AES S盒的分析及改进方案设计

崔 杰[1,2],刘连浩[2],刘上力[2],马虹博[2]
CUI Jie[1,2],LIU Lian-hao[2],LIU Shang-li[2],MA Hong-bo[2]

1.安徽大学 计算机科学与技术学院,合肥 230039
2.中南大学 信息科学与工程学院,长沙 410083
1.School of Computer Science and Technology,Anhui University,Hefei 230039,China
2.School of Information Science and Engineering,Central South University,Changsha 410083,China
E-mail:cvjxabcd@126.com

CUI Jie,LIU Lian-hao,LIU Shang-li,et al.Analysis of AES S-box and design of its improved method.Computer Engineering and Applications,2007,43(25):143-146.

Abstract: This paper studies the construction principle and main algebraic properties of AES S-box,points out the S-box has these characteristics that periods of affine transformed pair is 4,periods of iterative-output is less than 88,strict avalanche criterion distance is 432,the algebraic expression has only 9 items and so on.Based on that,an improved S-box has been constructed.Periods of affine transformed pair is 16 and periods of iterative-output is 256 and both the algebraic expression of S-box and InvS-box have 254 items in the improved S-box.The improved S-box has been compared with AES S-box in 10 algebraic properties,such as balanceness,strict avalanche criterion,non-linear degree,resistance against the XSL attack etc.The experimental results suggest that the improved S-box has better characteristics.
Key words: S-box;multi-output boolean permutation;affine transformation;algebraic expression

摘 要:研究了AES S盒的构造原理和主要代数性质,指出了AES S盒的仿射变换对周期为4,迭代输出周期不大于88,严格雪崩准则距离为432,代数表达式只有9项等。基于这些不足提出了构造S盒的改进方案。改进S盒的仿射变换对周期为16,迭代输出周期为256,而且S盒和逆S盒代数表达式项数均达到254项。将改进S盒与AES的S盒在平衡性、严格雪崩准则、非线性度、抗代数攻击阻力等10种代数性质上进行比较,实验结果表明改进S盒具有更好的性质。
关键词:S盒;多输出布尔置换;仿射变换;代数表达式
文章编号:1002-8331(2007)25-0143-04 **文献标识码**:A **中图分类号**:TP309.7

1 引言

自从Rijndael被确定为美国高级加密标准(AES)以来,一直受到密码学界的关注,出现了许多攻击AES方法[1,2],但目前尚未存在对完整Rijndael算法的成功攻击。S盒作为AES的唯一的非线性部件,对算法抵抗各种攻击起着关键性的作用。文献[3]通过对S盒的仿射变换的分析,指出其仿射变换对的周期为4,并没有达到最大的周期16,文献[4]指出S盒的迭代输出具有短周期的现象,且周期均不大于88,而文献[5]指出AES S盒的代数表达式只有9项,存在表达式过于简单的问题。鉴于S盒存在的不足,本文分析了S盒布尔置换的6种代数性质和只有9项的代数表达式,并提出了构造S盒的改进方案。采用该方案构造的S盒具有周期为16的仿射变换对, 迭代输出周期达到256,严格雪崩准则距离为372,S盒和逆S盒代数表达式均为254项。实验结果表明本文改进S盒比AES的S盒和文献[5]中的S盒具有更好的代数性质。

2 AES S盒构造原理及仿射变换对周期和迭代输出周期

2.1 AES S盒构造原理

AES的S盒运算是一个独立作用于状态字节的非线性变换,包括在有限域$GF(2^8)$中的求乘法逆运算和$GF(2)$下的仿射变换运算两个步骤。

(1)输入$x'\in GF(2^8)$,求$x=(x')^{-1}$,其中$(x')^{-1}$定义如下:

$$x=(x')^{-1}=\begin{cases}(x')^{254} & x'\neq 0\\ 0 & x'=0\end{cases}$$

(2)在$GF(2^8)$中的元素分量为$(x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0)$,仿射变换定义:

作者简介:崔杰(1980-),男,硕士研究生,主要研究方向:信息安全;刘连浩(1959-),男,教授,主要研究方向:信息安全与网络通信;刘上力(1978-),男,硕士研究生,工程师,主要研究方向:信息安全;马虹博(1981—),男,硕士研究生,主要研究方向:信息安全与密码学。

$$\boldsymbol{y}=\boldsymbol{L}_A\times\boldsymbol{x}=\begin{bmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{bmatrix}\begin{bmatrix}x_0\\x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\end{bmatrix}+\begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix}$$

即 $b(x)=a(x)(x^7+x^6+x^5+x^4+1)+(x^7+x^6+x^2+x)\bmod(x^8+1)$，$a(x),b(x)$分别是 $GF(2)$域下 x 和 y 的代数表达式。

2.2 AES S 盒仿射变换对周期

定义 1 $\boldsymbol{L}_{u,v}(a(x)):a(x)\mapsto b(x)=u(x)a(x)+v(x)\bmod(x^8+1)$，其中 $\boldsymbol{u}(x)=\sum_{i=0}^{7}u_ix^i$，$\boldsymbol{v}(x)=\sum_{i=0}^{7}v_ix^i$，$\boldsymbol{a}(x)=\sum_{i=0}^{7}a_ix^i$。简记为：$\boldsymbol{L}_{u,v}(a)=\boldsymbol{L}_{u,v}(a(x))$。

AES S 盒的仿射变换：$\boldsymbol{L}_{143,99}:u(x)=1+x^4+x^5+x^6+x^7$，$v(x)=x+x^2+x^6+x^7$。

若记

$$\boldsymbol{F}=\begin{bmatrix}u_7&u_6&u_5&u_4&u_3&u_2&u_1&u_0\\u_0&u_7&u_6&u_5&u_4&u_3&u_2&u_1\\u_1&u_0&u_7&u_6&u_5&u_4&u_3&u_2\\u_2&u_1&u_0&u_7&u_6&u_5&u_4&u_3\\u_3&u_2&u_1&u_0&u_7&u_6&u_5&u_4\\u_4&u_3&u_2&u_1&u_0&u_7&u_6&u_5\\u_5&u_4&u_3&u_2&u_1&u_0&u_7&u_6\\u_6&u_5&u_4&u_3&u_2&u_1&u_0&u_7\end{bmatrix}\quad\boldsymbol{a}=\begin{bmatrix}a_0\\a_1\\a_2\\a_3\\a_4\\a_5\\a_6\\a_7\end{bmatrix}\quad\boldsymbol{v}=\begin{bmatrix}v_0\\v_1\\v_2\\v_3\\v_4\\v_5\\v_6\\v_7\end{bmatrix}$$

则仿射变换 $\boldsymbol{L}_{u,v}(a)=\boldsymbol{F}\boldsymbol{a}+\boldsymbol{v}$，记 $\boldsymbol{L}_{u,v}^k(\boldsymbol{a})=\boldsymbol{L}_{u,v}(\boldsymbol{L}_{u,v}^{k-1}(\boldsymbol{a}))$，则有 $\boldsymbol{L}_{u,v}^k(\boldsymbol{a})=\boldsymbol{F}^k\boldsymbol{a}+\boldsymbol{F}^{k-1}\boldsymbol{v}+\boldsymbol{F}^{k-2}\boldsymbol{v}+\cdots+\boldsymbol{F}\boldsymbol{v}+\boldsymbol{v}$，令 $\boldsymbol{H}_{k-1}=\boldsymbol{F}^{k-1}+\boldsymbol{F}^{k-2}+\cdots+\boldsymbol{F}+\boldsymbol{E}$，$\boldsymbol{L}_{u,v}^k(\boldsymbol{a})=\boldsymbol{F}^k\boldsymbol{a}+\boldsymbol{H}_{k-1}\boldsymbol{v}$，其中 $\boldsymbol{E}$ 为 8×8 的单位阵。

定义 2 如果存在正整数 n 满足 $\boldsymbol{L}_{u,v}^n=\boldsymbol{E}$，则称 $\boldsymbol{L}_{u,v}$ 是周期的。若 n 是周期中最小的正整数，则称 $\boldsymbol{L}_{u,v}$ 的周期为 n。

