密码学进展—CHINACRYPT'96

第四届中国密码学学术会议论文集

裴定一　赵仁杰　周锦君　编

科学出版社

密码学进展——CHINACRYPT'96

第四届中国密码学学术会议论文集

裴定一　赵仁杰　周锦君 编

科学出版社

1996

(京)新登字 092 号

内 容 简 介

本书是 1996 年 4 月在郑州召开的第四届中国密码学学术会议论文集。书中收录了涉及密码学各分支的研究论文 40 篇。主要内容包括：序列密码和线性阵列，分组密码和公钥密码，自动机密码，认证理论和秘密共享，杂凑函数和数字签名，布尔函数，与密码有关的代数、逻辑、混沌理论和微分方程，密码学的应用等。

本书可供从事密码学、数学和计算机通信专业的科技人员和高校师生参考。

密码学进展——CHINACRYPT'96

第四届中国密码学学术会议论文集

裴定一 徐茂杰 周锦君 编

责任编辑 那莉莉

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

北京兰空印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1996 年 3 月第 一 版 开本：787×1092 1/16

1996 年 3 月第一次印刷 印张：17 5/8

印数：1—2 000 字数：405 000

ISBN 7-03-005111-4/TP・533

定价：33.00 元

前　言

第四届中国密码学学术会议于1996年4月在郑州召开。本书收集了在这次会议上报告的40篇论文，内容涉及序列密码和线性阵列，分组密码，公钥密码，自动机密码，认证理论和秘密共享，杂凑函数和数字签名，以及密码的应用等研究方向。这些论文反映了我国密码学学术界近年来的研究动态，从中可以看到，我们的研究工作正在不断地走向深入。

本届会议共收到论文53篇。每篇收到的论文都由程序委员会中2名以上的专家主审。在1995年8月15日的程序委员会会议上，委员们经过认真讨论，决定了录用的论文。我们感谢所有的投稿者对会议的关心和支持。

郑州解放军信息工程学院为本届会议提供了赞助，并为会议的召开做了大量的组织工作。在此，向他们表示衷心的感谢。

第四届中国密码学学术会议程序委员会

第四届中国密码学学术会议程序委员会

主　席　裘定一　中国科学院研究生院

副主席　赵仁杰　郑州信息工程学院

周锦君　郑州信息工程学院

委　员　（以姓氏笔画为序）

于秀源　杭州师范学院

王育民　西安电子科技大学

王鹏芳　北京大学

卢开澄　清华大学

冯克勤　中国科技大学

冯培荣　中国科学院软件研究所

刘木兰　中国科学院系统科学研究所

许以超　中国科学院数学研究所

朱　洪　复旦大学

何大可　西南交通大学

何松涛　中国科学院软件研究所

李大兴　山东大学

李　祥　贵州大学

肖国镇　西安电子科技大学

杨义先　北京邮电大学

杨君辉　中国科学院软件研究所

张焕国　武汉大学

黄民强　中国科学院系统科学研究所

龚奇敏　电子部第三十研究所

曹珍富　哈尔滨工业大学

戴宗铎　中国科学院研究生院

目　录

序列密码和线性阵列

分组密码和公钥密码

自动机密码

认证理论和秘密共享

移位-删除钟控序列的安全性

奚邦余　魏振军　赵仁杰
（郑州信息工程学院信息研究系，郑州 450002）

摘要　移位-删除钟控序列是应用较为广泛的一类钟控序列。本文给出其中的一种较简单的移位-删除钟控序列的攻击方法，讨论了这种钟控序列的安全性，并给出提高其安全性的方法。

关键词　移位-删除钟控序列　0-游程　初始状态

一、引　言

移位-删除钟控序列是应用较为广泛的一类钟控序列。本文研究了一种较简单的移位-删除钟控序列的表示方法、周期及特性，证明了其控制序列的一个周期中长度大于等于其级数的 0-游程不少于其 0-游程总数的 1/4，并利用这一性质给出了一种攻击方法，讨论了这种序列的安全性，给出提高其安全性的一种方法，一方面，有些钟控序列（例如[1]）的安全性可以用与本文类似的方法加以讨论，而另一些钟控序列（例如[2]）经过适当的变换也可以用与本文类似的方法讨论其安全性；另一方面，本文的结果对设计移位-删除钟控序列也有一定的参考价值。

二、主 要 结 果

图 1 是一种钟控序列产生器的模型（称为移位-删除钟控序列产生器）。其中 LFSR1 和 LFSR2 各自单独运行，且有相同的时钟脉冲控制移位。LFSR1 的最后两级输出相乘后控制 LFSR2 的输出。如果 $c_j=1$，LFSR2 移位一步，但不输出；如果 $c_j=0$ 则 LFSR2 移位一步，且输出 b_j。得到的序列 $\{z_j\}$ 称为移位-删除钟控序列。

