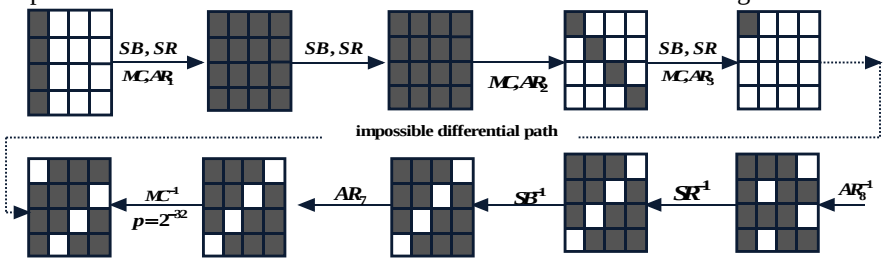

Figure 4. 8-round impossible differential path of AES

Step 6. Surmise the corresponding keys $k8^{(8)}$, $k5^{(8)}$, $k2^{(8)}$, $k15^{(8)}$ of the Byte 8, 5, 2, 15 of the 8th-round ciphertexts, and do the inverse operation of S-box $S^{-1}(C8^{(8)} \oplus k8^{(8)})$, $S^{-1}(C5^{(8)} \oplus k5^{(8)})$, $S^{-1}(C2^{(8)} \oplus k2^{(8)})$, $S^{-1}(C15^{(8)} \oplus k15^{(8)})$, carry out the inverse operation MC^{-1} of MixColumns for the achieved results, select the ciphertexts whose intermediate states before the 7th MixColumns have the characteristic that only the Byte 10 equals zero (other bytes are non-zero), there are 2^{31} ($2^{39-8}=2^{31}$) possible ciphertexts.

Step 7. Surmise the corresponding keys $k12^{(8)}$, $k9^{(8)}$, $k6^{(8)}$, $k3^{(8)}$ of the Byte 12, 9, 6, 3 of the 8th-round ciphertexts, and do the inverse operation of S-box $S^{-1}(C12^{(8)} \oplus k12^{(8)})$, $S^{-1}(C9^{(8)} \oplus k9^{(8)})$, $S^{-1}(C6^{(8)} \oplus k6^{(8)})$, $S^{-1}(C3^{(8)} \oplus k3^{(8)})$, carry out the inverse operation MC^{-1} of MixColumns for the achieved results, select the ciphertexts whose intermediate states before the 7th MixColumns have the characteristic that only the Byte 10 equals zero (other bytes are non-zero), there are 2^{23} ($2^{31-8}=2^{23}$) possible ciphertexts. Screen out the corresponding plaintexts of the 2^{23} ciphertexts.

Step 8. Surmise the corresponding keys $k12^{(8)}$, $k9^{(8)}$, $k6^{(8)}$, $k3^{(8)}$ of the Byte 12, 9, 6, 3 of the Round 0 and 1, calculate the corresponding output of Round 1with Equation (7).

$$\begin{bmatrix} C0^{(1)} \\ C1^{(1)} \\ C2^{(1)} \\ C3^{(1)} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} SB(P0^{(0)} \oplus K0^{(0)}) \\ SB(P5^{(0)} \oplus K5^{(0)}) \\ SB(P10^{(0)} \oplus K10^{(0)}) \\ SB(P15^{(0)} \oplus K15^{(0)}) \end{bmatrix} + \begin{bmatrix} K0^{(1)} \\ K5^{(1)} \\ K10^{(1)} \\ K15^{(1)} \end{bmatrix} \quad (7)$$

Step 9. Figure out the corresponding differentials of the achieved output pairs in Step 8, if the

