域元素分量代数表达式的研究

韦宝典[1,2], 刘景伟[1], 王新梅[1]
(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. 中山大学信息科学与技术学院, 广东广州 510275)

摘 要: 本文提出了有限域上的一个新性质: 用变元为域元素的多项式表示域元素的分量. 基于等价类的划分、线性方程组的求解和标准基之对偶基的计算, 提出了域元素分量代数表达式的三种求法. 以此解释了 Rijndael 算法 S 盒代数表达式复杂度低的本质原因, 给出其分量函数间等价关系的一种直接证明方法.

关键词: 等价类; 线性变换; 迹; 对偶基; Rijndael; S 盒
中图分类号: TP309. 2 文献标识码: A 文章编号: 0372-2112 (2005) 01-0174-03

Study on Algebraic Representations of Coordinates of Finite Fields

WEI Bao-dian[1,2], LIU Jing-wei[1], WANG Xin-mei[1]
(1. National Key Lab. of Integrated Service Networks, Xidian University, Xi. an Shaanxi 710071, China;
2. School of Information Science and Technology, Sun Yat-sen University, Guangzhou, Guangdong 510275, China)

Abstract: The determination of the algebraic representations of coordinates of finite field elements with the elements themselves as the variables, which is a new property of finite fields, is investigated. Based on the partition of equivalent classes, the resolving of a linear system of equations and the calculation of the dual basis of the standard basis, three methodologies are presented. With those results, we have successfully given an essential explanation to the simplicity of the algebraic representation of Rijndael S-box and provided a direct proof to the equivalence between any two coordinate functions of Rijndael S-box.

Key words: equivalent class; linear transformation; trace; dual basis; Rijndael; S-box

1 引言

插入攻击[1] (Interpolation attacks) 对代数次数和复杂程度低的分组密码尤其凑效. Rijndael 算法[2] S 盒九项的简单代数表达式使人们对其安全性产生怀疑[3], 文[4]利用这一简单性给出了算法简洁的代数表示形式, 其他相关代数分析见文[5, 6]. 要从本质上解释 Rijndael 算法 S 盒代数式的简单性, 进而提出相应的改善方案, 可从其求解方法着手. 仔细考察 Rijndael 算法 S 盒代数结构不难发现: S 盒代数表达式的复杂程度取决于域元素分量代数表达式的复杂程度. 因此, 有必要研究域元素分量代数表达式的求解方法.

除了代数式表达过于简单, 文[7]还指出并使用 56 个八阶 GF(2) 矩阵间接证明了 Rijndael 算法 S 盒分量函数之间存在等价关系, 文[8]刻划这种等价关系也使用了同样数量的矩阵. 分量函数之间的等价关系虽然能够降低 S 盒硬件实现成本, 但也可能引发对 Rijndael 算法的有效攻击. 利用本文求解域元素分量迹函数表达式的结果, 我们给出 Rijndael 算法 S 盒分量函数间等价关系一种更为直接、简单的证明, 而且等价关系的完整刻划仅用一个八阶 GF(2^8) 矩阵.

2 划分等价类的方法

考察有限域 GF(p^n) 上的一个新性质: 以元素 x 为变元的代数表达式 $G^i(x)=\sum_{j=1}^{p^n-2} c_j x^j$ 表示其第 i 个分量 x_i, 满足当 $x_i=r$ 时 $G^i(x)=r$. 显然, $G^i(x)$ 中不含次数高于 p^n-2 的项, 也不含常数项 c_0.

根据分量 x_i 取值不同, 将域元素划分到以下 p 个集合中, 其中: r= 0, 1, , , p- 1:

$$F_r^i=\{A\mid A_i=r\}=\{A_k^{i\alpha}\mid k=0,1,\ldots,p^{n-1}-1\}$$

此集合又可写成 $F_r^i=\{\alpha B_k^{i0}\mid k=0,1,\ldots,p^{n-1}-1\}$.

在 GF(p^n) 上定义关系 R_i: 对 P a, b, aR_ib 当且仅当 a 和 b 的第 i 分量相同, 即 a I F_r^i 同时 b I F_r^i. 显然, R_i 为一等价关系, 将 GF(p^n) 上的元素划分到 p 个等价类中, 我们将在此等价类划分的基础上确定域元素分量代数表达式.

