Rijndael 算法的代数方程系统改进

肖皇培[①]　张国基[②]
[①](华南理工大学计算机科学与工程学院　广州　510640)
[②](华南理工大学数学科学学院　广州　510640)

摘　要：该文根据 Rijndael 算法中 S 盒的代数表达式，通过合理假设 S 盒变量，利用各变量之间的关系建立方程，把 Rijndael 加密算法描述成 GF(2^8)上的一个多变量二次方程系统。该二次方程系统是稀疏的且是超定(Overdefined)的，可以认为恢复 Rijndael 的密钥等同于求解这个方程系统。与其他描述 Rijndael 密码的方程系统相比，该文中描述 S 盒方程的项数与变量更少，因此用 XSL(eXtended Sparse Linearization)技术求解该系统的计算复杂度更低。

关键词：密码学；分组密码；代数攻击；Rijndael 算法；XSL 技术
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2008)10-2459-05

The Improvement on Algebraic System of Multivariate Quadratic Equations for Rijndael

Xiao Huang-pei[①]　Zhang Guo-ji[②]
[①](*School of Computer Science and Engineering*, *South China University of Technology*, *Guangzhou* 510640, *China*)
[②](*School of Mathematical Sciences*, *South China University of Technology*, *Guangzhou* 510640, *China*)

Abstract: According to the algebraic expression of the S-box in Rijndael algorithm, an algebraic system of multivariate quadratic equations over GF(2) are proposed to describe Rijndael. The variables of S boxes are supposed rationally and the relations between these variables are used to establish equations in this paper. The derived system of multivariate quadratic equations is sparse and overdefined. The key recovery of Rijndael can be regarded as a problem of solving this system. By comparing with other parallel systems, this system has fewer terms and variables. So it has a lower complexity while applying the XSL (eXtended Sparse Linearization) technique.

Key words: Cryptography; Block cipher; Algebraic attack; Rijndael algorithm; XSL technique

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和技术研究所(NIST)确定为美国高级加密标准 AES(Advanced Encryption Standard)[1, 2]。从那时起，密码分析者们对该密码算法的研究兴趣日益俱增，AES 的密码分析已成为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和线性分析，而 Rijndael 算法的最主要设计指标就是抗差分和线性分析能力。因此，基于差分和线性分析的一些攻击对 Rijndael 算法难以取得实质性的进展[3]。

最近，代数攻击已经成为对 Rijndael 最有希望的分析方法，很多人将希望寄托于代数攻击，因此代数攻击深受当前密码学界的广泛关注。最简洁的代数攻击由两步组成：第 1 步是建立一个简单的代数方程系统，该方程系统描述密码系统的明文、密文和密钥是怎样关联的；第 2 步通过一些已知的明密文来求解方程系统以获取密钥。第 1 步已经获得了研究者的一些关注[4−8]，他们以不同的方式描述 Rijndael 算法：Ferguson[4]等人把 Rijndael 算法描述为有限域 GF(2^8)上一个简单的，非常结构化的非线性方程，该方程对 10 轮的 Rijndael 算法共有 2^{50} 项；Courtois 和 Pieprzyk[5, 6]通过建立一个 GF(2)上含有 8000 个二次方程和 1600 个变量的方程系统来描述 Rijndael；Murphy 和 Robshaw[7]得出一个 GF(2^8)上非常稀疏的超定多变量二次方程系统，且有充分的理由认为该系统比 GF(2)上相应的系统更容易求解；文献[8]给出了一个 GF(2^8)上描述 Rijndael 更简单的方程系统，求解该方程系统比求解 Murphy-Robshaw 方程系统复杂度更低。第 2 步中的求解多变量二次方程系统仍然是一个研究中的问题，这个问题被认为是相当难的(NP-complete)[9]。

目前，一般求解多变元高次方程系统的方法有 Linearization、Relinearization、XL 和 Grobner Bases 等。2002 年，Courtois 等人[5]在这些方法的基础之上引入一种新的多变元高次方程系统求解方法——XSL 技术，XSL 技术的特点是可利用方程系统的特殊结构及稀疏性来降低求解的