AES S 盒的仿射变换对(143,99)，$\boldsymbol{u}=143=(11110001)_2$，$\boldsymbol{v}=(11000110)_2$，满足 $\boldsymbol{L}_{143,99}^4(a)=a$，故 S 盒的仿射变换周期为 4。而根据 AES 的 S 盒的仿射变换的构造方法，经计算对于任意 $\boldsymbol{u},\boldsymbol{v}\in GF(2^8)$形成的可逆仿射变换对的周期只有 1,2,4,8,16 五种情况，也就是说周期最大可达到 16，而 AES 的 S 盒选用了周期为 4 的仿射变换对。

2.3 AES S 盒的迭代输出周期

AES 的 S 盒的迭代输出周期有 5 个[4]，分别是 87,81,59,27,2，且，所以每个周期轨道之间没有交叉点。S 盒全空间的容量是 256，但元素点的周期都小于 88，还有周期为 2 的迭代轨道，所以 S 盒的迭代输出存在短周期现象。

3 布尔置换的代数性质

一个具有良好的代数性质的 S 盒能够保证算法抵抗各种密码分析的攻击。在 AES 算法中对长度为 128 bit 的明文加密运算，S 盒共要用到 160 次，因此 S 盒的任何不好的性质都将影响到整个算法的安全性。S 盒是一个 8 位输入 8 位输出的多输出布尔函数，8 个布尔函数之间的相互制约、相互影响。即使 8 个函数同时具有某种性质，它们构成的多输出布尔函数却未必具有类似的性质[6]，所以必须对 S 盒的整体代数性质进行分析。

定义 3 设 $F(x)=(f_1(x),\cdots,f_n(x))$是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换，称 $\max\limits_{\substack{\alpha\in GF(2)^n\\ \beta\in GF(2)^n\\ \alpha\neq 0}}|\{x|F(x)+F(x+\alpha)=\beta\}|$为 $F(x)$的差分均匀度。

差分均匀度是用来衡量算法抵抗差分攻击能力的指标。布尔置换的差分均匀度越接近最小值 1，抗差分分析能力越强[6]。AES S 盒的差分均匀度是 4，具有一定的抵抗差分攻击的能力。

定义 4 设 $F(x)=(f_1(x),\cdots,f_n(x))$是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换，若 $\alpha\in GF(2)^n$，满足 $F(x)+F(x+\alpha)$常量，则称 α 为 $F(x)$的线性结构。

AES S 盒没有非零线性结构[6]。

文献[6]指出，对于 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换 $F(x)=(f_1(x),\cdots,f_n(x))$，如果对 $\forall\alpha\in GF(2)^n$ 且 $w(\alpha)=1$ 即 α 的汉明重量为 1 时，有 $w(f_i(x+\alpha)+f_i(x))=2^{n-1}$ $(1\leqslant i\leqslant n)$，则称 $F(x)$满足严格雪崩准则(SAC)。

定义 5 设 $F(x)=(f_1(x),\cdots,f_n(x))$是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换，称 $l=\sum_{i=1}^{n}\sum_{\substack{\alpha\in GF(2)^n\\ w(\alpha)=1}}\left|w(f_i(x+\alpha)+f_i(x))-2^{n-1}\right|$为 $F(x)$的严格雪崩准则距离。

显然当 $l=0$ 时，$F(x)$满足严格雪崩准则。当 $F(x)$不满足严格雪崩准则时，l 越小布尔置换越接近严格雪崩准则。AES S 盒并不满足严格雪崩准则，其严格雪崩准则距离是 432。

定义 6 $F(x)=(f_1(x),\cdots,f_n(x))$是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换，称 $N_F=\min\limits_{\substack{0\neq u\in GF(2)^n\\ l(x)\in L_n[X]}}d(u\cdot F(x),l(x))$为的非线性度。$L_n[X]$表示全体线性函数之集。

非线性度是衡量密码系统抗线性攻击能力强弱的指标。从这个意义上讲，非线性度越高越好，但当非线性度达到最高时，其他性能将变弱。计算发现 AES S 盒的 $N_F=112$，而在文献[6]中指出完全非线性函数的非线性度 $N_F=2^{n-1}-2^{n/2-1}$，即 $2^{8-1}-2^{8/2-1}=120$，所以 S 盒不是完全非线性函数，但是其非线性度已经非常接近完全非线性函数的非线性度。

