基于 AES 算法中 S 盒的分析研究与改进

张丽红[1] 凌朝东[1,2]
(1. 华侨大学 信息科学与工程学院, 福建厦门 361000; 2. 厦门市专用集成电路系统重点实验室, 福建 厦门 361008)

摘 要: 由于 AES S 盒代数式只有 9 项过于简单且仿射变换对周期和迭代输出周期过短的原因, 提出了一种新的构造 S 盒的解决方法。该方法通过在有限域上利用拉格朗日插值公式完全展开的系数求解方法得出了 S 盒和逆 S 盒的代数式系数表。与 AES S 盒构造原理导出的代数式相比, 该方法具有直观且简单通用的特性。MATLAB 仿真结果显示, 新 S 盒的构造时间最短。其仿射变换周期和迭代输出周期分别高达 16 和 256。S 盒和逆 S 盒的严格雪崩准则距离分别降为 376 和 304。S 盒的代数式项数提高到 253 项。表明新 S 盒具有更复杂的代数结构、较好的差分特性以及非线性, 同时根据仿射变换次数和 S 盒的构造时间进一步说明新 S 盒的设计既简洁又高效。

关键词: 高级加密标准; S 盒; MATLAB; 拉格朗日插值; 仿射变换; 代数式
中图分类号: TP309.7 **文献标识码**: A **文章编号**: 1003-0530(2011)09-1428-06

The analysis and improvement of S box based on AES

ZHANG Li-hong[1] LING Chao-dong[1,2]
(1. College of Information Science & Engineering, Huaqiao University, Quanzhou 361000, Fujian;
2. Key Laboratory of ASIC and System of Xiamen, Xiamen 361008, Fujian)

Abstract: Because the algebraic expression of AES S box only has nine items, which is too simple. Meanwhile, the period of affine transform pair and iterative output is also too short. A new solution is proposed to deal with these problems. By using the coefficients of fully expanded Lagrange interpolation formula in finite field, the algebraic expression coefficients of the S box and Inv S box can be obtained. Compared with the algebraic expression deriving through the AES S box construction principle, this new method is intuitive and simple universal. The MATLAB simulation results show that the new S box has the shortest construction time. The periods of affine transform pair and iterative output are up to 16 and 256 respectively. The strict avalanche criterion distance of S box and Inv S box reduce to 376 and 304 separately. The algebraic expression items of S box are improved to 253. All of these denote that the new S box has a more complex algebraic structure, better difference characteristics and nonlinearity. Moreover, the affine transform and construction time of S box further explains its conciseness and high efficiency.

Key words: Advanced Encryption Standard; S box; MATLAB; Lagrange interpolation; affine transform; algebraic expression

1 引言

随着计算机技术和网络技术的不断发展,信息安全也越来越受到人们的重视,密码学的研究也随之扩大。当前安全性最好、应用最广泛的加密算法是高级加密标准 AES 算法[1-2]。AES 算法中字节代换层和密钥扩展层多次用到了 S 盒的置换,S 盒在算法中起到混淆作用,是算法中唯一的非线性组件,可以说 S 盒的安全性是算法安全性的关键所在。因此,S 盒的安全性一直受到密码学界的关注[3-6]。

刘连浩、崔杰等[6]提出通过两次仿射变换来构造 S 盒的改进方案,虽然使 S 盒具有更好的代数性质,但同时使 S 盒的运算量增大,又由于 AES S 盒代数式只有 9 项,且仿射变换对周期和迭代输出周期过短原因,本文在深入研究 AES S 盒的设计原理及代数性质之后,提出了一种新 S 盒的构造方法。该方法构造的 S 盒是先对字节元素在 $GF(2)$ 域下做仿射运算,然后对元素求乘法逆元,最后再对元素做常量加法运算。通过 MATLAB 验证,结果表明新 S 盒的构造时间最短,且仿射变换周期和迭代输出周期均达到最大值分别为 16 和 256,S 盒和逆 S 盒的严格雪崩准则距离分别为 376 和 304,对应的代数式项数分别为 253 和 254。

2 S 盒和逆 S 盒

2.1 S 盒构造原理

AES 算法中独立作用于状态字节的 S 盒是基于数

收稿日期: 2011 年 5 月 21 日; 修回日期: 2011 年 9 月 1 日
基金项目: 国家自然科学基金项目(60772164); 厦门市科技计划项目(3502Z20080010)