2006-04-09 收到，2006-09-17 改回

复杂性。本文在文献[8]的基础上把 Rijndael 算法描述成 GF(2^8)上的一个多变量二次方程系统，通过利用 XSL 技术对该方程系统进行分析，证明该系统比其它现有的方程系统更简单，应用 XSL 技术求解其计算复杂度更低，仅为 $2^{104.31}$ 次 GF(2^8)上的运算量。

2 Rijndael 算法的简要描述

2.1 Rijndael 加密算法

Rijndael 加密算法是一个具有 SPN 结构的迭代分组密码，其分组长度和密钥长度可以分别独立地指定为 128 比特、192 比特和 256 比特，各种密钥长度对应的加密轮数分别为 10 轮、12 轮和 14 轮。本文假定读者熟悉全部的 Rijndael 算法，详细的算法描述可参考相关文献[1, 2]，在此仅以分组长度和密钥长度都是 128 比特的 Rijndael 算法为例对其轮函数进行简要描述。

128 比特的分组长度可以表示为 4×4 的字节状态矩阵 $\boldsymbol{A}=(a_{ij})$, $0\le i,j\le 3$，其加密算法共有 10 轮，除了最后一轮之外，每一轮皆由 4 种变换所组成，依次为：字节替换(SubBytes)、行移位(ShiftRows)、列混合(MixColumns)和轮密钥加(AddRoundKey)。第 1 轮之前先进行轮密钥加变换，最后一轮(FinalRound)无列混合变换，其它中间各轮变换皆相同。

ShiftRows 变换和 MixColumns 变换可通过对状态矩阵左乘一个 GF(2^8)上的矩阵来实现，记实现 ShiftRows 和 MixColumns 变换的矩阵分别为 $\boldsymbol{R}$ 和 $\mathbf{Mix}$。因此，一个完整的 AES 轮函数可以表示为 $\mathrm{Round}(\boldsymbol{A},\boldsymbol{K}_i)=\mathbf{Mix}(\boldsymbol{R}(S(\boldsymbol{A})))+\boldsymbol{K}_i$，可简记为 $\mathrm{Round}(\boldsymbol{A},\boldsymbol{K}_i)=\boldsymbol{M}\cdot S(\boldsymbol{A})+\boldsymbol{K}_i$，其中 $S(\boldsymbol{A})$ 表示对状态矩阵 $\boldsymbol{A}$ 的每个字节作 SubBytes 变换，$\boldsymbol{M}=\mathbf{Mix}\cdot\boldsymbol{R}$，$\boldsymbol{K}_i$ 为第 i 轮子密钥矩阵。最后一轮的轮函数为 $\mathrm{FinalRound}(\boldsymbol{A},\boldsymbol{K}_{10})=\boldsymbol{M}^*\cdot S(\boldsymbol{A})+\boldsymbol{K}_{10}$，其中 $\boldsymbol{M}^*=\boldsymbol{R}$。

2.2 Rijndael 算法的密钥编排方案

共有 11 轮子密钥，其中第 1 轮子密钥为原始密钥，后 10 轮子密钥由原始密钥经过密钥扩展算法而得。设第 i 轮子密钥为 $\boldsymbol{K}_i=(k^{(i)}_{(j,l)})_{4\times 4}=[\boldsymbol{K}_{i,0},\boldsymbol{K}_{i,1},\boldsymbol{K}_{i,2},\boldsymbol{K}_{i,3}]$，其中列向量 $\boldsymbol{K}_{i,l}=[k^{(i)}_{0,l},k^{(i)}_{1,l},k^{(i)}_{2,l},k^{(i)}_{3,l}]^{\mathrm{T}}$，$k^{(i)}_{j,l}$ 表示第 i 轮子密钥的第 (j,l) 个字节，$0\le i\le 10$，$0\le j,\ l\le 3$。

