AES 密码分析的若干新进展

肖国镇[1],白恩健[1],刘晓娟[2]
(1. 西安电子科技大学综合业务网国家重点实验室,陕西西安 710071;2. 西安电子科技大学应用数学系,陕西西安 710071)

摘 要: 2001 年 11 月,美国国家标准和技术研究所(NIST)确定 Rijndael 算法为新的数据加密标准-高级数据加密标准(AES). AES 的密码分析是目前最受注目的一个研究问题. 本综述介绍 AES 密码分析的一些新进展:包括积分密码分析,功耗分析和代数攻击等. 作者就目前国内外的研究现状作了评述,并提出了 AES 密码分析的一些研究方向,希望能引起大家的重视.

关键词: AES; 积分分析; 功耗分析; 代数攻击
中图分类号: TP391 **文献标识码**: A **文章编号**: 0372-2112 (2003) 10-1549-06

Some New Developments on the Cryptanalysis of AES

XIAO Guo-zhen[1],BAI En-jian[1],LIU Xiao-juan[2]
(1. *P. O. Box* 119 *Key Lab. on ISN, Xidian Univ., Xi'an, Shaanxi* 710071, *China*;
2. *Department of Applied Mathematics of Xidian Univ., Xi'an, Shaanxi* 710071, *China*)

Abstract: Rijndael has been selected by NIST to become the Advanced Encryption Standard (AES) and published as FIPS 197 in November 2001. The cryptanalysis of AES is the most attentive problem at present. In this paper, some new developments on cryptanalysis of AES including Integral Cryptanalysis, Power Analysis and Algebraic Attack are introduced and some potential research ways are presented so as to draw our attention.

Key words: AES; integral cryptanalysis; power analysis; algebraic attack

1 引言

美国国家标准和技术研究所(NIST)经过三轮侯选算法筛选,从众多的分组密码中选中 Rijndael 算法[1,2]作为新的数据加密标准-高级数据加密标准(AES). Rijndael 密码是一个迭代型分组密码,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的指定为 128 比特,192 比特或者 256 比特. AES 的密码分析是当前国际密码学界比较关注的一个问题,在传统的分组密码分析中最为有力的两个攻击方法是差分分析[3]和线性分析[4]. 在 Rijndael 算法中,最主要的设计指标就是具有强的抗差分和线性分析能力. 因此,目前国外的研究工作主要集中在三个方面:积分分析(Integral Cryptanalysis),功耗分析(Power Analysis)和代数攻击(Algebraic Attack). 其中代数攻击方法是目前讨论最多也是最有前途的一种攻击方法. 国内对 AES 的密码分析才刚刚起步,还没有看到有价值的研究成果. 本文从以上三个方面介绍 AES 密码分析的一些新进展,希望引起大家的重视.

本文内容安排如下:第 2 节介绍 AES 算法的基本结构;第 3 节介绍积分密码分析;第 4 节介绍功耗分析;第 5 节介绍代数攻击;最后,在第 6 节给出我们的结论,指出 AES 密码分析的一些研究方向.

2 AES 算法的基本结构

我们假定读者熟悉全部的算法,以 128-比特分组长度 128-比特密钥长度为例简要描述 AES 算法的轮函数(详细的算法描述参考文献[1]). AES 轮函数的输入可以看成是一个 4 ×4 的字节矩阵 (a_{ij}),也可看成一个 16 ×1 的列向量,即 $(a_{ij}) = (a_{00}, \cdots, a_{30}, a_{01}, \cdots, a_{31}, \cdots, a_{33})^T$. 在 AES 的轮函数中包括四个变换(除最后一轮),依次为:字节替换(Byte-Sub),行移位(ShiftRow),列混合(MixColumns)和轮密钥加(AddRoundKey).

2.1 非线性混乱

字节矩阵中的每个元素按照 $S[\cdot]$ 进行查表替换. 替换表由三个变换组成.

(1) 在 $GF(2^8)$ 中计算 $y = x^{-1}(0^{-1} = 0)$;

(2) 计算 $z = L_A \cdot y$,这里 L_A 是一个 $GF(2)$ 上的 8 ×8 矩阵;

(3) S-盒输出为 $L_A \cdot y + 63$.