differentials meet the $\Delta SRi^{(2)}$ (i=0, 1, 2, 3) in linear table L_3, store their corresponding plaintexts and keys $k0^{(0)}$, $k5^{(0)}$, $k10^{(10)}$, $k15^{(0)}$, $k0^{(1)}$, $k5^{(1)}$, $k10^{(1)}$, $k15^{(1)}$ into the linear table L_4. As proved in Theorem 2, with $k0^{(0)}$, $k5^{(0)}$, $k10^{(10)}$, $k15^{(0)}$, $k0^{(1)}$ fixed, a value of c_1 can be determined by a group of (m_{22}, m_{33}, m_{44}). Therefore, a group of (m_{22}, m_{33}, m_{44}) determines a group of ($k0^{(0)}$, $k5^{(0)}$, $k10^{(0)}$, $k15^{(0)}$, $k0^{(1)}$). Similarly, a group of (m_{12}, m_{23}, m_{34}), (m_{13}, m_{24}, m_{42}), or (m_{14}, m_{32}, m_{43}) decides a group of ($k0^{(0)}$, $k5^{(0)}$, $k10^{(0)}$, $k15^{(0)}$, $k5^{(1)}$), ($k0^{(0)}$, $k5^{(0)}$, $k10^{(0)}$, $k15^{(0)}$, $k10^{(1)}$), or ($k0^{(0)}$, $k5^{(0)}$, $k10^{(0)}$, $k15^{(0)}$, $k15^{(1)}$), respectively. Since there are 2^{23} qualified plaintexts, at most 2^{23} groups of ($k0^{(0)}$, $k5^{(0)}$, $k10^{(0)}$, $k15^{(0)}$, $k0^{(1)}$, $k5^{(1)}$, $k10^{(1)}$, $k15^{(1)}$) can be determined. Namely, the 4-byte initial keys are decided in Step 9.

Step 10. With the same method as exhibited in Step 9, the rest 12-byte initial keys can be decided. There are 2^{92} ($2^{23\times4}=2^{92}$) pairs of possible keys.

Step 11. Carry out key expansion on the 2^{92} initial keys, filter out the one that fails to agree with the linear table L_2. If there is a plaintext qualified, its corresponding key is the correct initial key with a error probability of 2^{-64}.

B. COMPLEX ANALYSIS AND STORAGE SPACE ANALYSIS

AES can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum.

TABLE I.
THE RESULTS OF THIS WORK COMPARED WITH OTHER REPORTED RESULTS

Source	Round	chosen plaintexts (data)	words of memory (space)	Number of encryptions (time)
[11]	5	$2^{29.5}$	2^{38}	2^{31}
[12]	6	$2^{91.5}$	2^{89}	2^{122}
[13]	6	$2^{99.5}$	2^{57}	2^{86}
[14]	7	$2^{115.5}$	2^{109}	2^{119}
[15]	7	2^{106}	$2^{90.2}$	2^{110}
[16]	7	2^{80}	2^{113}	2^{122}
This work	8	2^{87}	2^{99}	2^{96}

The Shift Rows step operates on the rows of the state in bytes, In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. With a pair of (x_i, x_j) chosen and by changing m_{jk}, according to Theorem 1 and 2 the complexity of the related parameters that agree with the differential paths in Figure 2 is 2^{96}. The required storage space are 2^{79} ($25\times2^{74}\approx2^{79}$) words of memory. In Step 2, 2^{87} plaintexts are selected to encrypted 8-round, thus the complexity is 2^{89} ($2^{87}\times2=2^{89}$), and 2^{88} words of space are required. The complexity for Step 3 is 2^{33} ($2^{32}\times2=2^{33}$). From Step 4 to Step 7, the unqualified ciphertexts are filtered out with a complexity of 2^{10} ($2^{8}\times4=2^{10}$). Since 2^{64} groups of keys require to be surmised in Step 8, so the complexity is 2^{87} ($2\times2^{64}\times2^{22}=2^{87}$), and 2^{66} ($2^{64}\times4=2^{66}$) words of memory are required. The rest 12-byte initials keys are figured out in Step 9, hence the complexity is 2^{89} ($2^{87}\times4=2^{89}$), and 2^{68} ($2^{64}\times12\approx2^{68}$) words of memory are required. In Step 10, 2^{92} encryptions and 2^{99} ($2^{92}\times2^{7}=2^{99}$) words of memory are demanded. Therefore, during the whole attack process, the highest complexity will not exceed 2^{96} and 2^{97} words of memory are enough to work. Table 1 display the results of this work compared with other reported results.

V. CONCLUSION

In this study, we have deduced a novel property of the 3-round AES encryption and further analyzed the 8-round AES-128 with the impossible differential cryptanalysis method, The analysis method requires 2^{87} pairs of chosen plaintexts, about 2^{99} words of memory and 2^{96} encryption and decryption computations. It is found that the confusing level of the MixColumns transformation in AES algorithm is insufficient, which provides a theoretical basis to improve the AES security. The 8-round analyzed in this work is the highest round of AES-128 reported so far.

