一种新的9轮AES_256不可能差分分析

胡志华[1,2] 覃中平[2,3] 张 青[1]

(湖北黄冈师范学院数学与信息科学学院 黄冈 438000)[1]

(武汉大学计算机学院 武汉 430079)[2] (华中科技大学软件学院 武汉 430079)[3]

摘 要 通过分析高级加密标准(AES)的4轮内部加密特征,推导出一个新的4轮差分路径,该路径存在的可能性为2^{-30},在该性质的基础上利用不可能差分分析方法,分析了9轮AES_256。该分析方法需要2^{95}对明文、约2^{163}个存储单元和约2^{193}加解密运算。通过该分析可以看出AES算法的行列变换的混淆程度不够,这为提升和改进AES安全性提供了理论依据。

关键词 AES_256,不可能差分分析,差分特征

中图法分类号 TP393 **文献标识码** A DOI 10.11896/j.issn.1002-137X.2014.08.043

Novel Method for Impossible Differential Cryptanalysis of 9-Round AES_256

HU Zhi-hua[1,2] QIN Zhong-ping[2,3] ZHANG Qing[1]

(College of Mathematical and Information Sciences, Huanggang Normal University, Huangang 438000, China)[1]

(College of Computer, Wuhan University, Wuhan 430079, China)[2]

(School of Software Engineering, Huazhong University of Science and Technology, Wuhan 430079, China)[3]

Abstract Through profound study of the 4-round encryption characteristics of advanced encryption standard (AES), a new 4-round differential path with an existing probability to of 2^{-30} has been derived. Based on this path, a novel method was proposed for impossible differential cryptanalysis of 9-round AES_256. The analysis method requires 2^{95} pairs of chosen plaintexts, about 2^{163} words of memory and 2^{193} encryption/decryption computations. According to the analysis process, it was found that the confusing level of the MixColumns transformation in AES algorithm is insufficient, which provides a theoretical basis to improve the AES security.

Keywords AES_256, Impossible differential cryptanalysis, Differential character

1 引言

美国联邦政府选择比利时密码学家Joan Daemen和Vincent Rijmen设计的Rijndael加密算法作为美国政府的高级加密标准AES(Advanced Encryption Standard)[1]。AES是在替代置换网络结构基础上设计的一种新的分组加密算法,其输入的分组长度为128bit,以字节为处理单元,密钥长度有128bit、192bit和256bit这3种选择,常用AES_128、AES_192和AES_256表示。AES在设计之初就考虑到差分和线性攻击,由于线性置换层的不完全扩散性,导致近几年出现了飞来器攻击、矩形攻击、不可能差分攻击、相关密钥攻击、旁路攻击、中间相遇攻击、内部结构碰撞攻击、代数攻击等几种新的分析方法[2]。不可能差分攻击是针对高级加密标准AES提出的一种有效的密码攻击方法。该方法也是近几年分析其他分组密码的有效方法之一。由于密钥编排的原因,AES_192和AES_256的线性置换层的不完全扩散性比AES_128更为显著,致使AES_192和AES_256的攻击进展速度更快[2,3]。

2000年Biham等人第一次提出了针对4轮AES_128的不可能差分攻击方法[4]。2002年Cheon等人又提出了6轮AES_128的不可能差分攻击方法[5]。2004年Raphael等人提出了7轮AES_192和AES_256的不可能差分攻击方法[6],该方法攻击7轮AES_192需要2^{92}选择明文,2^{186}次7轮加密和2^{153}组记忆存储空间;攻击AES_256需要$2^{92.5}$选择明文,$2^{250.5}$的7轮加密和2^{153}组记忆存储空间。2006年陈杰等人给出了改进的6轮AES_128不可能差分攻击方法[7]。2007年陈杰、胡予濮等人把该方法应用到8轮AES_256中,该方法需要2^{101}组选择明文,2^{228}次8轮加密,2^{201}组记忆存储空间[8]。2008年Bahrak等人用该方法把分析AES_128的轮数提高到7轮[9]。2010年Hamid Mala等人给出了该方法攻击AES_128的7轮改进方法[2]。2010年刘景美、赵林森等人设计了一种改进的7轮AES_192的不可能差分分析方法,该方法需要2^{78}的选择明文,2^{155}的7轮加密,以及2^{79}分组的记忆存储空间[9]。通过研究,可以发现上述分析方法的一个共同点:先利用AES的列变换的一个性质来构造一个4轮的不

到稿日期:2013-12-05 返修日期:2014-02-21 本文受国家自然科学基金(60673071),湖北省自然科学基金(2012FFC034,2011CDC028,2013CFB473),湖北省教育厅项目(D20132903)资助。

胡志华(1976—),男,博士,副教授,主要研究方向为密码分析与设计,E-mail:huzhihua123@126.com;覃中平(1949—),男,教授,博士生导师,主要研究方向为密码分析与设计;张 青(1965—),女,博士,教授,主要研究方向为信息系统安全。

可能差分路径[4,9,10]，然后在该路径的前面和后面分别加上一个可能的差分路径，再通过差分分析的方法来恢复部分初始密钥位。2009年，针对AES_192和AES_256的分析取得重要进展，Biryukov A、Khovratovich D等人假设在一对有一定差分关系密钥的作用下可以分析12轮AES_192和14轮的AES_256，揭示了这两种密码体制的内部结构[11,12]。2012年，胡志华、覃中平将该结果与不可能差分结合分析了14轮AES_256，进一步揭示了该体制内部结构的脆弱性[13]。但是，在2010年，Orr Dunkelman、Nathan Keller和Adi Shamir在文献[16]中就指出文献[11,12]中的分析方法是一种不切实际的分析方法，同时针对该文献中的结果，提出了一种新的分析8轮AES_192和AES_256中间相遇攻击方法，该方法分析AES_192需要2^{127}对明文，2^{128}组存储单元，2^{188}次加解密；分析AES_256需要2^{113}对明文，2^{129}组存储单元，2^{196}次加解密[14]。

