文章编号: 1001- 2486(2008) 01- 0125- 04

AES 密码的三种等价形式*

冯国柱[1], 多 磊[1], 李 超[1,2]
(1. 国防科技大学 理学院, 湖南 长沙 410073;
2. 福建师范大学 网络安全与密码技术重点实验室, 福建 福州 350007)

摘 要: 分离了 AES 密码中 S 盒的仿射变换, 得到了与原密码 S 盒不同的三种等价密码。研究发现列混合矩阵在很大程度上影响仿射变换的提取, 在这种意义上提出了对列混合变换的改进建议。

关键词: AES; S 盒; 仿射变换; 等价密码
中图分类号: TN918.1 文献标识码: A

Three Kinds of Equivalent Cipher of AES

FENG Guo-zhu[1], DUO Lei, LI Chao
(1. College of Science, National Univ. of Defense Technology, Changsha 410073, China;
2. Key Lab of Network Security and Cryptology, FuJian Normal University, Fuzhou 350007, China)

Abstract: Three kinds of equivalent ciphers of AES are presented by separating S-box' s affine transformation. Results from research showed that MixColumn matrix influenced the separation of S-box' s affine transformation to a great extent. As a result, suggestions to the improvement of MixColumn algorithms were made.

Key words: AES; S-box; affine transformation; equivalent cipher

2000 年 10 月, NIST 决定选用 Rijndael 密码[1] 作为高级加密标准(AES)。本文讨论了 AES 密码的结构特点, 研究发现, 列混合矩阵在很大程度上影响仿射变换的提取, 将 S 盒的仿射变换从 S 盒中分离出来可以得到与原密码等价的三种形式。

1 AES 密码

AES 密码是一种迭代分组密码, 其分组长度和密钥长度都是可变的。分组长度和密钥长度可以独立地指定 128bit、192bit 或者 256bit。这里只介绍明文、密钥均为 128bit 的密码算法。

密码中变换最小单位是字节, 密码有 10 圈, 每圈进行如下四个变换:

(1) 字节替换 SubByte(S_B), 密码中唯一非线性变换;

(2) 行移位 ShiftRow(S_R), 1、2、3 和 4 行分别循环左移 0、1、2、3 位;

(3) 列混合 MixColumn(M_C), 左乘一列混合矩阵;

(4) 圈密钥加 AddRoundKey(A_R)。

字节替换(SubByte)是一个非线性的字节替代, 它在每个状态字节上独立地进行运算。替代表(或 S - 盒)是可逆的, 并且是由如下两个变换的合成而构造出来的: 有限域 $GF(2^8)$ 中取乘法逆, '00' 映射到它自身; 再经式(1)定义的 $GF(2)$ 上的仿射变换作用。记 A 是式(1)定义的仿射变换矩阵, $A = [a_{ij}]$, $B = [b_{ij}]$ 分别是 S 盒变换前、后的状态矩阵, 令 $b_{ij} = Aa_{ij}^{-1} \oplus c_0$, 则 S 盒变换可以表示成 $B = S_B(A)$。

* 收稿日期: 2007- 05- 16
基金项目: 国家自然科学基金资助项目(60573028); 国防科技大学预研基金项目(JC07- 02- 03); 福建师范大学网络安全与密码技术重点实验室开放课题资助项目(07A0003)
作者简介: 冯国柱(1977—), 男, 博士生。

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{1}$$

在行移位中,状态行循环移动不同的位移量。第一行不移位,第二、三、四行分别循环移位一、二、三个字节。按指定位移量进行循环移位的状态行移位运算记为 $C = S_R(B)$。如图 1 所示。

