现代密码学

第二十六讲 有限域基础

信息与软件工程学院

第二十六讲 有限域基础

- 有限域的基本概念
- GF（2^8）域

什么是域

- F是一个非空集合，定义了加法、乘法两个二元运算，对这两个运算封闭
- 加法满足：对于任意a,b,c∈F
  - a+b=b+a；交换律
  - (a+b)+c=a+(b+c)；结合律
  - 存在0 ∈F，使得a+0=a；有零元
  - 存在-a ∈F，使得a+(-a)=0；有负元
- 乘法满足：对于任意a,b,c∈F
  - a·b=b·a；交换律
  - (a·b)·c=a·(b·c)；结合律
  - 存在e ∈F，使得a·e=a；有单位元
  - 存在a^{-1} ∈F，使得a·a^{-1}=e；有逆元
- 乘法对加法满足分配率
  - a·(b+c)=a·b+a·c

域的例子

- Z_n={0,1,2,…，n-1}$_{modn}$，加法和乘法都是模n的运算，运算封闭
- 加法满足结合律和交换律，有零元0，有负元
- 乘法满足结合律和交换律，有单位元1，不一定有逆元
- Z_n中的数什么时候才有乘法逆元呢？
- 引理：整数a在模n乘法下有逆元，当且仅当a与n互素。
- 所有与n互素的元素在模n乘法下构成乘法交换群
- 1…n-1都与n互素，则n为素数
- 对于任一素数p，Z_p为域，其元素个数为p个

域的例子（续）

- $F[x]/(f(x))=\{r(x)=r_{n-1}x^{n-1}+r_{n-2}x^{n-2}+\cdots+r_1x+r_0 \mid r_i\in F,\ 0\le i\le n-1\}$，加法和乘法都是模$f(x)$的运算，运算封闭
- 加法满足结合律和交换律，有零元0，有负元
- 乘法满足结合律和交换律，有单位元1，不一定有逆元
- $F[x]/(f(x))$中的多项式什么时候才有乘法逆元呢？

域的例子（续）

- 引理：r(x)在模f(x)乘法下有逆元，当且仅当r(x)与f(x)互素。
- 所有与f(x)互素的元素在模f(x)乘法下构成乘法交换群
- 次数比f(x)的次数低的多项式都与f(x)互素，则f(x)为不可约多项式
- 对于任一首项系数为1的不可约多项式，F[x]/(f(x))为域
- 若$F=Z_p$，则F[x]/(f(x))中元素个数为p^n个
- p^n域的构造方法是首先选取Z_p中的一个n次不可约多项式，然后构造集合

$$F[x]/(f(x))=\{r(x)=r_{n-1}x^{n-1}+r_{n-2}x^{n-2}+\ldots+r_1x+r_0 | r_i\in F,\ 0\le i\le n-1\}$$

集合中的加法和乘法运算为模多项式f(x)的运算

有限域的定义及性质

- 一个有限域F是指只含有限个元素的域，F的阶是指F中元素的个数。有限域又称为Galois域。若域F的阶为n，则可将F记为F_n或GF(n)。
- 定理1 设F是一个特征为素数p的有限域，则F中的元素个数为p^n，n是一个正整数。
- 定理2 （存在性）对于任何素数p和任意正整数n，总存在一个有限域恰好含有p^n个元素。
- 定理3 （惟一性）任意两个$q=p^n$元域都同构，即p^n元域在同构意义下是惟一的。

定理 4 设F_q是q元域，则其乘法群F_q^*是一个循环群。

- F_q^* 指的是 F_q 中所有非零元构成的集合。

第二十六讲 有限域基础

有限域的基本概念

GF（2^8）域

AES中的处理单元

- AES加密标准算法中是以字节为处理单元
- 可以将每一字节看作是有限域$GF(2^8)$上的一个元素，分别对应于一个次数不超过7的多项式。如$b_7b_6b_5b_4b_3b_2b_1b_0$可表示为多项式

$$b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$$

- 还可以将每个字节表示为一个十六进制数，即每4比特表示为一个十六进制数，代表较高位的4比特的符号仍在左边。例如，01101011可表示为6B
- 它们之间的运算为$GF(2^8)$中的运算

