基于 Grobner 基的 Rijndael-192 代数攻击方案

崔 杰[1,2],黄刘生[1,3],仲 红[2],杨 威[1,3]
(1.中国科学技术大学计算机科学与技术学院,安徽合肥 230026;2.安徽大学计算机科学与技术学院,安徽合肥 230039;
3.中国科学技术大学苏州研究院,江苏苏州 215123)

摘 要: 由于对 Rijndael 算法实施 Grobner 基攻击的一个关键环节是构造出其零维 Grobner 基,本文对 Rijndael-192 密码的线性变换和多变元方程系统进行了深入研究,通过选择合理的项序及变量次序,提出了 Rijndael-192 零维 Grobner 基的构造方法.文中详述了该 Grobner 基的构造方法,并给出了相关性质的理论证明.此外,本文提出了一种 Rijndael-192 的 Grobner 基攻击方案,攻击复杂度低于穷举攻击.

关键词: Rijndael 算法; Grobner 基; 代数攻击; 多变元方程系统
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2013)05-0833-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.05.001

Algebraic Attack on Rijndael-192 Based on Grobner Basis

CUI Jie[1,2], HUANG Liu-sheng[1,3], ZHONG Hong[2], YANG Wei[1,3]
(1. *School of Computer Science and Technology, University of Scienc and Technology of China, Hefei, Anhui* 230026, *China*;
2. *School of Computer Science and Technology, Anhui University, Hefei, Anhui* 230039, *China*;
3. *Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou, Jiangsu* 215123, *China*)

Abstract: Because a key step of Grobner basis attack on Rijndael is constructing its zero-dimensional Grobner basis, authors perform some particular studies on the linear transformation and the system of multivariate polynomial equations of Rijndael-192, and propose its zero-dimensional Grobner basis construction method through choosing suitable term order and variable order. After presenting the construction method of the Grobner basis, authors give the necessary theorical proves. Moreover, authors propose an algebraic attack on Rijndael-192 based on Grobner basis. Analysis suggest that the attack complexity is lower than exhaustive attack.

Key words: Rijndael algorithm; Grobner basis; Algebraic attack; Multivariate equation system

1 引言

2000 年 10 月 2 日,由比利时密码学家 Daemen 和 Rijmen 设计的 Rijndael 算法被美国国家标准技术研究所(NIST)确定为美国高级加密标准 AES (Advanced Encryption Standard)[1].自从 Rijndael 算法被提出以来,一直受到密码学界的关注,出现了许多攻击方法,但目前尚未存在对完整 Rijndael 算法的成功攻击[2,3].

近年来,代数攻击的分析手段成为了密码分析学的研究热点.代数攻击主要由两步组成:第 1 步是建立一个代数方程系统以描述密码算法的明文、密文和密钥之间的关系;第 2 步是通过一些已知的明密文对来求解方程系统以得到密钥.第 1 步已经取得一些研究成果,学者们提出了多种描述 Rijndael 算法的方程系统[4,5].第 2 步中的求解多变元方程系统仍然是一个研究中的问题,尽管求解多变元方程系统是 NP 难问题,但求解稀疏超定方程组的复杂度远远低于 NP 难问题.

目前,求解多变元高次方程系统的方法主要有 XL、XSL 和 Grobner basis 等.由于 Rijndael 算法的代数表达式是稀疏且结构化的,因此对其直接应用 XL 攻击方法是低效的.2002 年,Courtois 等人提出了 XSL 攻击方法,并声称在理论上攻破了密钥长度为 256 位的 Rijndael 算法,但之后学术界对 XSL 攻击产生线性独立方程数量的估计有很大争议,对攻击的有效性表示质疑[6,7].Grobner 基方法是一种在国外被普遍认同的用于求解多变元高次方程系统的有效方法,其概念最早由 Buch

收稿日期:2012-05-16;修回日期:2012-08-10
基金项目:国家自然科学基金(No.60903217,No.61173188,No.61173187);中央高校基本科研业务费专项资金(No.WK0110000027);国家自然科学基金数学天元基金(No.11126174);安徽省高校自然科学研究重点项目(No.KJ2013A017);江苏省自然科学基金(No.BK2011357);安徽大学博士科研启动经费项目

berger 提出.其本质是从多项式环中任意理想的生成元出发,刻画和计算出一组具有良好性质的生成元,进而研究理想的结构并进行理想计算[3].

Grobner 基是多项式理想的标准表示法,该表示方法具有一些有用的性质[8].任意理想都存在 Grobner 基,可以使用 Buchberger 算法、F4 算法或 F5 算法来计算任意理想的 Grobner 基[6].字典序是一种常用的消元序,使用字典序 Grobner 基计算时,基的系数矩阵呈三角形,最后一行是一元方程,这就是字典序 Grobner 基能求解方程系统的原因.但直接计算字典序 Grobner 基将产生过多的系数.通用的做法是先计算理想的总次数序 Grobner 基,然后使用项序转化算法将总次数序 Grobner 基转化为字典序 Grobner 基.项序转化算法主要包括 Grobner Walk 算法和 FGLM 算法[6],与 Grobner Walk 算法相比,FGLM 算法简单高效,但 FGLM 算法只能将零维理想下的任何项序的 Grobner 基转化为字典序 Grobner 基[9,10].因此,构造 Rijndael 算法零维理想的 Grobner 基对实施 Grobner 基攻击至关重要.本文在研究 Rijndael-192 密码的线性变换和方程系统基础上,通过选择合理的项序,提出了其零维 Grobner 基的构造方法,给出了相关结论的理论证明,并提出了 Rijndael-192 的 Grobner 基攻击方案.

