一种 AES S 盒改进方案的设计

刘连浩，崔　杰，刘上力，马虹博

(中南大学 信息科学与工程学院, 湖南 长沙, 410083)

摘　要： S 盒作为 AES 算法惟一的非线性运算，直接决定算法的性能。针对 S 盒的仿射变换对周期为 4，迭代输出周期不大于 88，而且代数表达式只有 9 项的缺陷提出了改进方案，并构造新的 S 盒。该改进 S 盒具有周期 16 仿射变换对，迭代输出周期为 256，而且 S 盒和逆 S 盒代数表达式项数分别达到 252 项和 254 项。将改进的 S 盒与 AES 的 S 盒在平衡性、严格雪崩准则、非线性度等 10 种代数性质方面进行比较，结果表明改进 S 盒具有更好的代数性质，抗代数攻击的能力更强。

关键词： AES S 盒；仿射变换；代数表达式

中图分类号： TP309.7　　**文献标识码：** A　　**文章编号：** 1672-7207(2007)02−0339−06

Design of an improved method of AES S-box

LIU Lian-hao, CUI Jie, LIU Shang-li, MA Hong-bo

(School of Information Science and Engineering, Central South University , Changsha 410083, China)

Abstract: S-box is the unique nonlinear operation for advanced encryption standard (AES) and affects the capability of the algorithm. For S-box, the period of affine transformed pair is 4, the period of iterative-output is less than 88 and algebraic expression has only 9 items. Based on these characteristics, an improved S-box was constructed, with period of affine transformed pair as 16, period of iterative-output as 256 and algebraic expression of improved S-box and InvS-box as 252 items and 254 items respectively. The improved S-box was compared with AES S-box in 10 algebraic properties, such as the balance, strict avalanche criterion, non-linear degree, resistance against the XSL attack, etc. The results suggest that the improved S-box has better algebraic characteristics and stronger resistance against algebraic attack.

Key words: AES S-box; affine transform; algebraic expression

随着信息技术的发展，人们对信息安全越来越重视，对加密性能的要求越来越高[1−4]。Rijndael 在 2000 年 10 月 2 日被确定为美国高级加密标准(AES)，自从 Rijndael 算法被提出以来，一直受到密码学界的关注，出现了许多攻击 AES 的方法，但目前尚未存在对完整 Rijndael 算法的成功攻击[5−9]。S 盒作为 AES 惟一的非线性部件，对算法抵抗各种攻击起着关键性的作用[10−11]。王珩波[12−13]通过分析 S 盒的仿射变换，指出其仿射变换对的周期为 4，没有达到最大的周期 16，S 盒的迭代输出具有短周期现象，且周期均不大于 88，而 LIU 等[14]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 盒存在的以上不足，本文作者分析了 S 盒布尔函数的 6 种代数性质和只有 9 项的代数表达式，并提出构造 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

收稿日期： 2006−12−20

作者简介： 刘连浩(1959−)，男，教授；从事信息安全与网络通信研究

通讯作者： 崔　杰；电话：0731-8837871；E-mail: cvjxabcd@126.com

盒和逆 S 盒代数表达式分别为 252 项和 254 项。

1 AES S 盒构造原理

1.1 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 2 个步骤：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。

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

$$\boldsymbol{x}=(x')^{-1}=\begin{cases}(x')^{254}, & x'\neq 0\text{时};\\ 0, & x'=0\text{时}。\end{cases}$$

b. 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：

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

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

1.2 AES S 盒仿射变换对周期

定义 1 $L_{u,v}(a(x)):a(x)\mapsto b(x)=u(x)a(x)+v(x)\bmod x^8+1$。

其中 $u(x)=\sum_{i=0}^{7}u_ix^i$，$v(x)=\sum_{i=0}^{7}v_ix^i$，$a(x)=\sum_{i=0}^{7}a_ix^i$。简记为：$L_{u,v}(a)=L_{u,v}(a(x))$。