定义 7 在域 $GF(2^8)$中，给定 r 个含有 t 项的方程，定义式 $\Gamma=((t-r)/n)^{\lceil(t-r)/n\rceil}$为抗代数攻击的阻力（Resistance of Algebraic Attacks，RAA）。

对于 AES，$t=81$，$r=23$，$n=8$，计算得到 AES S 盒的抗代数攻击阻力 $\Gamma\approx2^{22.9}$。文献[7]指出，安全密码的 S 盒的抗代数攻击阻力应不小于 232，而 AES S 盒的 $\Gamma\approx2^{22.9}$，这可能成为其遭受攻击的切入点。

从上面的分析可以看出，AES 的 S 盒多输出布尔置换存在

着一些缺陷,而且代数表达式尽管有足够高的次数,但只有9项被认为过于简单[5]。AES S盒的代数表达式如下:

$$y='05'x^{-1}+'09'x^{-2}+'f9'x^{-4}+'25'x^{-8}+'f4'x^{-16}+'01'x^{-32}+'b5'x^{-64}+'8f'x^{-128}+'63'='05'x^{254}+'09'x^{253}+'f9'x^{251}+'25'x^{247}+'f4'x^{239}+'01'x^{223}+'b5'x^{191}+'8f'x^{127}+'63'$$

文献[5]中针对S盒的代数表达式只有9项的问题,提出了将求乘法逆运算和仿射变换的计算顺序调换,使改进S盒具有255项的代数表达式,而且其严格雪崩准则距离是408,但是通过求逆S盒的表达式发现其代数表达式只有9项,而且这样构造的S盒的仿射变换周期仍然是4,迭代输出周期也小于88,并没有达到改进的效果,与AES的S盒具有几乎相同的代数性质。

4　S盒的改进方案及性能比较

通过以上对AES S盒及文献[5]构造S盒的构造原理和性能的分析,发现S盒或逆S盒的代数表达式过于简单是与构造S盒的求乘法逆元和仿射变换的计算顺序有关,而仿射变换周期和迭代输出周期则与所采用的仿射变换对有关,所以S盒的代数性质是可以通过修改仿射变换对和调整S盒的计算顺序以达到比较好的效果。但是如果仅仅采用一次仿射变换无法满足所构造的S盒和逆S盒的代数表达式都具有较多项数。本文针对以上问题提出了构造S盒的改进方案,本方案采用三个步骤实现,即对字节元素做一次仿射变换后求乘法逆元,然后再做一次仿射变换,仿射变换对分别为('6B','5D')和('97','6C')。S盒改进方案的运算步骤如下:

(1)首先做一次仿射变换,选取的仿射变换对为('6B','5D'),具体运算如下:

$$\boldsymbol{x}'=\boldsymbol{L}_B\times\boldsymbol{x}+'5D'=\begin{bmatrix}1&0&1&1&0&1&0&1\\1&1&0&1&1&0&1&0\\0&1&1&0&1&1&0&1\\1&0&1&1&0&1&1&0\\0&1&0&1&1&0&1&1\\1&0&1&0&1&1&0&1\\1&1&0&1&0&1&1&0\\0&1&1&0&1&0&1&1\end{bmatrix}\begin{bmatrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{bmatrix}+\begin{bmatrix}0\\1\\0\\1\\1\\1\\0\\1\end{bmatrix}$$

(2)求乘法逆元 $x''=(x')^{-1}=\begin{cases}(x')^{254} & x'\neq 0\\ 0 & x'=0\end{cases}$

(3)再做一次仿射变换,选取的仿射变换对为('97','6C'),具体运算过程及S盒运算结果如下:

$$\boldsymbol{y}'=\boldsymbol{L}_C\times\boldsymbol{x}''+'6C'=\begin{bmatrix}1&1&0&0&1&0&1&1\\1&1&1&0&0&1&0&1\\1&1&1&1&0&0&1&0\\0&1&1&1&1&0&0&1\\1&0&1&1&1&1&0&0\\0&1&0&1&1&1&1&0\\0&0&1&0&1&1&1&1\\1&0&0&1&0&1&1&1\end{bmatrix}\begin{bmatrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{bmatrix}+\begin{bmatrix}0\\1\\1\\0\\1\\1\\0\\0\end{bmatrix}$$