2.2 线性扩散

(1) 字节矩阵的每一行进行循环移位. 字节 a_{ij} 变为 $a_{i(j-i \bmod 4)}$,可以用一个 16 ×16 的字节矩阵 R_A 来完成行移位操作,即

收稿日期:2002-12-02;修回日期:2003-04-23
基金项目:973 项目(G1999035804);武器装备预研基金项目(51436030201DZ0105)

$$\left(a_{i(j-i \bmod 4)} \right)_{16\times 1} = R_A \cdot \left(a_{ij} \right)_{16\times 1}$$

(2) 把字节矩阵的每一列看成是 4 维 $GF(2^8)$-向量,然后计算 $y = D \cdot x$,这里 D 是一个 4 ×4 的 $GF(2^8)$-矩阵. 同样的,可以用一 16 ×16 的块对角矩阵 Mix_A (每一块都是 D) 来完成列混合操作. 即线性扩散的输出为

$$\mathrm{Mix}_A \cdot \left(a_{i(j-i \bmod 4)} \right) = \begin{bmatrix} D & 0 & 0 & 0 \\ 0 & D & 0 & 0 \\ 0 & 0 & D & 0 \\ 0 & 0 & 0 & D \end{bmatrix} \cdot R_A \cdot \left(a_{ij} \right)$$

2.3 轮密钥加

字节矩阵的每一个字节与相应的轮子密钥字节进行异或.

因此,AES 的轮函数可以表示为

$$\begin{aligned} \mathrm{Round}_A(x, (k_A)_i) &= \mathrm{Mix}_A(R_A(S(x))) + (k_A)_i \\ &= \mathrm{Mix}_A(R_A(L_A(x^{-1}) + 63)) + (k_A)_i \end{aligned} \quad (1)$$

事实上,式 (1) 可以简记为

$$\begin{aligned} \mathrm{Round}_A(x, (k_A)_i) &= \mathrm{Mix}_A(R_A(L_A(x^{-1}))) + (K_A)_i \\ &= (\mathrm{Mix}_A \cdot R_A \cdot L_A)\, x^{-1} + (K_A)_i \\ &= M_A(x^{-1}) + (K_A)_i \end{aligned} \quad (2)$$

式中 $(K_A)_i = (k_A)_i + 63$.

3 积分密码分析

积分密码分析最初被用来攻击 Square 算法[5],即 Square 攻击方法. 后来 Knudsen[6] 和 Hu 等[7] 分别独立的提出了以积分分析命名的攻击方法. 最近 Lars Knudsen 又根据高阶差分分析的思想提出了高阶积分分析[8]. 已经知道利用一阶积分分析可以成功破译六轮以下的 Rijndael[1,9].

设 $(G, +)$ 表示阶数为 k 的有限 Abelian 群,乘群 $G^n = G \times \cdots \times G$,即群元素为 $v = (v_1, \cdots, v_n)$, $v_i \in G$. 在 G^n 中定义加法 $u + v = (u_1 + v_1, \cdots, u_n + v_n)$, $u, v \in G_n$. 设向量集合

$$S = \{ v : v \in G^n \} \subseteq G^n, \ |S| = m,$$

定义 S 的积分为 $\int S = \sum_{v \in S} v$,这里 $\sum$ 按照 G^n 的加法规则进行.

积分密码分析特别适用于面向字节结构和只采用双射部件的分组密码,其主要思想就是攻击者通过预测经过几轮加密操作之后的积分值来猜测密钥字节. 为了实现这个目的,考虑以下三种情形 $(m = k)$

$$\begin{cases} (a) & v_i = c, \text{对所有 } v \in S \\ (b) & \{ v_i : v \in S \} = G \\ (c) & \sum_{v \in S} v_i = c' \end{cases} \quad (3)$$

这里 $c, c' \in G$ 是已知的. 式 (3) 中 (a) 式表示所有字都是相同的,由 Lagrange 定理 $\int S = 0$ 确定; (b) 式表示所有字都是不同的,由群论的知识可以得到 $\int S$ 的值; (c) 式表示所有字的和等于一个预先给定的值 c',根据下面两个定理可以计算 $\int S$.

定理 1[8] 设 $(G, +)$ 为有限 Abelian 加群, $H = \{ g \in G : g + g = 0 \}$ 是元素阶为 1 或 2 的子群. 令

$$s(G) = \prod_{g \in G} g,$$

则 $s(G) = \prod_{h \in H} h$,而且 $s(G) \in H$,即 $s(G) + s(G) = 0$.

定理 2[8] 设 $(G, *)$ 为有限 Abelian 乘群, $H = \{ g \in G : g * g = 1 \}$ 是元素阶为 1 或 2 的子群. 令

$$p(G) = \prod_{g \in G} g,$$

则 $p(G) = \prod_{h \in H} h$,而且 $p(G) \in H$,即 $p(G) * p(G) = 1$.