针对AES的分析方法，中间相遇攻击也是研究的热点，2009年，Demirci等人在文献[15]中分析AES加密算法内部结构，给出4轮AES加密的映射性质。通过该性质，给出分析7轮AES_128的一种新的中间相遇攻击方法，该方法需要2^{80}的选择明文，2^{113}的7轮加密，以及2^{122}组记忆存储空间。2010年，Dunkelman、Keller、Shamir[14]在该性质的基础上构造了一个4轮的差分特征，用来攻击8轮的AES_192和AES_256。本文在文献[14,15]的基础上推导出4轮AES的一个新性质，在该性质的基础上利用不可能差分分析方法，分析了9轮AES_256。该结果也是目前公开的文献上在没有任何假设条件下分析AES_256轮数最高的方法。

2 预备知识

高级加密标准AES的分组输入长度是128bit。128bit数据可用4行4列的方阵表示，方阵中以字节为计算单元，每列可以看成是4字节的字。根据需要，其初始密钥有128bit、192bit和256bit这3种选择[1]，每一轮的加密密钥可用列$Nk=4,6,8$，每列4字节的矩阵表示。针对选择不同的初始密钥，加解密过程中迭代的轮数也各不相同：AES_128、AES_192和AES_256需要迭代$Nr=10,12,14$轮。AES算法在第一轮之前执行输入明文和初始密钥的密钥加法运算AddRoundKey()。在最后一轮无列混淆变换MixColumns()外，其他轮函数均由非线性S盒替换SubBytes()、行循环移位ShiftRows()、列混淆变换MixColumns()及密钥加运算AddRoundKey()这4个部件构成[1]。

2.1 符号表示

我们常用0,1,…,15对AES方阵中的元素从上到下、从左到右进行编号，也常用行列坐标来进行编号，行和列均可用a,b为1,2,3,4编号。用(P,P')表示一对输入的明文，(C,C')则表示一对输出的密文，$m_{ab}^{(k)}$表示第k轮输入a行、b列所对应的单元($k=0$时表示为初始输入)，$C_{ab}^{(k)}$表示第k轮加密输出第a行、b列对应的单元。$SR_{ab}^{(k)}$表示第k轮行变换后第a行、b列所对应的单元。用SB表示非线性S盒层替换，SR表示行循环左移位，MC表示列混淆线性变换，AR表示密钥加运算。SB^{-1}、SR^{-1}、MC^{-1}、AR^{-1}分别表示其对应的逆运算。

2.2 AES的列混淆变换

高级加密标准AES中列变换MixColumns()是以每一列为单位的线性变换，可用如下的一个矩阵乘积表示：

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \tag{1}$$

其中，$[a_0\ a_1\ a_2\ a_3]^{\mathrm{T}}$为4字节的输入，$[b_0\ b_1\ b_2\ b_3]^{\mathrm{T}}$为4字节的输出。

性质1 如果高级加密标准中列变换输出对的差分为$[\gamma\ 0\ 0\ 0]^{\mathrm{T}}$，则输入对的差分为$[0E\gamma\ 09\gamma\ 0D\gamma\ 0B\gamma]^{\mathrm{T}}$。

证明：根据列变换MixColumns()有

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}^{-1} \times \begin{bmatrix} \gamma \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0E\gamma \\ 09\gamma \\ 0D\gamma \\ 0B\gamma \end{bmatrix} \tag{2}$$

式中，02、03、01为十六进制常量。输入差分为非零时输出差分必定为非零，并且输出差分只有1个非零字节的情况有4种可能，因此输出差分只有1个非零字节概率是$(2^8-1)\times 4/2^{32}\approx 2^{-22}$。性质1的逆命题也是成立的，即当输入差分满足$[0E\gamma\ 09\gamma\ 0D\gamma\ 0B\gamma]^{\mathrm{T}}$时，输出差分满足$[\gamma\ 0\ 0\ 0]^{\mathrm{T}}$。

3 一种新的4轮差分路径

文献[15]中Demirci等人设计了一个新的4轮区分器，在该区分器中可用25个字节变量来表示$C_{11}^{(4)}$。文献[14]中Dunkelman等人设计了一个特殊的4轮差分路径，在该路径中，当输入差分在第一个字节为非零，其他字节的差分为零时，经过4轮加密以后，输出差分如果满足仅在第一个字节为非零，则第1轮加密后输出差分可能最多有2^{32}种情况。在上述4轮区分器和4轮差分路径的基础之上可以推导出一个重要的4轮区分器及一个新的4轮差分路径。

3.1 新的4轮AES区分器

构造如图1中所示的明文，令其满足$m_{11}^{(0)}+k_{11}^{(0)}=x$，$m_{21}^{(0)}+k_{21}^{(0)}=0$，$m_{31}^{(0)}+k_{31}^{(0)}=0$，$m_{41}^{(0)}+k_{41}^{(0)}=0$，一轮加密后，其密文满足图1。

$m_{11}^{(0)}+k_{11}^{(0)}=x$	$m_{12}^{(0)}+k_{12}^{(0)}$	$m_{13}^{(0)}+k_{13}^{(0)}$	$m_{14}^{(0)}+k_{14}^{(0)}$
$m_{21}^{(0)}+k_{21}^{(0)}$	$m_{22}^{(0)}+k_{22}^{(0)}=0$	$m_{23}^{(0)}+k_{23}^{(0)}$	$m_{24}^{(0)}+k_{24}^{(0)}$
$m_{31}^{(0)}+k_{31}^{(0)}$	$m_{32}^{(0)}+k_{32}^{(0)}$	$m_{33}^{(0)}+k_{33}^{(0)}=0$	$m_{34}^{(0)}+k_{34}^{(0)}$
$m_{41}^{(0)}+k_{41}^{(0)}$	$m_{42}^{(0)}+k_{42}^{(0)}$	$m_{43}^{(0)}+k_{43}^{(0)}$	$m_{44}^{(0)}+k_{44}^{(0)}=0$