例 1　给定 $\{a_j\}=\{1011\cdots\}$ 和 $\{b_j\}=\{1001\cdots\}$ 的连接多项式分别为 $f(x)=x^4\oplus x\oplus 1$ 和 $g(x)=x^4\oplus x^3\oplus 1$，则有

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\{a_j\}$	1	0	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1	0
$\{c_j\}$	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	0	0	
$\{b_j\}$	1	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	
$\{z_j\}$	1	0	0	1	0	1	0	1	1	1	0	1	0	0	1	0	1						

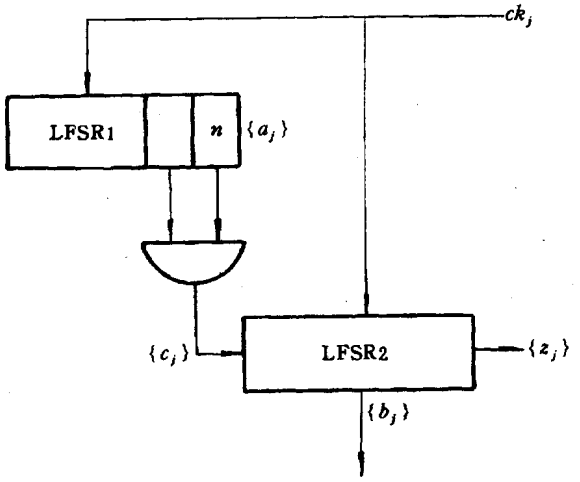

图 1　移位-删除钟控序列产生器

记

$$z_j = b_{j+s(j)} \quad w(j) = j + s(j-1) - 1 \tag{1}$$

则有求 $s(j)$的递归算法如下：

$$\begin{cases} s(0) = 0, \\ s(j) = \sum_{k=0}^{w(j)+t(j)} c_k \quad \text{如果 } c_{w(j)} = 0, \text{取 } t(j) = 0, \text{如果 } c_{w(j)} = 1, \text{取} \\ \qquad\qquad t(j) \text{ 等于 } c_{w(j)} \text{ 所属 1- 游程长度} \end{cases} \tag{2}$$

$\{c_j\}$唯一确定一个递增的整数序列 $s(j)$，而 $s\{j\}$也唯一确定$\{c_j\}$。

设控制序列$\{c_j\}$的周期为 p_1，LFSR2 正常情况下的输出序列的周期为 p_2，那么，当且仅当 LFSR2 跑过$[p_1, p_2]$个比特后，$\{c_j\}$和$\{b_j\}$才返回到各自的初始值。令 $\sum_{j=0}^{p_1-1} c_j = w_1$，则$\{z_j\}$的周期

$$p = p_2(p_1 - w_1)/(p_1, p_2) \tag{3}$$

特别，当 $p_1 = p_2 = 2^n - 1$ 时，

$$p = p_1 - w_1 = 2^n - 2^{n-2} - 1 \tag{4}$$

其中$[a,b]$和(a,b)分别表示 a 与 b 的最小公倍数和最大公因数。

假定 LFSR1 和 LFSR2 的连接多项式 $f(x)$和 $g(x)$都是 F_2 上的本原三项式，且是已知的，它们各自的初始状态 $S(a)$和 $S(b)$是用户的秘密密钥(又称实际密钥)。当我们获得序列$\{z_j\}$后，试图攻击秘密密钥 $S(a)$和 $S(b)$。实施攻击的关键是恢复序列$\{b_j\}$，从而得到 $S(b)$和整数序列 $s(j)$，再由 $s(j)$求出$\{c_j\}$，根据$\{c_j\}$就很容易求出 $S(a)$。为此，先分析$\{c_j\}$中长度大于等于 LFSR2 的级数的 0-游程的个数。