2 Rijndael-192 加密算法数学模型

Rijndael 密码算法的分组长度和密钥长度可分别独立地指定为 128 位、192 位或 256 位,算法相应要进行 10 轮、12 轮或 14 轮运算.每轮由 4 个变换组成:S 盒替换(ByteSub)、行移位(ShiftRow)、列混和(MixColume)、轮密钥加(AddRoundKey).算法由轮密钥加开始,接着 11 轮迭代,最后一轮迭代不包含列混和.本文研究分组长度和密钥长度均为 192 位的 Rijndael 加密算法,下面以一轮加密过程为例解释其数学模型.

2.1 S 盒替换

S 盒运算是一个独立作用于状态字节的非线性变换,简记为 S.包括有限域 $GF(2^8)$ 中的求逆运算和 $GF(2)$域中的仿射变换两个步骤.

(a)在 $GF(2^8)=\dfrac{Z_2[x]}{(x^8+x^4+x^3+x+1)}$ 域中求乘法的逆运算,即输入 $\omega\in GF(2^8)$,求 $\upsilon\in GF(2^8)$满足:

$$\omega * \upsilon = 1 \mod (x^8+x^4+x^3+x+1)$$

则有

$$\upsilon=\omega^{-1}=\begin{cases}\omega^{254}, & \omega\neq 0\\ 0, & \omega=0\end{cases}$$

(b)令 $x=\upsilon$ 在 $GF(2)^8$ 中的元素分量为$(x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0)$,仿射变换如下:

$$\boldsymbol{y}=\boldsymbol{La}\times\boldsymbol{x}+\text{'63'}=\begin{bmatrix}1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\\1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\end{bmatrix}\begin{bmatrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{bmatrix}+\begin{bmatrix}0\\1\\1\\0\\0\\0\\1\\1\end{bmatrix}$$

常量'63'的选择确保了 S 盒没有不动点 $S(a)=a$ 和对立不动点 $S(a)=\bar{a}$,输入位的线性组合与输出位的线性组合之间的最大平凡相关性是 2^{-3},异或差分表的非平凡最大输出差分概率是 2^{-6},S 盒具有抵抗线性攻击和差分攻击的能力[1].

2.2 ShiftRow 与 MixColumn 变换

通过 S 盒替换得到 4×6 字节矩阵,其中 $S_{i,j}$是第 i 行第 j 列的字节,$0\leqslant i\leqslant 3$,$0\leqslant j\leqslant 5$.SR(ShiftRow)变换使矩阵的第 i 行左移 i 个字节:

$$\begin{bmatrix}s_{0,0}&s_{0,1}&s_{0,2}&s_{0,3}&s_{0,4}&s_{0,5}\\s_{1,0}&s_{1,1}&s_{1,2}&s_{1,3}&s_{1,4}&s_{1,5}\\s_{2,0}&s_{2,1}&s_{2,2}&s_{2,3}&s_{2,4}&s_{2,5}\\s_{3,0}&s_{3,1}&s_{3,2}&s_{3,3}&s_{3,4}&s_{3,5}\end{bmatrix}$$

$$\rightarrow\begin{bmatrix}s_{0,0}&s_{0,1}&s_{0,2}&s_{0,3}&s_{0,4}&s_{0,5}\\s_{1,1}&s_{1,2}&s_{1,3}&s_{1,4}&s_{1,5}&s_{1,0}\\s_{2,2}&s_{2,3}&s_{2,4}&s_{2,5}&s_{2,0}&s_{2,1}\\s_{3,3}&s_{3,4}&s_{3,5}&s_{3,0}&s_{3,1}&s_{3,2}\end{bmatrix}$$

MC(MixColume)变换对每列进行独立操作以达到混淆的目的.把每列中的每个字节映射为新值 ,此值由该列中的 4 个字节通过函数变换得到.变换如下:

$$\begin{bmatrix}s'_{0,0}&s'_{0,1}&s'_{0,2}&s'_{0,3}&s'_{0,4}&s'_{0,5}\\s'_{1,0}&s'_{1,1}&s'_{1,2}&s'_{1,3}&s'_{1,4}&s'_{1,5}\\s'_{2,0}&s'_{2,1}&s'_{2,2}&s'_{2,3}&s'_{2,4}&s'_{2,5}\\s'_{3,0}&s'_{3,1}&s'_{3,2}&s'_{3,3}&s'_{3,4}&s'_{3,5}\end{bmatrix}=\boldsymbol{D}\cdot\begin{bmatrix}s_{0,0}&s_{0,1}&s_{0,2}&s_{0,3}&s_{0,4}&s_{0,5}\\s_{1,0}&s_{1,1}&s_{1,2}&s_{1,3}&s_{1,4}&s_{1,5}\\s_{2,0}&s_{2,1}&s_{2,2}&s_{2,3}&s_{2,4}&s_{2,5}\\s_{3,0}&s_{3,1}&s_{3,2}&s_{3,3}&s_{3,4}&s_{3,5}\end{bmatrix},$$

其中,$\boldsymbol{D}=\begin{bmatrix}02&03&01&01\\01&02&03&01\\01&01&02&03\\03&01&01&02\end{bmatrix}$.