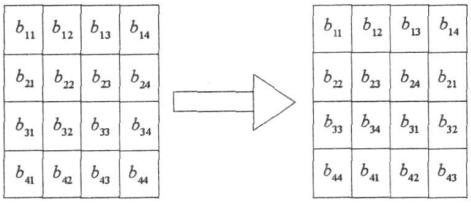

图 1 ShiftRow 变换

Fig. 1 The ShiftRow transformation

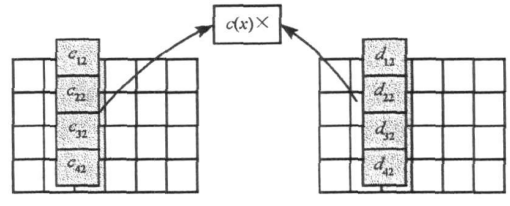

图 2 MixColumn 变换

Fig. 2 The MixColumn transformation

在列混合中,状态的列视为有限域 $GF(2^8)$ 上的多项式的系数且被一个固定的多项式 $c(x)$ 进行模 x^4+1 的乘法,这里 $c(x) = \text{'03'}\,x^3 + \text{'01'}\,x^2 + \text{'01'}\,x + \text{'02'}$,此多项式与 x^4+1 互素,因此是可逆的。这一乘法可以写成矩阵乘法。令 $b(x) = c(x) \times a(x)$, $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$, 这一运算在状态的所有列上的变换记为 $D = M_c(C)$。如图2 所示。

在圈密钥加的运算中,用简单的比特异或 EXOR 将一个圈密钥作用在状态上,圈密钥是通过密钥调度过程从密码密钥中获得的,圈密钥长度等于分组长度。将一个圈密钥异或到状态上所构成的变换记为 AddRoundKey(State, RoundKey),如图 3 所示,定义为 $E = A_R(D)$。

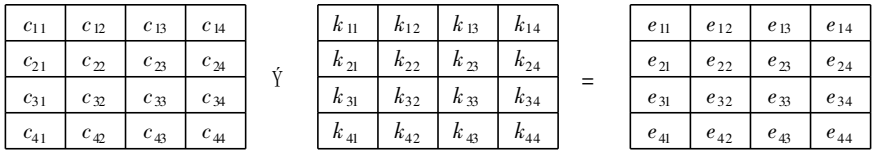

图 3 密钥加

Fig. 3 The key addition

AES 的密钥扩展算法是以 4 字节为单位的扩展算法。图 4 给出了第 $i-1$ 轮密钥和第 i 轮密钥。图中,i 表示第 i 个字节; $S[i]$ 表示对字节 i 做 $S-$ 盒变换,"+"为模二加。

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

⇨

$1+S[8]+r[i]$	$1+2+S[8]+r[i]$	$1+2+3+S[8]+r[i]$	$1+2+3+4+S[8]+[i]$
$5+S[12]$	$5+6+S[12]$	$5+6+7+S[12]$	$5+6+7+8+S[12]$
$9+S[16]$	$9+10+S[16]$	$9+10+11+S[16]$	$9+10+11+12+S[16]$
$13+S[4]$	$13+14+S[4]$	$13+14+15+S[4]$	$13+14+15+16+S[4]$

图 4 AES 密钥扩展算法

Fig. 4 Key expansion algorithm of AES

2 AES 的等价密码

2.1 改变 S 盒中常量得到的等价密码

AES 密码 S 盒中仿射变换的常量为 0×63, 它的作用并没有明确, 但设计者认为 S 盒变换中应没有不动点和反不动点, 常量加保证了密码的这种性质。我们通过研究各种变换中常量变换的作用得到了一种等价密码的结构。为描述方便, 对变量 a_{ij} 的 S 盒变换记为 $S[a_{ij}]=S[a_{ij}]\oplus c_0$, 其中 $S[a_{ij}]=Aa_{ij}^{-1}$ 是只对 a_{ij} 作逆变换和仿射矩阵的乘变换, c_0 代表常量 0×63。令 C_0 为一个 4×4 的矩阵, 其中元素 $c_{ij}=c_0$, $1\leqslant i\leqslant 4$, $1\leqslant j\leqslant 4$。