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

若记

$$\boldsymbol{F}=\begin{bmatrix}u_7&u_6&u_5&u_4&u_3&u_2&u_1&u_0\\u_0&u_7&u_6&u_5&u_4&u_3&u_2&u_1\\u_1&u_0&u_7&u_6&u_5&u_4&u_3&u_2\\u_2&u_1&u_0&u_7&u_6&u_5&u_4&u_3\\u_3&u_2&u_1&u_0&u_7&u_6&u_5&u_4\\u_4&u_3&u_2&u_1&u_0&u_7&u_6&u_5\\u_5&u_4&u_3&u_2&u_1&u_0&u_7&u_6\\u_6&u_5&u_4&u_3&u_2&u_1&u_0&u_7\end{bmatrix},$$

$$\boldsymbol{a}=\begin{bmatrix}a_0\\a_1\\a_2\\a_3\\a_4\\a_5\\a_6\\a_7\end{bmatrix},\ \boldsymbol{v}=\begin{bmatrix}v_0\\v_1\\v_2\\v_3\\v_4\\v_5\\v_6\\v_7\end{bmatrix},$$

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

定义 2 如果存在正整数 n 满足 $\boldsymbol{L}_{u,v}^{n}=E$，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)，u=143=$(11110001)_2$, v=$(11000110)_2$，满足 $L_{143,99}^{4}(a)=a$，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 $u,v\in GF(2^8)$ 形成的可逆仿射变换对的周期只有1，2，4，8，16共5种情况，即周期最大可达到16，而AES的S盒选用了周期为4的仿射变换对。

1.3 AES S 盒的迭代输出周期

AES 的 S 盒的迭代输出周期有 5 个[13]，分别是 87，81，59，27，2，且 $87+81+59+27+2=256$，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。

2 AES S 盒的代数性质

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 128bit 的明文加密运算，S 盒共用到 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 1 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[15]，所以，有必要对 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

$$\max_{\substack{\alpha\in GF(2)^n\\ \beta\in GF(2)^n\\ \alpha\neq 0}} |\{x \mid F(x)+F(x+\alpha)=\beta\}|$$

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[15]。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[15]。

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，如果对 $\forall\alpha\in GF(2)^n$ 且 $w(\alpha)=1$ 即 α 的汉明重量为 1 时，有

$$w(f_i(x+a)+f_i(x))=2^{n-1}(1\leqslant i\leqslant n),$$

则称 $F(x)$满足严格雪崩准则(SAC)。

定义 6　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

$$l=\sum_{i=1}^{n}\sum_{\substack{\alpha\in GF(2)^n\\ w\alpha=1}} |w(f_i(x+a)+f_i(x))-2^{n-1}|$$

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 7　$F(x)=(f_1(x), \cdots, f_n(x))$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 $F(x)$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。通过计算发现 AES S 盒的 N_F=112，而文献[15]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 8　在域 $GF(2^8)$中，给定 r 个含有 t 项的方程，定义式 $\Gamma=((t-r)/n)^{[(t-r)/n]}$ 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 $\Gamma\approx 2^{22.9}$。Hee 等[16]指出，安全密码的 S 盒的抗代数攻击阻力应不小于 2^{32}，而 AES S 盒的 $\Gamma\approx 2^{22.9}$，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[14]。AES S 盒的代数表达式如下：

$$y='05'x^{-1}+'09'x^{-2}+'F9'x^{-4}+'25'x^{-8}+'F4'x^{-16}+$$
$$'01'x^{-32}+'BB5'x^{-64}+'8F'x^{-128}+'63'='05'x^{254}+'09'x^{253}+$$
$$'F9'x^{251}+'25'x^{247}+'F4'x^{239}+'01'x^{223}+'B5'x^{191}+$$
$$'8F'x^{127}+'63'$$

LIU 等[14]中针对 S 盒的代数表达式只有 9 项的问题，提出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，而且这种构造的 S 盒的仿射变换周期仍是 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。