学理论构造的,它的构造原理是先对字节元素在有限域 $GF(2^8)$ 中求乘法逆运算,然后在有限域 $GF(2)$ 中通过构造一个 8×8 的非线性变换矩阵来做仿射运算,最后再对元素做常量'63' 的加法运算。

1、求乘法逆运算

有限域 $GF(2^8)$ 中两个元素相乘,如果满足 $a(x)\cdot b(x) \bmod m(x)=1$,则称 $b(x)$ 是 $a(x)$ 的逆元,其中 $m(x)=x^8+x^4+x^3+x+1$。但是在实际计算中很少用此方法,因为需要很多次的尝试才能找到 $b(x)$,所以常用扩展的欧几里德算法计算并得出 $b(x)$。

2、仿射运算和加法运算

定义 1

仿射变换[3]:$L_{u,v}:a(x)\mid\rightarrow L_{u,v}(a(x))\rightarrow L_{u,v}(a(x))=u(x)a(x)+v(x) \bmod (x^8+1)$

若记:

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

则仿射变换表达式为 $L_{u,v}(a)=Fa+v$。

综上所述可得:S 盒的非线性变换表达式为 $y=L_a\cdot x^{-1}+v$。其中 L_a 即为 F 矩阵,x 即为 a 向量。而通过已知参数 AES S 盒仿射变换对 (u,v) 可知:$u=(1F)_{16}=(00011111)_2$,$v=(63)_{16}=(01100011)_2$,因此可以构造出 AES S 盒的替换表。

2.2　逆 S 盒构造原理

由上述 S 盒的非线性变换 $y=L_a\cdot x^{-1}+v$ 可知,逆 S 盒的非线性变换为 $x=(L_a^{-1}\cdot y+L_a^{-1}\cdot v)^{-1}$。由于 L_a^{-1} 未知,因此要在有限域 $GF(2)$ 中求矩阵 L_a 的逆矩阵,即:L_a^{-1}。方法是先将 8 阶方阵 L_a 扩展成一个 8×16 的矩阵 $\langle L_a\mid E\rangle$ 记为 L_aE,然后对其施以初等行变换,即:$\langle L_a\mid E\rangle\rightarrow\langle E\mid L_a^{-1}\rangle$。最后将 $u=(1F)_{16}=(00011111)_2$,代入 F 矩阵可得:

$$L_a=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

进而得:

$$L_a^{-1}=\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

又由于 u' 可以用 L_a^{-1} 中的分量组成,v' 为 $v'=L_a^{-1}\cdot v$。因此得:$u'=(4A)_{16}=(01001010)_2$,$v'=(05)_{16}=(00000101)_2$,从而构造出了 AES 逆 S 盒表。

2.3　S 盒与逆 S 盒代数式系数求解

S 盒与逆 S 盒代数式系数表的求解[7-9],可通过在有限域 $GF(2^8)$ 上利用拉格朗日插值公式完全展开的方法得到。

若给定有限域 $GF(2^m)$ 上彼此互异的 $n+1$ 个输入点 $x_0,x_1,x_2,\cdots,x_n$ 处,对应的函数值 $y_0,y_1,y_2,\cdots,y_n$,则可利用拉格朗日插值多项式表示为:

$$L_n(x)=y_0l_0(x)+y_1l_0(x)+\cdots++y_nl_n(x)=\sum_{i=0}^{n}y_il_i(x) \tag{1}$$

其中

$$l_i(x)=\frac{(x-x_0)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_0)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}=\prod_{\substack{j=0\\ j\neq i}}^{n}\frac{x-x_j}{x_i-x_j} \tag{2}$$

要求解 $l_i(x)$ 的多项式系数,由于公式(2)包含了 n 个不同的一次因式连乘,则需要将公式(2)转化为一般多项式表达式即:

$$\prod_{i=1}^{n}(x+a_i)=D_0x^n+D_1x^{n-1}+\cdots+D_{n-1}x+D_n \tag{3}$$

由文献[8]可知,实数域上的一次因式连乘展开的系数 D_i 具有递归性,若将其应用到有限域 $GF(2^m)$ 上同样也符合。那么系数 D_i 的计算方法如下:

$D_0=1$,

$D_1=a_1+a_2+\cdots+a_n=T_{11}+T_{12}+\cdots+T_{1n}$,

……

$D_i=\sum_{j=1}^{n-i+1}a_j\left(\sum_{k=j+1}^{n-i+2}T_{i-1,k}\right)$,其中 $T_{i-1,k}$ 是计算 D_{i-1} 和式的第 k 项。