引理 1　设 $c = \{c_j\}$是图 1 中的参数为(0,1)的二端单与门序列，则 c 的自相关函数

$$C_c(1) = 2^{n-1} - 1$$

引理 2　c 的一个周期中 1-游程和 0-游程的个数均为 2^{n-3}。

[证明]　把 c 中形如 01 和 10 的相邻分量分别叫做从 0 到 1 的转换和从 1 到 0 的转

换，则在 c 的周期圆上，0 到 1 的转换次数等于 1 到 0 的转换次数，这表明 c 中 1-游程和 0-游程的个数相等，设此个数为 m，则由引理 1 可得

$$C_c(1) = \sum_{i=0}^{p-1}\eta(c_i)\eta(c_{i+1})$$

$$= m[(-1)\times 1] + m[1\times(-1)] + (p-2m) = P - 4m = 2^{n-1} - 1$$

因为 $p=2^n-1$，故 $m=2^{n-3}$。这里 η 是加法群 F_2 到实数乘群 $\{1,-1\}$ 的同构映射。

设 c 为二元周期序列，用 $N_c(1)$ 和 $N_c(0)$ 分别表示 c 的一个周期中 1 的个数和 0 的个数，用 $N_c(t,1)$ 和 $N_c(t,0)$ 分别表示 c 的一个周期中长为 t 的 1-游程和长为 t 的 0-游程的个数，则有下述引理 3。

引理 3 c 中各种长度的 1-游程的个数为

$$N_c(i,1) = \begin{cases} 2^{n-3-i} & 1 \leqslant i \leqslant n-3 \\ 1 & i = n-1 \\ 0 & i = n-2, i \geqslant n \end{cases}$$

[证明] 注意到 m 序列的 1-游程分布即可。

定义 1 设 $a=(a_0,a_1,\cdots)$ 和 $b=(b_0,b_1,\cdots)$ 为二元周期序列，称

$$d = a \vee b = (a_0 \vee b_0, a_1 \vee b_1, \cdots) = (d_0, d_1, \cdots)$$

为序列 a 与 b 的逻辑或。其中 $d_k=0$ 当且仅当 $a_k=b_k=0$。

引理 4 设 $c=c_1 \vee c_2 \vee \cdots \vee c_t$，其中 c_i 为任意与门网络序列，令

$$d_{i_1 i_2 \cdots i_m} = c_{i_1} \cdot c_{i_2} \cdot \cdots \cdot c_{i_m} \qquad 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant t$$

$$S_m = \sum_{1 \leqslant i_1 < \cdots < i_m \leqslant t} N_{d_{i_1 \cdots i_m}}(1)$$

则

$$N_c(1) = \sum_{k=1}^{t}(-1)^{k-1}S_k$$

令 $d^{(t-1)} = c \vee (Lc) \vee \cdots \vee (L^{t-1}c)$，则有下述引理 5。

引理 5 设 c 为二元周期序列，则

$$N_c(t,0) = 2N_{d^{(t)}}(1) - N_{d^{(t-1)}}(1) - N_{d^{(t+1)}}(1)$$

引理 6 设 $c=c_1 \oplus c_2 \oplus \cdots \oplus c_t$，其中 c_i 为任意与门网络序列，令

$$d_{i_1 i_2 \cdots i_m} = c_{i_1} \cdot c_{i_2} \cdots c_{i_m} \qquad 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant t$$

$$S_m = \sum_{1 \leqslant i_1 < \cdots < i_m \leqslant t} N_{d_{i_1 \cdots i_m}}(1)$$

则

$$N_c(1) = \sum_{k=1}^{t}(-1)^{k-1}2^{k-1}S_k$$

定理 设 $c=\{c_j\}$ 是图 1 中二元周期序列，则当 $n \geqslant 6$ 时，c 中长度大于等于 n 的 0-游程的个数大于 2^{n-5}。

[证明] 由引理 5 可得

$$\sum_{t=1}^{n-1} N_c(t,0) = N_{d^{(1)}}(1) - N_{d^{(0)}}(1) + N_{d^{(n-1)}}(1) - N_{d^{(n)}}(1)$$

因为 $d^{(0)}=c$，$d^{(1)}=c \vee (Lc)$，所以，由引理 4 可得

$$N_{d^{(1)}}(1) - N_{d^{(0)}}(1) = N_c(1) + N_{Lc}(1) - N_{c(Lc)}(1) - 2^{n-2}$$
$$= 2^{n-2} + 2^{n-2} - 2^{n-3} - 2^{n-2} = 2^{n-3}$$

因为

$$d^{(n)} = (c \vee (Lc) \vee \cdots \vee (L^{n-1}c)) \vee L^n c$$
$$= (c \vee (Lc) \vee \cdots \vee (L^{n-1}c)) \oplus L^n c \oplus (c \vee (Lc) \vee \cdots \vee (L^{n-1}c)) \cdot L^n c$$
$$= d^{(n-1)} \oplus L^n c \oplus d^{(n-1)}(L^n c)$$

