描述 Rijndael 的一个新的方程组 [1]

李 娜 陈卫红

(信息工程大学信息工程学院应用数学系 郑州 450002)

摘 要: 由于 Rijndael 的 S 盒的代数表达式是逆函数合成 GF(2^8) 上一个 q- 多项式，该文合理假设 S 盒的变量并通过讨论各变量之间的关系，把 Rijndael 用 GF(2^8) 上一个多变量二次方程组来表示，使得 Rijndael 的密钥恢复等同于求解这个方程组. 该方程组较 Murphy-Robshaw 方程组更简单，用 XSL 技术求解复杂度更低.

关键词: XSL 攻击，多变量二次方程组， Rijndael

中图分类号: TN918.1 **文献标识码**: A **文章编号**: 1009-5896(2004)12-1990-06

A New System of Multivariate Quadratic Equations for Rijndael

Li Na Chen Wei-hong

(*Dept of Appl. Math., Info. Eng. Inst., Info. Eng. Univ., Zhengzhou* 450002, *China*)

Abstract Because the algebraic expression of Rijndael S box is a composition of the converse function with a q-polynomial over GF(2^8), in this paper the variables of S box are supposed rationally and the relations between these variables are analyzed, then a new system of multivariate quadratic equations over GF(2^8) are used to describe completely Rijndael, the cryptanalysis of Rijndael can be written as a problem of solving the system of multivariate quadratic equations. This system is simpler than Murphy and Robshaw's, and has a lower complexity while applying XSL technique.

Key words XSL attack, System of multivariate quadratic equations, Rijndael

1 引言

自分组密码 Rijndael[1] 被 NIST 选做新的加密标准 (AES) 以来，研究是否存在一种对 Rijndael 的有效攻击方法成为分组密码研究领域的新挑战。 Rijndael 能够抵抗差分攻击和线性攻击，在提交 Rijndael 的同时它的设计者给出了一种分析方法—— Square 攻击。 Square 攻击对于 128-bit 分组长度和密钥长度的 Rijndael 最多只能对六轮攻击有效。 2002 年 4 月 Courtois 等人用 GF(2) 上一个大的多变量稀疏二次方程组描述 Rijndael, 将密钥恢复等同于这个二次方程组的求解，利用该方程组的特殊结构和稀疏性引入了一种新的求解方法—— XSL(eXtended Sparse Linearization 或 multipl(X) by Selected monomials and Linearization) 技术 [2] 。用该技术来求解 128-bit 的 Rijndael 二次方程组需要大约 2^{230} 步，远远大于穷举量。文献 [3] 中 Murphy 和 Robshaw 通过引入 BES(Big Encryption System) 分组密码，将 Rijndael 用 GF(2^8) 上一个大的多变量二次方程组来描述，该方程组比 GF(2) 上的方程组更稀疏，用 XSL 技术求解只需要相当于 $2^{109.2}$ 次 GF(2^8) 上运算的计算量。本文由 S 盒的代数表达式的特殊形式，合理假设变量，分析变量之间的关系，从而给出了 GF(2^8) 上一个新的多变量二次方程组来描述

[1] 2003-07-25 收到， 2004-01-12 改回

Rijndael, 密钥恢复等同于这个二次方程组的求解。这个方程组和 Murphy-Robshaw 方程组非常相似，比 Murphy-Robshaw 方程组更简单，且应用 XSL 技术求解所需的工作量更少，只需要相当于 $2^{106.8}$ 次 GF(2^8) 上运算的计算量。

2 Rijndael 密码简述

2.1 加密算法

本文以明文分组和密钥长度都是 128bits 的 Rijndael 为例进行说明。共有 10 轮变换，第 1 轮前先轮密钥加，最后 1 轮中无列混合，其它中间轮变换相同，每一轮由 4 个变换组成:

(1) 字节替换 (ByteSub, BS), 采用的是一个双射 S 盒变换。

(2) 行移位变换 (ShiftRow, SR), 第 1, 2, 3, 4 行分别循环左移 0, 1, 2, 3 byte 。

(3) 列混合变换 (MixColumn, MC), 将每列左乘一 4×4 混合矩阵 $\boldsymbol{M}$ 得到新的一列。

(4) 轮密钥加变换 (KeyAddition, KA), 将中间状态和轮密钥的对应字节做模二加运算。其中只有 BS 变换是非线性变换，构成非线性层， SR, MC, KA 变换构成线性层。