一轮加密

$2x+k_{11}^{(1)}$	$m_{12}^{(1)}+k_{12}^{(1)}$	$m_{13}^{(1)}+k_{13}^{(1)}$	$m_{14}^{(1)}+k_{14}^{(1)}$
$x+k_{21}^{(1)}$	$m_{22}^{(1)}+k_{22}^{(1)}$	$m_{23}^{(1)}+k_{23}^{(1)}$	$m_{24}^{(1)}+k_{24}^{(1)}$
$x+k_{31}^{(1)}$	$m_{32}^{(1)}+k_{32}^{(1)}$	$m_{33}^{(1)}+k_{33}^{(1)}$	$m_{34}^{(1)}+k_{34}^{(1)}$
$3x+k_{41}^{(1)}$	$m_{42}^{(1)}+k_{42}^{(1)}$	$m_{43}^{(1)}+k_{43}^{(1)}$	$m_{44}^{(1)}+k_{44}^{(1)}$

图1 构造明文结构图

当改变图1中x的值(即改变$m_{11}^{(0)}$的值)，固定其它输入字节时，可以构造不同的输入差分；当选定一个输入差分，改变其它输入字时，则可以构造不同的输入对。

定理1 如果输入对(P,P')满足图1的结构，3轮加密变换以后，能用20个1字节的常量表示第三轮输出差分中的$\Delta C_{11}^{(3)}$，$\Delta C_{22}^{(3)}$，$\Delta C_{33}^{(3)}$，$\Delta C_{44}^{(3)}$；4轮加密以后，可用24个1字节的常量表示第四轮输出差分中的$\Delta C_{11}^{(4)}$。

证明：输入对(P,P')经过2轮变换以后，$C_{11}^{(2)}$可以用如下

形式表示：

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

同理，$C_{22}^{(2)}$、$C_{33}^{(2)}$、$C_{44}^{(2)}$可以用如下形式表示：

$$C_{22}^{(2)}=S(x+k_{41}^{(1)})+c_2$$
$$C_{33}^{(2)}=2S(x+k_{31}^{(1)})+c_3$$
$$C_{44}^{(2)}=S(3x+k_{21}^{(1)})+c_4$$

进一步推导，$C_{11}^{(3)}$，$C_{22}^{(3)}$，$C_{33}^{(3)}$，$C_{44}^{(3)}$可用如下形式表示：

$$C_{11}^{(3)}=2S(2S(2x+k_{11}^{(1)})+c_1)+3S(S(x+k_{41}^{(1)})+c_2)+S(2S(x+k_{31}^{(1)})+c_3)+S(S(3x+k_{21}^{(1)})+c_4)+k_{11}^{(3)}$$

$$C_{22}^{(3)}=S(S(x+k_{41}^{(1)})+c_5)+2S+(3S(x+k_{31}^{(1)})+c_6)+3S(S(3x+k_{21}^{(1)})+c_7)+S(3S(2x+k_{11}^{(1)})+c_8)+k_{22}^{(3)}$$

$$C_{33}^{(3)}=S(S(x+k_{31}^{(1)})+c_9)+S(2S(3x+k_{21}^{(1)})+c_{10})+2S(S(2x+k_{11}^{(1)})+c_{11})+3S(2S(x+k_{41}^{(1)})+c_{12})+k_{33}^{(3)}$$

$$C_{44}^{(3)}=3S(3S(3x+k_{21}^{(1)})+c_{13})+S(S(2x+k_{11}^{(1)})+c_{14})+S(3S(x+k_{41}^{(1)})+c_{15})+2S(S(x+k_{31}^{(1)})+c_{16})+k_{44}^{(3)}$$

其中 $c_1,c_2,\cdots,c_{16},k_{11}^{(1)},k_{21}^{(1)},k_{31}^{(1)},k_{41}^{(1)}$ 均为 1 字节常量，S() 为 S 盒变换，所以 $C_{11}^{(3)}$，$C_{22}^{(3)}$，$C_{33}^{(3)}$，$C_{44}^{(3)}$ 可以用一个 24 字节的常量表示。当改变 x 的值，就构造了不同的输入对，经过 3 轮加密后，输出差分中的 $\Delta C_{11}^{(3)}$，$\Delta C_{22}^{(3)}$，$\Delta C_{33}^{(3)}$，$\Delta C_{44}^{(3)}$ 可用如下的形式表示：

$$\Delta C_{11}^{(3)}=2S(2S(2x+k_{11}^{(1)})+c_1)+2S(2S(2x'+k_{11}^{(1)})+c_1)+3S(S(x+k_{41}^{(1)})+c_2)+3S(S(x'+k_{41}^{(1)})+c_2)+S(2S(x+k_{31}^{(1)})+c_3)+S(2S(x'+k_{31}^{(1)})+c_3)+S(S(3x+k_{21}^{(1)})+c_4)+S(S(3x'+k_{21}^{(1)})+c_4) \quad (3)$$

$$\Delta C_{22}^{(3)}=S(S(x+k_{41}^{(1)})+c_5)+S(S(x'+k_{41}^{(1)})+c_5)+2S(3S(x+k_{31}^{(1)})+c_6)+2S(3S(x'+k_{31}^{(1)})+c_6)+3S(S(3x+k_{21}^{(1)})+c_7)+3S(S(3x'+k_{21}^{(1)})+c_7)+S(3S(2x+k_{11}^{(1)})+c_8)+S(3S(2x'+k_{11}^{(1)})+c_8) \quad (4)$$