所以，由引理 6 可得

$$N_{d^{(n)}}(1) = N_{d^{(n-1)}}(1) + N_{L^n c}(1) + N_{d^{(n-1)}(L^n c)}(1)$$
$$- 2[N_{d^{(n-1)}(L^n c)}(1) + N_{d^{(n-1)}(L^n c)}(1) + N_{d^{(n-1)}(L^n c)}(1)]$$
$$+ 2^2 N_{d^{(n-1)}(L^n c)}(1)$$
$$= N_{d^{(n-1)}}(1) + N_{L^n c}(1) - N_{d^{(n-1)}(L^n c)}(1)$$

故

$$N_{d^{(n-1)}}(1) - N_{d^{(n)}}(1) = N_{d^{(n-1)}(L^n c)}(1) - N_{L^n c}(1)$$
$$= N_{d^{(n-1)}(L^n c)}(1) - 2^{n-2}$$

于是

$$\sum_{t=1}^{n-1} N_c(t,0) = N_{d^{(n-1)}(L^n c)}(1) - 2^{n-3}$$

注意到 c 中 0-游程的总数为 2^{n-3} 可得

$$\sum_{t \geqslant n} N_c(t,0) = 2^{n-2} - N_{d^{(n-1)}(L^n c)}(1)$$

为了计算上式右边的值，令

$$e = d^{(n-1)}(L^n c) = (c \vee (Lc) \vee \cdots \vee (L^{n-1}c)) \cdot (L^n c) = (e_0, e_1, \cdots)$$

并注意到由 $f(x) = x^n \oplus x^k \oplus 1$ 可得 $a_{i+n} = a_i \oplus a_{i+k}$，则有

$$e_i = (c_i \vee c_{i+1} \vee \cdots \vee c_{i+n-1}) \cdot c_{i+n} = 1$$

当且仅当 $c_{i+n} = 1$ 且 $(c_i \vee c_{i+1} \vee \cdots \vee c_{i+n-1}) = 1$；

当且仅当 $a_{i+n} = a_{i+n-1} = 1$ 且 $c_i, c_{i+1}, \cdots, c_{i+n-1}$ 中至少有一个为 1；

当且仅当 (a_i, a_{i+k}) 与 (a_{i+1}, a_{i+k+1}) 取 (1,0) 或 (0,1) 且 $c_i, c_{i+1}, \cdots, c_{i+n-1}$ 中至少有一个为 1。于是有以下四种情况：

a_i	$a_{i+1} \cdots a_{i+k}$	$a_{i+k+1} \cdots a_{n-1}$	
0	0 $\cdots$ 1	1 $\cdots$	(5)
0	1 $\cdots$ 1	0 $\cdots$	(6)
1	0 $\cdots$ 0	1 $\cdots$	(7)
1	1 $\cdots$ 0	0 $\cdots$	(8)

对于情况(5)和(8)，分别有 $c_{i+k} = a_{i+k} a_{i+k+1} = 1$ 和 $c_i = a_i a_{i+1} = 1$，所以，在这两种情况下，其余各分量可以任取，各有 2^{n-4} 种不同取法。对于情况(6)和(7)，如果 $a_{n-1} = 1$，则有 2^{n-4} 种不同的取法；如果 $a_{n-1} = 0$，则至少还有一个分量要定为 1，其余分量可以任取，共有 2^{n-5} 种不同取法。由于 $a_{n-1} = 1$ 和 $a_{n-1} = 0$ 可以认为是随机的，所以

$$N_{d^{(n-1)}(L^n c)}(1) \leqslant 2^{n-4} + 2^{n-4} + 2^{n-5} + 2^{n-4} = 2^{n-3} + 2^{n-4} + 2^{n-5}$$

故

$$\sum_{t\geqslant n} N_c(t,0) \geqslant 2^{n-2} - 2^{n-3} - 2^{n-4} - 2^{n-5} = 2^{n-5} \qquad \square$$

该定理表明，$\{c_j\}$中不小于 n 的 0-游程至少占 0-游程总数的 1/4。因此，如果 LFSR2 的级数小于等于 n，且把$\{z_j\}$看成是$\{b_j\}$按顺序依次截取的一个个截段连接而成，则$\{z_j\}$的这些截段中至少有 1/4 的截段的长度大于等于 n。这样，我们可以按如下方法由$\{z_j\}$恢复$\{b_j\}$和$\{a_j\}$：