2.2 密钥扩展方案

共有 11 个轮密钥，第 1 个轮密钥为原始密钥，其它由原始密钥经过密钥扩展得到。设第 i $(i=0,\cdots,10)$ 轮轮密钥为 $[W_{i,0},W_{i,1},W_{i,2},W_{i,3}]$, $W_{i,j}=[k^{(i)}_{(0,l)},k^{(i)}_{(1,l)},k^{(i)}_{(2,l)},k^{(i)}_{(3,l)}]$, $k^{(i)}_{(j,l)}$ 表示第 i 轮轮密钥的第 (j,l) 个字节， $j,l=0,1,2,3$ 。

当 $j=1,2,3$ 时， $W_{i+1,j}=W_{i,j}+W_{i+1,j+1},i=0,\cdots,9$;

当 $j=0$ 时， $W_{i+1,0}=W_{i,0}+\mathrm{ByteSub}(\mathrm{RotByte}(W_{i,3}))+\mathrm{Rcon}(i),i=0,\cdots,9$ 其中 $\mathrm{RotByte}(a,b,c,d)=(b,c,d,a)$, $\mathrm{Rcon}(i)=[(1<<i)\mathrm{mod}(0x11b),0,0,0]$ 。

由密钥方案可知， 11 个轮密钥的所有字节中有 56 个 (例如第 1 个轮密钥的 16 个字节和其它轮密钥的第 1 列的 4 个字节) 是线性无关的，其它密钥字节可由这些密钥字节线性表出，选一组这样的字节作为基，记密钥字节 $k_{(j,l)}$ 写成基中字节的线性组合为 $[k_{(j,l)}]$ 。

3 描述 Rijndael 的 GF(2^8) 上二次方程组

3.1 关于 S 盒的二次方程

Rijndael 的 S 盒的代数表达式为

$$\begin{aligned}z&=63+8fx^{127}+b5x^{191}+01x^{223}+f4x^{239}+25x^{247}+f9x^{251}+09x^{253}+05x^{254}\\&=63+8f(x^{-1})^{2^7}+b5(x^{-1})^{2^6}+01(x^{-1})^{2^5}+f4(x^{-1})^{2^4}+25(x^{-1})^{2^3}+f9(x^{-1})^{2^2}\\&\quad+09(x^{-1})^2+05x^{-1}\end{aligned}$$

易知上式是逆函数合成 GF(2^8) 上 q 多项式，我们假设变量:

$$y_0=x^{-1},\quad y_1=(x^{-1})^2,\quad y_2=(x^{-1})^{2^2},\quad y_3=(x^{-1})^{2^3}$$
$$y_4=(x^{-1})^{2^4},\quad y_5=(x^{-1})^{2^5},\quad y_6=(x^{-1})^{2^6},\quad y_7=(x^{-1})^{2^7}$$

记第 i 轮第 (j,l) 个 S 盒的输入字节变量为 $x^{(i)}_{0\ (j,l)}$, 输出字节变量为 $z^{(i)}_{(j,l)}$, 中间变量为 $y^{(i)}_{0\ (j,l)},\cdots,y^{(i)}_{7\ (j,l)}$, 这些变量都称作状态变量。我们假设在加密和密钥方案中 S 盒的输入不出现零元，这个假设对于加密过程有 53% 的概率正确，对于密钥方案有 85% 的概率正确 (即使假

设不成立，下列方程也只有第一个是错误的)。则由 S 盒的代数表达式知第 i 轮第 (j,l) 个 S 盒变换可以用下列一些 GF(2^8) 上二次方程来描述 ($i=1,2,\cdots,10;\ \ j,l=0,\cdots,3$)：

$$x_{0\ (j,l)}^{(i)}y_{0\ (j,l)}^{(i)}=1,\quad y_{1\ (j,l)}^{(i)}=(y_{0\ (j,l)}^{(i)})^2,\quad y_{2\ (j,l)}^{(i)}=(y_{1\ (j,l)}^{(i)})^2,\quad y_{3\ (j,l)}^{(i)}=(y_{2\ (j,l)}^{(i)})^2$$