3　S 盒的代数性质

如果算法中 S 盒的代数性质越好,就说明该算法越能抗击各种密码分析的攻击。不同的密码学代数性质分别用于抗击不同的攻击:平衡性用于抵抗相关攻击;差分均匀度用于抵抗差分分析;代数表达式的项数用于抵抗插值攻击等。因此须对 S 盒的各种代数性质进行分析。

本文在深入研究 S 盒代数性质后,发现 AES 算法 S 盒在平衡性、正交性、差分均匀度、非线性度等方面均具有较好的性质,但是在仿射变换周期、迭代输出周期、严格雪崩准则距离、S 盒代数表达式项数上均可进行不同程度上的改进。

定义 2

平衡性[11]:设 $F(x)=(f_1(x),\ldots,f_n(x))$ 是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换,若满足 $\sum_{x=0}^{2^n-1}f_i(x)=2^{n-1}(1\leq i\leq n)$,则称 $F(x)$ 满足平衡性。

定义 3

正交性[11]:设 $F(x)=(f_1(x),\ldots,f_n(x))$ 是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换,若对任意 $\beta\in GF(2)^n$,集合 $\{\alpha\mid\alpha\in GF(2)^n,F(\alpha)=\beta\}$ 中恰有 1 个元素,则称 $F(x)$ 是正交的。

正交性是确保 S 盒安全性的一个必要条件。如果 S 盒不满足正交性,那么在随机均匀输入下,S 盒就会出现某些输出重复的现象,这一不平衡性就会成为密码分析者攻击基于此 S 盒的密码体制。

定义 4

差分均匀度[6]:设 $F(x)=(f_1(x),\ldots,f_n(x))$ 是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换,称

$$\delta(F)=\max\{\lambda_{ij}\mid i,j=1,2,\ldots,2^n-1\}$$

$$=\max\left\{\left|\left\{x\in GF(2)^n\mid F(x)\oplus F(x+\alpha_i)=\beta_j\right\}\right|\ \middle|\ \begin{array}{c}\alpha_i\in GF(2)^n\\ \alpha_i\neq 0\\ \beta_j\in GF(2)^n\end{array}\right\}$$

为 $F(x)$ 的差分均匀度。其中,α_i 和 β_j 分别为 i,j 的二进制表示。

差分均匀度是用来衡量算法抗击差分分析的指标。布尔置换的差分均匀度越接近最小值 1,算法抵抗差分分析的能力越强。

定义 5

非线性度[11]:设 $F(x)=(f_1(x),\ldots,f_n(x))$ 是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换,称 $N_F=\min\left\{d(u\cdot F(x),l(x))\ \middle|\ \begin{array}{c}u\in GF(2)^n\\ u\neq 0\\ l(x)\in L_n\end{array}\right\}$ 为 $F(x)$ 的非线性度,其中,$d(u\cdot F(x),l(x))$ 表示 $u\cdot F(x)$ 与 $l(x)$ 之间的汉明距离。记 $L_n=\left\{u\cdot x+v\mid u=(u_1,u_2,\ldots,u_n)\in GF(2)^n,v\in GF(2)\right\}$ 为 $GF(2)$ 上所有仿射函数所构成的集合(亦称之为仿射函数类),即表示全体线性函数集。

非线性度是衡量布尔函数的非线性程度的一个重要指标,也是衡量密码系统中抵抗线性攻击性能强弱的指标,非线性度越高越好,但当非线性度达到最高的函数,其他性能将变弱。

定义 6

非零线性结构[6]:设 $F(x)=(f_1(x),\ldots,f_n(x))$ 是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换,对于给定 $\alpha\in GF(2)^n$,若 $F(x)+F(x+\alpha)=$ 常量,则称 α 为 $F(x)$ 的线性结构。

定义 7

严格雪崩准则 SAC[6]:设 $F(x)=(f_1(x),\ldots,f_n(x))$ 是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换,如果对任意 $\alpha\in GF(2)^n$ 且 $w(\alpha)=1$ 即 α 的汉明重量为 1 时,有 $w(f_i(x+\alpha)+f_i(x))=2^{n-1}(1\leq i\leq n)$,则称 $F(x)$ 满足严格雪崩准则 SAC(Strict Avalanche Criterion)。