$$\Delta C_{33}^{(3)}=S(S(x+k_{31}^{(1)})+c_9)+S(S(x'+k_{31}^{(1)})+c_9)+S(2S(3x+k_{21}^{(1)})+c_{10})+S(2S(3x'+k_{21}^{(1)})+c_{10})+2S(S(2x+k_{11}^{(1)})+c_{11})+2S(S(2x'+k_{11}^{(1)})+c_{11})+3S(2S(x+k_{41}^{(1)})+c_{12})+3S(2S(x'+k_{41}^{(1)})+c_{12}) \quad (5)$$

$$\Delta C_{44}^{(3)}=3S(3S(3x+k_{21}^{(1)})+c_{13})+3S(3S(3x'+k_{21}^{(1)})+c_{13})+S(S(2x+k_{11}^{(1)})+c_{14})+S(S(2x'+k_{11}^{(1)})+c_{14})+S(3S(x+k_{41}^{(1)})+c_{15})+S(3S(x'+k_{41}^{(1)})+c_{15})+2S(S(x+k_{31}^{(1)})+c_{16})+2S(S(x'+k_{31}^{(1)})+c_{16}) \quad (6)$$

因此，可用 8 字节常量 $k_{11}^{(1)}$、$k_{21}^{(1)}$、$k_{31}^{(1)}$、$k_{41}^{(1)}$、c_1、c_2、c_3、c_4 表示 $\Delta C_{11}^{(3)}$。同理，$\Delta C_{22}^{(3)}$、$\Delta C_{33}^{(3)}$、$\Delta C_{44}^{(3)}$ 均可以用一个 8 字节的常量表示。因此，$\Delta C_{11}^{(3)}$、$\Delta C_{22}^{(3)}$、$\Delta C_{33}^{(3)}$、$\Delta C_{44}^{(3)}$ 可以用一个 20 字节的常量表示。$C_{11}^{(4)}=2S(C_{11}^{(3)})+3S(C_{22}^{(3)})+S(C_{33}^{(3)})+S(C_{44}^{(3)})$，而 $C_{11}^{(3)}$、$C_{22}^{(3)}$、$C_{33}^{(3)}$、$C_{44}^{(3)}$ 需用 24 个 1 字节的常量表示，因此，可以用一个 24 字节的常量表示 $\Delta C_{11}^{(4)}$。

3.2 新的 4 轮差分路径

利用 3.1 节中设计的 4 轮区分器，可设计一个新的 4 轮差分路径，具体如图 2 所示。

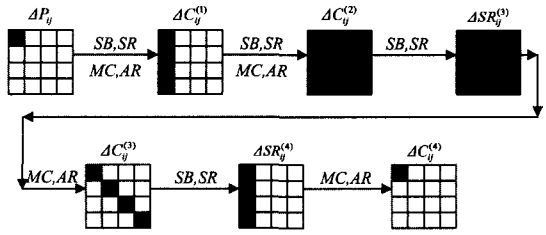

图 2 4 轮的差分路径

图 2 中，$\Delta SR_{mn}^{(4)}$ 可用式(7)表示：

$$\Delta SR_{mn}^{(4)}=\begin{bmatrix}0E\Delta C_{11}^{(4)} & 0 & 0 & 0\\ 0B\Delta C_{11}^{(4)} & 0 & 0 & 0\\ 0D\Delta C_{11}^{(4)} & 0 & 0 & 0\\ 09\Delta C_{11}^{(4)} & 0 & 0 & 0\end{bmatrix} \quad (7)$$

图 2 中，还有如下等式成立：

$$SB(C_{11}^{(3)})\oplus SB(C'^{(3)}_{11})=\Delta SR_{11}^{(4)}$$
$$SB(C_{22}^{(3)})\oplus SB(C'^{(3)}_{22})=\Delta SR_{21}^{(4)}$$
$$SB(C_{33}^{(3)})\oplus SB(C'^{(3)}_{33})=\Delta SR_{31}^{(4)}$$
$$SB(C_{44}^{(3)})\oplus SB(C'^{(3)}_{4})=\Delta SR_{41}^{(4)}$$

因此，$\Delta SR_{mn}^{(3)}$ 中的每一个单元可用式(8)表示：

$$\Delta SR_{mn}^{(3)}=\begin{bmatrix}0E\Delta C_{11}^{(3)} & 09\Delta C_{22}^{(3)} & 0D\Delta C_{33}^{(3)} & 0B\Delta C_{44}^{(3)}\\ 0B\Delta C_{11}^{(3)} & 0E\Delta C_{22}^{(3)} & 09\Delta C_{33}^{(3)} & 0D\Delta C_{44}^{(3)}\\ 0D\Delta C_{11}^{(2)} & 0B\Delta C_{22}^{(2)} & 0E\Delta C_{33}^{(2)} & 09\Delta C_{44}^{(2)}\\ 09\Delta C_{11}^{(2)} & 0D\Delta C_{22}^{(2)} & 0B\Delta C_{33}^{(2)} & 0E\Delta C_{44}^{(2)}\end{bmatrix} \quad (8)$$

定理 2 构造满足如图 1 所示输入明文对，并且其差分满足如图 2 所示的输入结构，经 4 轮加密以后，其输出差分满足图 2 所示的结构，其存在的概率是 2^{-30}。