这样,对式 (3) 中的三种情况都能够找到方法求出 $\int S$ 的值. 设 $\omega_j = u_j + v_j$,这里 $u_j, v_j, \omega_j \in S$. 则

$$\sum \omega_j = \sum u_j + \sum v_j.$$

因此,如果 $\sum u_j$, $\sum v_j$ 能够确定,则 $\sum \omega_j$ 也能够确定. 而且如果 u_j 全部相同, v_j 全部不同,则 ω_j 也不相同. 同样的,设 $v_j = f(u_j)$, f 为一个线性置换 (双射),而且 u_j 不相同,则 v_j 也不相同.

类似于高阶差分,可以定义高阶积分. 考虑集合

$$\tilde{S} = S_1 \cup \cdots \cup S_s,$$

如果能够确定每个 $\sum_{v \in S_i} S_i$,则 $\sum_{v \in \tilde{S}} \tilde{S}$ 也能够被确定. 假设 G 中的字可以取 m 种不同的值, S 中包含只有一个字不同的 m 组向量,所有这些向量的和定义为 1 阶积分. 如果 S 中包含 m^d 组互不相同的向量,在这些向量中只有 d 个字不同,则定义所有这些向量的和为 d 阶积分.

1 阶积分分析可以成功攻击六轮以下的 Rijndael,这种方法已经没有什么前途,因为它过分依赖轮数,要想对 AES 构成很大的威胁可能性不大. 但是高阶积分分析是否能够攻击更多轮数的 Rijndael,目前还没有结论,值得研究.

另外,积分分析可以与插入分析[10] 结合起来. 把一个分组算法划分为两部分,前一部分采用积分分析方法,后一部分用一个低次多项式去逼近. 设 (P_i, C_i) 为一组明密文对, Z_i 表示相应的积分值, $\sum_i Z_i = 0$. 如果能够把 Z_i 表示成密文的多项式形式,即 $Z_i = p(C_i)$, $p(x) = a_d x^d + \cdots + a_1 x + a_0$. 则

$$0 = \sum_i Z_i = \sum_i p(C_i) = \sum_i \sum_{j=0}^{d} \tau_j a_j \quad (4)$$

这里 $\tau_j = \sum_i C_i^j$ 是已知的. 式 (4) 给出了包含 $d + 1$ 个未知量的线性关系. 选取 $d + 2$ 组明密文对,可以获得 $d + 2$ 个线性方程,因为只有 $d + 1$ 个未知量,所以可以求出 $p(x)$. 尽管现在还没有具体的例子表明这种攻击方法可以改善对分组密码的攻击,我们仍对这种方法持乐观态度.

4 功耗分析

在 1997 年 Paul Kocher 给出了一个比较有效的功耗分析方法[11],引起了学术界的广泛关注. 这一方法的主要特点是采用适当仪器对加密设备在加密算法运行时所泄露出来的能量信息 (电磁辐射) 进行测量,得到功率曲线,然后再对所得的大量功率曲线进行统计分析,推测出密钥,来实现密码算法的破译,这种方法需要一定的实验条件.

在传统的密码分析中,人们主要是从算法的设计角度来考虑.重点对算法的数学结构进行研究,附以关于算法输入/输出的某些假设,结合统计测试进行分析,这对高安全强度密码算法设计是必要的.但是从算法实现的角度来考虑安全问题就有些复杂了,单纯的数学结构的研究和统计测试理论的应用已经远远不够.在算法实现过程中,电磁辐射的物理特性产生了边带信道,出现了对加密过程的某些中间状态的信息泄露现象,而人们的测量手段也大大提高,功耗分析正是在这种情况下被提出的.因此它一经提出立即引起了广泛的兴趣.功耗分析特别适用于加密芯片,智能卡等小型系统(严格说不能成为系统,是一种指令集),因为它们的电磁泄露易于测量,而且也有分析价值.

常见的功耗分析方法主要有两种:简单功耗分析(SPA)与差分功耗分析(DPA)[12].SPA 是指在算法执行过程中,引入的噪声和其它干扰较少,这时所测量的指令和操作数等的功耗大小具有明显特征,而且如果我们将测量结果绘制出功耗曲线就可以结合一些指令瞬间功耗经验值来直接推断运行指令顺序,如对 DES 的密钥编排过程进行分析,最终可以提取密钥比特,攻击成功的速度极快.特别是具有条件选择和跳转的指令表现出很好的 SPA 特性,可以直接反映在所测量的功率曲线上.如果指令或操作数的汉明重量与功耗强烈相关,这是比较危险的,我们容易获得密钥的汉明重量.但是在一般情况下,操作指令的功耗比较接近,变化较小,测量时不可避免的要产生一定的误差,再加上设备及环境噪声的影响,用 SPA 的方法就很难攻击.这时可以采用 DPA 攻击.DPA 的方法是对大量的曲线样点进行功耗统计测试,令 p_1 和 p_2 是两个关于算法内部的某个相关状态 s 的不同的概率分布,按 p_1 分布的状态的瞬间功耗与按 p_2 分布的状态的瞬间功耗可能有一定的差别,可以对同一操作所测得的大量功耗样点就某个相关状态进行统计测试.这种寻找不同分布的差别和可区分性的思想是进行 DPA 分析的基础,一般情况下单一概率分布足以实现攻击.