(1) 设 LFSR2 的级数 $m\leqslant n$，且$\{z_j\}$的状态依次记为 $s_0, s_1, s_2, \cdots$，依次对每个 $s_i=(z_i, z_{i+1}, \cdots, z_{i+m-1})$按 LFSR2 的连接多项式 $g(x)$计算 $z'_{i+m}, z'_{i+m+1}, \cdots$，并与 $z_{i+m}, z_{i+m+1}, \cdots$比较，如果 $z'_{i+m}, z'_{i+m+1}, \cdots, z'_{i+t}$依次与 $z_{i+m}, z_{i+m+1}, \cdots, z_{i+m+t}$相等，而 $z'_{i+m+t+1}\neq z_{i+m+t+1}$，计算停止，并把这样得到的$\{z_j\}$的截段记为 $Z(s_i)$。

(2) 选取最长的 $Z(s_i)$的前 m 个分量 s_i 作为$\{b_j\}$在某时刻的状态，并由 $g(x)$和 s_i 依次反向递推出 $z'_{i-1}, z'_{i-2}\cdots$这样得到的序列实际上就是$\{b_j\}$，只是起点尚未确定。

(3) 在$\{b_j\}$上从 s_i 往前，将$\{b_j\}$和$\{z_j\}$比较，写出$\{c_j\}$的部分分量，并由此求出$\{a_j\}$的某个状态 x。

(4) 由 x 和 LFSR1 的连接多项式 $f(x)$依次往前递推，同时计算出$\{c_j\}$，并按$\{c_j\}$作出$\{z_j\}$和$\{b_j\}$的对应，直到到达 z_0 时为止。

按照以上过程，我们就可以求得$\{a_j\}$和$\{b_j\}$的初始状态。

例 2 已知$\{a_j\}$和$\{b_j\}$的连接多项式分别为 $f(x)=x^6\oplus x^5\oplus 1$ 和 $x^6\oplus x\oplus 1$，$\{z_j\}=$ 1111000100001101001010100011101001011 0111…求$\{a_j\}$和$\{b_j\}$的初始状态。

[解] 按上述方法得到最长的 $Z(s_i)$为

$$Z(s_{29}) = 010010110111$$

以 010010 和 $g(x)$生成$\{b_j\}$，且与$\{z_j\}$对应比较，求出$\{c_j\}$的部分序列和$\{a_j\}$的某个状态 x 如下：

$\{a_j\}$ 011110

$\{c_j\}$ 000000111000000000001000000

$\{b_j\}$ 111111000001000011000100101111010001110010010

$\{z_j\}$ 010010 101000111 010010

再按(5)即可恢复$\{a_j\}$和$\{b_j\}$且得到它们的初始状态分别为(011011)和(111111)。

根据以上讨论容易看出，LFSR2 的级数 m 小于等于 LFSR1 的级数 n 的情况下，此种钟控序列是不安全的。因为 c 中 0-游程的最大长度为 $C_n^1+C_n^2-1$，所以要使此种钟控序列安全可靠，m 应大于 $C_n^1+C_n^2-1$。于是，要么 n 很小，要么 m 很大。而当 n 很小时，容易为穷举攻击所破，m 很大时，硬件的实现上又相当浪费。为了解决这个矛盾，要么用 c 去控制由 LFSR2 及某个前馈函数组成的大于 2 端的前馈网络的输出，要么在 LFSR1 上设计一个前馈网络，让其输出序列 d 与 Ld 相与后作为 LFSR2 的控制序列 C。这样改进后的移位-删除钟控序列的安全性仍有待于进一步讨论。

参考文献

[1] Bernard Smeets, A Note on Sequences Generated by Clock Controlled Shift Registers.

[2] Rueppel R. A., When Shift Registers Clock Themselves Eurocrypt'87, 1988.

[3] Gollman D., Pseudo Random Properties of Cascade Connection of Clock Controlled Shift Registers, Eurocrypt'84, 1985.

[4] Gunther C. G., A Generator of Pseudorandom Sequences with Colck Controlled Linear Feedback Shift Registers, Eurocrypt'87, 1988.

The Security of Shift-Decimated Clock Controlled Sequences

Xi Bangyu Wei Zhenjun Zhao Renjie

(Department of Information Research, Zhengzhou Information Engineering Institute, Zhengzhou 450002, PRC)

Abstract Shift-Decimated clock controlled sequences is a kind of clock controlled sequences applied widely. This paper gives an attactted method of simple shift-decimated clock controlled sequence and discusses its security, gives a method which ensure its security.