3　S 盒的改进方案设计

通过以上对 AES 的 S 盒的结构和代数性质的分析，发现 S 盒之所以存在代数表达式只有 9 项的不足是与构造 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 盒的代数性质可以通过修改仿射变换对和构造 S 盒的计算顺序来达到比较好的效果。但采用一次仿射变换无法满足所构造的 S 盒和逆 S 盒的代数表达式均具有较多项数的不足，所以，针对以上问题提出构造 S 盒的改进方案。本方案采用仿射变换对('6B','5D')替换原来 S 盒的仿射变换对('F1','63')，并采用 3 步实现，即对字节元素进行 1 次仿射变换后求乘法逆元，然后再进行 1 次仿射变换。S 盒改进方案的运算步骤如下：

a. 首先进行 1 次仿射变换对为('6B','5D')的仿射变换，该仿射变换定义如下：

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

b. 求乘法逆元：$x'=(x^n)^{-1}=\begin{cases}(x^n)^{254}, & x''\neq 0\text{时；}\\ 0, & x''=0\text{时。}\end{cases}$

c. 再进行 1 次仿射变换对为('6B','5D')的仿射变换，输出结果 y。

$$y=Lb\times x''+\text{'5}D\text{'}。$$

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

a. 首先进行 1 次仿射变换，选取的仿射变换对为('70','4A')：

$$x''=Lb^{-1}\times y+\text{'4}A\text{'}=$$
$$\begin{bmatrix}0&0&1&1&1&0&0&0\\0&0&0&1&1&1&0&0\\0&0&0&0&1&1&1&0\\0&0&0&0&0&1&1&1\\1&0&0&0&0&0&1&1\\1&1&0&0&0&0&0&1\\1&1&1&0&0&0&0&0\\0&1&1&1&0&0&0&0\end{bmatrix}\begin{bmatrix}y_7\\y_6\\y_5\\y_4\\y_3\\y_2\\y_1\\y_0\end{bmatrix}+\begin{bmatrix}0\\1\\0\\0\\1\\0\\1\\0\end{bmatrix}。$$

b. 求乘法逆元 $x'=(x'')^{-1}=\begin{cases}(x'')^{254}, & x''\neq 0\text{时；}\\ 0, & x''=0\text{时。}\end{cases}$

c. 再进行仿射变换对为('70','4A')的仿射变换，输出结果 x：

$$x=Lb^{-1}\times x'+\text{'4}A\text{'}。$$

通过运算得到新 S 盒替换表如表 1 所示，通过编程计算得到新 S 盒的代数表达式系数表如表 2 所示。

4 本文 S 盒与 AES S 盒性能的比较

从上面的构造方法可以看出，与文献[14]中的构造方法相比，本文作者提出的 S 盒的构造方法与 AES 的构造方法多进行了 1 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 1 次仿射变换，解决了 AES 中 S 盒及文献[14]中逆 S 盒表达式过于简单的问题，使改进方案所构造 S 盒及逆 S 盒的表达式都具有较多项。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

表 1 本文改进方案构造的 S 盒替换表

Table 1 S-box substitution table of improved method in this paper

十六进制		S 盒的低 4 位															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S 盒的高 4 位	0	8E	77	C2	00	A3	94	86	36	33	E1	17	E3	64	9C	E2	99
	1	01	3C	27	A4	2D	4F	FC	70	7A	43	55	A2	41	1E	97	DC
	2	30	9F	78	D5	2E	84	B7	05	AF	4D	51	90	58	4B	39	8C
	3	0A	67	76	0C	BC	6B	18	11	C7	5F	7B	8D	B6	9E	AA	BF
	4	6E	E6	A7	C6	7D	80	21	D2	8F	AB	5D	15	EC	F1	34	3B
	5	9A	0F	F4	F9	B3	50	F0	60	D9	32	56	E9	6D	7C	C4	85
	6	8B	65	E7	FF	F2	DE	45	C8	07	C3	42	81	EA	DB	62	61
	7	B2	EE	FD	D8	12	72	2A	1F	79	31	A9	C5	74	BB	10	87
	8	FA	53	6F	B9	7F	BA	DF	EB	CD	71	3F	EF	23	B1	E0	98
	9	37	96	28	5B	48	A5	92	52	19	B5	C0	1A	4A	20	1D	93
	A	2C	F5	D3	FE	CA	40	75	26	D6	9B	38	89	DD	7E	66	AD
	B	0D	35	AC	08	46	5C	1B	A6	D1	F7	BE	D0	47	69	F6	A8
	C	49	F3	44	83	CB	3E	F8	14	06	04	0E	B0	AE	3D	6A	54
	D	E8	02	6C	1C	CF	03	63	3A	C9	2F	E4	82	2B	5A	B4	C1
	E	5E	4C	4E	16	CE	95	25	73	D4	BD	CC	E5	24	22	A1	09
	F	88	DA	FB	59	29	57	13	B8	D7	9D	0B	91	ED	8A	A0	68