功耗分析作为一种重要的测试手段对所有的 AES 候选算法进行了分析[13~15].恢复密钥是功耗分析的主要目的,到目前为止,对 Rijndael 的功耗分析还主要是集中在 Rijndael 的密钥表上.通过分析密钥扩展算法的结构可以发现密钥表的弱点.图 1 是用 C 语言实现的密钥扩展算法.

在图 1 中第一个"while"循环对功耗分析最敏感,因为第一轮的轮密钥为初始密钥,它直接复制到第一轮的密钥阵列而且没有经过任何的操作.这使得功耗分析与时间攻击(Timing Analysis)结合在一块相对简单.由于没有轮密钥加密过程就不能进行,因此可以只观察最初的存储器复制操作的能量信号.第二个"while"循环指明了字节替换,环移和常数加的循环方式,可以很容易与最初的存储器复制操作进行隔离.因为能量耗费是密钥汉明重量的函数,一旦得到密钥的汉明重量,攻击者就可以通过解一些线性方程恢复出密钥.这些线性方程的系数是从功耗曲线根据经验获得.为了能够抵抗功耗分析,主要是对算法进行盲化处理.在文献[16]中,作者给出了一种盲化方法,把一般的二元加法盲化与数据的乘法盲化结合在一块,在盲化过程中不需要做大量的重新计算,S-盒的 RAM 存储也很小.随后 Jovan Dj. Golic 指出[17]这种盲化方法事实上并不能抗差分功耗分析.

```
KeyExpansion(unsigned char key[4 *Nk],int w[Nb *(Nr + 1)])
{
  int i = 0
  while(i < Nk)//loop though all bytes of key
  {
    //copy bytes from key to int array
    memcpy(&w[i],&key[4 *i],4 *sizeof(unsigned char));
    i + +;
  }
  i = Nk
  while(i < Nb *(Nr + 1))
  {
    int temp = w[i - 1];
    if(i %Nk = = 0)
        temp = xor(Sub Word(RotWord(temp)),Rcon(1/Nk));
    else
        temp = Sub Word(temp);
    w[i] = xor(w[i - Nk],temp);
    i + +;
  }
}
```

图 1　密钥扩展算法

5　代数攻击

Rijndael 算法是一种明显依托于数学理论的加密算法,依靠有限域/有限环的有关性质给加解密,特别是解密提出了良好的理论基础.目前讨论最多的就是对 Rijndael 算法代数结构的分析[18~24],由此产生了一种攻击方法 XSL,统称为代数攻击.

XSL 攻击是基于这样的假设:分组算法的 S-盒能够用一个超定代数方程系统来描述.由于 Rijndael 算法本身所固有的代数性质使得可以用这样的代数方程系统来描述算法.因此,如果能够找到有效的方法来解这样的方程系统就可以破译 AES.在文献[26]中,有一个被称之为 XL 的算法可以用来解超定系统方程问题.但是该算法对 Rijndael 无效.由于用来描述 Rijndael 算法的超定代数方程非常稀疏和一些特定的结构,可以用 XSL 算法进行分析.XSL 攻击需要一个参数 P,理论上 P 为常数.文献[25]的研究表明:当 P 很大时,XSL 攻击是算法轮数 N_r 的多项式时间.即 AES 算法的安全性并不是随着轮数的增加成指数级的增加.

在 Rijndael 算法中,S-盒是唯一的非线性部件,算法的安全性完全依赖于 S-盒性质的好坏.关于 S-盒性质的分析有许多有意义的成果.

定义 1　称两个布尔函数 $b_i(x)$ 和 $b_j(x)$ 是等价的,如果存在可逆矩阵 A_{ij} 和二元常数 c_{ij},满足 $b_j(x) = b_i(A_{ij}x) \oplus c_{ij}$.

Joanne Fuller 等[24]利用布尔函数局部结构特征和布尔函数等价分类的一些新结果发现 Rijndael 算法的 S-盒输出分量

函数是等价的. 最近, Youssef 等[23]把该结果进一步推广到 Rijndael 算法的轮函数输出分量函数也是等价的.