为了数学表达的方便,本文采用一个列向量取代原有的矩阵表示,即采用 24×1 矩阵来表示中间状态和密钥.列向量中元素与原矩阵中元素的映射关系如下:

$$\varphi:\ F^{4\times 6}\to F^{24},\ \begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5}\\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5}\\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5}\\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5}\end{pmatrix}\mapsto (s_{0,0},s_{1,0},\cdots,s_{0,1},s_{1,1},\cdots)^{\mathrm{T}}$$

对于有限域 $GF(2^8)$,简记为 F.本文引入一个 24×24的 0-1 变换矩阵 M_{SR},使 SR 变换等价于左乘矩阵 M_{SR}.该矩阵的每行每列均只有一个元素为 1,其余都为 0.同理,引入另一变换矩阵 $\boldsymbol{M}_{MC}$,使 MC 变换等价于左乘 $\boldsymbol{M}_{MC}$.$\boldsymbol{M}_{MC}$的构造原理为 $\boldsymbol{M}_{MC}=\boldsymbol{D}\otimes\boldsymbol{I}_6\in\boldsymbol{F}^{24\times 24}$,其中,$\otimes$ 表示张量积,$\boldsymbol{I}_6$ 表示 6 阶单位阵.将这两个变换合记为 $\boldsymbol{M}$,则 $\boldsymbol{M}=\boldsymbol{M}_{MC}\cdot\boldsymbol{M}_{SR}$.根据 $\boldsymbol{M}_{SR}$和 $\boldsymbol{M}_{MC}$,容易得到:

$$\boldsymbol{M}=\boldsymbol{M}_{MC}\cdot\boldsymbol{M}_{SR}=\begin{bmatrix}
02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00\\
01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00\\
01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00\\
03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00\\
00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00\\
00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&0&00&01&00&00&00&00\\
00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00\\
00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00\\
00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01\\
00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01\\
00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03\\
00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02\\
00&00&00&01&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00\\
00&00&00&01&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00\\
00&00&00&03&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00\\
00&00&00&02&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00\\
00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00\\
00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00\\
00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00\\
00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00\\
00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&02&00&00&00\\
00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&01&00&00&00\\
00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&01&00&00&00\\
00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&03&00&00&00
\end{bmatrix}$$

因而,由 SR 和 MC 组成的线性变换可以表示为:$(s''_{0,0},s''_{1,0},\cdots,s''_{0,1},s''_{1,1},\cdots)^{\mathrm{T}}=\boldsymbol{M}\cdot(s_{0,0},s_{1,0},\cdots,s_{0,1},s_{1,1},\cdots)^{\mathrm{T}}$

2.3 AddRoundKey

轮密钥加就是输入与轮密钥异或.简记为 $Y=X\oplus K$,其中 K 是轮密钥.

2.4 Key Schedule 算法

密钥调度由两个模块组成:密钥扩展和轮密钥选择.N_b、N_k 分别表示分组长度和密钥长度,单位是 4 字节字.即 N_b = 分组位数/32,N_k = 密钥位数/32.R 是加密轮数.

对于 Rijndael-192,$N_b=6$,$N_k=6$,$R=12$.Rijndael-192 的密钥扩展是将 6 个 4 字节字的密钥扩展成 78 个 4 字节字 $W[\cdot]$,其中 $W[0]$,$W[5]$为原始密钥.扩展算法如下:

for ($i=6;i<78;i++$){
  if ($i\%6=0$)
    $W[i]=W[i-6]\oplus BS(\mathrm{RotByte}(W[i-1]))\oplus \mathrm{const}(i/6)$;
  else $W[i]=W[i-6]\oplus W[i-1]$}

由上面扩展算法,可以进一步得到 $N_k=6$ 时密钥扩展的递归模型为

$$W_i=\begin{cases}(Key[4i],Key[4i+1],Key[4i+2],Key[4i+3]), & 0\leqslant i\leqslant 6\\ W_{i-N_k}\oplus BS(RotByte(W_{i-1}))\oplus const[i/6], & i\%6=0\\ W_{i-N_k}\oplus W_{i-1}, & \text{其他}\end{cases}$$

3 Grobner 基理论

对于环 R 中给定的理想 I,其 Grobner 基一般并不唯一[11].这些 Grobner 基与选择的项序密切相关,下面给出相关定义.

定义 1　集合 $T(R)$上的序$\leqslant$称为项序(term order),是指$\leqslant$是一个线序,同时满足下面两个性质

(1)对所有 $t\in T(R)$,都有 $t\geqslant 1$.

(2)对任何 $s,t_1,t_2\in T(R)$,如果 $t_1\leqslant t_2$,则 $st_1\leqslant st_2$.