$$y_{4\ (j,l)}^{(i)}=(y_{3\ (j,l)}^{(i)})^2,\quad y_{5\ (j,l)}^{(i)}=(y_{4\ (j,l)}^{(i)})^2,\quad y_{6\ (j,l)}^{(i)}=(y_{5\ (j,l)}^{(i)})^2,\quad y_{7\ (j,l)}^{(i)}=(y_{6\ (j,l)}^{(i)})^2$$

$$y_{0\ (j,l)}^{(i)}=(y_{7\ (j,l)}^{(i)})^2$$

$$z_{(j,l)}^{(i)}=63+8fy_{7\ (j,l)}^{(i)}+b5y_{6\ (j,l)}^{(i)}+01y_{5\ (j,l)}^{(i)}+f4y_{4\ (j,l)}^{(i)}+25y_{3\ (j,l)}^{(i)}$$
$$+f9y_{2\ (j,l)}^{(i)}+09y_{1\ (j,l)}^{(i)}+05y_{0\ (j,l)}^{(i)} \tag{1}$$

3.2 线性层变换

第 1 轮前的密钥加可以表成线性方程 ($j,l=0,1,2,3$):

$$x_{0\ (j,l)}^{(1)}=p_{(j,l)}+[k_{0\ (j,l)}^{(0)}]$$

其中 $p_{(j,l)}$ 是明文的第 (j,l) 个字节，现用 $k_{0\ (j,l)}^{(i)}$ 表示第 i 轮轮密钥的第 (j,l) 个字节。

第 $i(i=1,\cdots,10)$ 轮线性层的输出为第 $i+1$ 轮非线性层的输入。经线性层变换后第 (j,l) 个字节可表成一个线性方程：

$$x_{0\ (j,l)}^{(i+1)}=a_{(j,0)}z_{(0,l)}^{(i)}+a_{(j,1)}z_{(1,l+1)}^{(i)}+a_{(j,2)}z_{(2,l+2)}^{(i)}+a_{(j,3)}z_{(3,l+3)}^{(i)}+[k_{0\ (j,l)}^{(i)}] \tag{2}$$

其中 $x_{0\ (j,l)}^{(11)}$ 为密文第 (j,l) 个字节，这里 $l+1$， $l+2$， $l+3$ 均为模 4 加。

当 $i=10$ 时常系数 $a_{(j,k)}=1,\ k=l;\ a_{(j,k)}=0,\ k\neq l$；

当 $i=1,2,\cdots,9$ 时 $a_{(j,l)}$ 为矩阵 M 中第 (j,l) 个元素。

将 $z_{(0,l)}^{(i)}$， $z_{(1,l+1)}^{(i)}$， $z_{(2,l+2)}^{(i)}$， $z_{(3,l+3)}^{(i)}$ 代入到式 (2) 消去变量 z，得到线性方程

$$x_{0\ (j,l)}^{(i+1)}=g_0(y_{0\ (0,l)}^{(i)},\cdots,y_{7\ (0,l)}^{(i)},y_{0\ (1,l+1)}^{(i)},\cdots,y_{7\ (1,l+1)}^{(i)},$$
$$y_{0\ (2,l+2)}^{(i)},\cdots,y_{7\ (2,l+2)}^{(i)},y_{0\ (3,l+3)}^{(i)},\cdots,y_{7\ (3,l+3)}^{(i)},k_{0\ (j,l)}^{(i)}) \tag{3}$$

g_0 中的各项系数由式 (1) 和式 (2) 得到。

3.3 增加线性方程个数

这样确定的线性方程个数太少，应用 XSL 技术时参数 P 值 [2] 太大。我们采用增加状态变量 $x_{1\ (j,l)}^{(i)},x_{2\ (j,l)}^{(i)},x_{3\ (j,l)}^{(i)},x_{4\ (j,l)}^{(i)},x_{5\ (j,l)}^{(i)},x_{6\ (j,l)}^{(i)},x_{7\ (j,l)}^{(i)}$ 和密钥变量 $[k_{1\ (j,l)}^{(i)}],[k_{2\ (j,l)}^{(i)}],[k_{3\ (j,l)}^{(i)}],[k_{4\ (j,l)}^{(i)}],[k_{5\ (j,l)}^{(i)}],[k_{6\ (j,l)}^{(i)}],[k_{7\ (j,l)}^{(i)}]$ 的方法增加线性方程。将式 (3) 两边同时做 $2,2^2,2^3,2^4,2^5,2^6,2^7$ 次方得到