定义函数 $g^{i0}(x)=\prod_{k=0}^{p^{n-1}-1}(x-A_k^{i0})$, 并将等价类 F_r^i 中所有元素之积记为 g_r^{i*}.

收稿日期: 2003-06-02; 修回日期: 2004-08-31
基金项目: 国家 973 项目(No. G1999035804); 863 重大项目(No. 2002AA143021); / 十五0国家密码发展基金

定理 1　按上述符号的定义有

(1) 对 $C_m^{i\alpha}, C_n^{i\alpha} \neq 0$, $r \neq 0$ 有 $g^{i0}(C_m^{i\alpha}) = g^{i0}(C_n^{i\alpha})$.

(2) $g_r^{io^*} = r g_1^{io^*}$.

(3) $G^i(x) = (g_1^{io^*})^{-1} \# g^{i0}(x)$　　(1)

(4) $G^i(x)$ 中包含且仅包含形如 x^{p^k} ($k = 0, 1, \cdots, n-1$) 的项, 即 $G^i(x) = \sum_{d=0}^{n-1} c_{i,d} x^{p^d}$.

证明

(1) $g^{i0}(C_m^{i\alpha}) = \sum_{k=0}^{p^{n-1}} (C_m^{i\alpha} - A_k^{i0}) = \sum_{k=0}^{p^{n-1}} H_k^{i\alpha}$; 同样 $g^{i0}(C_n^{i\alpha}) = \sum_{k=0}^{p^{n-1}-1} L_k^{i\alpha}$. $g^{io0}(C_m^{i\alpha}) = g_r^{io^*} = g^{io0}(C_n^{i\alpha})$.

(2) $g_r^{io^*} = \sum_{k=0}^{p^{n-1}} H_k^{i\alpha} = \sum_{k=0}^{p^{n-1}-1} (rB_k^{id}) = r^{p^{n-1}} @ \sum_{k=0}^{p^{n-1}-1} B_k^{id} = r \sum_{k=0}^{p^{n-1}-1} B_k^{id} = r g_1^{io^*}$.

(3) 当 $x = A_k^{i0} \in F_1^0$ 时 $G^i(x) = 0$, 而右式中 $g^{io0}(A_k^{io0}) = 0$, 等式成立; 当 $x = A_k^{i\alpha} \in F_i^r$ ($r \neq 0$) 时 $G^i(x) = r$, 右式为 $(g_1^{io^*})^{-1} \# g^{io0}(A_k^{i\alpha}) = (g_1^{io^*})^{-1} \# g_r^{io^*} = (g_1^{io^*})^{-1} \# r \# g_1^{io^*} = r$, 等式成立. 显然, $G^i(x)$ 最高次数为 p^{n-1}, 其值域为 GF(p).

(4) $G^i(x)$ 的次高项为 $x^{p^{n-2}}$. 否则, 假设在 $x^{p^{n-2}}$ 和 $x^{p^{n-1}}$ 之间存在某项 $x^{p^{n-2}+k}$. 由 $G^i(x) \in GF(p)$ 有 $(G^i(x))^p = G^i(x)$, $(x^{p^{n-2}+k})^p = x^{p^{n-1}+kp}$ 必存在于 $G^i(x)$ 中, 这与 $G^i(x)$ 最高次数 p^{n-1} 矛盾. 由此可继续推断 $G^i(x)$ 的次次高项为 $x^{p^{n-3}}$, $\cdots$, 最低项为 x. 因此, $G^i(x)$ 中仅包含 x^{p^k} ($k = 0, 1, \cdots, n-1$) 项. 又由 $G^i(x) \in GF(p)$ 有 x^{p^k} ($k = 0, 1, \cdots, n-1$) 必同时存在或同时不存在于 $G^i(x)$ 中, 显然同时不存在是不可能的, 否则 $G^i(x)$ 恒为零.

定理 1 给出了有限域上的一个新性质: 域元素分量可以用元素幂的固定组合来表示.

3　解线性方程组的方法

文[9] 指出并证明扩域 $K = GF(p^n)$ 到基域 $F = GF(p)$ 上的线性变换 L_B 与迹函数 $Tr_{K/F}(Bx)$ 存在一一对应关系, 但未给出 B 的求法. 本文提出了线性变换迹函数的一种计算方法, 给出一个存在性和构造性并存的定理, 可直接用于域元素分量代数表达式的计算.