当 $l=0$ 时，有 $\boldsymbol{K}_{i+1,0}=\boldsymbol{K}_{i,0}+\mathrm{SubBytes}(\mathrm{RotByte}(\boldsymbol{K}_{i,3}))+\mathrm{Rcon}(i)$；当 $l=1,2,3$ 时，有 $\boldsymbol{K}_{i+1,l}=\boldsymbol{K}_{i,l}+\boldsymbol{K}_{i+1,l-1}$，其中 $\mathrm{RotByte}(a,b,c,d)=(b,c,d,a)$，$\mathrm{Rcon}(i)=[(1<<i)\bmod(0x11),0,0,0]$。

3 描述 Rijndael 算法的二次方程系统

3.1 S 盒的二次方程

根据有限域上的 GF(2^8)的性质 $x^{255}=1$ 及拉格朗日插值公式，S 盒的代数表达式可写为

$$\begin{aligned}S(x)&=05x^{254}+09x^{253}+F9x^{251}+25x^{247}+F4x^{239}\\&\quad+01x^{223}+B5x^{191}+8Fx^{127}+63=05x^{-1}\\&\quad+09(x^{-1})^2+F9(x^{-1})^{2^2}+\cdots+8F(x^{-1})^{2^7}+63\\&=05y_0+09y_1+\cdots+8Fy_7+63\end{aligned}\tag{1}$$

其中 $y_0=x^{-1}$，$y_1=(x^{-1})^2$，$y_2=(x^{-1})^{2^2}$，…，$y_7=(x^{-1})^{2^7}$，可以简记为 $S(x)=g(y_0,y_1,\cdots,y_7)$。

记第 i 轮的第 (j,k) 个S盒的输入字节变量为 $x^{(i)}_{0,(j,k)}$，中间变量为 $y^{(i)}_{0,(j,k)},y^{(i)}_{1,(j,k)},\cdots,y^{(i)}_{7,(j,k)}$，输出变量为 $z^{(i)}_{(j,k)}$。由 S 盒的代数表达式，第 i 轮的第 (j,k) 个 S 盒的变换可用下列 GF(2^8)上的二次方程来描述(其中$0\le i\le 9;0\le j,k\le 3$)：

$$\begin{cases}x^{(i)}_{0,(j,k)}y^{(i)}_{0,(j,k)}=1\\(y^{(i)}_{m,(j,k)})^2=y^{(i)}_{m+1,(j,k)},\ (0\le m\le 7,\text{其中}m+1\text{为模8加})\\z^{(i)}_{(j,k)}=g(y^{(i)}_{0,(j,k)},y^{(i)}_{1,(j,k)},\cdots,y^{(i)}_{7,(j,k)})\end{cases}\tag{2}$$

最后一个线性方程可看作是 S 盒之后的又一个线性变换。上述方程假设了加密过程和密钥编排过程中的 S 盒输入均不出现零元，这种假设对于加密过程有 53.4%的概率正确，对于密钥编排过程有 85.5% 的概率正确，即使假设无效，上述方程也只有第 1 个不正确。从式(2)可知，对每个 S 盒，只有 9 个二次方程，方程量太少似乎不够超定(XSL 技术要求描述 S 盒的二次方程组是超定的[5, 6])，可以在不增加变量的情况下增加如下二次方程：

$$x^{(i)}_{0,(j,k)}y^{(i)}_{1,(j,k)}=y^{(i)}_{0,(j,k)}\tag{3}$$

通过设 $(x^{(i)}_{0,(j,k)})^2=x^{(i)}_{1,(j,k)}$ 和 $(x^{(i)}_{1,(j,k)})^2=x^{(i)}_{2,(j,k)}$ 增加两个变量 $x^{(i)}_{1,(j,k)}$ 和 $x^{(i)}_{2,(j,k)}$，可以得到如下 6 个二次方程：

$$\begin{cases}(x^{(i)}_{0,(j,k)})^2=x^{(i)}_{1,(j,k)}\\(x^{(i)}_{1,(j,k)})^2=x^{(i)}_{2,(j,k)}\\x^{(i)}_{1,(j,k)}y^{(i)}_{1,(j,k)}=1\\x^{(i)}_{2,(j,k)}y^{(i)}_{2,(j,k)}=1\\y^{(i)}_{1,(j,k)}x^{(i)}_{2,(j,k)}=x^{(i)}_{1,(j,k)}\\y^{(i)}_{0,(j,k)}x^{(i)}_{1,(j,k)}=x^{(i)}_{0,(j,k)}\end{cases}\tag{4}$$

