文章编号:1674-7070(2013)04-0352-06

对称密码算法 S 盒安全性分析

刘佳[1]

摘要

S 盒是大多数对称密码算法中唯一的非线性结构,其密码学特性直接决定了密码算法的好坏. 该文对美国高级加密标准 AES 算法、韩国对称加密标准 SEED 算法、欧洲对称加密标准 Camellia 算法和中国商用密码标准 SMS4 算法的 S 盒密码学性质进行了深入的探讨,研究各种算法中 S 盒的代数性质和布尔函数性质,分析各种算法抵抗差分密码分析和线性密码分析等攻击的能力. 通过对比 S 盒的优缺点,揭示了各种算法的安全性.

关键词

对称密码;S 盒;布尔函数

中图分类号 TP393.08

文献标志码 A

收稿日期 2012-07-15

资助项目 广东省教育部产学研结合项目(2011B090400507);广东省科技计划高新技术产业化项目(2012B010100048);广东省科技计划项目(2011B020313022);广州市科技计划项目(11C42190700)

作者简介

刘佳,女,博士,讲师,从事信息安全技术及可靠编码传输技术研究.

ljia2@mail2.sysu.edu.cn

1 仲恺农业工程学院 信息科学与技术学院,广州,510225

0 引言

由于计算机网络并行计算能力的不断提高,美国数据加密标准 DES(Data Encryption Standard)在 1998 年被攻破. 1997 年初,美国已经开始计划建立高级加密标准 AES(Advanced Encryption Standard),并在世界范围内公开征集 AES 算法,经过历时 3 年的遴选和评估,比利时密码学家 Daemen 等[1]提交的 Rijndael 算法成为美国的高级加密标准. 继 AES 算法之后,韩国信息安全协会于 1998 年确定了 128 bit 对称加密标准 SEED 算法[2],并服务于很多安全系统. 2000 年 1 月 1 日,欧洲启动了欧洲签名、完整性和加密新方案 NESSIE(New European Schemes for Signatures, Integrity, and Encryption)[3]计划,3 年后确定了 Camellia 算法[4]为其对称密码标准算法之一. 2006 年 1 月 6 日,中国国家密码管理局发布第 7 号公告,将用于我国无线局域网产品的加密算法确定为 SMS4 算法[5],这是国内官方公布的第 1 个商用密码算法. 随着各种对称加密算法在实际生活中的不断应用[6-9],算法的安全性值得深入探讨与研究.

对于大多数对称密码而言,安全性取决于一个重要组成部分,即 S 盒. 这个非线性结构任何不好的性质都会影响到整个密码算法的安全性,对 S 盒密码学性质的研究可以直接反映对称密码算法抵抗差分密码分析和线性密码分析等的攻击能力. 本文深入分析美国高级加密标准 AES 算法、韩国对称加密标准 SEED 算法、欧洲对称加密标准 Camellia 算法和中国商用密码新标准 SMS4 算法 S 盒的密码学性质,研究各种算法中 S 盒的代数表达式、差分特性、线性特性等代数性质及 S 盒的平衡性、非线性、Walsh 谱等布尔函数性质,通过相互比较,揭示各种对称密码算法的安全性.

本文结构如下:第 1 节研究各种对称密码算法 S 盒的代数表达式、差分特性和线性特性等代数性质;第 2 节分析各种对称密码算法 S 盒布尔函数所具有的性质;第 3 节通过对比各种对称密码算法 S 盒的密码学性质,分析算法抵抗各种攻击的能力,揭示算法具有的安全隐患;第 4 节对全文进行总结.

1 S 盒代数性质分析

大多数对称密码算法中,S 盒是唯一的非线性结构,它的密码特性直接决定了密码算法的好坏. 本节从代数表达式、差分特性和线性

特性3个方面对AES算法(含有1个S盒)、SEED算法(含有2个S盒)、Camellia算法(含有4个S盒)、SMS4算法(含有1个S盒)中的S盒进行分析对比.