$$x_{1\ (j,l)}^{(i+1)}=g_1,\quad x_{2\ (j,l)}^{(i+1)}=g_2,\quad x_{3\ (j,l)}^{(i+1)}=g_3,\quad x_{4\ (j,l)}^{(i+1)}=g_4$$
$$x_{5\ (j,l)}^{(i+1)}=g_5,\quad x_{6\ (j,l)}^{(i+1)}=g_6,\quad x_{7\ (j,l)}^{(i+1)}=g_7$$

由特征为 2 的有限域上 2^m 次方运算的性质 ($(a+b)^{2^m}=a^{2^m}+b^{2^m}$)，以及 $y_{0\ (j,l)}^{(i)},\cdots,y_{7\ (j,l)}^{(i)}$ 之间的关系可知 $g_1,g_2,g_3,g_4,g_5,g_6,g_7$ 都是关于状态变量 $y_{0\ (0,l)}^{(i)},\cdots,y_{7\ (0,l)}^{(i)},y_{0\ (1,l+1)}^{(i)},\cdots,$

$y_{7\ (1,l+1)}^{(i)}, y_{0\ (2,l+2)}^{(i)}, \cdots, y_{7\ (2,l+2)}^{(i)}, y_{0\ (3,l+3)}^{(i)}, \cdots, y_{(3,l+3)}^{(i)}$ 和密钥变量 $[k_{0\ (j,l)}^{(i)}], \cdots, [k_{7\ (j,l)}^{(i)}]$ 的线性表达式。系数由 g_0 的系数分别做 $2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7$ 次方得到；变量由 g_0 的变量经过适当调整或替换得到，其中状态变量 $y_{0\ (j,l+j)}^{(i)}, \cdots, y_{7\ (j,l+j)}^{(i)}$ 分别循环左移 1, 2, 3, 4, 5, 6, 7 次，密钥变量 $[k_{0\ (j,l)}^{(i)}]$ 分别由 $[k_{1\ (j,l)}^{(i)}], \cdots, [k_{7\ (j,l)}^{(i)}]$ 代替 $([k_{m\ (j,l)}^{(i)}] = [k_{0\ (j,l)}^{(i)}]^{2^m})$。

同时增加一些状态变量的二次方程：

$$x_{1\ (j,l)}^{(i)} = (x_{0\ (j,l)}^{(i)})^2, \quad x_{2\ (j,l)}^{(i)} = (x_{1\ (j,l)}^{(i)})^2, \quad x_{3\ (j,l)}^{(i)} = (x_{2\ (j,l)}^{(i)})^2, \quad x_{4\ (j,l)}^{(i)} = (x_{3\ (j,l)}^{(i)})^2$$

$$x_{5\ (j,l)}^{(i)} = (x_{4\ (j,l)}^{(i)})^2, \quad x_{6\ (j,l)}^{(i)} = (x_{5\ (j,l)}^{(i)})^2, \quad x_{7\ (j,l)}^{(i)} = (x_{6\ (j,l)}^{(i)})^2, \quad x_{0\ (j,l)}^{(i)} = (x_{7\ (j,l)}^{(i)})^2$$

3.4 将 Rijndael 描述成 GF(2^8) 上多变量二次方程组

这样我们就得到了以字节为变量的 GF(2^8) 上的二次方程组描述 Rindael 加密过程：

线性方程：

$$x_{m\ (j,l)}^{(1)} = (p_{(j,l)})^{2^m} + [k_{m\ (j,l)}^{(0)}]$$

$$x_{m\ (j,l)}^{(i+1)} = g_m, \qquad i = 1, 2, \cdots, 10$$

S 盒方程组：

$$x_{0\ (j,l)}^{(i)} y_{0\ (j,l)}^{(i)} = 1, \qquad i = 1, 2, \cdots, 10$$

$$y_{m+1\ (j,l)}^{(i)} = (y_{m\ (j,l)}^{(i)})^2, \qquad i = 1, 2, \cdots, 10$$

$$x_{m+1\ (j,l)}^{(i)} = (x_{m\ (j,l)}^{(i)})^2, \qquad i = 1, 2, \cdots, 10$$

其中 $x_{m\ (j,l)}^{(11)}$ 为密文第 (j,l) 个字节的 2^m 次方，$j,l = 0,1,2,3$，$m = 0,1,\cdots,7$，$m+1$ 为模 8 加。