至此，已得到描述 S 盒的二次方程共 16 个。

3.2 线性层方程

第 1 轮加密变换之前的轮密钥加变换可表示为线性方程：$x^{(0)}_{0,(j,k)}=p_{(j,k)}+[k^{(0)}_{0,(j,k)}]$，其中 $0\le j,\ k\le 3$，$p_{(j,k)}$ 表示明文的第 (j,k) 个字节，$[k^{(i)}_{0,(j,k)}]$ 表示第 i 轮子密钥的第 (j,k) 个字节被密钥字节基的线性表出。由密钥编排方案可知，11 轮子密钥的所有字节可以由其中的 56 个字节线性表出(第 1 轮子密钥的全部 16 个和其它每轮第 1 列的 4 个密钥字节，且是线性无关的)。

第 i $(i=1,2,\cdots,9)$ 轮的线性层的输入为第 $i-1$ 轮非线性 S 盒的输出，用矩阵 $\boldsymbol{Z}^{(i-1)}$ 表示第 $i-1$ 轮 S 盒的输出状态矩阵，经第 i 轮线性层变换后的第 (j,k) 字节可表示为线性方程：$x^{(i)}_{0,(j,k)}=(\boldsymbol{M}\cdot\boldsymbol{Z}^{(i-1)})_{(j,k)}+[k^{(i)}_{0,(j,k)}]$，其中 $\boldsymbol{M}=\mathbf{Mix}\cdot\boldsymbol{R}$ 分

别为 ShiftRows 和 MixColumns 的变换矩阵之积。最后一轮的输出可表示为 $c_{(j,k)}=(\boldsymbol{M}^*\cdot\boldsymbol{Z}^{(9)})_{(j,k)}+[k_{0,(j,k)}^{(10)}]$，其中 $\boldsymbol{M}^*=\boldsymbol{R}$。

分别用 $\alpha_{(j,l)}$和$\beta_{(j,l)}$ 表示矩阵 $\boldsymbol{M}$和$\boldsymbol{M}^*$的第 (j,l) 个字节，所有线性层变换可用下列方程表示 $(1\le i\le 9;0\le j,k\le 3)$：

$$\begin{cases}x_{0,(j,k)}^{(0)}=p_{(j,k)}+[k_{0,(j,k)}^{(0)}]\\ x_{0,(j,k)}^{(i)}=\sum_{l=0}^{3}\alpha_{(j,l)}z_{(l,k)}^{(i-1)}+[k_{0,(j,k)}^{(i)}],\ (i=1,2,\cdots,9)\\ c_{(j,k)}=\sum_{l=0}^{3}\beta_{(j,l)}z_{(l,k)}^{(9)}+[k_{0,(j,k)}^{(10)}]\end{cases}\tag{5}$$

通过对式(5)中的方程进行 2 和 4 次方，还可以得到如下的方程(其中$0\le n\le 2$)：

$$\begin{cases}x_{n,(j,k)}^{(0)}=(p_{(j,k)})^{2^n}+[k_{n,(j,k)}^{(0)}]\\ x_{n,(j,k)}^{(i)}=\left(\sum_{l=0}^{3}\alpha_{(j,l)}z_{(l,k)}^{(i-1)}\right)^{2^n}+[k_{n,(j,k)}^{(i)}],\ (i=1,2,\cdots,9)\\ (c_{(j,k)})^{2^n}=\left(\sum_{l=0}^{3}\beta_{(j,l)}z_{(l,k)}^{(9)}\right)^{2^n}+[k_{n,(j,k)}^{(10)}]\end{cases}\tag{6}$$