在某一项序$\leqslant$下,多项式 p 的项的集合的最大元素被称为p 的首项(head term),简记为 $HT(p)$.

令$\mathbb{N}$是自然数集合,n 是一给定的正整数,$x_1, x_2, \cdots, x_n$ 表示环 R 上的 n 个变元.令项的集合

$$T(R)=\{x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}\mid \alpha_i\in\mathbb{N}, i=1,2,\cdots,n\},$$

即 $T(R)$是 n 个变元幂积的集合.项 $t=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}\in T(R)$的次数记为 $\deg(t)=\sum_{i=1}^{n}\alpha_i$.令 $X=(x_1, x_2, \cdots, x_n)$,下面介绍三个常用项序的定义.

定义 2 $T(R)$上相对 $x_1>x_2>\cdots>x_n$ 的字典序(lexicographical order),简记为 lex,定义如下:

对于 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n), \beta=(\beta_1,\beta_2,\cdots,\beta_n)\in\mathbb{N}^n$,则 $X^\alpha <_{lex} X^\beta \Leftrightarrow$存在 $0\leqslant k\leqslant n-1$,使得 $\alpha_j=\beta_j, j=0,1,\cdots,k$,且 $\alpha_{k+1}<\beta_{k+1}$(约定 $\alpha_0=\beta_0$).

定义 3 $T(R)$上相对 $x_1>x_2>\cdots>x_n$ 的次数字典序(degree lexicographical order),简记为 deglex,定义如下:

对于 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n), \beta=(\beta_1,\beta_2,\cdots,\beta_n)\in\mathbb{N}^n$,则

$$X^\alpha <_{deglex} X^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^{n}\alpha_i < \sum_{i=1}^{n}\beta_i, \text{或} \\ \sum_{i=1}^{n}\alpha_i = \sum_{i=1}^{n}\beta_i, \text{且按字典序有} \\ X^\alpha <_{lex} X^\beta \end{cases}$$

定义 4 $T(R)$上相对 $x_1>x_2>\cdots>x_n$ 的次数反字典序(degree reverse lexicographical order),简记为 degrevlex,定义如下:

对于 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n), \beta=(\beta_1,\beta_2,\cdots,\beta_n)\in\mathbb{N}^n$,则

$$\begin{aligned} X^\alpha <_{degrevlex} X^\beta \Leftrightarrow & \sum_{i=1}^{n}\alpha_i < \sum_{i=1}^{n}\beta_i, \text{或} \\ & \sum_{i=1}^{n}\alpha_i = \sum_{i=1}^{n}\beta_i, \alpha_n=\beta_n, \cdots, \alpha_{i+1}=\beta_{i+1}, \\ & \alpha_i\neq\beta_i \text{ 且 } \alpha_i>\beta_i, \text{即在 } \alpha \text{ 和} \beta \text{ 中右数} \\ & \text{第一个不同的坐标,有 } \alpha_i>\beta_i. \end{aligned}$$

定义 5 设 I 是环 R 中任意给定的一个非零理想,$G=\{g_1,\cdots,g_m\}\subset I$.称 G 是理想 I 的 Grobner 基(Grobner basis),当且仅当有:

$$\langle HT(g_1),\cdots,HT(g_m)\rangle=\langle\{HT(p): p\in I\}\rangle$$

利用 Buchberger 算法,可以得到任何非零理想的 Grobner 基[11].在 Buchberger 算法实现中,可以采用 Buchberger 准则来消去不必要的多项式[11,12].基于 Buchberger 准则可以得到如下结论.

定理 1 设 G 是一个多项式集合,$H=\{HT(f): f\in G\}$,若 H 中所有元素两两互素,则 G 是 Grobner 基.

证明参见文献[13].

0 维理想指的是在域内有有限个解的理想.这个性质有利于 Grobner 基的相关计算.利用文献[14]中的推论 6.56 可以判定一个理想是否是 0 维的,下面给出该推论的简化结论.

定理 2 设 G 是理想 I 的 Grobner 基,则 $\dim(I)=0$ 当且仅当对任一 $1\leqslant i\leqslant n$ 存在一个多项式 $g\in G$ 使得 $HT(g)=x_i^{d_i}$.

4 Rijndael-192 方程系统

本文中令$((p_0,\cdots,p_{23}),(c_0,\cdots,c_{23}))\in F^{24}\times F^{24}$为已知明密文对.$x_{i,j}$表示第 i 轮轮密钥加后的状态的第 j 个元素变量,$k_{i,j}$表示第 i 轮轮密钥的第 j 个元素变量,特别地,$k_{0,j}$表示原始密钥 $0\leqslant i\leqslant 12, 0\leqslant j\leqslant 23$. $GF(2^8)$上的方程系统由如下四部分组成:

(1)初始轮(第 0 轮)方程和密文方程:

$$\begin{matrix} x_{0,0}+k_{0,0}+p_0=0 & x_{12,0}+c_0=0 \\ \vdots & \vdots \\ x_{0,23}+k_{0,23}+p_{23}=0 & x_{12,23}+c_{23}=0 \end{matrix} \tag{1}$$