定义 8

严格雪崩准则距离[6]:设 $F(x)=(f_1(x),\ldots,f_n(x))$ 是 $GF(2)^n$ 到 $GF(2)^n$ 的多输出布尔置换,称 $l=\left\{\sum_{i=1}^{n}\sum\left|w(f_i(x+\alpha)+f_i(x))-2^{n-1}\right|\ \middle|\ \begin{array}{c}\alpha\in GF(2)^n\\ w(\alpha)=1\end{array}\right\}$ 为 $F(x)$ 的严格雪崩准则距离。

当 $F(x)$ 满足严格雪崩准则时,有 $l=0$。当 $F(x)$ 不满足严格雪崩准则时,如果 l 越小,即 $F(x)$ 越接近严格雪崩准则,就说明 S 盒的扩散性能越好。

定义 9

仿射变换周期[3]:如果存在正整数 n,使得 $L_{u,v}^n=E$,则称 $L_{u,v}$ 是周期的,若 n 是其中最小的正整数,则称 $L_{u,v}$ 的周期为 n。其中 $L_{u,v}^n(\alpha)=L_{u,v}^n(L_{u,v}^{n-1}(\alpha))$,$E$ 为 8 阶单位矩阵。

如果仿射变换对的周期越长,就说明 S 盒的安全性越好,其中仿射变换周期最大值为 16。

定义 10

迭代输出周期[4]:S 盒的迭代输出周期是指从某一元素开始通过连续 S 盒替换回到元素本身所经过的元素数。

如果 S 盒中的任一元素都有迭代输出周期 256 这么一个轨道,即 S 盒具有唯一一个迭代输出周期为 256 的置换表,就说明 S 盒在迭代输出周期上达到最佳值。

4 AES S 盒的改进方案

4.1 新 S 盒的构造

改进的 S 盒构造仍由有限域 $GF(2^8)$ 中乘法逆运

算和有限域 $GF(2)$中仿射运算复合而成。改进 S 盒的非线性变换为 $y=(L_a\cdot x)^{-1}+\nu$,则对应逆 S 盒的非线性变换为 $x=L_a^{-1}(y+\nu)^{-1}$。关键是在如何寻找仿射变换对,使构造出来的新 S 盒替换表具有较好的性能。

寻找最佳的仿射变换对(u,ν)的思路:首先根据定义 9 得到仿射变换对周期为 16 的(u,ν)组合共有 8192 对,实验流程如图 1 所示。然后根据新 S 盒的构造原理从 8192 对(u,ν)组合中选择 64 对,使 S 盒具有唯一一个周期 256 的置换表[4],其流程如图 2 所示。最后再从选择出的 64 对(u,ν)组合中选择使严格雪崩准则距离 l 最小的仿射变换对,即$(u,\nu)=(52,186)_{10}=(34,BA)_{16}$,操作流程如图 3 所示。

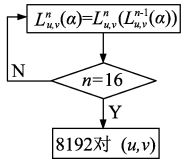

图 1　8192 对仿射变换对的产生

Fig. 1　Generation of 8192 affine transform pairs

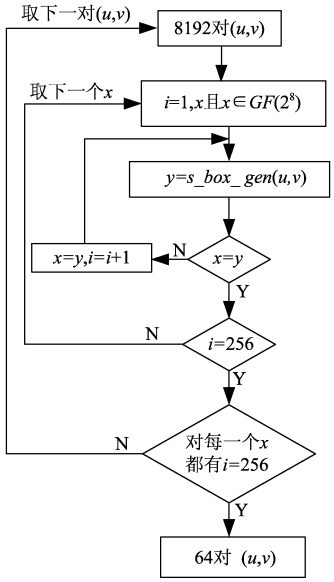

图 2　64 对仿射变换对的产生

Fig. 2　Generation of 64 affine transform pairs

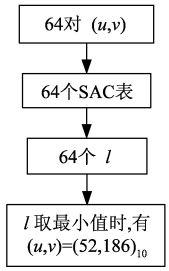

图 3　最小严格雪崩准则距离的求解

Fig. 3　The minimum strict avalanche criterion distance solution

4.2　仿真结果

将上述得到的仿射变换对$(u,\nu)=(52,186)_{10}=(34,BA)_{16}$代入新 S 盒和逆 S 盒非线性变换表达式中,构造出新 S 盒和对应逆 S 盒的替换表分别如表 1、表 2 所示,其对应的系数表如表 3、表 4 所示。由于表 1 至表 4 内容较多,占用空间大,因此论文以附录形式列出表 1 至表 4,详见附一。