1.1 S盒代数表达式

插入攻击是Jakobsen等[10]于1997年提出的一种针对对称密码算法的攻击方法,在这种攻击中,攻击者利用密码的一些输入/输出对来构造一组多项式.如果密码中的元素有一个紧凑的代数表达式,而且这些元素能够被组合成具有可控制复杂性的表达式,那么这种插值攻击方法对于该密码来说就是可行的.特别地,此攻击方法对变换代数次数和复杂度低的密码尤为奏效.因此,在密码设计中,为了防止插入攻击,通常要求变换的代数式具有足够高的次数和项数.

S盒的代数表达式可以用如下拉格郎日插值多项式求出:

$$f(x)=\sum_{i=0}^{255}y_i\prod_{j\neq i,j=0}^{255}\frac{x-x_j}{x_i-x_j},$$
$$i=0,1,\cdots,255;\quad j=0,1,\cdots,255. \tag{1}$$

上述S盒代数表达式的运算是在有限域$GF(2^8)$上实施的,为与AES算法的S盒保持一致,本文构造的有限域以不可约多项式$m(x)=x^8+x^4+x^3+x^1+1$为生成多项式,以元素$\alpha=x+1$为生成元.分别将AES算法、SEED算法、Camellia算法、SMS4算法中S盒表中的256对数值代入式(1),求得4种算法S盒的代数表达式,8个S盒代数表达式的项数和次数如表1所示.

表1 S盒代数表达式比较

Table 1 Comparison of S-boxes' algebraic expressions

算法	S盒	次数	项数
AES	S	254	9
SEED	S1	254	255
	S2	254	255
Camellia	S1	254	254
	S2	254	253
	S3	254	254
	S4	254	255
SMS4	S	254	255

由表1可知,虽然AES算法、SEED算法、Camellia算法和SMS4算法S盒的代数表达式的次数均为254,但SMS4算法、SEED算法和Camellia算法的项数多至255,而AES算法的仅为9.可见,SEED算法、Camellia算法和SMS4算法S盒的代数表达式要比AES算法的更为复杂,在一定程度上更好地保证算法的安全性,能更有效地抵抗插入攻击.

1.2 差分特性

差分密码分析[11]是一种选择明文攻击,其基本思想是通过分析特定明文差对相应密文差的影响来获得可能性最大的密钥,它是目前对对称密码算法最为有效的攻击方法之一.差分密码分析主要利用了S盒差分分布矩阵中的特殊元素,如果某些元素值明显大于其他元素值,则这些位置将有助于差分攻击.因此,S盒抗差分密码分析能力的研究主要从其差分分布矩阵着手.

采用类似文献[12]的思想,本文对S盒的差分分布矩阵和差分均匀度进行如下定义:

定义1 S盒差分分布矩阵定义为

$$\boldsymbol{\kappa}(f)=\begin{bmatrix}\lambda_{00} & \lambda_{01} & \cdots & \lambda_{0(2^m-1)}\\ \lambda_{10} & \lambda_{11} & \cdots & \lambda_{1(2^m-1)}\\ \vdots & \vdots & & \vdots\\ \lambda_{(2^n-1)0} & \lambda_{(2^n-1)1} & \cdots & \lambda_{(2^n-1)(2^m-1)}\end{bmatrix}, \tag{2}$$

其中,$\lambda_{ij}=|\{x\in GF(2^n)\mid f(x)\oplus f(x\oplus\alpha_i)=\beta_j\}|$,$\alpha_i,\beta_j$分别为$i,j$的二进制表示,$i=0,1,\cdots,2^n-1$;$j=0,1,\cdots,2^m-1$.

定义2 $n\times m$ S盒$f:GF(2^n)\to GF(2^m)$的差分均匀度定义为

$$\delta_f=\max\{\lambda_{ij}\mid i=0,1,\cdots,2^n-1;j=0,1,\cdots,2^m-1\}. \tag{3}$$

具有较小的δ_f是S盒抗击差分攻击的必要条件.分别计算AES算法、SEED算法、Camellia算法、SMS4算法中S盒的256×256的差分矩阵.4种算法中的8个S盒的差分矩阵的最大值均为4,且最大值在每一行每一列(首行首列除外)中出现且仅出现1次.因此,可以认为AES算法、SEED算法、Camellia算法和SMS4算法S盒的差分特性是相当的,且能有效地抵抗差分密码分析攻击.

