密码算法中的循环移位“异或”运算实质性研究

成 彬[1],王冬艳[2],韩宪生[3],胡 波[1]

(1.河北省科学院应用数学研究所,河北 石家庄 050081;
2.河北华烨冀科信息技术公司,河北 石家庄 050081;
3.河北省科学院,河北 石家庄 050081)

摘 要:针对移位和“异或”运算的复合运算进行了研究,指出了 m 位二进制数的循环移位“异或”变换和移位“异或”变换等同于 GF(2)上的多项式乘法问题,并给出了这种变换的可逆性判断的充分必要条件。

关键词:循环移位;异或;逆变换

中图分类号:TP309.7 **文献标识码**:A **文章编号**:1674-7720(2011)11-0079-02

Research of the nature of cyclic shift XOR in cryptography

Cheng Bin[1], Wang Dongyan[2], Han Xiansheng[3], Hu Bo[1]

(1.Institute of Applied Mathematics, Hebei Academy of Sciences, Shijiazhuang 050081, China;
2.Hebei Hua Ye Ji Ke Information Technology Co., Ltd., Shijiazhuang 050081, China;
3.Hebei Academy of Sciences, Shijiazhuang 050081, China)

Abstract: This paper researched cycles shift XOR and cyclic XOR, and indicated that the essence of m bit binary number of cycles shift XOR and cyclic XOR is the polynomial multiplication on GF (2), and given the necessary and sufficient condition to judge the reversibility of this transformation.

Key words: cyclic shift; XOR; inverse transformation

在计算机网络信息传输中,保证信息在发送方和接收方之间传送时不被窃密者窃取破译最成功有效的方法是采用加密机制来保护通信信息。针对保密算法中所采用密钥的特点,Simmons[1]将密码体制区分为对称密码和非对称密码。对称密码也称为私钥或传统密码体制,非对称密码又称为公钥密码体制。在对称密码体制中,加密密钥能够根据解密密钥推算出来,反之也成立。此外按加密方式,对称密码体制又分为流密码和分组密码。在流密码算法中,明文消息是按字符逐位加密。而在分组密码中,明文消息分成多个分组(每组含有多个字符),逐组进行加密。分组密码具有较强的抗攻击能力、易于伪造伪随机数生成器、流密码、消息认证函数和杂凑函数,并且容易实现,速度快,适合大量数据加密。本文对移位和“异或”运算的复合运算进行了研究,指出了“异或”和移位运算的数学本质,对设计分组密码算法具有一定的指导作用。

1 二进制数的多项式表示

一个 n bit 的二进制数可以用一个多项式表示[2-3]:

$$c=\{c_{n-1},c_{n-2},c_1,c_0\}\Rightarrow c(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0 \quad (1)$$

其中 x^i 表示第 i 个位置(从 c 的右边起从 0 数),$c_i\in\{0,1\}$是第 i bit 的值。其中$\{0,1\}=GF(2)$是模 2 剩余类环,它是特征为 2 的素域。即任何一个二进制数可以用 GF(2)的多项式表示。如果 c 中第 i 比特是 1,再往左都是 0,则称 $c(x)$为 i 次多项式。m bit 二进制数对应最多 $m-1$ 次多项式。

注意:把二进制数对应到多项式时,有左右顺序的问题。这个问题并无实质差别,只要约定清楚即可。缺省假设向量中的 bit 从左到右对应多项式从高到低的系数。二进制情况下,次数不超过 $m-1$ 的多项式 $c(x)$总共有 2^m 个[4-5]。

如同整系数多项式、实系数多项式,称式(1)中这个多项式为系数在 GF(2)上的多项式。

2 移位和循环移位操作

按照式(1)的对应关系,两个二进制数的“异或”运算对应 GF(2)上的多项式的加法运算。左移一位运算对应多项式的乘以 x 运算。左移 k 位对应多项式的乘以 x^k 运算。