(2)中间轮方程,即第 i 轮加密方程,$1\leqslant i\leqslant 11$:

$$\begin{pmatrix} x_{i,0}+k_{i,0} \\ x_{i,1}+k_{i,1} \\ \vdots \\ x_{i,23}+k_{i,23} \end{pmatrix} + \boldsymbol{M}\cdot\begin{pmatrix} S(x_{i-1,0}) \\ S(x_{i-1,1}) \\ \vdots \\ S(x_{i-1,23}) \end{pmatrix} = 0 \tag{2}$$

(3)最后一轮方程:

$$\begin{pmatrix} x_{12,0}+k_{12,0} \\ x_{12,1}+k_{12,1} \\ \vdots \\ x_{12,23}+k_{12,23} \end{pmatrix} + M_{SR}\cdot\begin{pmatrix} S(x_{11,0}) \\ S(x_{11,1}) \\ \vdots \\ S(x_{11,23}) \end{pmatrix} = 0 \tag{3}$$

(4)密钥调度方程:

$$\begin{pmatrix} k_{i,0} \\ k_{i,1} \\ k_{i,2} \\ k_{i,3} \\ k_{i,4} \\ k_{i,5} \\ \vdots \\ k_{i,23} \end{pmatrix} = \begin{pmatrix} k_{i-1,0}+S(k_{i-1,21})+\xi^{i-1} \\ k_{i-1,1}+S(k_{i-1,22}) \\ k_{i-1,2}+S(k_{i-1,23}) \\ k_{i-1,3}+S(k_{i-1,20}) \\ k_{i-1,4}+k_{i,0} \\ k_{i-1,5}+k_{i,1} \\ \vdots \\ k_{i-1,23}+k_{i,19} \end{pmatrix} \tag{4}$$

其中,$\xi^{i-1}(1\leqslant i\leqslant 12)$是轮常量.

5 Rijndael-192 的 Grobner 基攻击方案

定义 6 记 Rijndael 中有限域 $GF(2^8)$为 F,则 F 上的多变元多项式环 R 定义为:

$$R:=F[x_{i,j}, k_{i,j}: \{0\leqslant i\leqslant 23, 0\leqslant j\leqslant 12\}]$$

为了构造 Rijndael-192 的 Grobner 基,需要对上一节得到的多变元方程系统进行改进以满足 Grobner 基的要

求,即方程左边的多项式首项两两互素.

5.1 Rijndael-192 Grobner 基的构造方法

Rijndael-192 Grobner 基的构造步骤如下:

步骤 1 该步骤的目的是构造 S 盒及逆 S 盒的多项式集合.在此步骤中,我们利用了已有的 S 盒及逆 S 盒的代数表达式.

Rijndael 中的 S 盒是基于明显的数学理论构造的,因此可以将其写成代数表达式的形式.S 盒在有限域 F 上的稀疏代数表达式如下[15]

$$\begin{aligned}S:F\to F,x\mapsto\ & 05x^{FE}+09x^{FD}+F9x^{FB}+25x^{F7}+\\ & F4x^{EF}+B5x^{DF}+B9x^{BF}+8Fx^{7F}+63\end{aligned}$$

逆 S 盒非稀疏的代数表达式包含 255 项.由于项数较多,在此只给出简式:

$$S^{-1}:F\to F,x\mapsto\sum_{i=0}^{254}c_ix^i$$

其中,c_i 是次数为 i 的项对应的系数,逆 S 盒的代数表达式系数表见文献[16].

步骤 2 该步骤的目的是构造线性变换阶段的多项式集合.在此步骤中,我们用到了上一节给出的方程系统.

由方程组(1),容易得到明文方程即初始轮方程组如式(5)所示,密文方程组如式(6)所示.

$$x_{0,i}+k_{0,i}+p_i=0,\quad p_i\in F,0\leqslant i\leqslant 23 \tag{5}$$

$$x_{12,i}+c_i=0,\quad c_i\in F,0\leqslant i\leqslant 23 \tag{6}$$

由于 $x_{0,i}$和 $k_{0,i}$具有相同的次数,因此方程组(5)的多项式首项是 $x_{0,i}$或 $k_{0,i}$,如果选择项序 $x_{0,i}<k_{0,i}$,则多项式首项为 $k_{0,i}$,$0\leqslant i\leqslant 23$.对于方程组(6),其多项式首项是 $x_{12,i}$,$0\leqslant i\leqslant 23$.

对于方程组(2)和(3),需要进行改进以符合 Grobner 基的要求.由方程组(2)容易得到第 $i(1\leqslant i\leqslant 11)$轮的 24 个多项式方程组如式(7)所示.

$$\begin{pmatrix}S(x_{i-1,0})\\S(x_{i-1,1})\\\vdots\\S(x_{i-1,23})\end{pmatrix}+\boldsymbol{M}^{-1}\cdot\begin{pmatrix}x_{i,0}+k_{i,0}\\x_{i,1}+k_{i,1}\\\vdots\\x_{i,23}+k_{i,23}\end{pmatrix}=0 \tag{7}$$

同理,由方程组(3)容易得到最后一轮的 24 个方程如式(8)所示.

$$\begin{pmatrix}S(x_{11,0})\\S(x_{11,1})\\\vdots\\S(x_{11,23})\end{pmatrix}+\boldsymbol{M}_{SR}^{-1}\cdot\begin{pmatrix}x_{12,0}+k_{12,0}\\x_{12,1}+k_{12,1}\\\vdots\\x_{12,23}+k_{12,23}\end{pmatrix}=0 \tag{8}$$

对于次数字典序,方程组(7)和方程组(8)的多项式首项是 $x_{i,j}^{254}$,$0\leqslant i\leqslant 11$,$0\leqslant j\leqslant 23$.容易看出这些首项没有非平凡的公因子,即最大公因子为 1.