例 Rijndael 算法的 S-盒输出分量函数为

$$f_0(x)=Tr(\beta^{66}x^{-1})+1,\ f_1(x)=Tr(\beta^{33}x^{-1})+1,$$
$$f_2(x)=Tr(\beta^{96}x^{-1}),\quad f_3(x)=Tr(\beta^{81}x^{-1})+1,$$
$$f_4(x)=Tr(\beta^{72}x^{-1}),\quad f_5(x)=Tr(\beta^{76}x^{-1})+1,$$
$$f_6(x)=Tr(\beta^{31}x^{-1})+1,\ f_7(x)=Tr(\beta^{86}x^{-1}),$$

式中 $\beta=1+\alpha$, α 是 $p(x)=x^8+x^4+x^3+x+1$ 的根. 采用下面的变换可以把 f_0 映到 f_1.

$$\begin{pmatrix}x'_0\\x'_1\\x'_2\\x'_3\\x'_4\\x'_5\\x'_6\\x'_7\end{pmatrix}=\begin{pmatrix}1&0&0&0&1&1&0&0\\0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\\1&0&0&1&1&1&1&0\\1&1&0&0&0&0&1&1\\0&1&1&0&0&0&0&1\\0&0&1&1&0&0&0&0\\0&0&0&1&1&0&0&0\end{pmatrix}\begin{pmatrix}x_0\\x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\end{pmatrix}$$

上述结果产生的原因是由于 S-盒采用域 $GF(2^8)$ 上的逆映射 $y=x^{-1}$ 构造, 所有采用这种变换来构造 S-盒的算法都存在这种弱点. 到目前为止, 还没有分析结果表明这种结构上的弱点对 AES 的安全性造成威胁.

另外, Niels Ferguson 等[21]指出用一个非常简单的代数表达式可以将 Rijndael 算法描述出来. 我们知道,

$$S(x)=\omega_8+\sum_{d=0}^{7}\omega_d x^{255-2^d},$$

做两个简化之后得到[21]

$$S(x)=\sum_{d=0}^{7}\omega_d x^{-2^d} \tag{5}$$

这样, 状态字节 $a_{ij}^{(r)}$ 经过轮变换操作后变为

$$a_{ij}^{(r+1)}=k_{ij}^{(r)}+\sum_{e_r=0}^{3}\sum_{d_r=0}^{7}\omega_{i,e_r,d_r}\left(a_{e_r(e_r+j)}\right)^{-2^{d_r}},$$

定义 $\varepsilon=\{0,\cdots,3\}$, $D=\{0,\cdots,7\}$, 则上式可记为

$$a_{ij}^{(r+1)}=k_{ij}^{(r)}+\sum_{e_r\in\varepsilon,d_r\in D}\frac{\omega_{i,e_r,d_r}}{\left(a_{e_r(e_r+j)}\right)^{2^{d_r}}}.$$

利用上式, 五轮加密操作之后得到

$$a_{ij}^{(6)}=K+\sum_{\substack{e_r\in\varepsilon\\d_r\in D}}\frac{C}{K^*+\sum_{\substack{e_r\in\varepsilon\\d_r\in D}}\frac{C}{K^*+\sum_{\substack{e_r\in\varepsilon\\d_r\in D}}\frac{C}{K^*+\sum_{\substack{e_r\in\varepsilon\\d_r\in D}}\frac{C}{K^*+\sum_{\substack{e_r\in\varepsilon\\d_r\in D}}\frac{C}{K^*+p^*}}}}} \tag{6}$$

式中符号的意义详见文献[21]. 式(6)可以推广到全部十轮加密操作之后的结果. 到目前为止, 还没有发现其它已知的分组加密算法具有如此简单的代数表达式. 但是基于这种简单的代数表达式能否找到攻击方法仍是一个公开问题. 注意到式(6)的结构与连分式的表达方式是类似的, 有可能利用连分式的理论找到某种方法求得式中包含的密钥字节.

至此, 所有的研究都是在两个不同的域 $GF(2^8)$ 和 $GF(2)$ 上进行的. XSL 攻击[25]也是在这两个域上(以 128-比特 Rijndael 为例, 恢复密钥字节需要解 8000 个二次方程, 在这些方程里面有 1600 个二元未知量. 因此 Rijndael 的安全性基于没有有效的算法解这样的方程系统. 关于 XSL 攻击方法及结果建议读者仔细阅读文献[25～27]), 因此导致 AES 密码分析非常困难和复杂. S Murphy 和 M J B Robshaw 巧妙的构造了一个新的加密体制[22] BES(Big Encryption System), AES 能够嵌入到 BES 中. 在 BES 中所有的操作都在域 $GF(2^8)$ 上进行. 因此, 对 BES 的密码分析要比 AES 简单得多. 他们的研究结果表明 AES 可以用一个 $GF(2^8)$ 上非常稀疏的超定多变量二次系统(Overdefined Multivariate Quadratic System, 简记为 MQ)来描述, 该系统的解能够恢复 AES 密钥. 下面简要介绍这一工作.

$$F=GF(2^8)=\frac{GF(2)[x]}{(x^8+x^4+x^3+x+1)}=GF(2)(\theta),$$

式中 θ 是 $x^8+x^4+x^3+x+1$ 的根. 设 $A(A\in F^{16})$ 表示 AES 的状态, $B(B\in F^{128})$ 表示 BES 的状态. 对应于 16-字节分组和 16-字节密钥长度的 AES, BES 是一个分组长度和密钥长度都是 128-字节或 1024-比特的加密算法.