其中 $p_{(j,k)}$ 和 $c_{(j,k)}$ 是用于攻击的已知明文和密文，假设变量 $k_{1,(j,k)}^{(i)}=(k_{0,(j,k)}^{(i)})^2$ 和 $k_{2,(j,k)}^{(i)}=(k_{1,(j,k)}^{(i)})^2$，且记 $[k_{1,(j,k)}^{(i)}]=[k_{0,(j,k)}^{(i)}]^2$ 和 $[k_{2,(j,k)}^{(i)}]=[k_{1,(j,k)}^{(i)}]^2$，由特征为 2 的有限域上 2^m 次方运算性质 $(a+b)^{2^m}=a^{2^m}+b^{2^m}$ 可知，上述方程均是 GF(2^8)上关于变量 $x_{0,(j,k)}^{(i)}$，$x_{1,(j,k)}^{(i)}$，$x_{2,(j,k)}^{(i)}$，$y_{0,(j,k)}^{(i)},\cdots,y_{7,(j,k)}^{(i)}$，$k_{0,(j,k)}^{(i)}$，$k_{1,(j,k)}^{(i)}$，$k_{2,(j,k)}^{(i)}$ 和 $z_{(j,k)}^{(i)}$ 的性线方程。

3.3 Rijndael 算法的二次方程系统

由式(2)-式(6)，Rijndael 的加密算法可以描述为 GF(2^8)上的二次方程系统如下(其中$0\le j\le 3;0\le k\le 3;0\le n\le 2;0\le m\le 7$)：

$$\begin{cases}0=x_{n,(j,k)}^{(i)}y_{n,(j,k)}^{(i)}+1 & (0\le i\le 9)\\ 0=(y_{m,(j,k)}^{(i)})^2+y_{m+1,(j,k)}^{(i)} & (0\le i\le 9)\\ 0=(x_{0,(j,k)}^{(i)})^2+x_{1,(j,k)}^{(i)} & (0\le i\le 9)\\ 0=(x_{1,(j,k)}^{(i)})^2+x_{2,(j,k)}^{(i)} & (0\le i\le 9)\\ 0=x_{0,(j,k)}^{(i)}y_{1,(j,k)}^{(i)}+y_{0,(j,k)}^{(i)} & (0\le i\le 9)\\ 0=y_{0,(j,k)}^{(i)}x_{1,(j,k)}^{(i)}+x_{0,(j,k)}^{(i)} & (0\le i\le 9)\\ 0=y_{1,(j,k)}^{(i)}x_{2,(j,k)}^{(i)}+x_{1,(j,k)}^{(i)} & (0\le i\le 9)\\ 0=z_{(j,k)}^{(i)}+g\left(y_{0,(j,k)}^{(i)},y_{1,(j,k)}^{(i)},\cdots,y_{7,(j,k)}^{(i)}\right) & (0\le i\le 9)\\ x_{n,(j,k)}^{(0)}=(p_{(j,k)})^{2^n}+[k_{n,(j,k)}^{(0)}] & \\ x_{n,(j,k)}^{(i)}=\left(\sum_{l=0}^{3}\alpha_{(j,l)}z_{(l,k)}^{(i-1)}\right)^{2^n}+[k_{n,(j,k)}^{(i)}] & (1\le i\le 9)\\ (c_{(j,k)})^{2^n}=\left(\sum_{l=0}^{3}\beta_{(j,l)}z_{(l,k)}^{(9)}\right)^{2^n}+[k_{n,(j,k)}^{(10)}] & \end{cases}\tag{7}$$

其中前 7 行为描述 S 盒的二次方程，共 2560 个；后 4 行为线性方程，共 688 个。整个加密过程由 3248 个方程、1760 个状态变量和 168 个密钥变量组成。每个 S 盒可由 16 个二次方程来描述，其中仅仅含有 11 个变量：$x_{0,(j,k)}^{(i)}$，$x_{1,(j,k)}^{(i)}$，$x_{2,(j,k)}^{(i)}$，$y_{0,(j,k)}^{(i)},\cdots,y_{7,(j,k)}^{(i)}$。这 16 个二次方程中共含有 28 项，分别是：1, $x_{0,(j,k)}^{(i)}$，$x_{1,(j,k)}^{(i)}$，$x_{2,(j,k)}^{(i)}$，$y_{0,(j,k)}^{(i)},\cdots,y_{7,(j,k)}^{(i)}$，$(y_{0,(j,k)}^{(i)})^2$，$\cdots,(y_{7,(j,k)}^{(i)})^2$，$(x_{0,(j,k)}^{(i)})^2$，$(x_{1,(j,k)}^{(i)})^2$，$x_{0,(j,k)}^{(i)}y_{0,(j,k)}^{(i)}$，$x_{1,(j,k)}^{(i)}y_{1,(j,k)}^{(i)}$，$x_{2,(j,k)}^{(i)}y_{2,(j,k)}^{(i)}$，$x_{0,(j,k)}^{(i)}y_{1,(j,k)}^{(i)}$，$y_{0,(j,k)}^{(i)}x_{1,(j,k)}^{(i)}$ 和 $y_{1,(j,k)}^{(i)}x_{2,(j,k)}^{(i)}$。