表 2　改进 S 盒的代数表达式系数表

Table 2　Algebraic expression coefficient table of improved S-box

十六进制		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	8E	A2	62	55	27	E5	7B	E9	B3	3A	0A	E5	91	7D	6B	C2
	1	EC	A6	53	F9	D4	2A	9E	53	5C	69	33	E1	CD	A2	B7	0B
幂	2	97	10	CB	4D	98	52	75	81	E5	37	0B	14	96	6C	A1	18
指	3	91	A9	82	2E	34	81	00	47	94	69	C2	70	16	E2	51	D9
数	4	80	26	C6	73	26	9F	D5	67	D0	E1	D1	E5	C6	47	64	C2
十	5	FD	86	57	18	A0	2E	C0	E3	12	87	35	F2	D3	AD	86	C1
六	6	07	48	7E	0C	73	76	8B	CE	5C	0E	88	57	2A	79	2B	BB
进	7	3A	0D	22	61	A6	49	2C	D1	62	DB	92	E8	EF	CC	EC	A0
制	8	0E	62	77	97	54	2F	BD	8D	9B	22	42	9E	44	3A	57	81
数	9	8F	2F	1B	DF	19	9E	3B	B3	C3	38	9B	90	03	10	94	BD
高	A	01	BF	01	B9	00	CE	F4	F5	57	5A	A3	99	58	99	F9	A2
4	B	30	BF	0F	8D	09	3E	98	68	5B	20	4A	0B	08	0A	69	9C
位	C	26	DB	84	37	0F	9C	A6	05	04	FE	62	5D	13	9C	9E	AA
	D	39	D4	4E	D8	3D	25	5C	15	D5	5A	40	55	00	1B	A3	B4
	E	DF	C9	18	41	6E	7E	83	5E	D9	FE	D8	6D	89	D5	80	93
	F	1D	BB	0E	E3	99	F5	ED	C3	D4	36	27	67	DA	D2	CE	00

准则，同时在平衡性、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方面与 AES 的 S 盒相同。本文作者测试了改进 S 盒的各项代数性质，并与 AES 的 S 盒、文献[14]中改进的 S 盒进行比较，结果如表 3 所示。

表 3　3 种 S 盒代数性质对比表

Table 3　Comparison of algebraic properties of three S-box

性质	AES S 盒	改进 S 盒[14]	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	无	无	无
抗代数攻击阻力	约 $2^{22.9}$	约 $2^{22.9}$	约 $2^{22.9}$
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	252 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 3 可以看出，本文作者提出的改进 S 盒的严格雪崩准则距离为 372，优于 AES S 盒的 432 和文献[14]中改进 S 盒的 408；本文改进的 S 盒及其逆 S 盒的代数表达式项数分别达到 252 项和 254 项，解决了 AES 中 S 盒及文献[14]中逆 S 盒表达式过于简单的问题。本改进方案所采用的仿射变换对周期为 16，明显优于 AES S 盒和文献[14]中 S 盒所采用的周期为 4 的仿射变换对；本构造 S 盒的迭代输出周期为 256，而另 2 种方案构造的 S 盒的迭代输出周期均不超过 88。总之，本文构造的 S 盒具有更好的代数性质。