定理 2　对扩域 $K = GF(p^n)$ 到基域 $F = GF(p)$ 上的任意线性变换 L(x), 存在 K 上一个元素 B 使得 $L(x) = Tr(Bx)$; B 可通过解以下方程组式(2) 求得: 任意选择 K 上一组基 $A = (A_0, A_1, \cdots, A_{n-1})$, 将这 n 个元素分别代入线性变换 L(x) 和迹函数 Tr(Bx), 联立以 B 为变元的方程组:

$$\begin{cases} A_0 B + A_0^p B^{p+} \cdots + A_0^{p^{n-1}} B^{p^{n-1}} = L(A_0) \\ A_1 B + A_1^p B^{p+} \cdots + A_1^{p^{n-1}} B^{p^{n-1}} = L(A_1) \\ \cdots \\ A_{n-1} B + A_{n-1}^p B^{p+} \cdots + A_{n-1}^{p^{n-1}} B^{p^{n-1}} = L(A_{n-1}) \end{cases} \quad (2)$$

定理第一部分已经在文[9] 中证明; 第二部分构造了一个一元 p^{n-1} 次方程组, 可把高次项 B^{p^i} 看成一变元 B_i, 从而将一元高次方程组转化成多元线性方程组; 选择的基 A 使方程组系数矩阵满秩, 从而确保有解.

方程组的联立仅需选择一组构成基的 n 个域元素, 求解复杂度为 $O(n^3)$.

利用定理 2 可以求解域元素分量的代数表达式, 如定理 3 所示.

定理 3　对域 $GF(p^n)$ 上元素 x 有 $x_i = Tr(B_i x)$, 即 $x = (Tr(B_0 x), Tr(B_1 x), \cdots, Tr(B_{n-1} x))$, 其中的 $B_i \in GF(p^n)$ 可通过解方程组式(2) 求得.

虽然有限域 $GF(p^n)$ 的结构与其生成多项式无关, 但域的乘法规则是由生成多项式定义的, 对不同的生成多项式, 用定理 3 求得的 B_i 一般来说是不同的.

4　求标准基之对偶基的方法

用计算标准基之对偶基[10] 的方法求解域元素分量代数表达式, 一次性可以求出所有域元素分量的代数表达式, 但要求必须使用标准基.

不妨设域 $GF(p^n)$ 是由既约多项式 g(x) 生成的, A 为 g(x) 的根, 向量 $(1, A, A^2, \cdots, A^{n-1})$ 是 $GF(p^n)$ 上的标准基, 其对偶基为 $(B_0, B_1, \cdots, B_{n-1})$. 任意元素都可以写成 $x = \sum_{i=0}^{n-1} x_i A^i$ 的形式, 任意双射函数都可写成 $f(x) = \sum_{j=0}^{n-1} f_j(x) A^j$ 的形式.

由对偶基性质 $Tr(A^i B_j) = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$ 有 $Tr(f(x) B_i) = Tr\left(\left(\sum_{j=0}^{n-1} f_j(x) A^j\right) B_i\right) = \sum_{i=0}^{n-1} (f_j(x) Tr(A^i B_i)) = f_i(x)$.

用恒等映射函数 $ID(x) = x$ 替换上述函数 f(x), 可得到域元素分量的迹函数表达式, 如定理 4 所述.

定理 4　设有限域 $GF(p^n)$ 的生成多项式为 g(x), $g(A) = 0$, 标准基 $(1, A, A^2, \cdots, A^{n-1})$ 的对偶基为 $(B_0, B_1, \cdots, B_{n-1})$, 则域元素分量 $x_i = Tr(B_i x)$, 即 $x = (x_0, x_1, \cdots, x_{n-1}) = (Tr(B_0 x), Tr(B_1 x), \cdots, Tr(B_{n-1} x))$.

表 1 为以上三种方法的计算复杂度. 划分等价类的方法在数据量和计算量方面都是指数复杂度的; 后两种方法所需数据量都仅为 n, 其计算是低幂次复杂度的, 可操作性强, 更具实用价值.