证明：可使用 $c_1,c_2,\cdots,c_{16}$ 表示 $\Delta C_{11}^{(4)}$，构造明文的数量取决于 $c_1,c_2,\cdots,c_{16}$ 的可能性。在一次加密的过程中 $k_{11}^{(1)}$、$k_{22}^{(1)}$、$k_{33}^{(1)}$、$k_{44}^{(1)}$、$k_{11}^{(2)}$ 是固定的，因此，一个 c_1 的值取决于 $m_{22}^{(1)}$、$m_{33}^{(1)}$、$m_{44}^{(1)}$ 的可能性，其值为 2^{16}。同理，c_2 的值取决于 $m_{12}^{(1)}$、$m_{23}^{(1)}$、$m_{34}^{(1)}$ 的可能性；c_3 的值取决于 $m_{13}^{(1)}$、$m_{24}^{(1)}$、$m_{42}^{(1)}$ 的可能性；c_4 的值取决于 $m_{14}^{(1)}$、$m_{32}^{(1)}$、$m_{43}^{(1)}$ 的可能性，其值均为 2^{16}。因此，1 组 c_1、c_2、c_3、c_4 的值可由 2^{64} 组 $m_{22}^{(1)}$、$m_{33}^{(1)}$、$m_{44}^{(1)}$、$m_{12}^{(1)}$、$m_{23}^{(1)}$、$m_{34}^{(1)}$、$m_{13}^{(1)}$、$m_{24}^{(1)}$、$m_{42}^{(1)}$、$m_{14}^{(1)}$、$m_{32}^{(1)}$、$m_{43}^{(1)}$ 得到。同理，c_5、c_6、c_7、c_8；c_9、c_{10}、c_{11}、c_{12} 和 c_{13}、c_{14}、c_{15}、c_{16} 均可以由 $m_{33}^{(1)}$、$m_{44}^{(1)}$、$m_{12}^{(1)}$、$m_{23}^{(1)}$、$m_{34}^{(1)}$、$m_{13}^{(1)}$、$m_{24}^{(1)}$、$m_{42}^{(1)}$、$m_{14}^{(1)}$、$m_{32}^{(1)}$、$m_{43}^{(1)}$ 得到，其值均为 2^{64}。c_i 的值决定了 $\Delta C_{11}^{(3)}$、$\Delta C_{22}^{(3)}$、$\Delta C_{33}^{(3)}$、$\Delta C_{44}^{(3)}$ 的值。根据性质 1 中证明存在的可能性，满足第三轮的输出差分 $\Delta C_{11}^{(3)}\neq 0$、$\Delta C_{21}^{(3)}=0$、$\Delta C_{31}^{(3)}=0$、$\Delta C_{41}^{(3)}=0$ 的 c_1、c_2、c_3、c_4 有 $2^{32-22}=2^{10}$ 组。即 $\Delta C_{11}^{(3)}$ 存在互不相同的差分数量为 2^{10}。同理可以证明 $\Delta C_{22}^{(3)}$、$\Delta C_{33}^{(3)}$、$\Delta C_{44}^{(3)}$ 存在互不相同的差分数量均为 2^{10}。根据性质 1 中证明存在的可能性，$\Delta C_{11}^{(4)}$ 存在的差分数量为 $2^{40-22}=2^{18}$。由于存在重复的差分特征，c_1、c_2、c_3、c_4 存在的最大值为 2^{10} 组。由此可以证明满足图 2 中的 4 轮差分路径的输入有 $2^{64+10}=2^{74}$ 对。构造如图 1 所示的明文，固定一个图 2 所示的输入差分，在一次加密过程中加密密钥是固定的，并且 $m_{21}^{(0)}+k_{21}^{(0)}=0$、$m_{31}^{(0)}+k_{31}^{(0)}=0$、$m_{41}^{(0)}+k_{41}^{(0)}=0$，因此，$m_{21}^{(0)}$、$m_{31}^{(0)}$、$m_{41}^{(0)}$ 也被固定。因此，改变余下 $m_{ij}^{(0)}$ 的值，可构造的输入对为 2^{104} 对。由此可以证明，满足图 2 中 4 轮差分路径存在的概率为 $2^{74-104}=2^{-30}$。