5　结　论

a. 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，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。

b. 提出构造 S 盒的改进方案，先对字节元素在 $GF(2)$域下进行仿射变换，然后对元素求乘法逆元，最后再对元素乾地仿射变换，这样，使改进的 S 盒和逆 S 盒均具有复杂的代数表达式，S 盒和逆 S 盒代数表达式项数分别达到 252 项和 254 项，而采用的仿射变换对 ('6B','5D') 的仿射变换对周期达到 16，并且改进

S 盒的迭代输出周期达到 256。

c. 实验结果表明本文构造的 S 盒比 AES 的 S 盒和文献[14]中改进的 S 盒的严格雪崩准则距离都小。改进的 S 盒具有复杂的代数结构和良好的非线性特性，具有很强的安全性。

参考文献：

[1] 刘连浩. 计算机实时通信中一种新的数据加密技术[J]. 中南工业大学学报：自然科学版，2000，31 (1)：84-86.
LIU Lian-hao. A new date encryption technology in computer real-time communication[J]. Journal of Central South University of Technology：Natural Science, 2000, 31(1): 84−86.

[2] 孙克辉，盛利元，张纪成，等. 机动车身份信息 IC 卡读写系统的设计与实现[J]. 中南工业大学学报：自然科学版，2002, 33(5): 543−546.
SUN Ke-hui, SHENG Li-yuan, ZHANG Ji-cheng, et al. Design and implement of an IC card read-write system for vehicle identity information[J]. Journal of Central South University of Technology：Natural Science, 2002, 33(5): 543−546.

[3] 刘颖琦，周学军. 网络信息系统安全研究[J]. 中南工业大学学报：自然科学版，2002，8 (3)：249−251.
LIU Ying-qi, ZHOU Xue-jun. Study on security of network information system[J]. Journal of Central South University of Technology：Natural Science，2002，8 (3)：249−251.

[4] Matsui M. Linear cryptanalysis method for DES cipher[C]// Advances in Cryptology-EuroCrypt'93. Berlin: Springer- Verlag, 1994: 386−397.

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

[6] Ferguson N, Kelsey J. Improved cryptanalysis of Rijndael[C]// Fast Software Encryption, 7'th International Workshop. New York: Springer-Verlag，2001: 213−230.

[7] Coron J. Resistance against differential power analysis for elliptic curve cryptosystems[C]//Proceedings of CHES'99, LNCS1717. Berlin: Springer-Verlag, 1999: 292−302.

[8] Murphy S，Robshaw M J B. Essential algebraic structure within the AES[C]//Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 2002: 1−16.

[9] Kocher P, Jaffe J, Jun B. Introduction to differential power analysis and related attacks[EB/OL]. http:// www.cryptography.com/dpa/technical/, 1998.

[10] 卢开澄. 计算机密码学[M]. 北京：清华大学出版社，2003.
LU Kai-cheng. Computer cryptology[M]. Beijing: Tsinghua University Press, 2003.

[11] Daemen J, Rijmen V. AES proposal: Rijndael[EB/OL]. http://www.east.kuleuven.ac.be/~rijmen/rijndael, 1999.

[12] 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.
WANG Yan-bo. Property of affine transformation in S-box of AES[J]. Journal of PLA University：Science and Technology，2002, 4(2): 5−9.

[13] 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 Yan-bo. Analysis of structure of AES and its S-box[J]. Journal of PLA University: Science and Technology, 2002, 3(3): 13−17.

[14] 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.

[15] 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.
WEN Qiao-yan, NIU Xin-yi, YANG Yi-xian. Boolean function in modern cryptology[M]. Beijing: Science Press, 2000.

[16] Hee J, Lee D H. Resistance of S-boxes against algebraic attacks[EB/OL]. http://www.math.snu.ac.kr/ jhcheon/Published/2004_FSE/FSE04_CL.pdf, 2004.