表 1　三种方法的复杂度

方法	数据量	乘法个数	加法个数	取逆个数
第 2 节	$2np^{n-1}$	$n(p^{2n-2}-1)/2$	$n(p^{n-1}-1)^2/2$	n
第 3 节	n	$(5n^3+3n^2-2n)/6$	$(5n^3-6n^2+n)/6$	$(n^2+n)/2$
第 4 节	n	$(p-1)(n^3-n)/2$	$(n^3-n)/2$	0

5　两个应用

Rijndael 算法 S 盒建立在以 $m(x) = x^8 + x^4 + x^3 + x + 1$ 为生成多项式的有限域 $GF(2^8)$ 上, 利用前面的方法可计算出该

域元素与分量之间的关系:

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} 41 & 45 & 61 & 38 & 120 & 156 & 209 & 43 \\ 176 & 237 & 12 & 80 & 176 & 237 & 12 & 80 \\ 88 & 240 & 70 & 191 & 184 & 173 & 167 & 227 \\ 5 & 17 & 26 & 95 & 229 & 76 & 251 & 3 \\ 166 & 226 & 89 & 241 & 71 & 190 & 185 & 172 \\ 83 & 181 & 252 & 22 & 15 & 85 & 161 & 247 \\ 164 & 230 & 73 & 234 & 25 & 90 & 244 & 86 \\ 82 & 180 & 253 & 23 & 14 & 84 & 160 & 246 \end{pmatrix} \# \begin{pmatrix} x \\ x^2 \\ x^4 \\ x^8 \\ x^{16} \\ x^{32} \\ x^{64} \\ x^{128} \end{pmatrix}$$

Rijndael 算法 S 盒中 GF(2)上的矩阵运算是矩阵输入分量的一些线性组合,而每一个矩阵输入分量又是 S 盒输入逆 8 个幂的固定组合,最终 S 盒输出即为输入之幂的某种组合,因此,不难计算出其完整的代数表达式 $S(x) = c_{63}c + c_{8f}cx^{127} + c_{b5}cx^{191} + c_{01}cx^{223} + c_{f4}x^{239} + c_{25}x^{247} + c_{f9}x^{251} + c_{09}x^{253} + c_{05}x^{254}$. 显然,这与生成多项式、仿射矩阵和仿射常量无关. 避免 S 盒代数表达式过于简单的方法是将之替换为随机的、非代数的 S 盒.

此外,文[7]还指出 Rijndael 算法 S 盒分量函数之间存在等价关系 $S_i(x) = S_j(D_{ij}x + a) + bx + c$,其中 D_{ij} 为八阶 GF(2)矩阵,a,b ∈ GF(2^8),c ∈ GF(2). 从实现角度来看,这种等价关系有助于降低 S 盒硬件实现成本;但从安全角度来看,这一特性的存在可能会引发对 Rijndael 算法的有效攻击. 文[7]利用布尔函数局部结构中的关联性(Connectivity),通过寻找等价参数 D_{ij}、a、b 和 c 的方法来证明分量函数之间的等价关系. 这种间接的证明方法完全刻划分量函数之间的等价关系需用多达 56 个八阶 GF(2)矩阵,文[8]也使用了同样多的矩阵. 利用求解域元素分量迹函数表达式的结果,我们给出 Rijndael 算法 S 盒分量函数间等价关系一种更为直接、简单的证明,等价关系 $S_i(x) = S_j(a_{ij}x) + c$,($a_{ij} \in GF(2^8)$)的完整刻划只需一个八阶 GF($2^8$)矩阵.

Rijndael 算法 S 盒域中元素与分量之间的关系还可以写作 $x = ID(x) = (Tr(41x), Tr(176x), Tr(88x), Tr(5x), Tr(166x), Tr(83x), Tr(164x), Tr(82x)) = (Tr(43x^{127}), Tr(180x^{127}), Tr(22x^{127}), Tr(3x^{127}), Tr(172x^{127}), Tr(247x^{127}), Tr(86x^{127}), Tr(246x^{127}))$. 实施 GF(2)上的仿射运算,得到 Rijndael 算法 S 盒形如 $S_i(x) = Tr(C_ix^{127}) + c_i$ 的分量迹函数,其中 $c_i \in GF(2)$. 由此,不难证明 Rijndael 算法 S 盒分量函数之间的等价关系,如定理 5 所述.