与加密过程相似，密钥编排方案也可描述成一个与之相类似的多变量二次方程系统。密钥编排方案中共有 D=40 个 S 盒，涉及变量个数为 $11\times D$。另外根据密钥编排，还需要增加 8×3 个密钥字节变量以构成一个“人工 S 盒”[5]才能线性表出所有的密钥字节，因此密钥编排方案共有 $S_k=11\times D+24=464$ 个变量。所有密钥字节变量中含有线性关系，其中基中的变量个数为 $L_k=3\times 56=168$，即 S_k 中有 S_k-L_k 个字节变量由 L_k 线性表出。描述密钥编排的方程一部分由类似于加密过程中的二次方程表出，另一部分由 S_k 中线性相关字节构成的线性方程表出。将加密过程和密钥编排方案的方程组加在一起可构成一个 GF(2^8)上完整描述 Rijndael 的多变量二次方程系统，该方程系统稀疏且是超定的，恢复密钥的过程可归结为求解这个方程系统。

4 与现有方程系统的比较

文献[5,6]首先把 Rijndael 算法描述为 GF(2)上的二次方程系统并应用于XSL技术；在文献[7]中，Murphy和Robshaw通过从 AES 引入 BES 分组密码，使 BES 只包含 GF(2^8)上的运算(AES 既有 GF(2)上的运算，又有 GF(2^8)上的运算)，并由此得出一个 GF(2^8)上的多变量二次方程系统，有理由相信应用 XSL 技术于该方程系统比 GF(2)上的方程系统更容易求解[10]；文献[8]不必引入 BES 密码，从 S 盒的代数表达式入手也得到一个 GF(2^8)上描述 Rijndael 的方程系统；本文的方程系统与文献[8]相似，直接从S盒的代数表达式得出，但方程的变量与项数更少。对于上述不同方程系统，其参数值可归纳如表 1 所示。

从表 1 可以看出，对于每个 S 盒，文献[6]方程系统中有 GF(2)上 23 个二次方程、39 项；文献[7]有 GF(2^8)上 24 个二次方程、41 项；文献[8]有 GF(2^8)上 17 个二次方程、34 项；本文仅有 GF(2^8)上 16 个二次方程、28 项，且本文描述每个 S 盒的变量比文献[8]更少，仅为 11 个变量(3 个输入变量和 8 个输出变量，文献[8]为 16 个)。根据 XSL 技术中 S 盒方程对计算复杂性贡献 Γ 的定义[5]：$\Gamma=\left((t-r)/s\right)^{\lfloor(t-r)/s\rfloor}$，经计算文献[6]中的 Γ 的值为 $2^{22.9}$，而文献[7]和文献[8]的 Γ 值均约为 9.6，本文的 Γ 值为 2.25，这说明应用 XSL 技术在 GF(2^8)上求解二次方程系统远比在 GF(2)上求解更有效，且本文的方程系统求解比其它相应系统的计算复杂性更低。

5 应用 XSL 技术求解结果

文献[5]给出了 XSL 技术的“第 2 个攻击”(考虑了密钥编排方案)：首先从原来的方程中产生较高次数的方程；再把这些方程看作一些项的线性组合；最后求解这些线性方程(可能的话)。高次方程通过将一个 S 盒(称为“活动”S 盒)的方