1.3 线性特性

线性密码分析是一种已知明文攻击,最早由Matsui[13]在1993年的欧密会上提出.该攻击方法的目标是寻找到并利用明文P、密文C和密钥K的若干位之间的一个线性表达式$(P\cdot\alpha)\oplus(C\cdot\beta)=(K\cdot\gamma)$.该表达式成立的概率与1/2的偏差大小是线性密码分析成功的一个重要的衡量指标.线性密码分

析思想归结到核心部件 S 盒就是要考察其输入输出比特之间的相关关系,用以下的线性分布矩阵来刻画.

定义 3 $n \times m$ S 盒 $f: GF(2^n) \to GF(2^m)$ 的线性分布矩阵定义为

$$\boldsymbol{\theta}(f) = \begin{bmatrix} \eta_{00} & \eta_{01} & \cdots & \eta_{0(2^m-1)} \\ \eta_{10} & \eta_{11} & \cdots & \eta_{1(2^m-1)} \\ \vdots & \vdots & & \vdots \\ \eta_{(2^n-1)0} & \eta_{(2^n-1)1} & \cdots & \eta_{(2^n-1)(2^m-1)} \end{bmatrix}, \quad (4)$$

其中, $\eta_{\alpha\beta} = \left| \left\{ x \mid x \in GF(2^n) \wedge \sum_{s=0}^{n-1} x_{[s]} \cdot \alpha_{[s]} = \sum_{t=0}^{m-1} x_{[t]} \cdot \beta_{[t]} \right\} \right| - 2^{n-1}$,此处 $\sum_{s=0}^{n-1} x_{[s]} \cdot \alpha_{[s]}$ 和 $\sum_{t=0}^{m-1} x_{[t]} \cdot \beta_{[t]}$ 为二进制向量的内积运算($\alpha \in GF(2^n)$, $\beta \in GF(2^m)$).

通过计算 AES 算法、SEED 算法、Camellia 算法、SMS4 算法中 S 盒的 256×256 的线性分布矩阵,发现矩阵元素的最大绝对值都是 16,且最大值在每一行每一列(首行首列除外)中出现且仅出现 5 次,这意味着 S 盒的线性逼近概率较低(16/256),即线性性较弱,符合对称密码非线性性较强的要求. 因此,可以认为 AES 算法、SEED 算法、Camellia 算法和 SMS4 算法 S 盒的线性特性是相当的,且能有效地抵抗线性密码分析攻击.

2 S 盒布尔函数的性质

对于对称密码算法 S 盒的密码特性而言,其输出比特的布尔函数所具有的密码学性质是另一个重要的研究内容,其性质直接反映了对称密码算法抵抗各种攻击的能力. 本节给出 S 盒布尔函数的定义和 3 种等价的表示方法,求出 AES 算法、SEED 算法、Camellia 算法、SMS4 算法 S 盒布尔函数多项式表达式,研究布尔函数所具有的代数性质及 Walsh 谱信息,并进行比较说明.

2.1 布尔函数的定义与表示

本小节给出了 S 盒布尔函数的定义和表示方法,通过比较 S 盒布尔函数的代数表达式,分析 AES 算法、SEED 算法、Camellia 算法、SMS4 算法 S 盒的代数复杂度,从而揭示各种算法的安全性.

定义 4[14] n 元布尔函数 $f(x)$ 定义为如下映射:

$$f: GF(2^n) \to GF(2), \quad (5)$$

其中, $x \in GF(2^n)$, $f(x) \in GF(2)$.

对于 4 种算法 S 盒 $y = S(x) \in GF(2^8)$ 来说,每一个输出比特与输入 $x \in GF(2)^8$ 的关系对应一个布尔函数,共有 8 个,即, $y = S(x) = (f_7(x), \cdots, f_0(x))$,其中,

$$f_i(x): GF(2^8) \to GF(2), \quad i = 0,1,\cdots,7. \quad (6)$$

布尔函数表达式给出了 S 盒的输入比特与输出比特之间的代数逻辑关系,这种表达式的次数和所含项数表明了 S 盒的代数复杂度. 通常,S 盒的设计准则要求布尔函数表达式的次数尽可能高,项数尽可能多.