循环移位操作分循环左移和循环右移两种。假定循环移位的位数为 m,那么循环移位的位数 k 在 $1\sim m^{-1}$ 之间。对于一个 m 位数,循环右移 k 位等价循环左移 $m-k$ 位。因此,循环右移可以转化为循环左移来实现(这里只考虑循环左移)。

以下用 $a<<<k$ 表示二进制数 a 循环左移 k 位;用 $a<<k$ 表示二进制数 a 左移 k 位。

对 m 位的二进制数的循环左移 k 位就是整个 m 位二进制数左移 k 位,若有移出的 bit 则从右边环回。它等价于多项式乘以 x^k 然后对多项式 x^m+1 取模,即:

若 $a=\{a_{m-1},a_{m-2},\cdots,a_1,a_0\}\Rightarrow a(x)$,则 $a<<<k\Rightarrow x^k a(x) \bmod (x^m+1)$

循环移位后多项式的次数不会超出 $m-1$。

对 m 位的二进制数的左移 k 位就是整个 m 位二进制数左移 k 位,若有移出的 bit 将其截去。它等价于多项式乘以 x^k 然后对多项式 x^m 取模,即:

若 $a=\{a_{m-1},a_{m-2},\cdots,a_1,a_0\}\Rightarrow a(x)$,则 $a<<k\Rightarrow x^k a(x) \bmod (x^m)$

这样移位后多项式的次数不会超出 $m-1$。

定义 1:对 m 位的二进制数 $a=\{a_{m-1},a_{m-2},\cdots,a_1,a_0\}$,$a_i\in\{0,1\}$,的线性变换。

$$L(a)=a<<<k_1\oplus a<<<k_2\oplus\cdots\oplus a<<<k_n$$

其中 $0\leqslant k_i<m$,叫做 a 的循环移位“异或”变换。

定义 2:对 m 位的二进制数 $a=\{a_{m-1},a_{m-2},\cdots,a_1,a_0\}$,$a_i\in\{0,1\}$,的线性变换。

$$H(a)=a<<h_1\oplus a<<h_2\oplus\cdots\oplus a<<h_n$$

其中 $0\leqslant h_i<m$,叫做 a 的移位“异或”变换。

3 循环移位“异或”变换和移位“异或”变换的表示

定理 1:对 m 位的二进制数 $a=\{a_{m-1},a_{m-2},\cdots,a_1,a_0\}$,$a_i\in\{0,1\}$,的每个循环移位“异或”变换。

$$L(a)=a<<<k_1\oplus a<<<k_2\oplus\cdots\oplus a<<<k_n \tag{2}$$

有多项式 $k(x)$ 使得,$L(a)\Rightarrow k(x)a(x) \bmod (x^m+1)$,其中 $k(x)=\sum_{i=1}^{n}x^{k_i}$。则称为 $k(x)$ 循环移位“异或”变换 $L(a)$ 的变换多项式。

证明:式(2)中的每一项 $a<<<k_i$ 由前面讨论有一个 x^{k_i} 与之对应,使得:

$$a<<<k_i\Rightarrow x^{k_i}a(x) \bmod (x^m+1)$$

因此,由于 $L(a)$ 是线性变换,所以:

$$L(a)\Rightarrow x^{k_1}a(x)+x^{k_2}a(x)+\cdots+x^{k_n}a(x) \bmod (x^m+1)=$$
$$(x^{k_1}+x^{k_2}+\cdots+x^{k_n})a(x) \bmod (x^m+1)=$$
$$k(x)a(x) \bmod (x^m+1)。$$

同样可得:

定理 2:对 m 位的二进制数 $a=\{a_{m-1},a_{m-2},\cdots,a_1,a_0\}$,$a_i\in\{0,1\}$,的每个移位“异或”变换。

$$H(a)=a<<h_1\oplus a<<h_2\oplus\cdots\oplus a<<h_n$$

有多项式 $h(x)$ 使得,$L(a)\Rightarrow h(x)a(x) \bmod (x^m)$,其中 $h(x)=\sum_{i=1}^{n}x^{h_i}$。称为 $h(x)$ 移位“异或”变换 $H(a)$ 的变换多项式。