定义 2 共轭映射 $\Phi: F^n\to F^{8n}$ 定义为

$$\tilde{a}=\Phi(a)=(\phi(a_0),\cdots,\phi(a_{n-1})),$$

这里, $a=(a_0,\cdots,a_{n-1})\in F^n$,

$$\phi(a_i)=\left(a_i^{2^0},a_i^{2^1},a_i^{2^2},a_i^{2^3},a_i^{2^4},a_i^{2^5},a_i^{2^6},a_i^{2^7}\right).$$

不难验证, Φ 是一一映射. 记 $B_A=\Phi(A)\in B$, AES 在共轭映射 Φ 作用下嵌入到 BES 的过程可以用图 2 表示.

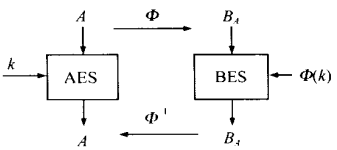

图 2 AES 与 BES 的关系

令 $a=(a_{ij})\in A$, $b=\Phi(a)\in B$. b 可以表示成 128×1 的列向量

$$b=\left(\phi(a_{00},\cdots,\phi(a_{33})\right)^{\mathrm{T}}=\left(b_{000},\cdots,b_{007},b_{100},\cdots,b_{330},\cdots,b_{337}\right)^{\mathrm{T}}$$

BES 算法轮函数的结构如下:

(1) 非线性混乱 S-盒由两个变换组成;

(a) 在 F 中计算 b^{-1};

(b) S-盒输出为 $y=Lin_B(b^{-1})$, $Lin_B=Diag_{16}(L_B)$ 为 128×128 的块对角 F-矩阵, 有 16 个相同的块 L_B.

(2) 线性扩散

(a) 在向量 y 中进行字节位置的移动. $z=R_B\cdot y$, 这里 R_B 为 128×128 的 F-矩阵;

(b) 对 z 进行字节混合操作, 混合矩阵

$$\mathrm{Mix}_B=Diag_{32}\left(C_B^{(k)}\right)$$

为 128×128 的块对角 F-矩阵.

(3) 轮密钥加 状态向量的每一个字节与相应的轮密钥字节相加, BES 的密钥表为 $(K_B)_i=\Phi((K_A)_i)$. 这里 $(K_A)_i=(k_A)_i+63$.

因此,BES 的轮函数可以表示为

$$\begin{aligned}\mathrm{Round}_B(b,(K_B)_i) &= \mathrm{Mix}_B(R_B(\mathrm{Lin}_B(b^{-1}))) + (K_B)_i\\ &= M_B\cdot(b^{-1}) + (K_B)_i \end{aligned} \quad (7)$$

这里 M_B 是 128 ×128 的 F-矩阵. L_B 与 $C_B^{(k)}$ 的意义见文献[22].

显然,BES 中的所有操作都是在域 F 上进行的,而且由共轭映射 ϕ 的性质

$$\mathrm{Round}_A(a,(K_A)_i) = \phi^{-1}(\mathrm{Round}_B(\phi(a),\phi((K_A)_i))) \quad (8)$$

因此,对 AES 的密码分析等价于 BES 的密码分析.

由文献[18,22]知, $\exists P_B \in F$, $\exists r_B = P_B^{-1}\cdot M_B\cdot P_B$, r_B 是 M_B 的 Jordan 标准型. r_B 是一个非常稀疏的矩阵,112 行有两个 1,16 行只有一个 1,其余元素全为 0. 这样,可以用下面的 MQ 系统来描述 BES.