步骤 3 该步骤的目的是构造密钥调度阶段的多项式集合.在此步骤中,我们同样用到了上一节给出的方程系统.

为了得到包含整个加密算法产生的多项式的 Grobner 基,需要对密钥调度方程进行改进.对方程组(4)稍加变换得到方程组(9).

$$\begin{pmatrix}k_{i,0}\\k_{i,1}\\k_{i,2}\\k_{i,3}\\k_{i,4}\\k_{i,5}\\\vdots\\k_{i,23}\end{pmatrix}=\begin{pmatrix}k_{i-1,0}\\k_{i-1,1}\\k_{i-1,2}\\k_{i-1,3}\\k_{i-1,4}\\k_{i-1,5}\\\vdots\\k_{i-1,23}\end{pmatrix}+\begin{pmatrix}S(k_{i-1,21})\\S(k_{i-1,22})\\S(k_{i-1,23})\\S(k_{i-1,20})\\k_{i,0}\\k_{i,1}\\\vdots\\k_{i,19}\end{pmatrix}+\begin{pmatrix}\xi^{i-1}\\0\\0\\0\\0\\0\\\vdots\\0\end{pmatrix} \tag{9}$$

为了使密钥调度产生的多项式首项互素,需要对方程组(9)进行逆 S 盒变换,变换后如式(10)所示.

$$\begin{pmatrix}S^{-1}(k_{i,0}+k_{i-1,0}+\xi^{i-1})\\S^{-1}(k_{i,1}+k_{i-1,1})\\S^{-1}(k_{i,2}+k_{i-1,2})\\S^{-1}(k_{i,3}+k_{i-1,3})\\k_{i,4}+k_{i-1,4}\\k_{i,5}+k_{i-1,5}\\\vdots\\k_{i,23}+k_{i-1,23}\end{pmatrix}+\begin{pmatrix}k_{i-1,21}\\k_{i-1,22}\\k_{i-1,23}\\k_{i-1,20}\\k_{i,0}\\k_{i,1}\\\vdots\\k_{i,19}\end{pmatrix}=0 \tag{10}$$

根据逆 S 盒的代数表达式,可以得到方程组(10)包含的各个方程.如果选定如下项序:

$$k_{i,23}>k_{i,22}>\cdots>k_{i,0}>k_{i-1,23}>\cdots>k_{i-1,1}>k_{i-1,0}$$

其中,$1\leqslant i\leqslant 12$,则密钥调度方程组(10)的多项式首项集为:

$$\{k_{i,j}^{254},k_{i,h}:1\leqslant i\leqslant 12,0\leqslant j\leqslant 3,4\leqslant h\leqslant 23\}$$

容易看出,此首项集中的元素没有非平凡的公因子.

步骤 4 该步骤的目的是选择合理的项序及变量次序.若选择合理变量次序的次数字典序,则可以使整个加密算法产生的多项式首项两两互素.

由方程式(5)、(6)、(7)、(8)和(10)的左边构成的多项式集合记为 A,相对如下变量次序的次数字典序 $<_A$ 可以使 A 中多项式首相两两互素:

$$\begin{aligned}&\underbrace{x_{0,0}<\cdots<x_{0,23}}_{\text{initial round state variables}}<\underbrace{k_{0,0}<\cdots<k_{0,23}}_{\text{initial key variable}}<\\&\underbrace{k_{1,0}<\cdots<k_{1,23}}_{\text{first round key variables}}<\cdots<\underbrace{k_{12,0}<\cdots<k_{12,23}}_{\text{last round key variables}}<\\&\underbrace{x_{1,0}<\cdots<x_{1,23}}_{\text{first round internal state variables}}<\cdots<\underbrace{x_{11,0}<\cdots<x_{11,23}}_{\text{11th round internal state variables}}<\\&\underbrace{x_{12,0}<\cdots<x_{12,23}}_{\text{ciphertext variables}}\end{aligned}$$

经过上述四个步骤,在相序 $<_A$ 下的多项式集合 A 是环 R 中理想〈A〉的 Grobner 基,下面将给出相关性质及其理论证明.

5.2 Rijndael-192 Grobner 基的性质

Grobner 基是多项式理想的标准记法,这种记法有两个有用的性质:①给定一个理想的 Grobner 基,可以有效地判定一个多项式是否属于该理想;②对于合理的项序,可以有效地计算理想的种类,从而可以求出由这些理想导出的多项式方程系统的解.多项式集合 A 共包含 624 个多项式,其中 336 个是次数为 254 的多项式,288 个是线性多项式,共包含 624 个变量 $x_{i,j}, k_{i,j}, 0 \leqslant i \leqslant 12, 0 \leqslant j \leqslant 23$.对于多项式集合 A,有如下结论:

定理 3 多项式集合 A 相对次数字典序 $<_A$ 构成 Grobner 基.