Keywords shift-decimated clock controlled sequences a run of 0s initial state

两个符号替换下周期序列的线性复杂度

叶顶锋　戴宗铎

（中国科学院研究生院信息安全国家重点实验室，北京 100039）

摘要　证明了 $\mathbf{F}_q$ 上 n 级 m-序列在两个符号替换下线性复杂度的下确界为 $q^n-1-n-N$，其中 N 为 q^n-1 的最大真因子。

关键词　线性复杂度　符号替换

日本学者 Imamura 在 1994 年的第三届全国密码会议上报告了一些关于周期为 p^n-1, p^n 的线性递归序列在一个符号替换下的线性复杂度的结果[1]；稍后，这些结果被推广到一般的周期序列[2]。本文研究周期序列在两个符号替换下的线性复杂度。

设 $\mathbf{F}_q$ 为特征 p 的有限域。若 $f\in\mathbf{F}_q[x]$，记 $\Omega(f)$ 为 $\mathbf{F}_q$ 上所有以 f 为特征多项式的线性递归序列构成的集合。熟知，$\Omega(f)$ 是一个 $\mathbf{F}_q[x]$-模。$\mathbf{F}_q$ 上所有以 T 为周期的序列构成的集合即为 $\Omega(x^T-1)$。

给定 $\underline{a}=(a_i)\in\Omega(x^T-1)$，令 $\underline{a}(x)=\sum_{i=0}^{T-1}a_ix^{T-1-i}$，则 $\underline{a}\mapsto\underline{a}(x)$ 给出一个 $\Omega(x^T-1)\to\mathbf{F}_q[x]/(x^T-1)$ 的 $\mathbf{F}_q[x]$-模同构。

引理 1　设 $\underline{a}\in\Omega(x^T-1)$，则 $\underline{a}$ 的极小多项式为

$$(x^T-1)/\gcd(x^T-1,\underline{a}(x))$$

其中 gcd 表示最大公因子。

［证明］　$\underline{a}$ 的极小多项式为其零化理想的生成元，而 $\underline{a}$ 与 $\underline{a}(x)$ 有相同的零化理想，此即 $((x^T-1)/\gcd(x^T-1,\underline{a}(x)))$。　□

设

$$T=p^es,(s,p)=1$$

$$x^S-1=\prod_{i=1}^{\tau}f_i\qquad f_1=x-1,f_i\text{ 在 }\mathbf{F}_q\text{ 上不可约}$$

引理 2　设 $\underline{a}\in\Omega(x^T-1)$，则

$$\mathrm{LC}(\underline{a})=T-\sum_{i=1}^{\tau}\min(p^e,\mathrm{ord}_{f_i}\underline{a}(x))\deg f_i$$

其中 LC 表示线性复杂度，ord_{f_i} 表示含 f_i 因子的重数。

［证明］　由于 $\gcd(x^T-1,\underline{a}(x))=\prod_{i=1}^{\tau}f_i^{\min(p^e,\mathrm{ord}_{f_i}\underline{a}(x))}$，由引理 1，

$$\mathrm{LC}(\underline{a})=T-\deg\gcd(x^T-1,\underline{a}(x))$$

$$= T - \sum_{i=1}^{\tau} \min(\mathrm{ord}_{f_i}\underline{a}(x), p^e)\deg f_i \qquad \square$$

令 $B_{2,T}$为所有重量为 2 的周期 T 序列对应的多项式集合，即 $B_{2,T}=\{b_0x^{i_1}+b_1x^{i_2}:b_0b_1\neq 0, 0\leqslant i_1\neq i_2<T\}$对任意 $\underline{b}(x)\in B_{2,T}$，$\underline{a}\in\Omega(x^T-1)$，称 $\underline{a}+\underline{b}$ 为 $\underline{a}$ 的一个两符号替换。对任意 F_q 上不可约多项式 $g(x)$，我们说 $g(x)$具有性质 P，如果 $B_{2,T}(\mathrm{mod}\ g(x))\neq \mathrm{F}_q[x]/(g(x))$。类似于[2]中命题 2，我们有如下命题。

命题 1 存在 $\underline{a}\in\Omega(x^T-1)$，使得 $\underline{a}$ 的所有两符号替换均有线性复杂度 T 的充要条件是对所有 i，f_i 具有性质 P。

[证明] 由引理 2 和中国剩余定理，存在上述 $\underline{a}$ 的充要条件是对每个 i，都存在 $\underline{a}^{(i)}(x)$，使得对所有 $\underline{b}(x)\in B_{2,T}$，均有 $\mathrm{ord}_{f_i}(\underline{a}^{(i)}(x)+\underline{b}(x))=0$，即 $-\underline{a}^{(i)}(x)\neq \underline{b}(x)(\mathrm{mod}_{f_i})$对所有 $\underline{b}(x)\in B_{2,T}$成立，即 $-\underline{a}^{(i)}(x)\overline{\in} B_{2,T}(\mathrm{mod}_{f_i})$，即 f_i 具有性质 P。 $\square$