布尔函数有 3 种等价的表示形式:真值表表示、小项表示和多项式表示. 由真值表容易得到布尔函数的小项表示,将各变元的所有可能取值代入布尔函数的多项式或小项表达式可得到其真值表.

一个 n 元布尔函数 $f(x): F_2^n \to F_2$ 是否给定,关键在于该函数之值是否对于每一组自变量 $x = (x_{n-1}, x_{n-2}, \cdots, x_0)$ 均已确定. 把每一组自变量 $x = (x_{n-1}, x_{n-2}, \cdots, x_0)$ 与其对应的函数值列成表格,称为布尔函数的真值表.

对于 $x_i, c_i \in GF(2)$,约定 $x_i^1 = x_i, x_i^0 = \bar{x}_i = 1 + x_i$,于是 $x_i^{c_i} = \begin{cases} 1, x_i = c_i, \\ 0, x_i \neq c_i. \end{cases}$ 设整数 $c(0 \leqslant c \leqslant 2^n - 1)$ 的二进制表示是 $c_0 c_1 \cdots c_{n-1}$,约定 $x^c = x_0^{c_0} x_1^{c_1} \cdots x_{n-1}^{c_{n-1}}$,它具有下述“正交性”:

$$x_0^{c_0} x_1^{c_1} \cdots x_{n-1}^{c_{n-1}} = \begin{cases} 0, & (x_0, x_1, \cdots, x_{n-1}) \neq (c_0, c_1, \cdots, c_{n-1}), \\ 1, & (x_0, x_1, \cdots, x_{n-1}) = (c_0, c_1, \cdots, c_{n-1}). \end{cases}$$

由此可得

$$f(x) = \sum_{c=0}^{2^n-1} f(c_0, c_1, \cdots, c_{n-1}) x_0^{c_0} x_1^{c_1} \cdots x_{n-1}^{c_{n-1}}, \quad (7)$$

此式称为布尔函数 $f(x)$ 的小项表示.

若将 $x_i^1 = x_i, x_i^0 = \bar{x}_i = 1 + x_i$ 代入小项表达式中,经过化简得

$$f(x) = a_0 + a_1 x_0 + \cdots + a_n x_{n-1} + a_{12} x_0 x_1 + \cdots + a_{(n-1)n} x_{n-2} x_{n-1} + \cdots + a_{12\cdots n} x_0 x_1 \cdots x_{n-1} = \sum_{u \in GF(2)^n} a_u x_0^{u_0} \cdots x_{n-1}^{u_{n-1}}, \quad (8)$$

此式称为 $f(x)$ 的多项式表达式或代数标准型.

布尔函数多项式表达式中的系数 a_u 可用 Mobius 变换[15] 求得: $a_u = \oplus_{x \prec u} f(x)$,其中, $\prec$ 代表偏序关系,即,若对于所有 $0 \leqslant i \leqslant n-1$, $x_i \leqslant u_i$ 都成立,则 $x \prec u$.

定理 1 8×8 的 S 盒各输出比特布尔函数的代数次数上界为 7.

证明 8×8 的 S 盒各输出比特布尔函数记为

$f=(f_7,f_6,f_5,f_4,f_3,f_2,f_1,f_0)$,它是 $GF(2^8)$ 上的一个置换,当输入遍历 0 ~ 255 时,其输出也遍历 0 ~ 255. 因此,其小项表达式中含有 128 项,而每一项展开均含有 $x_7x_6x_5x_4x_3x_2x_1x_0$ 项,化简后 128 个 $x_7x_6x_5x_4x_3x_2x_1x_0$ 将相互抵消掉,所以最终的表达式中将不含 $x_7x_6x_5x_4x_3x_2x_1x_0$ 项,其代数次数不会达到 8,上界只能为 7.

通过计算,4 种算法的 S 盒布尔函数代数标准型的次数都达到了最大上限 7. 对于它们 S 盒布尔函数代数标准型的最小项数而言,Camellia 算法的为 126,SMS4 算法的为 123,比 SEED 算法的 111 和 AES 算法的 110 多,并且 SEED 算法的略大于 AES 算法的(如表 2 所示). 从这个方面来说,SEED 算法、Camellia 算法和 SMS4 算法 S 盒布尔函数代数标准型复杂度略优于 AES 算法.