证明 在项序 $<_A$ 下,方程组(5)的多项式首项集 $H_1 = \{k_{0,i}: 0 \leqslant i \leqslant 23\}$,方程组(6)的多项式首项集 $H_2 = \{x_{12,i}: 0 \leqslant i \leqslant 23\}$,方程组(7)和(8)的多项式首项集 $H_3 = \{x_{i,j}^{254}: 0 \leqslant i \leqslant 11, 0 \leqslant j \leqslant 23\}$,方程组(10)的多项式首项集 $H_4 = \{k_{i,j}^{254}, k_{i,h}: 1 \leqslant i \leqslant 12, 0 \leqslant j \leqslant 3, 4 \leqslant h \leqslant 23\}$,因此 A 的首项集 $H = H_1 \cup H_2 \cup H_3 \cup H_4$.由于 $\forall a, b \in H$, $gcd(a, b) = 1$,因此 H 中元素两两互素.根据定理 1,可以得到集合 A 相对项序 $<_A$ 构成 Grobner 基.

定理 3 说明本文构造的多项式集合 A 是环 R 中理想〈A〉的 Grobner 基,为进行 Rijndael-192 的理想计算提供了可能.

定理 4 Rijndael-192 的 Grobner 基 A 生成的理想〈A〉是零维的.

证明 由于 Rijndael-192 方程系统的变元集合是 $V = \{x_{i,j}, k_{i,j}: 0 \leqslant i \leqslant 12, 0 \leqslant j \leqslant 23\}$,因此变元数 $|V| = 624$.由定理 3 证明过程可知,在项序 $<_A$ 下,Rijndael-192 方程系统的多项式集合 A 的首项集是 H.由于 $\forall x \in V$,存在某个 $1 \leqslant d \leqslant 254$,使得 $x^d \in H$,即所有变元均以某个次数的形式出现在 H 中,因此对于任一变元 x,存在一个多项式 $g \in A$,使得 $HT(g) = x^d$.根据定理 2 可知,$\dim(\langle A \rangle) = 0$,即由 Grobner 基 A 生成的理想〈A〉是零维的.

定理 4 指出本文构造的 Grobner 基 A 是零维的.由于项序转化算法 FGLM 能将零维理想下的任何项序的 Grobner 基转化为字典序 Grobner 基,所以 FGLM 算法可以将次数字典序 Grobner 基 A 转化为字典序 Grobner 基.零维 Grobner 基的构造为简化 Grobner 基计算,进而为降低求解多变元高次方程系统的复杂度提供了可能.

5.3 Rijndael-192 攻击方案及复杂度

Rijndael-192 的 Grobner 基攻击步骤如下:

①列出 Rijndael-192 算法的 MQ 方程组.

②从已知的明密文对中选出一组代入 MQ 方程组中.

③用 5.1 节中的方法构造理想〈A〉的关于次数字典序的 Grobner 基 G_{grelex}.

④判断 Grobner 基解的结构.由于方程组包含域等式,解的结构为有限解或无解.当且仅当 $G_{grelex} = (1)$时,原 MQ 方程组无解.当为无解时另选一组明密文对重新计算第③步.

⑤用 FGLM 算法将 G_{grelex} 转化为基于字典序的 Grobner 基 G_{lex}.

⑥求解密钥变量.

⑦将密钥变量和明密文对代入 Rijndael 算法中验证.

计算 Grobner 基时的最大次数不超过 N,因此计算 Grobner 基的复杂度的上限是 $O(2^N)$.由于本方案的复杂度上限取决于 Grobner 基的计算,因此本方案的复杂度上限为 $O(2^N)$.而由文献[17]可知,穷举 MQ 方程组解的复杂度为 $O(N2^N)$,由此可以看出本攻击方案的复杂度低于穷举攻击的复杂度,即本方案是一种成功的攻击方案.此外,考虑到结构化的超定稀疏的 MQ 方程组和针对 Rijndael 的次数字典序设计,实际复杂度将远远低于穷举搜索.

MQ 方程组中并不是所有方程都总是成立,对于一个 S 盒来说,其中有一个等式成立的概率为 255/256,对于整个 Rijndael 算法,这类等式都成立的概率为 $(255/256)^{4 \cdot Nb \cdot Nr + 4(1 + 1_{Nk>6}) \cdot Nr}$.对 128 位 Rijndael 概率大约是 1/2,对 256 位 Rijndael 概率大约是 1/9,从概率上说需要 2~9 个明密密文对,在第三步计算 2~9 次,MQ 方程组一定会有一组有限解.

当对系数域的计算时间是恒定的情况下,项序转换算法 FGLM 的复杂度为(nD^3)次域运算[3].综合考虑,该攻击方案的代价明显比穷举攻击要小很多.