那么对于上面S盒的构造方案中的仿射变换对('6B','5D')和('97','6C'),其对应的逆S盒仿射变换对为('C2','5F')和('70','4A'),则对应的逆S盒构造方案如下:

(1)首先做一次仿射变换对为('C2','5F')的仿射变换。

$$\boldsymbol{x}''=\boldsymbol{L}_C^{-1}\times\boldsymbol{y}+'5F'=\begin{bmatrix}0&1&1&0&0&0&0&1\\1&0&1&1&0&0&0&0\\0&1&0&1&1&0&0&0\\0&0&1&0&1&1&0&0\\0&0&0&1&0&1&1&0\\0&0&0&0&1&0&1&1\\1&0&0&0&0&1&0&1\\1&1&0&0&0&0&1&0\end{bmatrix}\begin{bmatrix}y_7\\y_6\\y_5\\y_4\\y_3\\y_2\\y_1\\y_0\end{bmatrix}+\begin{bmatrix}0\\1\\0\\1\\1\\1\\1\\1\end{bmatrix}$$

(2)求乘法逆元 $x'=(x'')^{-1}=\begin{cases}(x'')^{254} & x''\neq 0\\ 0 & x''=0\end{cases}$

(3)再做仿射变换对为('70','4A')的仿射变换,得到输出结果 $\boldsymbol{x}$

$$\boldsymbol{x}=\boldsymbol{L}_B^{-1}\times\boldsymbol{x}'+'4A'=\begin{bmatrix}0&0&1&1&1&0&0&0\\0&0&0&1&1&1&0&0\\0&0&0&0&1&1&1&0\\0&0&0&0&0&1&1&1\\1&0&0&0&0&0&1&1\\1&1&0&0&0&0&0&1\\1&1&1&0&0&0&0&0\\0&1&1&1&0&0&0&0\end{bmatrix}\begin{bmatrix}y_7\\y_6\\y_5\\y_4\\y_3\\y_2\\y_1\\y_0\end{bmatrix}+\begin{bmatrix}0\\1\\0\\0\\1\\0\\1\\0\end{bmatrix}$$

从上面的构造方法可以看出,提出的S盒的构造方法与AES的构造方法和文献[5]的构造方法相比多做了一次仿射变换。这样就使得在S盒及逆S盒构造过程中求逆之前均有一次仿射变换,解决了AES中S盒及文献[5]中逆S盒表达式过于简单的问题,使得改进方案所构造S盒及逆S盒的表达式都具有较多的项数。而通过修改仿射变换对,增大了仿射变换周期和迭代输出周期,使S盒更加接近严格雪崩准则,而且在平衡性、差分均匀度、非零线性结构、非线性度和抗代数攻击阻力等性质上与AES的S盒相同。笔者编程测试了本文改进S盒的各项代数性质,并与AES的S盒、文献[5]中改进的S盒进行比较,比较结果如表1所示。

表1　三种S盒代数性质对比表

	AES S盒	文献[5]改进S盒	本文改进S盒
平衡性	平衡函数	平衡函数	平衡函数
差分均匀度	4	4	4
非零线性结构	没有	没有	没有
抗代数攻击阻力	$\Gamma\approx 2^{22.9}$	$\Gamma\approx 2^{22.9}$	$\Gamma\approx 2^{22.9}$
严格雪崩准则距离	432	408	372
非线性度	112	112	112
S盒代数表达式项数	9项	255项	254项
逆S盒代数表达式项数	255项	9项	254项
仿射变换周期	4	4	16
迭代输出周期	小于88	小于88	256

从表1中可以看出,提出的改进S盒的严格雪崩准则距离为372,优于AES S盒的432和文献[5]中改进S盒的408;本文的改进S盒及其逆S盒均有254项的代数表达式,解决了AES中S盒及文献[5]中逆S盒表达式过于简单的问题;本文改进方案采用周期为16的仿射变换对,明显优于AES S盒和文献[5]中S盒所采用的周期为4的仿射变换对;本文构造S盒的迭代输出周期为256,而另外两种方案构造的S盒的迭代输出周期均不超过88。总之,文中构造的S盒具有更好的代数性质。改进方案构造的S盒替换表如表2所示,S盒的代数表达式系数表如表3所示。