分别对表 1 和表 2 数据进行分析[10-12]可知该 S 盒与逆 S 盒均满足平衡性和正交性并无非零线性结构,且它们的差分均匀度均为 4,非线性度均为 112,严格雪崩准则距离均分别为 376 和 304,说明新 S 盒具有良好代数性质。由表 3 和表 4 可知,S 盒和逆 S 盒的代数式分别含有 253 项和 254 项,从而给出了 S 盒和逆 S 盒代数结构上的复杂度。

5　三种 S 盒的比较

实验表明:修改仿射变换对以及改变 S 盒构造原理中乘法逆元运算的位置,可以增大仿射变换周期和迭代输出周期,减少严格雪崩准则距离,提高新 S 盒代数式的复杂度,从而解决 AES 中 S 盒代数式项数过少的问题;改进方案所构造的新 S 盒与 AES 算法中 S 盒在平衡性、正交性、差分均匀度、非线性度以及非零线性结构等代数性质方面是相同的。本文作者对 AES 算法中 S 盒,文献[6]中构造的 S 盒以及本文提出的新 S 盒的各项性能进行了测试和比较,结果如表 5 所示。

表 5　三种 S 盒的对比

Tab. 5　the contrast table of three S boxes

性能	原始 S 盒	文献[6]S 盒	本文方法 S 盒
平衡性	平衡函数	平衡函数	平衡函数
正交性	是	是	是
差分均匀度	4	4	4
非线性度	112	112	112
非零线性结构	无	无	无
S 盒严格雪崩准则距离	432	372	376
逆 S 盒严格雪崩准则距离	536	412	304
仿射变换周期	4	16	16
迭代输出周期	小于 88	256	256
S 盒代数式项数	9 项	252 项	253 项
逆 S 盒代数式项数	255 项	254 项	254 项
仿射变换次数	1	2	1
构造 S 盒的运行时间	0.7413 秒	0.7603 秒	0.7207 秒

从代数性质上看,与原始 S 盒相比,本文方法 S 盒仿射变换周期由 4 变为 16,迭代输出周期由小于 88 变为全部为 256,严格雪崩准则距离由 432 变为 376,S 盒代数式项数由 9 项变为 253 项,同时逆 S 盒代数式项数为 254 项,严格雪崩准则距离为 304,明显优于 AES 逆 S 盒的 536 和文献[6]中构造的逆 S 盒的 412,且其他性质仍然保留了 AES 算法的优点。从构造原理上看,文献[6]改进的 S 盒方案采用了两次仿射变换,增加了 S 盒的运算量,而本文方法 S 盒只采用了一次仿射变换。从构造 S 盒的运行时间上看,在同等条件下,本文方法 S 盒的构造时间最短,提高了 S 盒的运行速度,进而提高了该算法的运行速度。

6 结论

一个“好”S 盒的设计需要满足很多的性质,新方案根据 S 盒的仿射变换周期、迭代输出周期及严格雪崩准则距离的代数性质来构造具有更好性能的新 S 盒,然后对改进 S 盒在平衡性、正交性、差分均匀度等代数性质方面进行进一步验证。本文构造的 S 盒是先对字节元素在 $GF(2)$ 域下做仿射运算,然后对元素求乘法逆元运算,最后再对元素做常量加法运算,这样增加了新 S 盒和逆 S 盒的代数式项数分别达到了 253 项和 254 项,同时采用的仿射变换对 $(34,BA)_{16}$ 在仿射变换周期和迭代输出周期上均达到最大值分别为 16 和 256。实验结果显示新 S 盒具有更复杂的代数结构、很好的差分特性以及非线性,表明改进 S 盒具有更好的安全性,同时根据仿射变换次数和 S 盒的构造时间进一步说明新 S 盒的设计既简洁又高效。

附一:

表 1 本文提出的 S 盒替换表

Tab. 1 S box substitution table proposed in this paper

186	73	78	235	192	124	31	77	198	48	157	160	13	139	133	254
221	134	175	8	215	242	26	92	108	88	47	60	40	193	152	155
4	165	164	126	61	21	227	147	115	241	179	188	54	25	32	240
110	153	93	174	145	212	64	222	243	87	10	72	171	57	39	178
91	143	28	230	66	244	207	196	116	144	96	225	27	29	35	128
83	106	18	16	51	168	185	149	9	111	236	85	163	122	5	105
99	237	81	80	74	129	214	107	34	84	141	0	199	22	136	223
19	119	65	98	226	138	195	151	253	86	187	131	52	184	189	180
71	24	45	79	233	251	148	62	135	30	217	23	101	173	76	248
132	41	255	232	36	6	183	97	103	161	100	53	123	69	167	170
67	156	210	177	238	12	239	206	1	245	158	228	234	49	201	90
209	89	203	58	125	213	249	112	59	17	218	224	104	37	94	130
229	75	56	169	181	142	216	50	194	197	42	109	140	191	95	154
246	172	205	82	44	182	231	46	252	146	102	114	247	14	159	202
208	2	38	70	68	15	176	250	150	113	162	137	11	127	33	7
20	117	204	3	55	220	43	219	63	211	118	120	121	200	190	166

表 2 本文提出的逆 S 盒替换表

Tab. 2 InvS box substitution table proposed in this paper

181	84	240	249	16	47	202	247	137	44	29	118	210	6	238	242
169	220	41	56	120	146	182	197	192	150	11	38	33	166	196	3
23	119	52	39	74	222	113	31	14	200	101	123	106	65	235	13
132	214	227	42	62	205	22	122	97	158	217	92	141	18	195	124
27	57	34	80	114	206	241	64	157	128	50	224	71	131	1	193
177	49	233	40	180	173	188	156	140	216	215	32	139	25	95	103
37	203	185	48	77	70	109	76	94	175	168	179	12	229	24	172
219	244	237	20	36	248	125	184	253	126	174	78	130	90	145	246
167	178	223	189	72	7	136	68	55	245	186	134	102	53	226	160
164	26	236	147	67	171	116	187	15	152	231	143	208	5	85	111
133	204	117	46	17	144	255	79	170	225	207	30	232	198	153	9
115	209	159	21	191	98	234	75	190	43	0	61	149	63	127	230
2	142	100	59	163	228	4	54	254	87	239	89	121	105	211	35
112	88	81	252	154	218	51	10	99	69	93	251	250	8	155	183
221	165	58	19	213	96	161	107	201	66	86	129	45	176	82	83
151	148	138	28	162	212	104	110	199	91	243	194	108	60	135	73

表 3 本文改进 S 盒的代数式系数表

Tab. 3 Algebraic expression coefficient list of improved S-box in this paper

186	170	223	14	81	86	125	210	169	198	20	23	75	43	70	94
78	54	76	47	200	49	15	193	77	130	30	143	250	19	144	160
129	166	103	186	237	126	148	165	116	106	249	206	161	94	52	58
239	140	191	62	57	135	76	185	94	13	210	179	35	185	189	210
0	187	237	229	199	114	227	33	148	113	106	52	168	161	238	167
49	39	107	121	80	72	77	130	209	148	244	1	213	131	98	225
16	6	128	115	158	87	230	24	145	176	15	21	51	122	55	28
220	16	142	236	49	81	192	59	181	114	185	90	81	135	99	135
168	94	212	159	203	62	74	230	224	184	124	74	29	91	161	222
226	211	47	65	0	73	14	78	11	43	197	90	134	144	9	3
2	138	130	23	248	22	218	186	12	112	125	160	4	174	75	143
122	1	5	249	104	192	129	60	168	211	228	74	225	16	88	21
94	12	1	126	95	160	85	92	89	147	215	218	205	230	251	146
87	110	13	69	70	237	85	31	236	99	55	154	121	57	76	219
28	252	39	220	204	44	99	157	215	219	134	215	52	168	106	151
153	128	94	61	43	89	135	245	69	33	56	107	100	221	71	0