6 结论

本文根据 Rijndael 密码轮变换的特点,将 Rijndael-192 的行移位和列混合变换归并为左乘矩阵 M 变换,使其在形式上具有线性变换的特征.对 Rijndael-192 的线性变换和多变元方程系统进行了深入研究,通过选择合理的项序,构造了 Rijndael-192 的 Grobner 基,指出该 Grobner 基是零维的,并给出了相关结论的理论证明.并在此基础上提出了 Rijndael-192 的 Grobner 基攻击方案,攻击复杂度大大低于穷举攻击.注意到本文攻击方案的复杂度还是太高,因而本文研究具有理论价值.但 Rijndael-192 零维 Grobner 基的发现,对进一步研究高效的 Grobner 基攻击方案具有指导意义.项序转化算法 FGLM 的复杂度和 Grobner 基攻击的有效性还有待于进

一步的研究.

参考文献

[1] Daemen J, Rijmen V. AES proposal: Rijndael[A]. the First Advanced Encryption Standard Candidate Coference[C]. USA, NIST, 1998. 1 – 45.

[2] 魏悦川,孙兵,李超. 对 Rijndael-256 算法新的积分攻击[J]. 电子学报,2011,39(2):476 – 480.
Wei Y C, Sun B, Li C. New integral attack on Rijndael-256 [J]. Acta Electronical Sinica, 2011, 39(2): 476 – 480. (in Chinese)

[3] Faugère J C, Gianni P, Lazard D, Mora T. Efficient computation of zero-dimensional gröbner bases by change of ordering [J]. Journal of Symbolic Computation, 1993, 16: 329 – 344.

[4] Courtois N T, Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations[OL]. LACR eprint server: www.iacr.org, April 2002.

[5] Yu SASAKI. Known-key attacks on rijndael with large blocks and strengthening shiftrow parameter[J]. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A (1): 21 – 28.

[6] Carlos Cid, Gaetan Leurent. An analysis of the XSL algorithm [J]. Lecture Notes in Computer Science, 2005, 3788: 333 – 345.

[7] Robshaw M J B, Murphy S. Comments on the security of the AES and the XSL technique[EB/OL]. http://www.cosic.esat.kuleuven.ac.be/nessie/reports/, May 2007.

[8] Johannes Buchmann, Andrei Pyshkin, Ralf-Philipp Weinmann. A zero-dimensional Grobner basis for AES-128[J]. Lecture Notes in Computer Science, 2006, 4047: 78 – 88.

[9] Satrajit Ghosh, Abhijit Das. An improvement of linearization-based algebraic attacks[J]. Lecture Notes in Computer Science, 2011, 7011: 157 – 167.

[10] Z'aba M. R, Wong K, Dawson E, et al. Algebraic analysis of small scale LEX-BES [A]. Malaysia, Proceedings of International Cryptology Conference 2010 [C]. Melaka: Universiti Teknikal Malaysia Melaka, 2010. 77 – 82.

[11] Ajwa I A, Liu Zhoujun, Wang Paul. Grobner bases algorithm [OL]. http://www.cm.mcs.kent.edu/reports/ 1995/gb.pdf, June 2, 2007.

[12] Zhou Yongbin, Wu Wenling, Xu Nannan, Feng Dengguo. Differential fault attack on camellia[J]. Chinese Journal of Electronics, 2009, 18(1): 13 – 19.

[13] Johannes Buchmann, Andrei Pyshkin, Ralf-Philipp Weinmann. Block ciphers sensitive to Grobner basis attacks[J]. Lecture Notes in Computer Science, 2006, 3860: 313 – 331.

[14] Thomas Becker, Volker Weispfenning. Grobner Bases-A Computational Approach to Commutative Algebra[M]. New York/Berlin: Springer-Verlag, 1991.

[15] Faugère, Jean-Charles. A new efficient algorithm for computing Grobner bases without reduction to 0 F5[A]. the 2002 international symposium on Symbolic and algebraic computation [C]. Lille: ACM, 2002. 44 – 60.

[16] 刘景伟,韦宝典. AES S 盒的密码特性分析[J]. 西安电子科技大学学报,2004,31(2):255 – 259.
Liu J W, Wei B D. Analysis of the cryptographic properties of the AES S-box[J]. Journal of Xidian University, 2004, 31(2): 255 – 259. (in Chinese)

[17] Jean-Charles Faugère, Antoine Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases[A]. Advances in Cryptology-CRYPTO 2003 [C]. California: Springer-Verlag, 2003. LNCS 2729. 44 – 60.

作者简介

崔　杰　男,1980 年生于河南淮阳,现为中国科学技术大学计算机科学与技术学院博士生,安徽大学计算机科学与技术学院讲师. 研究方向为信息安全.
E-mail: cuijie@mail.ustc.edu.cn

黄刘生　男,1957 年生,中国科学技术大学计算机科学与技术学院教授,博士生导师. 研究方向包括信息安全、分布式计算以及无线传感器网络.
E-mail: lshuang@ ustc.edu.cn

仲　红　女,1965 年生,安徽大学计算机科学与技术学院教授,博士生导师. 研究方向包括信息安全和无线传感器网络.
E-mail: zhongh@ mail.ustc.edu.cn

杨　威　男,1978 年生于安徽六安,中国科学技术大学计算机科学与技术学院博士后. 研究方向为信息安全和量子信息技术.
E-mail: qubit@ ustc.edu.cn