ACKNOWLEDGMENT

This work is supported by the Young people project Foundation of Hubei Province (Q20122703),

Supported by Natural Science Foundation of Hubei Province (2010CDZ019)

REFERENCES

[1] J. Daemen, and V. Rijmen, "The Design of Rijndael: AES—the Advanced Encryption Standard," *Berlin: Springer-Verlag*, pp. 31-148, 2002.

[2] E. Biham, A. Biryukov, and A. Shamir "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials". In: Proceedings of Eurocrypt'99. *Berlin: Springer-Verlag, LNCS*, vol. 1592, pp. 12—23, 1999.

[3] H. Demirci, and A. A. Selçuk, "A Meet-in-the-Middle Attack on 8-Round AES". FSE 2008, *Berlin: Springer-Verlag*, vol. 5086, pp .116-126.

[4] D. Wagner, "The boomerang attack". In: Proceedings of Fast Software Encryption'99. *Berlin: Springer-Verlag*, vol. 1636, pp. 156-170, 1999.

[5] E. Biham, O. Dunkelman, and N. Neller, The Rectangle Attack—Rectangling the Serpent. In: Proceedings of Eurocrypt'01. *Berlin: Springer-Verlag, LNCS*, 2001. 2045: 340—357.

[6] S. Lucks, "The Saturation Attack-A Bait for Two Fish". In: Proceeding of Fast Software Encryption'01. *Berlin: Springer-Verlag*, vol. 2355, pp. 1-5, 2001.

[7] S. Murphy, and M. Robshaw, "Essential Algebraic Structure Within the AES". In: Proceedings of Advanced in Cryptology'02. *Berlin: Springer-Verlag*, vol. 2442, pp. 1-16, 2002.

[8] W. L. Wu, and D. G Feng, "Collision Attack on Reduced-Round Camellia". *Sci China Ser F-Inf Sci*, vol. 48, no.1, pp 78-90, 2005,

[9] J. M. Liu, and L. S. Zhao "Impossible Differential Attacks on 7-Round AES-192". *Journal of Huazhong University of Science and Technology (Natural Science Edition)*, vol. 38, no. 12, pp. 73-76, 2010

[10] X. L. Dong, Y. P. Hu, and J. Chen, "Impossible Differential Cryptanalysis on 8-round AES- 256". *Geomatics and Information Science of Wuhan University*, vol.35, no. 5, pp. 595-598, 2010

[11] E. Biham, and N. Keller, "Cryptanalysis of Reduced Variant s of Rijndael" [OL]. http:// csrc.nist. gov/encryption/aes/ round2/ conf3/ aes3papers.html, 2000.

[12] J. H. Cheon, M. Kim, and K. Kim, "Improved Impossible Differential Cryptanalysis of Rijndael and Crypton". *Berlin:Springer-Verlag*, pp. 39-49, 2001.

[13] J. Chen, Y. Y. Zhang, and Y. P. Hu, "A New Method for Impossible Differential Cryptanalysis of the 6-Round Advanced Encryption Standard". *Journal of Xi'an Univeristy of Electronic Science and Technology (Natural Science Edition)*, vol. 33, no. 4, pp. 598-601, 2006.

[14] B. Bahrak, and M. R. Aref, "Impossible Differential Attack on 7-Round AES-128". *IET Information Security*, vol. 2, no. 2, pp. 28-32, 2008.

[15] M. Hamid, D. Mohammad, and R.Vincent, "Improved Impossible Differential Cryptanalysis of 7-Round AES-128". *Berlin:Springer-Verlag*, pp. 282-291, 2010

[16] J. Chen, Y. P. Hu, and Y. Y. Zhang, "Impossible differential cryptanalysis of Advanced Encryption Standard". *Science in China (Series E: Information Sciences)*, vol. 37, no. 2, pp. 191-198, 2007.

[17] H. Demirci, İ. Taşkın, M. Çoban, and A. Baysal, "Improved Meet-in-the-Middle Attacks on AES". *INDOCRYPT*, pp. 144–156, 2009.

[18] Orr Dunkelman, Nathan Keller and Adi Shamir. "Improved Single-Key Attacks on 8-Round AES-192 and AES- 256". *ASIACRYPT*, pp. 158–176, 2010.