4 9轮AES_256的不可能差分分析

下面给出一种攻击9轮AES_256的新方法。为了提升攻击的效果，在文献[4-8]的基础上先设计一个如图3所示的4轮不可能差分路径。

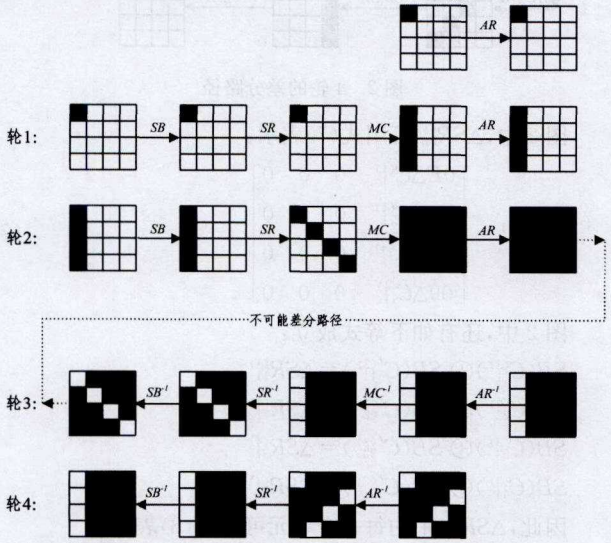

图3 4轮不可能差分路径

在图3的4轮不可能差分路径前面加4轮可能的差分路径，在其后面加1轮可能的差分路径来构造一个9轮的不可能差分路径。利用该路径攻击9轮AES_256，如图4所示。

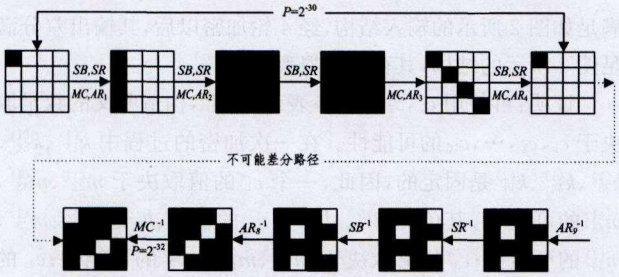

图4 9轮AES_256的不可能差分路径

4.1 攻击9轮AES_256的过程

根据定理2可以得知图4中前4轮路径存在的概率为2^{-30}，在4轮不可能差分路径后增加一轮的概率为2^{-32}。攻击9轮AES_256共12步，步骤如下：

Step 1 构造如图1中所示的明文，当改变图1中x的值(即改变$m_{11}^{(0)}$的值)时可以构造$2^8-1\approx 2^8$种输入差分，改变$m_{ab}^{(0)}$中非$m_{11}^{(0)}$的值可构造$2^{104+8}=2^{112}$对输入。固定一个差分特征值，如果$\Delta C_{11}^{(3)}$非零，$\Delta C_{11}^{(3)}$对应的列中其他字节差分值为零，需满足如下关系，$\Delta C_{11}^{(2)}=0E\gamma$、$\Delta C_{22}^{(2)}=09\gamma$、$\Delta C_{33}^{(2)}=0D\gamma$、$\Delta C_{44}^{(2)}=0B\gamma$($\gamma$为$\Delta C_{11}^{(3)}$的值)，并且存在的可能性为$2^{16}$种情况。所以，可用20个1字节中的$2^{64}$种情况表示$\Delta C_{11}^{(3)}$、$\Delta C_{22}^{(3)}$、$\Delta C_{33}^{(3)}$、$\Delta C_{44}^{(3)}$。猜测$k_{11}^{(3)}$、$k_{22}^{(3)}$、$k_{33}^{(3)}$、$k_{44}^{(3)}$，使$\Delta C_{11}^{(4)}$非零，$\Delta C_{11}^{(4)}$对于列的其他元素为零，能有24个1字节中的$2^{64+32-22}=2^{74}$种。计算$c_1$、$c_2$、$c_3$、$c_4$；$c_5$、$c_6$、$c_7$、$c_8$；$c_9$、$c_{10}$、$c_{11}$、$c_{12}$和$c_{13}$、$c_{14}$、$c_{15}$、$c_{16}$，使其满足图2中输出差分，其值存于线性表$L_1$中；计算$\Delta C_{11}^{(2)}$，$\Delta C_{22}^{(2)}$、$\Delta C_{33}^{(2)}$、$\Delta C_{44}^{(2)}$、$k_{11}^{(2)}$、$k_{22}^{(2)}$、$k_{33}^{(2)}$、$k_{44}^{(2)}$的值，其结果存于线性表$L_2$中；利用式(5)来计算$\Delta SR_{ab}^{(3)}$的值，其结果存于线性表$L_3$中。

Step 2 选择Step 1中的2^{95}明文对，对其进行9轮加密，得到相对应的2^{95}密文对。

Step 3 筛选输出差分在5,7,12,14字节处为零的密文对，可得到$2^{95-32}=2^{63}$密文对。

Step 4 猜测第9轮加密密钥中的$k0^{(9)}$，$k13^{(9)}$，$k10^{(9)}$，$k7^{(9)}$，并做逆S盒变换$S^{-1}(C0^{(9)}\oplus k0^{(9)})$、$S^{-1}(C13^{(9)}\oplus k13^{(9)})$、$S^{-1}(C10^{(9)}\oplus k10^{(9)})$、$S^{-1}(C7^{(9)}\oplus k7^{(9)})$，然后再做逆$MC^{-1}$变换，筛选第8轮列变换前第0字节处为零，该列对于的其他字节不为零的密文对有$2^{63-8}=2^{55}$对。

Step 5 猜测第9轮加密密钥中的$k4^{(9)}$，$k1^{(9)}$，$k14^{(9)}$，$k11^{(9)}$，并做逆S盒变换$S^{-1}(C4^{(8)}\oplus k4^{(8)})$，$S^{-1}(C1^{(8)}\oplus k1^{(8)})$，$S^{-1}(C14^{(8)}\oplus k14^{(8)})$，$S^{-1}(C11^{(9)}\oplus k11^{(9)})$。然后再做逆$MC^{-1}$变换，筛选第8轮列变换前第7字节处为零，该列对于的其他字节不为零的密文对有$2^{55-8}=2^{47}$对。

Step 6 猜测第9轮加密密钥中的$k8^{(9)}$，$k5^{(9)}$，$k2^{(9)}$，$k15^{(9)}$，并做逆S盒变换$S^{-1}(C8^{(9)}\oplus k8^{(9)})$，$S^{-1}(C5^{(9)}\oplus k5^{(9)})$，$S^{-1}(C2^{(9)}\oplus k2^{(9)})$，$S^{-1}(C15^{(9)}\oplus k15^{(9)})$。然后再做逆$MC^{-1}$变换，筛选第8轮列变换前第10字节处为零，该列对于的其他字节不为零的密文对有$2^{47-8}=2^{39}$对。

Step 7 猜测第9轮密文对12,9,6,3处对应的密钥$k12^{(9)}$，$k9^{(9)}$，$k6^{(9)}$，$k3^{(9)}$，并做S盒的逆运算$S^{-1}(C12^{(9)}\oplus k12^{(9)})$，$S^{-1}(C9^{(9)}\oplus k9^{(9)})$，$S^{-1}(C6^{(9)}\oplus k6^{(9)})$，$S^{-1}(C3^{(9)}\oplus k3^{(9)})$。把得到的结果作逆的列变换$MC^{-1}$，筛选第8轮列变换前第13字节处为零，该列对于的其他字节不为零的密文对有$2^{39-8}=2^{31}$对。并筛选出满足Step 4－Step 7中2^{31}对密文所对应的明文。