设明文 $p\in B$,密文 $c\in B$, ω_i, $x_i\in B$ $(0\le i\le 9)$ 分别表示第 i 轮中 BES S-盒求逆前后的值,则

$$\begin{cases} \omega_0 = p + K_0,\\ x_i = \omega_i^{-1}, & i=0,\cdots,9;\\ \omega_i = M_B x_{i-1} + K_i, & i=0,\cdots,9;\\ c = M_B^* x_9 + K_{10}, \end{cases} \quad (9)$$

这里 $M_B^*\cdot \mathrm{Lin}_B = \mathrm{Mix}_B^{-1}\cdot M_B$. 对式(9)做一些处理后[22]可以用下面的多变量二次方程来描述 BES 加密.

$$\begin{cases} 0 = \omega_{0,(j,m)} + p_{(j,m)} + K_{0,(j,m)},\\ 0 = x_{i,(j,m)}\omega_{i,(j,m)} + 1, & i=0,\cdots 9,\\ 0 = \omega_{i,(j,m)} + k_{i,(j,m)} + \sum_{(j',m')} \alpha_{(j,m),(j',m')} x_{i-1,(j',m')}, & i=0,\cdots 9,\\ 0 = c_{(j,m)} + k_{l_0,(j,m)} + \sum_{(j',m')} \beta_{(j,m),(j',m')} x_{9,(j',m')} \end{cases} \quad (10)$$

其中 $j=0,\cdots,15$, $m=0,\cdots,7$. 因此 BES 加密可以用 2688 个方程(F 上)来描述,其中 1280 个非常稀疏的二次方程,1408 个线性方程. 这些方程里面共包含 2560 个状态变量和 1408 个密钥变量.

考虑 AES 加密嵌入到 BES 的操作,可以得到更多的多变量二次方程,这些方程用式(11)来描述.

$$\begin{cases} 0 = \omega_{0,(j,m)} + p_{(j,m)} + K_{0,(j,m)},\\ 0 = \omega_{i,(j,m)} + k_{i,(j,m)} + \sum_{(j',m')} \alpha_{(j,m),(j',m')} x_{i-1,(j',m')}, & i=0,\cdots 9,\\ 0 = c_{(j,m)} + k_{l_0,(j,m)} + \sum_{(j',m')} \beta_{(j,m),(j',m')} x_{9,(j',m')}\\ 0 = x_{i,(j,m)} + \omega_{(j,m)} + 1, & i=0,\cdots 9,\\ 0 = x_{i,(j,m)}^2 + x_{i(j,m+1)}, & i=0,\cdots 9,\\ 0 = \omega_{i,(j,m)}^2 + \omega_{(j,m+1)}, & i=0,\cdots 9, \end{cases} \quad (11)$$

其中 $j=0,\cdots,15$, $m=0,\cdots,7$. 因此 AES 加密可以用 5248 个方程(F 上)来描述,其中 3840 个非常稀疏的二次方程,1408 个线性方程. 这些方程里面共包含 2560 个状态变量和 1408 个密钥变量.

从上面一系列的数据可以看出,采用 XSL 攻击方法分析 BES 要比直接分析 AES 简单的多. 显然,如果能够找到某种方法求解 MQ 系统,只需要很少的明密文对就可以攻击 BES,XSL 攻击方法可以求解 MQ 系统. 到目前为止还不知道这种攻击的确切复杂度,不清楚是否这种攻击方法能够成功,但是至少还没有证明这种攻击方法是不可行的. 或许将来对 AES 的最好攻击方法就是上述的代数攻击.

6 结束语

当前,AES 密码分析的研究方兴未艾,还有很多问题没有很好的解决,是密码理论研究中国内外学者研究的热点课题之一. 本文介绍了部分代表性的工作,总的来说,主要围绕两个方面:一是从密码算法的设计入手,分析算法的代数结构;二是从密码算法的实现入手,探索算法在实现上的一些弱点. AES 算法要获得真正意义上的"破译",还需要很长一段时间,需要密码分析者的不懈努力. 下面列出当前 AES 密码分析中急需解决和值得关注的几个问题:

(1) 研究高阶积分分析对 Rijndael 算法的可行性以及积分-插入攻击的实现方法;

(2) 寻求对 Rijndael 算法的其它部分实行功耗分析,寻找其它的盲化方法安全实现算法;

(3) 研究 MQ 系统的快速求解方法.

参考文献:

[1] Daemen, V Rijmen. AES proposal: Rijndael (Version 2) [EB]. Available: NIST AES website csrc. nist. gov/ encryption/ aes.

[2] J Daemen, V Rijmen. The Design of Rijndael: AES-The Advanced Encryption Stand[M]. Berlin: Springer-Verlag, 2002.

[3] E Biham, A Shamir. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3 - 72.

[4] M Matsui. Linear cryptanalysis method for DES cipher[A]. Advances in Cryptology, Proceedings of Eurocrypt '93 [C]. Lofthus, Norway: Springer-Verlag. 1994. 386 - 397.

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

[6] L R Knudsen. Block ciphers: state of the art[R]. Copies of transparencies for lecture at the International Course on State of the Art and Evolution of Computer Security and Industrial Cryptography. Katholieke Universiteit Leuven, Belgium, 1997.