GF(2^8) 中的运算

定义：在$GF(2^8)$ 上的加法定义为二进制多项式的加法，且其系数模2。

例如：‘57’+‘83’=‘D4’，用多项式表示为

$$(x^6+x^4+x^2+x+1)+(x^7+x+1)=x^7+x^6+x^4+x^2 \pmod{m(x)}$$

用二进制表示为

$$01010111+10000011=11010100$$

定义：在$GF(2^8)$上的乘法（用符号 · 表示）定义为二进制多项式的乘积模一个次数为8的不可约二进制多项式

$$m(x)=x^8+x^4+x^3+x+1$$

它的十六进制表示为‘11B’。

例如：‘57’·‘83’=‘C1’可表示为以下的多项式乘法：

$$(x^6+x^4+x^2+x+1)\cdot(x^7+x+1)=x^7+x^6+1 \pmod{m(x)}$$

GF(2^8)中的逆元和x乘法

定义： 对任何次数小于8的多项式b(x)，可用推广的欧几里得算法得

$$b(x)a(x)+m(x)c(x)=1$$

即$a(x)\cdot b(x)=1 \bmod m(x)$。因此a(x)是b(x)的乘法逆元。

定义： 函数xtime(x)定义为GF（2）上的$x\cdot b(x)$。其运算如下：若$b_7=0$，则$x\cdot b(x)$的结果就是把字节b左移一位，且在最右边补上上0；若$b_7=1$，则先对b(x)在字节内左移一位（最后一位补0），则再与‘1B’（00011011）做逐比特异或。

xtime(x)的例子

- 例如，‘57’·‘13’可按如下方式实现：
- ‘57’·‘02’=xtime(57)=‘AE’；
- ‘57’·‘04’=xtime(AE)=‘47’；
- ‘57’·‘08’=xtime(47)=‘8E’；
- ‘57’·‘10’=xtime(8E)=‘07’；
- ‘57’·‘13’=‘57’·(‘01’ ⊕ ‘02’ ⊕ ‘10’)
- =‘57’ ⊕ ‘AE’ ⊕ ‘07’=‘FE’

GF(2^8)上的模多项式运算

- 4个字节构成的向量可以表示为系数在GF(2^8)上的次数小于4的多项式
- 多项式的加法就是对应系数相加；换句话说，多项式的加法就是4字节向量的逐比特异或。
- 规定多项式的乘法运算必须要取模$M(x)=x^4+1$，这样使得次数小于4的多项式的乘积仍然是一个次数小于4的多项式，将多项式的模乘运算记为$\otimes$，设$a(x)=a_3x^3+a_2x^2+a_1x+a_0$，$b(x)= b_3x^3+b_2x^2+b_1x+b_0$，$c(x)= a(x)\otimes b(x)=c_3x^3+c_2x^2+c_1x+c_0$。由于$x^j \bmod (x^4+1)= x^{j \bmod 4}$，所以

$$c_0=a_0b_0\oplus a_3b_1 \oplus a_2b_2 \oplus a_1b_3;$$
$$c_1= a_1b_0 \oplus a_0b_1 \oplus a_3b_2 \oplus a_2b_3;$$
$$c_2= a_2b_0 \oplus a_1b_1 \oplus a_0b_2 \oplus a_3b_3;$$
$$c_3= a_3b_0 \oplus a_2b_1 \oplus a_1b_2 \oplus a_0b_3。$$

多项式乘法的矩阵表示

可将上述计算表示为

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

其中元素的加法和乘法为**GF（2^8）**域上的运算

模x^4+1逆元

定理： 系数在GF(2^8)上的多项式$a_3x^3+a_2x^2+a_1x+a_0$是模x^4+1可逆的，当且仅当矩阵

$$\begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix}$$

在GF(2^8)上可逆。

证明

证明： $a_3x^3+a_2x^2+a_1x+a_0$是模x^4+1可逆的，当且仅当存在多项式$h_3x^3+h_2x^2+h_1x+h_0$满足

$$(a_3x^3+a_2x^2+a_1x+a_0)(h_3x^3+h_2x^2+h_1x+h_0)=1 \bmod (x^4+1)$$

因此有

$$(a_3x^3+a_2x^2+a_1x+a_0)(h_2x^3+h_1x^2+h_0x+h_3)=x \bmod (x^4+1)$$

$$(a_3x^3+a_2x^2+a_1x+a_0)(h_1x^3+h_0x^2+h_3x+h_2)=x^2 \bmod (x^4+1)$$

$$(a_3x^3+a_2x^2+a_1x+a_0)(h_0x^3+h_3x^2+h_2x+h_1)=x^3 \bmod (x^4+1)$$

证明（续）

将以上关系写成矩阵形式即得

$$\begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} h_0 & h_3 & h_2 & h_1 \\ h_1 & h_0 & h_3 & h_2 \\ h_2 & h_1 & h_0 & h_3 \\ h_3 & h_2 & h_1 & h_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

（证毕）

感 谢 聆 听!

xynie@uestc.edu.cn