表 2 改进方案构造的 S 盒替换表

S盒的低4位	S盒的低4位															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	DA	4F	35	A1	7F	AA	BD	98	C7	9D	E9	44	B4	CD	A8	92
1	4D	26	BA	F9	04	7B	6B	C9	77	AF	0B	93	76	62	9F	F6
2	F2	F8	AE	7D	31	64	02	FE	AB	A2	B8	19	33	C8	79	03
3	1F	81	A3	75	50	55	08	83	6A	B5	9B	EF	EE	14	F4	65
4	0A	1B	CC	86	F1	D7	D0	FB	36	18	6C	30	A5	53	41	A0
5	A7	40	0C	34	B1	54	BF	07	A9	2B	3E	FA	3F	1D	5F	88
6	85	58	F7	5E	66	2F	C5	8B	27	D9	43	3B	CF	70	DE	EB
7	5D	7C	87	45	B6	10	82	8E	42	1E	C1	B3	7A	D6	6F	51
8	01	61	E6	0F	28	3A	C3	23	D4	25	13	90	09	68	71	7E
9	74	73	5B	06	FD	15	C0	8D	E4	DB	EC	D1	24	3C	57	2C
A	E8	E0	17	B2	52	9A	96	56	48	4B	95	5C	1A	C4	6D	72
B	99	AD	9E	C6	F0	80	3D	20	CE	39	89	22	1C	8C	D5	2D
C	11	8A	29	E2	BE	FF	D8	DC	CB	12	AC	84	47	CA	B9	E7
D	16	78	D3	BB	0D	94	32	4C	67	DD	C2	0E	6E	EA	37	00
E	59	4E	97	05	E1	46	63	FC	91	BC	38	2E	8F	E5	A6	2A
F	B0	9C	ED	DF	B7	D2	5A	E3	A4	21	F3	F5	49	69	4A	60

表 3 改进方案构造 S 盒的代数表达式系数表

幂指数十六进制数高4位	幂指数十六进制数低4位															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	DA	84	E5	2F	C8	AF	E4	3D	57	9B	7C	9A	46	5D	DD	3F
1	6E	0F	78	94	2E	B1	C9	E5	68	4C	4D	63	43	B7	B0	70
2	13	BE	64	87	0B	7E	BB	1D	72	EC	F3	FB	C6	F4	D1	D8
3	CD	37	01	25	17	78	26	4A	43	FB	EE	7F	EC	C6	8B	E6
4	AA	D9	C5	87	FA	23	1C	AF	AB	74	B0	95	5B	FB	14	53
5	F5	63	12	8A	67	47	4C	9E	79	14	39	2F	FF	EB	5B	8A
6	9F	C7	45	4D	F2	F8	00	3E	B7	9B	B8	C5	E3	07	C4	C9
7	A9	AC	80	E6	F4	E1	5C	EE	A9	A5	F0	CC	5E	30	89	5C
8	16	20	6F	90	E3	86	8E	B2	44	4F	7E	25	4A	B4	92	D9
9	5B	D8	79	CD	34	15	1D	8F	E3	19	B7	0D	4E	21	5E	90
A	2E	B2	51	57	DF	EF	24	F4	AD	61	90	6A	2C	9E	24	3D
B	79	97	2A	5A	3C	B9	93	8F	E9	B7	C4	60	9D	5C	EE	30
C	8B	36	3C	45	20	A6	B9	D0	2E	A5	A7	5C	D3	27	6B	9D
D	CB	AF	DB	E7	AF	91	3F	9A	6D	FC	DD	08	F2	4B	8B	BC
E	83	E5	9D	29	1B	ED	BE	DF	40	ED	8C	84	D9	2C	BD	02
F	FE	1F	77	76	B3	2F	7C	94	0E	CF	46	11	30	9D	95	00