[7] Y Hu, Y Zhang, G Xiao. Integral cryptanalysis of SAFER + [J]. Electronics Letters, 1999, 35(17): 1458 - 1459.

[8] L R Knudsen, D Wagner. Integral cryptanalysis [EB]. Available: https://www.cosic.esat.kuleuven.ac.be/nessie.

[9] N Ferguson, J Kelsey, et al. Improved cryptanalysis of Rijndael[A]. Fast Software Encryption, 7th International Workshop, FSE 2000[C]. New York, USA: Springer-Verlag. 2001. 213 - 230.

[10] T Jakobsen, L Knudsen. The interpolation attack on block ciphers[A]. Fast software encryption, fouth international workshop[C]. Haifa, Israel: Springer-Verlag. 1997. 28 - 40.

[11] Paul Kocher, Joshua Jaffe, Benjamin Jun, Introduction to differential power analysis and related attacks[EB]. Available: http://www.cryp-

tography.com/dpa/technical.

[12] P Kocher, J Jaffe, B Jun. Differential power analysis[A]. Advanced in Cryptology-CRYPTO '99[C]. California, USA: Springer Verlag. 1999. 388 - 397.

[13] J Damen, V Rijmen. Resistance againstimplementation attacks, a comparative study of the AES proposals[A]. Second AES Conference[C]. Rome, Itary, 1999. Available: http://csrc.nist.gov/CryptoToolkit/aes/round1/conf2/aes2conf.htm.

[14] E Biham, A Shamir. Power analysis of the key scheduling of the AES candidates[A]. Second AES Conference[C]. Rome, Itary, 1999. Available: http://csrc.nist.gov/CryptoToolkit/aes/round1/conf2/aes2conf.htm.

[15] S Chari, C Jutla, J R Rao, P Rohatgi. A cautionary note regarding evalu-rtion of AES candidates on smart cards[A]. Second AES Conference [C]. Rome, Itary, 1999. Available: http://csrc.nist.gov/CryptoToolkit/aes/round1/conf2/aes2conf.htm.

[16] M-L Akkar, C, Giraud. An implementation of DES and AES, secure against some attacks[A]. Cryptographic Hardware and Embedded Systems-CHES 2001[C]. Paris, France: Springer-Verlag. 2001. 309 - 318.

[17] Jovan Dj. Golic. Multiplicative masking and power analysis of AES [EB]. Available: http://citeseer.nj.nec.com/529351.html.

[18] S Murphy M J B. Robshaw. New observations on the structure of Rijndael[EB]. Available: 2000. NIST AES website csrc.nist.gov/encryption/aes.

[19] J Daemen, V Rijmen. Answers to "New Observations on Rijndael" [EB]. Available: NIST AES website csrc.nist.gov/encryption/aes.

[20] S Murphy, M J B Robshaw. Further comments on the structure of Rijndael[EB]. Availbale: 2000. NIST AES website csrc.nist.gov/encryption/aes.

[21] N Ferguson, R Shroeppel, D Whiting. A simple algebraric representation of Rijndael[A]. Proceedings of Selected Areas in Cryptography[C]. Las Vegas, USA: Springer-Verlag. 2001. 103 - 111.

[22] S Murphy, M J B Robshaw. Essential algebraic structure within the AES [A]. Advances in Cryrtology-CRYPTO 2002[C]. Amsterdam, Netherlands: Springer-verlag. 2002. 1 - 16.

[23] A M Youssef, S E Tavares. On some algebraic structures in the AES round function[DB]. Available: IACR eprint server http://www.iscr.org.

[24] J Fuller, W Millan. On linear redundancy in the AES S-box[DB]. Available: http://eprint.iacr.org.

[25] N Courtois, J Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations[DB]. Available: IACR eprint server http://www.iscr.org.

[26] N Courtois, A Klimov, J Patarin, A Shair. Efficient algorithms for solving overdefined systems of multivariate polynomial equations[A]. Proceedings of Eurocrypt 2000[C]. Bruges, Belgium: Springer-Verlag. 2000. 392 - 407.

[27] [27] N Courtois, L Goubin, W Meier, J Tacier. Solving underdefined systems of multivariate quadratic equations[A]. Proceedings of Public Key Cryptography 2002[C]. Paris, France: Springer-Verlag. 2002. 211-227.

作者简介:

肖国镇 男,1934 年 9 月生于吉林四平,教授,博士生导师,主要研究方向为信息论,编码学和密码学.

白恩健 男,1977 年 2 月生于山东肥城,博士研究生,主要研究方向为信息安全和密码学.