推论 若 $q>2$，则任给 $\underline{a}\in\Omega(x^T-1)$，总存在 $\underline{a}$ 的一个两符号替换其线性复杂度小于 T。

现在设 $\underline{a}\in\Omega(f_i^{b_i})$，$1\leqslant i\leqslant\tau$。

$$\underline{b}(x) = b_0x^{i_0}(x^t - b_1)^{b_i}, b_0b_1 \neq 0, (t,p) = 1, 0 < p^lt < T$$

易见，每个 $B_{2,T}$中元素都可写成这种形式。

令 $d=\gcd(t,T)=\gcd(t,s)$，$l'=\min(e,l)$。

命题 2 $\underline{a}$，$\underline{b}$ 如上则

(1) 若 $b_1^{s/d}\neq 1$，$\mathrm{LC}(\underline{a}+\underline{b})=T-\min(p^e,\mathrm{ord}_{f_i}(\underline{a}(x)+\underline{b}(x)))\deg f_i$。

(2) 若 $b_1^{s/d}=1$，

$$\mathrm{LC}(\underline{a}+\underline{b}) = T - p^{l'}d + p^{l'}\mathrm{ord}_{f_i}(x^t - b_1)\deg f_i - \min(p^e, \mathrm{ord}_{f_i}(\underline{a}(x) + \underline{b}(x)))\deg f_i$$

[证明] 当 $b_i^{s/d}\neq 1$ 时，注意到 x^t-b_1 与 x^s-1 无公共零点，所以 $\gcd(x^t-b_1,x^s-1)=1$，故对所有 j，均有 $\mathrm{ord}_{f_j}\underline{b}(x)=p^l\mathrm{ord}_{f_j}(x^t-b_1)=0$。利用 ord 函数的基本性质及引理 2 即得(1)；当 $b_1^{s/d}=1$ 时，注意到 x^t-b_1 与 x^s-1 有 d 个公共零点，所以 $\deg\gcd(x^t-b_1,x^s-1)=d$，即

$$\sum_{j=1}^{\tau}\mathrm{ord}_{f_j}(x^t - b_1)\deg f_j = d \qquad \square$$

当 $\underline{a}$ 为 m-序列时，我们将以下便于记忆的简单事实作为定理而结束本文。

定理 设 $T=q^n-1$，$\underline{a}$ 为 $\mathrm{F}q$ 上 n 级 m-序列，则

$$\inf_{\underline{b}(x)\in B_{2,T}} \mathrm{LC}(\underline{a}+\underline{b}) = q^n - 1 - n - N$$

其中 N 为 q^n-1 的极大真因子。

[证明] 由命题 2 知 $q^n-1-n-N$ 是 $\mathrm{LC}(\underline{a}+\underline{b})$的一个下界。设 $\underline{a}$ 的极小多项式为 f，则 $\underline{a}(x)(\mathrm{mod}f)\neq 0$；由于 f 本原，可选取 i_0，使得 $\underline{a}(x)\equiv -x^{i_0}(x^N-1)(\mathrm{mod}f)$。令 $\underline{b}(x)=-x^{i_0}(x^N-1)$，则 $\underline{b}(x)\in B_{2,T}$且由命题 3，

$$\mathrm{LC}(\underline{a}+\underline{b}) = q^n - 1 - n - N \qquad \square$$

参考文献

[1] K. Imamura, On Linear Complexities of Sequences Obtained by One Symbol Substitution from Periodic Sequences of Period P^n or P^n-1, P^a, 密码学进展——CHINACRYPT'94, 科学出版社, 1994.

[2] Z. D. Dai, K. Imamura, Linear Complexity for One Symbol Substitiution of A Periodic Sequence Over GF(q), 密码学理论问题文集, 信息安全国家重点实验室, 1995.

Linear Complexity of Periodic Sequences Under Two Symbol Substitutions

Ye Dingfeng Dai Zongduo

(*State Key Laboratory of Information Security Graduate School of Academia Sinica, Beijing* 100039, *PRC*)

Abstract It is proved that the precise lower bound of linear complexity of an msequence of degree n over F_q under two symbol substitutions is $q^n-n-N-1$, where N is the largest proper factor of q^n-1.