表 4 本文改进逆 S 盒的代数式系数表

Tab. 4 Algebraic expression coefficient list of improved InvS-box in this paper

181	197	146	222	100	5	248	105	174	227	27	38	116	36	80	165
59	100	196	84	118	200	154	67	90	212	154	67	97	176	218	199
203	144	105	45	155	53	238	103	129	101	37	247	195	13	27	38
129	101	19	187	36	129	152	175	144	50	150	29	237	253	89	78
89	78	38	109	123	224	132	208	58	18	178	156	66	104	30	147
1	118	57	136	58	18	174	227	132	208	216	43	72	25	175	149
106	183	122	150	43	69	172	15	156	108	124	185	226	57	20	226
12	94	130	255	57	136	207	83	210	90	250	133	201	124	131	137
185	155	129	101	253	220	122	150	189	88	53	214	6	47	141	59
90	212	67	30	174	227	129	101	67	30	234	164	37	247	213	3
111	2	229	96	183	41	125	207	91	162	210	90	111	2	248	105
7	89	192	151	241	130	217	93	120	122	9	235	107	193	231	140
199	206	24	188	21	148	9	235	118	200	189	88	119	190	195	13
3	154	50	143	167	8	64	132	23	120	193	225	197	34	213	3
129	101	233	62	48	99	244	55	96	198	1	118	217	93	20	226
139	20	217	93	47	134	249	31	254	70	228	22	132	208	0	0

参考文献

[1] 孙爱娟. 基于 AES 加密算法的改进及其 MATLAB 实

现[D]:[硕士论文]. 哈尔滨理工大学,2009.
Sun AJ. Improvement of the AES encryption algorithm and the realization with MATLAB[D]:[Master Thesis]. Harbin University of Science and Technology,2009. (in Chinese)

[2] Daemen J, Ri jmen V. The Design of Ri jndael: AES-The Advanced Encryption Standard[M]. Germany: Springer, 2002.

[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),2003,4(2):5-9.
Wang YB. Property of affine transformation in S-box of AES[J]. Journal of PLA University:Science and Technology, 2002, 4(2): 5-9. (in Chinese)

[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.
Wang YB. Analysis of structure of AES and its S-box[J]. Journal of PLA University: Science and Technology, 2002, 3(3): 13-17. (in Chinese)

[5] LIU Jing-mei, WEI Bao-dian, CHENG Xiang-guo, WANG Xin-mei. An AES S-Box to increase complexity and cryptographic analysis[C]// 19th International Conference on Advanced Information Networking and Applications. Taibei:ISI Proceedings,2005:724-728.

[6] 刘连浩,崔杰,刘上力,马虹博. 一种 AES S 盒改进方案的设计[J]. 中南大学学报(自然科学版),2007,38(2):339-344.
Liu LH, Cui J, Liu SL, Ma HB. Design of an improved method of AES S-box[J]. Journal of Central South University: Science and Technology, 2007, 38(2): 339-344. (in Chinese)

[7] 叶俊,苏跃斌. 有限域上插值多项式的两种构造方法[J]. 四川理工学院学报,2010,23(5):521-523.
Ye J, Sun YB. Tow Construction Methods of Interpolation Polynomial in Finite Field[J]. Journal of Sichuan University of Science &Engineering, 2010, 23(5): 521-523. (in Chinese)

[8] 吴燕仙,何妮. 拉格朗日插值公式的完全展开[J]. 通化师范学院学报,2007,28(2):10-12.

[9] 马虹博,刘连浩. AES 的 S 盒和逆 S 盒的代数表达式[J]. 计算机工程,2006,32(4):149-151.
Ma HB, Liu LH. Algebraic Expression for AES S-box and InvS-box[J]. Computer Engineering, 2006, 32(4): 149-151. (in Chinese)

[10] 冯国柱,李超,多磊,谢端强,戴清平. 变型的 Ri jndael 及其差分和统计特性[J],电子学报,2002,30(10):1544-1546.
Feng GZ, Li C, Duo L, Xie DQ, Dai QP. Transmutative Ri jndael with the Differential and Statistical Charactartic[J]. Acta Electronica Sinica, 2002,30(10):1544-1546. (in Chinese)

[11] 蔡海,周亮. 对 AES 算法的 S 盒布尔函数分析[J],信息安全与通信保密,2008,04(172):77-79
Cai H, Zhou L. Analysis of Boolean Functions in AES S Box[J]. Information Security and Communications Privacy, 2008, 04(172): 77-79. (in Chinese)

[12] ZENG Yong-hong, ZOU Xue-cheng, LIU Zheng-lin, LEI Jian-ming. A low-power Ri jndael S-Box based on pass transmission gate and composite field arithmetic[J]. Journal of Zhejiang University SCIENCE A, 2007 8(10): 1553-1559.

作者简介

张丽红(1986-),女,福建泉州人,硕士研究生,主要研究方向为信息安全与数字图像处理。E-mail: zlh840@qq.com;

凌朝东(1964-),男,福建泉州人,硕士,教授,主要研究方向为医学信号处理、信号处理专用芯片。
E-mail:edac@hqu.edu.cn