定义 1 将 AES 的 S 盒 $S[a_{ij}]=S[a_{ij}]\oplus c_0$ 变为 $S[a_{ij}]$, 密钥扩展算法中除第一轮变换外, 其余各轮均增加一个变换 $k_{ij}=k_{ij}\oplus c_0$, 称新的密码为 AES1。

定理 1 AES1 密码与 AES 密码等价。

证明 对任意 $j(j=1,2,3,4)$,

$$\begin{aligned}
c_{ij} &= 02b_{1j}+03b_{2j}+01b_{3j}+01b_{4j}\\
&= 02S(a_{1j})+03S(a_{2j})+01S(a_{3j})+01S(a_{4j})\\
&= 02(S(a_{1j})\oplus c_0)+03(S(a_{2j})\oplus c_0)+01(S(a_{3j})\oplus c_0)+01(S(a_{4j})\oplus c_0)\\
&= (02S(a_{1j})+03S(a_{2j})+01S(a_{3j})+01S(a_{4j}))\oplus(02+03+01+01)c_0\\
&= (02S(b_{1j})+03S(b_{2j})+01S(b_{3j})+01S(b_{4j}))\oplus c_0
\end{aligned}$$

故 $M_C(S_R(S_B(A)))=M_C(S_R(S_B(A)))+C_0$。同样在密钥扩展算法中, 也可提取矩阵 C_0, 因此 $M_C(S_R(S_B(A)))\oplus K=M_C(S_R(S_B(A)))\oplus K$。

推论 1 如果 AES 密码中列混合矩阵采用其他矩阵, 使得它的每一行的所有分量模二加不为 1, 则 AES1 与 AES 不等价。

2.2 改变仿射变换中乘矩阵后得到的等价密码

本节讨论的等价密码将在 AES1 的基础上进行讨论。记

$$A\leftarrow\begin{bmatrix}a_{11}&a_{12}&a_{13}&a_{14}\\a_{21}&a_{22}&a_{23}&a_{24}\\a_{31}&a_{32}&a_{33}&a_{34}\\a_{41}&a_{42}&a_{43}&a_{44}\end{bmatrix}\triangleq\begin{bmatrix}Aa_{11}&Aa_{12}&Aa_{13}&Aa_{14}\\Aa_{21}&Aa_{22}&Aa_{23}&Aa_{24}\\Aa_{31}&Aa_{32}&Aa_{33}&Aa_{34}\\Aa_{41}&Aa_{42}&Aa_{43}&Aa_{44}\end{bmatrix}$$

引理 1 记 $S(a_{ij})=a_{ij}^{-1}$, 则 $S(a_{ij})=AS(a_{ij})$。

引理 2 ShiftRow 变换与仿射矩阵 A 乘变换顺序互换, 密码值不改变。即:

$$S_R(A\leftarrow S_B(A))=A\leftarrow S_R(S_B(A))$$

引理 3 $M_C(A\leftarrow A)=A\leftarrow(A^{-1}\leftarrow(M_1(A\leftarrow A))\oplus A^{-1}\leftarrow(M_2(A\leftarrow A))\oplus(M_3A))$, 其中

$$M_1=\begin{bmatrix}02&00&00&00\\00&02&00&00\\00&00&02&00\\00&00&00&02\end{bmatrix},M_2=\begin{bmatrix}00&02&00&00\\00&00&02&00\\00&00&00&02\\02&00&00&00\end{bmatrix},M_3=\begin{bmatrix}00&01&01&01\\01&00&01&01\\01&01&00&01\\01&01&01&00\end{bmatrix},I=\begin{bmatrix}00&01&00&00\\00&00&01&00\\00&00&00&01\\01&00&00&00\end{bmatrix}$$