表 2 S 盒布尔函数代数标准型复杂度比较

Table 2 Complexity comparison of algebraic normal form of S-boxes' Boolean function

算法	S 盒	次数	项数
AES	S	7	110 ~ 145
SEED	S1	7	111 ~ 133
	S2	7	123 ~ 139
Camellia	S1	7	126 ~ 135
	S2	7	126 ~ 135
	S3	7	126 ~ 135
	S4	7	126 ~ 135
SMS4	S	7	123 ~ 135

2.2 S 盒布尔函数代数性质

一个好的 S 盒应该具有好的代数性质,良好的性质能保证算法抵抗各种密码分析的攻击. 对于大多数算法来说,S 盒是唯一的非线性结构,并在整个算法中多次使用,因此,S 盒布尔函数任何不好的代数性质都将影响到整个算法的安全性. 本小节讨论 AES 算法、SEED 算法、Camellia 算法和 SMS4 算法 S 盒布尔函数的平衡性和非线性度等密码学性质.

定义 5[14] 对 n 元布尔函数 $f:GF(2^n)\to GF(2)$,若其真值表中"1"的个数等于"0"的个数,即,均为 2^{n-1},则称 f 满足平衡性.

上述 4 种对称密码算法的 S 盒是一个 $GF(2^8)$ 到 $GF(2)$ 的一一映射,当输入遍历 0 ~ 255 时,输出也遍历 0 ~ 255,所以每一个输出比特位置上都含有 128 个"1",128 个"0",从而它们 S 盒的每一输出比特均是平衡的.

定义 6[14] 设 $f(x)$ 是一个 n 元布尔函数,记 $L_n[x]$ 为所有 n 元线性函数(包括仿射函数)之集. $f(x)$ 的非线性度定义为 $f(x)$ 与所有线性函数之最短距离:

$$N_f=\min_{l\in L_n[x]}d(f,l). \tag{9}$$

若 $f(x)$ 的非线性度满足 $N_f=2^{n-1}-2^{\frac{1}{2}n-1}$,则称 $f(x)$ 为 Bent 函数,也称完全非线性函数.

布尔函数 $f(x)$ 的非线性度 N_f 是用来衡量抵抗"线性攻击"能力的一个非线性准则,N_f 越大,则在某种意义上布尔函数 $f(x)$ 抵抗"线性攻击"的能力越强;反之,N_f 越小,则布尔函数 $f(x)$ 抵抗"线性攻击"的能力越弱.

通过计算可知,4 种算法 S 盒的所有布尔函数均是平衡函数,非线性度均为 112,与完全非线性函数有 6.67%((120 - 112)/120)的距离,因此,4 种算法均能有效地抵抗线性攻击.

2.3 S 盒布尔函数 Walsh 谱

Walsh 谱是研究布尔函数的另一种强有力的工具.

定义 7[14] n 元布尔函数的 Walsh 循环谱定义为

$$S_{(f)}(w)=2^{-n}\sum_{x=0}^{255}(-1)^{f(x)+x\cdot w}, \tag{10}$$

其中,$w\in GF(2^n)$,$x\in GF(2^n)$,$w\cdot x=w_0x_0+\cdots+w_{n-1}x_{n-1}$.

Walsh 循环谱衡量的是 $f(x)$ 与线性函数 $w\cdot x$ 的相符合程度,即 $f(x)$ 与线性函数 $w\cdot x$ 相符的 x 的个数减去 $f(x)$ 与线性函数 $w\cdot x$ 不相符的 x 的个数之差. 因此,布尔函数的 Walsh 循环谱的数值越大,说明布尔函数的 Walsh 循环谱与线性函数越接近,对应的 S 盒就越容易被攻击,对称密码算法性能越坏.

通过计算可知,4 种算法 S 盒布尔函数的循环谱绝对值的 256 倍最大值均为 32,说明其与线性函数相似程度之小. 零谱值个数均较小,仅为 17,再次说明其与线性函数相似程度之小,因为零谱值过大将导致非线性度的下降[11],反之非线性度上升.