定理 5 Rijndael 算法 S 盒分量函数之间存在等价关系 $S_i(x) = S_j(a_{ij}x) + c_{ij}$,其中 $c_{ij} = c_i - c_j \in GF(2)$,$a_{ij}$,为如下矩阵中的元素,i,j = 0,1,2,…,7.

$$[a_{ij}] = \begin{bmatrix} 1 & 63 & 32 & 16 & 186 & 239 & 250 & 125 \\ 25 & 1 & 13 & 139 & 72 & 164 & 82 & 41 \\ 58 & 225 & 1 & 141 & 55 & 106 & 53 & 151 \\ 116 & 217 & 2 & 1 & 110 & 212 & 106 & 53 \\ 118 & 167 & 66 & 33 & 1 & 17 & 133 & 207 \\ 179 & 143 & 145 & 197 & 180 & 1 & 141 & 203 \\ 125 & 5 & 57 & 145 & 115 & 2 & 1 & 141 \\ 250 & 10 & 114 & 57 & 230 & 4 & 2 & 1 \end{bmatrix}$$

证明 取 GF(2^8)上的生成元 g = x + 1,元素 $A = g^{\log(A)}$. 由 $s_i(x) = Tr(C_ix^{127}) + c_i$ 及 $s_j(x) = Tr(C_jx^{127} + c_j$ 有:$s_i(x) = [Tr(C_j(a_{i,j}x)^{127}) + c_j] + c_i - c_j = s_j(a_{ij}x) + c_{ij}$. 其中 a_{ij} 满足 $a_{ij}^{127}C_j = C_i$,即 $g^{127\log(a_{ij})} = g^{\log(C_iC_j^{-1})}$,$127\log(a_{ij}) \equiv \log(C_iC_j^{-1}) \bmod 255$. 由于 gcd(127,255) = 1,$127^{-1} \equiv 253 \bmod 255$,从而 $a_{ij} = g^{253\log(C_i, C_j^{-1}) \bmod 255}$.

6 结束语

本文提出了计算域元素分量代数表达式的三种方法,作为有限域上的一个新性质,解释 Rijndael 算法 S 盒代数表达式复杂度低的本质原因,给出 Rijndael 算法 S 盒分量函数间等价关系一种直接的证明方法. 本文部分成果得益于与武汉大学博士后曾祥勇的讨论,在此表示感谢!

参考文献:

[1] Thomas Jakobsen, Lars R Knudsen. The Interpolation Attack on Block Ciphers[A]. In Proc the 4th International Workshop, FSE. 97[C]. Haifa, Israel, 1997. 28-40.

[2] Joan Daemen, Vincent Rijmen. AES Proposal Rijndael[A]. In Proc the First Advanced Encryption Standard Candidate Conference[C]. Ventura CA: NIST. 1998. 1-45.

[3] Shroppel R. AES round 2 public comment[EB/OL]. http://www.nist.gov/aes. 2000.3-15.

[4] Niels Ferguson, Richard Schroeppel, Doug Whiting. A Simple Algebraic Representation of Rijndael[A]. In Proc the 8th Annual International Workshop, SAC 2001[C]. Toronto, Ontario, Canada, 2001. 103-111.

[5] Sean Murphy, Matthew J B. New observations on Rijndael[EB/OL]. http://www.nist.gov/aes/. 2000.8-7.

[6] Sean Murphy, Matthew J, B Robshaw. Essential Algebraic Structure Within AES[A]. In Proc Advances in Cryptology2CRYPTO 2002[C]. Santa Barbara, California, 2002. 1-16.

[7] Joanne Fuller, William Millan. On Linear Redundancy in the AES S2Box[EB/OL]. http://eprint.iacr.org. 2002.9-23.

[8] A M Youssef, S E Tavares. On Some Algebraic Structures in the AES Round Function[EB/OL]. http://eprint.iacr.org.2002.11-7.

[9] Rudolf Lidl, Harald Niederreiter. Finite Fields[M]. Massachusetts, Addison2Wesley Publishing Company, 1983. 54-56.

[10] R J McEliece. Finite Fields for Computer Scientists and Engineers [M]. Massachusetts, Kluwer Academic, 1987. 110-111.

作者简介:

韦宝典 男,1976 年 5 月出生于广西贵港市,2004 年获西安电子科技大学通信与信息系统专业博士学位,现为中山大学信息科学与技术学院讲师,目前研究兴趣为密码学和网络安全. E2mail: isdwbd@zsu.edu.cn.

刘景伟 男,1978 年 6 月出生于山东省滨州市,现为西安电子科技大学博士研究生,目前研究兴趣为信息论、密码学及电子商务.

王新梅 男,1937 年 11 月出生于浙江省浦江县,西安电子科技大学教授,博士生导师,中国电子学会会士,长期从事信息论、编码和密码学的教学与研究.