表 1 各个方程系统的参数对比

参数	符号	文献[6]	文献[7]	文献[8]	本文
域	GF(2^n)	GF(2)	GF(2^8)	GF(2^8)	GF(2^8)
分组长度	$32N_b$	128	128	128	128
每层 S 盒数	B	16	16	16	16
密钥长度	H_k	128	128	128	128
轮数	N_r	10	10	10	10
每个 S 盒方程数	r	23	24	17	16
每个 S 盒项数	t	39	41	34	28
S 盒大小	s	8	8	8	3
加密 S 盒	BN_r	160	160	160	160
密钥编排 S 盒	D+1	41	41	41	41
总共 S 盒	S	201	201	201	201
无关的密钥变量	L_k	448	448	448	168
密钥变量	S_k	704	704	704	464

程，乘以其它 P–1 个 S 盒(称为“被动”S 盒)的项来产生，所得方程的最高次数为 $2P$。这些方程与原来的方程一起形成新的方程组，将每个高次项看作一个新变量，高次方程组就成为线性方程组，再用高斯消元法求解。XSL 技术产生 3 类线性独立的高次方程，文献[5]给出了这 3 类线性独立方程个数的估计是：

$$R \approx \binom{S}{P}(t^P-(t-r)^P),\ R' \approx \binom{S}{P-1} sB(N_r+1)(t-r)^{P-1},$$
$$R'' \approx \binom{S}{P-1}(S_k-L_k)(t-r)^{P-1} \tag{8}$$

注意到本文中 S 盒的变量假设，上述第 2 个公式中的 s 应为 3。为了使方程系统可解，Courtois 等人[5]提出“T' 方法”，认为寻找足够大的 P 使 $R+R'+R''>T-T'$ 时，可能生成足够多的新方程，从而可用高斯消元法求解系统，其中 T 表示项的总数，T' 表示 T 项中的某些特殊项的个数，这些项乘以某个变量后仍在 T 项的集合中。攻击的复杂度是 $O(T^\omega)$，其中 ω 是高斯消元指数，一般 $\omega=3$。记 t' 为 S 盒方程中的特殊项的个数，这些项乘以某个变量后仍在 t 项的集合中，T 和 T' 的估计[5]如下：

$$T \approx \binom{S}{P}t^P,\quad T'=t't^{P-1}\binom{S-1}{P-1} \tag{9}$$

对本文中提及的方程系统应用 XSL 算法其结果估计如表 2 所示。对文献[7]中的方程系统，当 P=2 时，线性无关方程的个数小于项的总数；当 P=3 时，线性无关方程数多于项数，这暗示应用 XSL 技术将产生一个 GF(2^8)上大小约为 $2^{36.42}$ 的线性可解系统。对于文献[8]的方程系统，当 P=3 时，可得一个 GF(2^8)上大小约为 $2^{35.61}$ 的线性可解系统。对于本文的方程系统，当 P=3 时，可得一个 GF(2^8)上大小约为 $2^{34.77}$ 的线性可解系统。

表 2 应用 XSL 技术对各方程系统的求解结果

方程系统	文献[7]		文献[8]		本文	
P	2	3	2	3	2	3
R	$2^{24.74}$	$2^{36.31}$	$2^{24.05}$	$2^{35.42}$	$2^{23.62}$	$2^{34.65}$
R'	$2^{22.20}$	$2^{32.93}$	$2^{22.20}$	$2^{32.93}$	$2^{20.28}$	$2^{30.51}$
R''	$2^{19.74}$	$2^{30.47}$	$2^{19.74}$	$2^{30.47}$	$2^{19.45}$	$2^{29.67}$
$R+R'+R''$	$2^{25.00}$	$\mathbf{2^{36.47}}$	$2^{24.46}$	$\mathbf{2^{35.69}}$	$2^{23.82}$	$\mathbf{2^{34.772}}$
T	$2^{25.01}$	$\mathbf{2^{36.42}}$	$2^{24.47}$	$\mathbf{2^{35.61}}$	$2^{23.91}$	$\mathbf{2^{34.768}}$