同理，密钥方案也可以表成一个相似的多变量二次方程组。密钥方案共有 $D = 40$ 个 S 盒方程组，涉及变量个数为 $16 \times D$，由密钥方案知需要增加 $8 \times 8 = 64$ 个密钥字节才能线性表出所有的密钥字节 (包括原始字节 $k_{0\ (j,l)}^{(i)}$ 和增加的字节变量 $k_{m\ (j,l)}^{(i)}$)，增加的密钥字节构成一个 “人造 S 盒”。因此整个方程组里实际用到的密钥字节变量 (称为 “真密钥”) 一共有 $S_k = 16 \times D + 64 = 704$ 个。而密钥字节基中的字节个数为 $L_k = 56 \times 8 = 448$，故 S_k 中有 $S_k - L_k$ 个字节可以由 S_k 中其它字节线性表出。于是密钥方案有两部分方程组成：一部分是类似于加密过程的方程，另一部分是 S_k 中线性相关字节构成的线性方程。

将加密过程的方程组和密钥方案方程组合在一起组成一个大的二次方程组描述 Rijndael，恢复密钥就等于解这个二次方程组。

4 与 Murphy-Robshaw 方程组的比较

Murphy 和 Robshaw 引入 BES(Big Encryption System) 分组密码，它是由 AES(Rijndael) 演化得到的。AES 中有 GF(2^8) 上和 GF(2) 上两种有限域上的运算，而 BES 中只包含 GF(2^8) 上的一些简单运算，由这些简单的运算，Murphy 和 Robshaw 用一个多变量二次方程组描述 BES。AES 对应于一类明文分组和密钥都为特殊形式的 BES，因此将 BES 的方程组特殊化就得到了 AES 的 GF(2^8) 上多变量二次方程组。具体见文献 [3]。

而本文不必引入 BES 密码，从 S 盒的代数表达式入手得到了 GF(2^8) 上多变量二次方程组。比较二者发现它们非常相似，都非常稀疏，只是本文的方程组比 Murphy-Robshaw 方程组

少了一些项和方程。Murphy-Robshaw 方程组中每个 S 盒方程组中有 24 个二次方程，41 项。本文中每个 S 盒方程组中有 17 个二次方程，34 项。也就是说 Murphy-Robshaw 方程组中的每个 S 盒方程组比本文中的多了 7 个方程：$x^{(i)}_{m\ (j,l)}y^{(i)}_{m\ (j,l)}=1$，$m=1,2,\cdots,7$。多了 7 项：$x^{(i)}_{m\ (j,l)}y^{(i)}_{m\ (j,l)},m=1,2,\cdots,7$。

容易知道这 7 个方程都可以由本文 S 盒中的 17 个方程得到，这也说明本文的方程组可以完全描述 Rijndael。

5 应用 XSL 技术求解

XSL 技术 [2] 的主要思想是：将原二次方程组的每个方程都分别乘以一些特定的高次项得到一个新的高次方程组，次数由参数 P 决定。记其中线性独立的方程个数为 R，高次项的个数为 T。当 $R>T-T'$ 时，就可能再生成足够多的新的线性独立的高次方程。将这些新的高次方程和原来 R 个高次方程一起组成高次方程组，将每个高次项看作一个变量，高次方程组就成为线性方程组，用高斯消元法求解这个线性方程组。其中 T' 表示 T 个高次项中的一些特殊项的个数，这些项乘以 T 个高次项中的一个项后仍在 T 个高次项组成的集合中。