由定理 1 和定理 2 可知,讨论 m 位二进制数的循环移位“异或”变换和移位“异或”变换变成了讨论 GF(2)上多项式乘法了。

在计算机中一般都取 8 bit 为一个字节,16 bit 为一个字,32 bit 为一个双字,64 bit 为一个长整形数。它们共同特点是位长度为 2 的某次方幂。在这种情况下,多项式 $x^{2k}+1$ 可以完全分解成 $x^{2k}+1=(x+1)^{2k}$。它除了 $x+1$ 外没有其他因子,同样 x^m 也除了 x 外没有其他因子。因此,判断以 $x^{2k}+1$ 为模的重模多项式环中元素存在逆元就变成了被判断的多项式是否有 $x+1$ 因子;判断以 x^m 为模的重模多项式环中元素存在逆元就变成了被判断的多项式是否有 x 因子;判断是否有 x 因子,看多项式的常数项是否为 0 即可。判断 $\varphi(x)$ 是否有 $x+1$ 因子,只需判断 $\varphi(1)=0$ 与否,转化 $\varphi(x)$ 的系数为 1 的奇偶性,如果 $\varphi(x)$ 有偶数个为 1 的系数,那么 $\varphi(1)=0$,否则 $\varphi(1)\neq 0$。得到如下定理:

定理 3:在长度为 2 的方幂的二进制位串中,循环移位“异或”变换中,如果有奇数项,那么这个变换是可逆的,有偶数项则不可逆。

定理 4:不论多长的二进制位串移位“异或”变换,只要包含不移位的项,该变换就是可逆的,否则就是不可逆的。

根据定理 3,选择了 SMS4 密码算法标准里的线性变换[6-7],它是一个循环移位“异或”变换:

$$L(B)=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24)$$

为了解密,必须求出其逆变换,为此,从这个变换对应的重模多项式入手,计算其逆多项式。这个变换对应的多项式为:

$$\varphi(x)=x^{24}+x^{18}+x^{10}+x^2+x^1$$

计算 $\varphi(x)=x^{24}+x^{18}+x^{10}+x^2+x^1$ 的逆多项式为:

$$(\varphi(x))^{-1}=x^{30}+x^{24}+x^{22}+x^{18}+x^{16}+x^{14}+x^{12}+x^8+x^4+x^2+1$$

因此就找到了 $L(B)=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24)$ 的逆变换为:

$$L^{-1}(B)=B\oplus(B<<<2)\oplus(B<<<4)\oplus(B<<<8)\oplus(B<<<12)\oplus(B<<<14)\oplus(B<<<16)\oplus(B<<<18)\oplus(B<<<22)\oplus(B<<<24)\oplus(B<<<30)$$

L 变换有 5 项,其逆变换有 11 项,符合定理 3 的结论。

本文对密码算法中循环移位“异或”运算的本质进行了探讨，并且给出了这种变换的可逆性判断的充分必要条件，对设计新的密码算法具有一定的指导作用。

参考文献

[1] SIMMONS G J, Symmetric and asymmetric encryption[J]. Computing Surveys, 1979,11(4):305-330.

[2] 冯克勤，余红兵.整数与多项式[M].北京：高等教育出版社，1999.

[3] 万哲先.代数和编码(第三版)[M].北京：高等教育出版社，2007.

[4] 胡波，赵红芳，冯春雨.一种新的重模剩余类环中元素逆的求法[J].河北省科学院学报，2009，26(1)：1-3.

[5] 赵红芳，胡波，冯春雨.重模多项式环中逆元素的存在性判断及求法[J].中国科技信息，2009(8)：45-47.

[6] 李大为，赵旭鑫，武萌.SMS4 密码算法的高速流水线实现[J].电子器件，2007，30(2)：590-592.

[7] 郑秀林，金丽娜.SMS4 算法在 DSP 中的实现研究[J].北京电子科技学院学报，2006，14(4)：34-37.

(收稿日期：2011-01-11)

作者简介：

成彬，男，1973 年生，副研究员，硕士，主要研究方向：信息技术和偏微分方程。