5 结束语

本文分析了 AES S 盒的平衡性、严格雪崩准则、抗代数攻击阻力等 6 种代数性质，并指出 AES S 盒的仿射变换对周期小，迭代输出周期短，并且代数表达式只有 9 项。针对 S 盒以上的不足，提出了构造 S 盒的改进方案，先对字节元素在 $GF(2)$ 域下作仿射变换，然后对元素求乘法逆元，最后再对元素做仿射变换，这样使改进的 S 盒和逆 S 盒均具有复杂的代数表达式，其代数表达式项数均为 254 项，而采用的仿射变换对('6B','5D')和('97','6C')的仿射变换对周期均达到 16，并且改进 S 盒的迭代输出周期达到 256。实验结果表明本文构造的 S 盒比 AES 的 S 盒和文献[5]改进的 S 盒的严格雪崩准则距离都小。改进 S 盒有复杂的代数结构和良好的非线性特性，具有很好的安全性。（收稿日期：2006 年 9 月）

参考文献：

[1] Daemen J,Knudsen L,Rijnmen V.The block cipher Square[C]//Fast Software Encryption,4th International Workshop.Haifa,Israel:Springer-Verlag,1997:149-165.

[2] Ferguson N,Kelsey J.Improved cryptanalysis of Rijndael[C]//Fast Software Encryption,7th International Workshop,2001:213-230.

[3] 王衍波.AES 的 S-盒中仿射变换的性质[J].解放军理工大学学报:自然科学版,2002,4(2):5-9.

[4] 王衍波.AES 的结构及其 S-box 分析[J].解放军理工大学学报:自然科学版,2002,3(3):13-17.

[5] Jingmei L,Baodian W,Xiangguo C,et al.An AES S-box to increase complexity and cryptographic analysis[C]//19th International Conference on Advanced Information Networking and Applications,2005:724-728.

[6] 温巧燕,钮心忻,杨义先.现代密码学中的布尔函数[M].北京:科学出版社,2000.

[7] Hee Jung,Lee Dong Hoon.Resistance of S-boxes against Algebraic Attacks [EB/OL].[2004].Available http://www.math.snu.ac.kr/jhcheon/Published/2004_FSE/ FSE04_CL.pdf.

（上接 139 页）

[4] Bianchini R,Carrera E V.Analytical and experimental evaluation of cluster-based network servers[J].World Wide Web Journal,2000,3(4).

[5] Martinez K,Hart J K,Ong R.Environmental sensor networks[J].IEEE Computer,August 2004,37(8):50-56.

[6] Liu C,Layland J.Scheduling algorithms for multiprogramming in a hard real time environment[J].Journal of ACM,1973,20(1):46-61.

[7] Zhang Y,Sivasubramaniam A.Scheduling best-effort and real-time pipelined applications on time-shared clusters [C]//Proc the 13th ACM Symposium on Parallel Algorithms and Architectures(SPAA'2001),July 2001:209-218.

[8] Essafi L,Bolch G,de Meer H.Dynamic priority scheduling for proportional delay differentiated services [EB/OL].[2006-05].http://www4.informatik.uni-erlangen.de/TR/ps/TR-I4-01-03.ps.gz.

[9] Zhang W.Linux virtual server for scalable network services[C/OL]//Ottawa Linux Symposium,2000.http://www.linuxvirtualserver.org/Documents.html.

[10] Egevang K,Francis P.The IP network address translator(NAT) RFC 1631[S],1994-05.

[11] Zhu H,Tang H,Yang T.Demand-driven service differentiation for cluster-based network servers [C]//Proc IEEE INFOCOM 2001,Anchorage,2001-04.

[12] Nimmagadda S,Harari I.Scalability issues in cluster computing operating systems[C]//Proc of the First Workshop on Cluster-Based Computing,Rhodes,Greece,1999-06.

[13] Shen K,Tang H,Yang T,et al.Integrated resource management for cluster-based internet services [C]//Proc 5th Symposium on Operating Systems Design and Implementation,Boston,MA,2002-12.

[14] Tang R,Simha R.A delay differentiation approach to real-time scheduling on cluster-based multimedia servers[C]//ICT 2002.Beijing,2002-06.

[15] Shen K,Yang T,Zhu L.Cluster load balancing for fine-grain network services [C]//Proc 16th International Parallel and Distributed Processing Symposium,2002.

[16] Wolf J L,Yu P S.On balancing the load in a clustered web farm [J].ACM Trans Inter Tech,2001,1(2):231-261.