Step 8 猜测初始密钥的128位及$k0^{(1)}$，$k5^{(1)}$，$k10^{(1)}$，$k15^{(1)}$，加密Step 7中筛选出的2^{31}对明文，得到2^{159}对一轮加密结果中的$C_{11}^{(1)}$、$C_{22}^{(1)}$、$C_{33}^{(1)}$、$C_{44}^{(1)}$。猜测第2轮在0,1,2,3处对应的密钥$k0^{(2)}$、$k1^{(2)}$、$k2^{(2)}$、$k3^{(2)}$，输出对应的第二轮输出的第一列$C_{11}^{(2)}$、$C_{21}^{(2)}$、$C_{31}^{(2)}$、$C_{41}^{(2)}$并计算$\Delta S(C_{11}^{(2)})$、$\Delta S(C_{21}^{(2)})$、$\Delta S(C_{31}^{(2)})$、$\Delta S(C_{41}^{(2)})$，当$\Delta S(C_{11}^{(2)})$、$\Delta S(C_{21}^{(2)})$、$\Delta S(C_{31}^{(2)})$、$\Delta S(C_{41}^{(2)})$在线性表L_3中$\Delta SR_{11}^{(3)}$、$\Delta SR_{24}^{(3)}$、$\Delta SR_{33}^{(3)}$、$\Delta SR_{42}^{(3)}$有对应的值，将对应的128比特初始密钥和$k0^{(1)}$、$k5^{(1)}$、$k10^{(1)}$、$k15^{(1)}$、$k0^{(2)}$、$k1^{(2)}$、$k2^{(2)}$、$k3^{(2)}$存储在线性表L_6中并去掉不符合条件的明文对。

Step 9 将存储在线性表L_6中的128比特初始密钥一轮Step 8中剩下的明文，猜测$k3^{(1)}$、$k4^{(1)}$、$k9^{(1)}$、$k14^{(1)}$并得到$C_{41}^{(1)}$、$C_{12}^{(1)}$、$C_{23}^{(1)}$、$C_{34}^{(1)}$。猜测第2轮在4,5,6,7处对应密钥$k4^{(2)}$、$k5^{(2)}$、$k6^{(2)}$、$k7^{(2)}$，输出对应的第二轮输出的第一列$C_{11}^{(2)}$、$C_{21}^{(2)}$、$C_{31}^{(2)}$、$C_{41}^{(2)}$并计算$\Delta S(C_{11}^{(2)})$、$\Delta S(C_{21}^{(2)})$、$\Delta S(C_{31}^{(2)})$、$\Delta S(C_{41}^{(2)})$，当$\Delta S(C_{11}^{(2)})$、$\Delta S(C_{21}^{(2)})$、$\Delta S(C_{31}^{(2)})$、$\Delta S(C_{41}^{(2)})$在线性表L_3中$\Delta SR_{21}^{(3)}$、$\Delta SR_{12}^{(3)}$、$\Delta SR_{34}^{(3)}$、$\Delta SR_{43}^{(3)}$有对应的值，将对应的128比特初始密钥不符合条件的从线性表L_6中去掉并将$k3^{(1)}$、$k4^{(1)}$、$k9^{(1)}$、$k14^{(1)}$、$k4^{(2)}$、$k5^{(2)}$、$k6^{(2)}$、$k7^{(2)}$存储在线性表L_6中且去掉不符合条件的明文对。

Step 10 将存储在线性表L_6中的128比特初始密钥一轮Step 9中剩下的明文，猜测$k2^{(1)}$、$k7^{(1)}$、$k8^{(1)}$、$k13^{(1)}$并得到$C_{31}^{(1)}$、$C_{42}^{(1)}$、$C_{13}^{(1)}$、$C_{24}^{(1)}$。猜测第2轮在8,9,10,11处对应密钥$k8^{(2)}$、$k9^{(2)}$、$k10^{(2)}$、$k11^{(2)}$，输出对应的第二轮输出的第一列$C_{13}^{(2)}$、$C_{23}^{(2)}$、$C_{33}^{(2)}$、$C_{43}^{(2)}$并计算$\Delta S(C_{13}^{(2)})$、$\Delta S(C_{23}^{(2)})$、$\Delta S(C_{33}^{(2)})$、

$\Delta S(C_{43}^{(2)})$，当 $\Delta S(C_{13}^{(2)})$、$\Delta S(C_{23}^{(2)})$、$\Delta S(C_{33}^{(2)})$、$\Delta S(C_{43}^{(2)})$在线性表 L_3 中 $\Delta SR_{13}^{(3)}$、$\Delta SR_{22}^{(3)}$、$\Delta SR_{31}^{(3)}$、$\Delta SR_{44}^{(3)}$ 有对应的值，将对应的 128 比特初始密钥不符合条件的从线性表 L_6 中去掉并将 $k2^{(1)}$、$k7^{(1)}$、$k8^{(1)}$、$k13^{(1)}$、$k8^{(2)}$、$k9^{(2)}$、$k10^{(2)}$、$k11^{(2)}$ 存储在线性表 L_6 中并去掉不符合条件的明文对。

Step 11　将存储在线性表 L_6 中的 128 比特初始密钥一轮 Step 10 中剩下的明文，猜测 $k1^{(1)}$、$k6^{(1)}$、$k11^{(1)}$、$k12^{(1)}$ 并得到 $C_{21}^{(1)}$、$C_{32}^{(1)}$、$C_{43}^{(1)}$、$C_{14}^{(1)}$。猜测第 2 轮在 12,13,14,15 处对应密钥 $k12^{(2)}$、$k13^{(2)}$、$k14^{(2)}$、$k15^{(2)}$，输出对应的第二轮输出的第一列 $C_{14}^{(2)}$、$C_{24}^{(2)}$、$C_{34}^{(2)}$、$C_{44}^{(2)}$ 并计算 $\Delta S(C_{14}^{(2)})$、$\Delta S(C_{24}^{(2)})$、$\Delta S(C_{34}^{(2)})$、$\Delta S(C_{44}^{(2)})$，当 $\Delta S(C_{14}^{(2)})$、$\Delta S(C_{24}^{(2)})$、$\Delta S(C_{34}^{(2)})$、$\Delta S(C_{44}^{(2)})$ 在线性表 L_3 中 $\Delta SR_{41}^{(3)}$、$\Delta SR_{32}^{(3)}$、$\Delta SR_{23}^{(3)}$、$\Delta SR_{14}^{(3)}$ 有对应的值，将对应的 128 比特初始密钥不符合条件的从线性表 L_6 中去掉并将 $k1^{(1)}$、$k6^{(1)}$、$k11^{(1)}$、$k12^{(1)}$、$k12^{(2)}$、$k13^{(2)}$、$k14^{(2)}$、$k15^{(2)}$ 存储在线性表 L_6 中且去掉不符合条件的明文对。