我们与文献 [2,4] 一样，采用第二种 XSL 攻击 [2]。第二种 XSL 攻击产生 3 类高次方程，文献 [2] 分别估计了这 3 类高次方程中线性独立的方程个数：

$$R\approx\begin{bmatrix}S\\P\end{bmatrix}(t^P-(t-r)^P);\qquad R'\approx\begin{bmatrix}S\\P-1\end{bmatrix}sB(N_r+1)(t-r)^{P-1}$$

$$R''\approx\begin{bmatrix}S\\P-1\end{bmatrix}(S_k-L_k)(t-r)^{P-1}$$

生成的新的方程组中的项数为 $T=\begin{bmatrix}S\\P\end{bmatrix}t^P$。

S 是加密过程和密钥方案总的 S 盒的个数，$S=201$；t 是每个 S 盒方程组中项的个数，$t=34$；r 是每个 S 盒方程组中二次方程的个数，$r=17$；B 是状态的字节数，$B=16$；N_r 是轮数，$N_r=10$；s 是 S 盒变量的个数，$s=8$；S_k 是用到的“真密钥”变量总个数，$S_k=704$；L_k 是所有轮密钥字节中线性独立的变量个数，$L_k=448$；R 是由二次方程生成的线性独立的方程的个数；R' 是由线性方程生成的线性独立的方程的个数；R'' 是由密钥方案中其它线性方程生成的线性独立的方程的个数。

显然生成的线性独立的方程总数 $R+R'+R''$ 不会超过项的个数 T，文献 [2] 中 Courtois 等人提出“T' 方法”，认为只要找到足够大的 P 使得 $R+R'+R''>T-T'$ 就可能再生成足够多的新的方程，从而可以用高斯消元法。但是 Coppersmith 对“T' 方法”的可行性提出质疑，本文和文献 [4] 一样不用“T' 方法”，而找足够大的 P 使得 $R+R'+R''\geq T$。应用第二种 XSL 技术求解 Murphy-Robshaw 方程组，得 P 值为 3，项数为 $91.9\times10^9\approx2^{36.4}$[4]。对于一个 $n\times n$ 的矩阵用高斯消元法求解其对应的线性方程组的复杂度为 $O(n^3)$，因此文献 [3] 中方程组的求解计算复杂度大约为 $(2^{36.4})^3=2^{109.2}$ 次 $\mathrm{GF}(2^8)$ 上运算，应用 XSL 技术求解本文的 $\mathrm{GF}(2^8)$ 上多变量二次方程组，得到表 1 中的值：

表 1 XSL 技术求解的结果

	$P=2$	$P=3$
R	17,426,700	45.85×10^9
R'	4,811,136	8.18×10^9
R''	874,752	1.49×10^9
$R+R'+R''$	23,112,588	55.52×10^9
T	23,235,600	52.4×10^9

由表 1 看出 $P=3$ 时，$R+R'+R''>T$，计算复杂度大约为 $(52.4\times10^9)^3=(2^{35.6})^3=2^{106.8}$ 次 GF(2^8) 上运算．与 Murphy-Robshaw 方程组相比本文方程组中少的 7 个项和方程对于参数 P 值没有影响，但是因为项数减少了所以导致用高斯消元法求解时计算复杂度降低了．

需要特别说明的是 XSL 技术对 R, R' 和 R'' 的估计都比较粗，很显然线性无关的方程个数不可能超过项的个数，表 1 却得到了 $R+R'+R''>T$ ．因此 XSL 技术的有效性还需要进一步研究．

参　考　文　献

[1] Daemen J, Rijmen V. AES proposal: Rijndael, AES Round 1 Technical Evaluation CD-1: Documentation. National Institute of Standards and Technology, available from: http://www.nist.gov/aes, Aug. 1998.

[2] Courtois N, Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations. Advances in Cryptology-ASIACRYPT 2002, Berlin: Springer-Verlag, 2002: 267–287.

[3] Murphy S, Robshaw M. Essential algebraic structure within the AES. Advances in Cryptology-CRYPTO 2002, Berlin: Springer-Verlag, 2002: 1–16.

[4] Murphy S, Robshaw M. Comments on the security of the AES and the XSL technique. available from: http://www.cosic.esat.kuleuven.ac.be, Sep. 2002.

李　娜：　女，1980 年生，硕士生，主要从事代数、密码学等方面的研究．

陈卫红：　女，1966 年生，教授，主要从事代数、信息论、密码和编码学等方面的研究．