证明

$$\begin{aligned}
M_C(A\leftarrow A) &= (M_1\oplus M_2\oplus M_3)(A\leftarrow A)=AA^{-1}\leftarrow((M_1\oplus M_2\oplus M_3)(A\leftarrow A))\\
&= A\leftarrow(A^{-1}\leftarrow(M_1(A\leftarrow A))\oplus A^{-1}\leftarrow(M_2(A\leftarrow A))\oplus A^{-1}\leftarrow(M_3(A\leftarrow A)))\\
&= A\leftarrow(A^{-1}\leftarrow(M_1(A\leftarrow A))\oplus A^{-1}\leftarrow(M_2(A\leftarrow A))\oplus(M_3A))
\end{aligned}$$

引理 4 密钥扩展算法等价于如下变换:

$$K_{i+1}=\begin{bmatrix} 1+AS[8]+r[i] & 1+2+AS[8]+r[i] & 1+2+3+AS[8]+r[i] & 1+2+3+4+AS[8]+r[i] \\ 5+AS[12] & 5+6+AS[12] & 5+6+7+AS[12] & 5+6+7+8+AS[12] \\ 9+AS[16] & 9+10+v[16] & 9+10+11+AS[16] & 9+10+11+12+AS[16] \\ 13+AS[4] & 13+14+AS[4] & 13+14+15+AS[4] & 13+14+15+16+AS[4] \end{bmatrix}$$

定理 2 AES 密码存在等价密码 AES2, 它的算法是:

(1) S 盒变换只采用逆变换; (2) 行混合与 AES 相同; (3) 列混合如引理 3 所述; (4) 密钥扩展算法如引理 4 所述; (5) 在所有的变换外增加一个仿射变换。

由引理 1~ 引理 4 易证。

2.3 仿射变换与逆变换改变顺序的 S 盒变换

上节给出了 AES2 密码, 下面讨论将上一轮的仿射变换 A 移到下一轮变换中, 称为 AES3。

引理 5 令 $S'(a_{ij}) \triangleq S(Aa_{ij})$, 则 $S'(a_{ij})=(Aa_{ij})^{-1}$。

引理 6 在引理 5 的 S 盒条件下, AES 的密钥扩展算法等价于 AES3。

定理 3 AES3 与 AES2 等价。

3 三种等价密码的比较

如表 1、表 2 所示, 根据上面的分析, 可以发现 AES1 是最简单的一种形式, AES2 的密码结构看似相当复杂, 但 S 盒最简单。

表 1 等价密码的描述

Tab. 1 Description of the equivalent ciphers

	S 盒	行混合	列混合	密钥扩展算法
AES	$S(a_{ij})=Aa_{ij}^{-1}\oplus c_0$	相同	$D=M_C(C)$	简单
AES1	$S(a_{ij})=Aa_{ij}^{-1}$	相同	$D=M_C(C)$	简单
AES2	$S(a_{ij})=a_{ij}^{-1}$	相同	$D=T(C)\oplus T(IC))\oplus(M_3C)$	复杂
AES3	$S'(a_{ij})=(A^{-1}a_{ij})^{-1}$	相同	$D=T(C)\oplus T(IC))\oplus(M_3C)$	复杂

表 2 等价密码的抗攻击特性

Tab. 2 The anti-attack properties of the equivalent ciphers

	Square 攻击	线性攻击	差分攻击
AES	相同	相同	相同
AES1	相同	相同	相同
AES2	相同	相同	相同
AES3	相同	相同	相同

4 结 论

不同的 S 盒结构可以得到同样的密码, 因此在设计密码时不仅需要考虑 S 盒结构, 也要考虑非 S 盒结构。如果 AES 密码在设计中采用复杂的列混合结构, 则不易得到结构较简单的等价密码。

参 考 文 献:

[1] Daemen J, Rijmen V, AES Proposal: Rijndael[R]. AES Round 1 Technical Evaluation CD-1: Documentation. NIST, August 1998.

[2] Win E D, Bosselaers A, et al. The Cipher SHARK[C]//LNCS 1039: 99-112, 1996.

[3] Biham E, et al. Differential Cryptanalysis of DES-like Cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.

[4] Matsui M. Linear Cryptanalysis Method for DES Cipher[C]//LNCS, 765: 386-397, 1994.