Step 12　对最多 2^{160} 组初始密钥进行密钥扩展，筛选掉不符合存储在线性表 L_2 中的初始密钥，把符合条件的明文对和初始密钥进行一轮加密，加密的结果按照定理 1 中计算 c_1，c_2，…，c_{16}，如果有一组符合线性表 L_1 中的 c_1，c_2，…，c_{16}，则对应的密钥为正确的初始密钥，其猜错的概率为 2^{-64}。

4.2　复杂度和存储空间分析及比较

在 Step 1 中选择一个差分结构，改变 m_{jk}，根据定理 1 和定理 2 计算满足图 2 中差分路径的相关参数的复杂度为 2^{96}。所需的存储单元为 $25\times2^{74}\approx2^{79}$。对 Step 2 中选择的 2^{95} 对明文进行 9 轮加密，因此其计算复杂度为 $2^{95}\times2=2^{96}$，约需要 2^{96} 个存储单元。Step 3 筛选掉满足在 5,7,12,14 字节处差分为零的密文对，其计算复杂度为 $2^{32}\times2=2^{33}$。Step 4－Step 7 均为筛选不符合条件的密文，其计算复杂度为 $2^8\times4=2^9$。在 Step 8 中需要猜测 2^{160} 组密钥，因此其计算复杂度为 $2\times2^{160}\times2^{31}=2^{192}$，需要的存储单元为 $2^{160}\times4=2^{162}$。在 Step 9－Step 12 中，其计算复杂度最高为 $2\times2^{160}\times2^{31}=2^{192}$，需要的存储单元最多为 $2^{160}\times4=2^{162}$。

综上所述，该方法分析 9 轮 AES_256 的初始密钥，需要 2^{95} 明文对，其计算复杂度约为 2^{193}，需要的存储单元约为 2^{163}。与已有文献的比较结果见表 1。

表 1　分析结果比较

Reference	Round	Selected plaintext	Memory space	Computational complexity
[3]	8	2^{105}	2^{87}	$2^{229.58}$
[6]	8	$2^{92.5}$	2^{153}	$2^{250.5}$
[8]	8	2^{101}	2^{201}	2^{228}
[14]	8	2^{113}	2^{128}	2^{196}
[15]	8	2^{80}	2^{122}	2^{113}
本文	8	2^{87}	2^{97}	2^{96}
本文	9	2^{95}	2^{163}	2^{193}

从表 1 可以看出，攻击 9 轮 AES_256 所需要的选择明文数量、存储空间及计算复杂度都在有效的范围内。同时用该方法分析 8 轮 AES_256 的效果也比公开的文献[3,6,8,14,15]效果好，其分析方法与文献[16]中分析 AES_128 的方法一样。

结束语　本文设计并证明高级加密标准 AES 的一个新的差分路径，在该路径的基础上设计了一个新的 9 轮不可能差分路并攻击了 9 轮 AES_256。该攻击分析方法需要 2^{95} 明文对、约 2^{163} 组存储单元和约 2^{193} 加解密运算。通过分析可以看出 AES 算法的行列变换的混淆程度不够，这为我们提升和改进 AES 安全性提供理论依据。该结果也是目前公开的文献中在没有任何假设条件下分析 AES_256 轮数最高的方法。

参 考 文 献

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

[2] 刘景美，赵林森. 高级加密标准 AES-192 的 7 轮不可能差分分析[J]. 华中科技大学学报：自然科学版，2010，38(12)：73-76

[3] 董晓丽，胡予濮，陈杰. 不可能差分分析 8 轮 AES-256[J]. 武汉大学学报：信息科学版，2010，35(5)：595-598

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

[5] Cheon J H, Kim M, Kim K, et al. Improved Impossible Differential Cryptanalysis of Rijndael and Crypton[M]. Berlin: Springer-Verlag, 2002: 39-49

[6] Phan R C W. Impossible Differential Cryptanalysis of 7-round Advanced Encryption Standard (AES)[J]. Information Processing Letters, 2004, 91(1): 33-38

[7] 陈杰，张跃宇，胡予濮. 一种新的 6 轮 AES 不可能差分密码分析方法[J]. 西安电子科技大学学报：自然科学版，2006，33(4)：598-601

[8] 陈杰，胡予濮，张跃宇. 不可能差分分析高级加密标准[J]. 中国科学：信息科学，2007，37(2)：191-198

[9] Bahrak B, Aref M R. Impossible differential attack on seven-round AES-128[J]. IET Information Security, 2008, 2(2): 28-32

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

[11] Biryukov A, Dunkelman O, Keller N, et al. Key Recovery Attacks of Practical Complexity on AES-256 Variants With Up To 10Rounds[C]// Advances in Cryptology-EUROCRYPT. 2010, 6110: 299-319

[12] Biryukov A, Khovratovich D. Related-Key Cryptanalysis of the Full AES-192 and AES-256[C]// ASIACRYPT. 2009, 5912: 1-18

[13] Hu Zhi-Hua, Qin Zhong-Ping. Related Key Impossible Differential Cryptanalysis of AES_256[J]. International Journal of Advancements in Computing Technology, 2012, 4(3): 2233-9337

[14] Dunkelman O, Keller N, Shamir A. Improved Single-Key Attacks on 8-Round AES-192 and AES-256[C]// ASIACRYPT. 2010, 6477: 158-176

[15] Demirci H, Ta ISkin, Mustafa C, et al. Improved Meet-in-the-Middle Attacks on AES[C]// INDOCRYPT 2009. 2009, 5922: 144-156

[16] 胡志华，覃中平. 一种新的 8 轮 AES_128 不可能差分分析[J]. 小型微型计算机系统，2012，38(5)：73-79