对于一个 $n\times n$ 矩阵，用高斯消元法求解对应线性方程组的计算复杂度约为 $O(n^3)$ 次运算。Courtois[6]应用 XSL 技术求解 GF(2)上的二次方程系统需要 2^{230} 次 GF(2)上的运算，大于穷尽密钥的计算量。从表 2 可以看出，应用 XSL 技术求解上述 GF(2^8)上对应的方程系统，其复杂度约为 $O(T^3)$，分别为 $2^{109.26}$、$2^{106.83}$ 和 $2^{104.31}$ 次 GF(2^8)上的运算。这说明应用 XSL 技术，文献[8]比文献[7]的方程系统求解计算复杂度降低了大约 $2^{2.43}$ 倍，本文提出的方程系统比文献[7]的方程系统求解计算复杂度降低了大约 $2^{4.95}$ 倍，比文献[8]降低了大约 $2^{2.52}$ 倍。

6 结论

本文根据 Rijndael 算法中 S 盒的代数表达式，通过合理地假设变量，利用各变量之间的关系建立方程，把 Rijndael 加密算法描述成 GF(2^8)上的一个多变量二次方程系统。该系统与同类系统相比，描述 S 盒方程的项数与变量更少，因此利用 XSL 技术对该方程系统进行分析比其它系统更简单，应用 XSL 技术求解其计算复杂度更低。另外需要说明的是，在求解过程中线性无关的方程个数不可能超过项的个数，但在表 2 中，当 P=3 时，却有 $R+R'+R''>T$，这说明 XSL 技术对 R、R' 和 R'' 的估计比较粗糙，XSL 技术的有效性还需要进一步的研究。

参 考 文 献

[1] National Institute of Standards and Technology (NIST). Advanced Encryption Standard — Federal Information Processing Standards Publication 197(FIPS PUB 197)[S]. Washington D.C.: US Department of Commerce, Nov 2001.

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

[3] 肖国镇, 白恩健, 刘晓娟. AES 密码分析的若干新进展[J]. 电子学报. 2003, 31(10): 1549–1554.
Xiao Guo-zhen, Bai En-jian, and Liu Xiao-juan. Some new developments on the cryptanalysis of AES[J]. *Acta*

Electronica Sinica, 2003, 31(10): 1549–1554.

[4] Ferguson N, Schroeppel R, and Whiting D. A Simple Algebraic Representation of Rijndael[A]. Vaudenay S and Youssef A M(Eds.): Selected Areas in Cryptography-SAC 2001[C]. LNCS, Heidelberg: Springer-Verlag, 2001, Vol.2259: 103–111.

[5] Courtois N T and Pieprzyk J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations [EB/OL]. IACR eprint server: www.iacr.org, April 2002.

[6] Courtois N T and Pieprzyk J. Cryptanalysis of Block Ciphers With Overdefined Systems of Equations[A]. Zheng Y(Ed.): Advances in Cryptology-ASIACRYPT 2002[C]. LNCS, Heidelberg: Springer-Verlag, 2002, Vol.2501: 267–287.

[7] Murphy S and Robshaw M. Essential Algebraic Structure Within the AES[A]. Yung M(Ed.): Advances in Cryptology-CRYPTO 2002[C]. LNCS, Heidelberg: Springer-Verlag, 2002, Vol.2442: 1–16.

[8] 李娜, 陈卫红. 描述 Rijndael 的一个新的方程组. 电子与信息学报[J]. 2004, 26(12): 1990–1995.
Li Na and Chen Wei-hong. A new system of multivariate quadratic equations for rijndael [J]. *Journal of Electronics & Information Technology*, 2004, 26(12): 1990–1995.

[9] Courtois N, Klimov A, Patarin J, and Shair A. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomail Equations[A]. Preneel B(Ed.): EUROCRYPT 2000[C]. LNCS, Heidelberg: Springer-Verlag, 2000, Vol.1807: 392–407.

[10] Murphy S and Robshaw M. Comments on the Security of the AES and the XSL Technique [EB/OL]. http://www.cosic.esat. kuleuven.be/stork/public/documents, Dec 2006.

肖皇培： 男，1979 年生，博士生，从事密码学与信息安全研究.

张国基： 男，1953 年生，教授，博士生导师，主要从事人工智能、密码学及信息安全研究.