3 对称密码算法 S 盒安全性比较

3.1 S 盒代数性质的比较

将 AES 算法、SEED 算法、Camellia 算法和 SMS4 算法 S 盒的代数性质各项数据指标的计算结果列于表 3,以便对其表达式、抗攻击能力等进行全面的比较.

虽然 AES 算法、SEED 算法、Camellia 算法和

SMS4 算法 S 盒的代数表达式的次数均为 254,但 SEED 算法、Camellia 算法和 SMS4 算法的项数多至 255,而 AES 算法的仅为 9. 可见,SEED 算法、Camellia 算法和 SMS4 算法 S 盒的代数表达式要比 AES 算法的更为复杂,在一定程度上更好地保证算法的安全性,因此,在抵抗插入攻击方面,SEED 算法、Camellia 算法和 SMS4 算法比 AES 算法更安全.

表 3　S 盒代数性质比较

Table 3　Comparison of S-boxes' algebraic properties

算法	S 盒	次数	项数	差分矩阵最大值	线性矩阵最大绝对值
AES	S	254	9	4	16
SEED	S1	254	255	4	16
	S2	254	255	4	16
Camellia	S1	254	254	4	16
	S2	254	253	4	16
	S3	254	254	4	16
	S4	254	255	4	16
SMS4	S	254	255	4	16

4 种算法 S 盒的差分矩阵的最大值均为 4,且最大值在每一行每一列(首行首列除外)中出现且仅出现 1 次. 因此,可以初步认为 AES 算法、SEED 算法、Camellia 算法和 SMS4 算法 S 盒的差分特性是相当的. 此外,4 种算法 S 盒的线性矩阵中最大绝对值均为 16,且最大值在每一行每一列(首行首列除外)中出现且仅出现 5 次. 因此,它们的线性特性也是相当的. 通过上述分析比较,4 种算法在抵抗差分密码分析和线性密码分析的能力是相当的.

3.2　S 盒布尔函数性质比较

将 AES 算法、SEED 算法、Camellia 算法和 SMS4 算法 S 盒的布尔函数性质各项数据指标的计算结果列于表 4,以便对其布尔函数的表达式、非线性性和抗攻击能力等进行全面的比较.

由表 4 可知,4 种算法 S 盒的所有布尔函数都是平衡函数,次数都达到最大上限 7,非线性度都与完全非线性函数有 6.67%((120 - 112)/120)的距离,循环谱的最大值和零谱值个数也都一致. 仅有的区别在于 SMS4 算法 S 盒布尔函数的最小项数为 123,Camellia 算法的为 126,比 SEED 算法的最小项数 111 和 AES 算法的最小项数 110 多,并且 SEED 算法的最小项数略大于 AES 算法的. 因此,从该方面来说,SMS4 算法、SEED 算法和 Camellia 算法 S 盒布尔函数的复杂度略优于 AES 算法,具有较强的抗攻击能力.

4　结束语

对称密码算法中唯一非线性结构 S 盒的密码特性直接决定了密码算法的安全性. 设计优良的 S 盒能够保证密码算法较好地抵抗插入攻击、差分密码分析攻击和线性密码分析攻击等密码攻击,而 S 盒任何不好的性质都可能会影响到整个密码算法的安全性. 本文通过对 4 种著名的对称密码算法 S 盒的分析对比,在理论上揭示了 SEED 算法、Camellia 算法和 SMS4 算法 S 盒的密码性质在一定程度上要优于 AES 算法 S 盒,而 SEED 算法、Camellia 算法和 SMS4 算法 S 盒的密码性质相当.

表 4　S 盒布尔函数性质比较

Table 4　Comparison of S-boxes' Boolean function properties

算法	S 盒	平衡性	次数	项数	非线性度	Walsh 循环谱	
						最大绝对值的 256 倍	零谱值个数
AES	S	平衡	7	110 ~ 145	112	32	17
SEED	S1	平衡	7	111 ~ 133	112	32	17
	S2	平衡	7	123 ~ 139	112	32	17
Camellia	S1	平衡	7	126 ~ 135	112	32	17
	S2	平衡	7	126 ~ 135	112	32	17
	S3	平衡	7	126 ~ 135	112	32	17
	S4	平衡	7	126 ~ 135	112	32	17
SMS4	S	平衡	7	123 ~ 135	112	32	17

参考文献

References

[1] Daemen J, Rijmen V. AES proposal: Rijndael version 2 [EB/OL]. [2012-07-15]. http://www.east.kuleuven.ac.be/~rijmen/rijndael,1999

[2] Lee H J, Lee S J, Yoon J H, et al. The SEED encryption algorithm[S]. Request for Comments: 4009, Network Working Group,2005

[3] European IST. NESSIE project [EB/OL]. [2012-07-15]. https://www.cosic.esat.kuleuven.be/nessie/,1999

[4] Aoki K, Ichikawa T, Kanda M, et al. Camellia: A 128 bit block cipher suitable for multiple platforms [EB/OL]. [2012-07-15]. http://info.isl.ntt.co.jp/camellia,2000

[5] 国家密码管理办公室. 无线局域网产品使用的 SMS4 密码算法[EB/OL]. [2012-07-15]. http://www.oscca.gov.cn/News/200810/News_1104.htm,2006
National Password Management Office. SMS4 cipher algorithm used by WLAN products [EB/OL]. [2012-07-15]. http://www.oscca.gov.cn/News/200810/News_1104.htm,2006

[6] Li J, Gan L, Du F F. Research on encryption algorithm conforming to AES in WLAN[J]. Advanced Materials Research,2012,532/533(1):1517-1521

[7] 刘佳,韦宝典,戴宪华. 基于消息恢复型 Rabin-PSS 的无线局域网认证方案[J]. 南京信息工程大学学报:自然科学版,2009,1(3):223-228
LIU Jia, WEI Baodian, DAI Xianhua. WLAN authentication scheme based on message-recovery Rabin-PSS[J]. Journal of Nanjing University of Information Science & Technology: Natural Science Edition, 2009, 1(3): 223-228

[8] Lu Y, O'Neill M P, McCanny J V. Differential power analysis resistance of Camellia and counter measure strategy on FPGAs[C]// Proceedings of International Conference on Field-Programmable Technology,2009:183-189

[9] Kitsos P, Skodras A N. An FPGA implementation and performance evaluation of the seed block cipher[C]// Proceedings of 17th International Conference on Digital Signal Processing (DSP),2011:1-5

[10] Jakobsen T, Knudsen L R. The interpolation attack on block ciphers[C]// Proceedings of Fast Software Encryption:4th International Workshop,1997:28-40

[11] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[C]// Proceedings of Advances in Cryptology-EUROCRYPT,1991:2-21

[12] Nyberg K. Differentially uniform mappings for cryptography[C]// Proceedings of Advances in Cryptology-EUROCRYPT,1994:55-64

[13] Matsui M. Linear cryptanalysis method for DES cipher [C]// Proceedings of Advances in Cryptology-EUROCRYPT,1994:386-397

[14] 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 Qiaoyan, NIU Xinxin, YANG Yixian. Boolean function of modern cryptography [M]. Beijing: Science Press,2000

[15] Filiol E. A new statistical testing for symmetric ciphers and hash functions[J]. Information and Communications Security,2002,2513(1):342-353

Security analysis of S-boxes in symmetric ciphers

LIU Jia[1]

1 College of Information Science and Technology, Zhongkai University of Agriculture and Engineering, Guangzhou 510225

Abstract S-boxes bring the only nonlinearity to symmetric ciphers and strengthen their cryptographic security. A detailed analysis of the cryptographic properties of S-boxes in several symmetric ciphers, such as AES, SEED, Camellia and SMS4, is made in this paper. The algebraic properties and the Boolean functions of S-boxes are well investigated. Then the attack capability resisting to differential cryptanalysis and linear cryptanalysis are provided. At last, the security of AES, SEED, Camellia and SMS4 is revealed by comparing the advantages and disadvantages of the S-boxes used in these symmetric ciphers.

Key words symmetric cipher; S-box; Boolean function