Keywords linear complexity two symbol substitution

形如 $x_{i+2}\equiv ax_{i+1}+bx_i+c(\mathrm{mod}\ M)$的截尾同余序列的综合

王丽萍　周锦君　韩付成

（郑州信息工程学院应用数学系，郑州 450002）

摘要　本文就形如 $x_{i+2}\equiv ax_{i+1}+bx_i+c(\mathrm{mod}\ M)$的截尾同余序列的序列恢复和参数恢复问题进行讨论。主要结果是给出两个高效算法。首先当 a,b,c,M 已知，给定截尾同余序列的前几个输出值，a 为输出比例，$a>2/3$ 或 b 给定一定的范围，只要 $a>5/8$ 时给出多项式时间内恢复整个序列的算法。其次当参数 b 已知，$c=0$，a 要求同上，在给定一段连续长约为 $O(\sqrt{\log M})$的截尾同余序列时，给出多项式时间内恢复 a,M 的算法。

关键词　截尾同余序列　整数规划　格

一、引　　言

伪随机序列在概率算法、蒙特卡罗模拟，特别是在密码学上有重要的应用。目前产生伪随机序列比较常用的方法是 Knuth[5]提出的线性同余方法，即选择适当的模数 M，乘子 a，使 $(a,M)=1$，$b\in Z$，给定初始 x_0，由 $x_{i+1}\equiv a\ x_i+b(\mathrm{mod}\ M)$产生序列$\{x_i\}$，但这种序列是不安全的。Plumstead[11]证明，在给定一段连续的输出序列$\{x_i\}$时，即使模数 M，乘子 a，及 b 都未知，也可以准确地恢复整个序列。Hugo Krawczyk[9]还证明，若 Φ_i 为多项式时间内可计算函数，则对于由式 $x_{i+1}\equiv\sum a_j\Phi_j(x_{i-1},x_{i-2},\cdots,x_0)(\mathrm{mod}\ M)$产生的序列$\{x_i\}$也有多项式时间算法高效地预测整个序列。为了使序列变得不可预测，人们开始研究截尾同余序列。目前研究的截尾同余序列是线性的，即给定参数 $a_1,a_2,\cdots,a_k,c,M\in Z$ 及初值 $x_1,\cdots,x_k$，由 $x_{i+k}\equiv a_1x_{i+k-1}+a_2x_{i+k-2}+\cdots+a_kx_i+c(\mathrm{mod}\ M)$产生序列$\{x_i\}$，令 $x_i=2^my_i+z_i$，m 为正整数，$0\leqslant z_i<2^m$，则序列$\{y_i\}$就是序列$\{x_i\}$的截尾同余序列（截去 m 比特低位）。截尾序列综合问题就是已知一段连续长为 N 的截尾序列$\{y_i\}$，恢复原序列$\{x_i\}$，即恢复参数和初值。由 $x_{i+1}\equiv a\ x_i+b(\mathrm{mod}\ M)$产生的线性截尾序列的综合问题已有很多结果[2,5,6]，但一般的线性截尾序列的研究结果很少[8]。

本文研究了由 $x_{i+2}\equiv ax_{i+1}+bx_i+c(\mathrm{mod}\ M)$产生的截尾序列的综合问题。基本工具是 Lenstra，Lenstra 和 Lovasz 提出的格基归约算法，第二节给出了已知参数 a,b,c,M 恢复初值 x_1,x_2 的综合算法。第三节给出了已知参数 $b,c=0$，恢复参数 a,M 及初值 x_1,x_2 的综合算法。以上算法都是多项式时间算法。

二、已知参数 a,b,c,M 的综合算法

设已知参数 $a,b,c,M\in Z,2^{n-1}\leqslant M<2^n$，及 M 的二进制表示是 n 位，序列$\{x_i\}$由同余式

$$x_{i+2}\equiv ax_{i+1}+bx_i+c(\mathrm{mod}\ M) \qquad (*)$$

产生，m 是正整数，$1\leqslant m<n$ 令 $x_i=2^m y_i+z_i,0\leqslant z_i<2^m$，输出截尾序列$\{y_i\}$，称 $\alpha=1-m/n$ 是输出比例。本节给出由已知一段连续的$\{y_i\}$，恢复序列$\{x_i\}$，即 x_1,x_2 的算法。归结为求解 z_1,z_2 的算法，如不特别声明，本文将在整数上讨论。

将 $x_i=2^m y_i+z_i,i=1,2,3,4$。代入式(*)，得到一个整数规划问题：

$$\begin{cases} az_2+bz_1-z_3+Mp_1=Y_1 \\ az_3+bz_2-z_4+Mp_2=Y_2 \\ 0\leqslant z_i<2^m \\ p_1,p_2\text{ 为整数},i=1,2,3,4 \end{cases} \qquad (1)$$

其中 $Y_i=2^m(y_{i+2}-ay_{i+1}-by_i)-c,i=1,2$。

利用 Kannan 算法[1]可以对式(1)求整根。该算法解决了下述的整数规划问题：给定整数矩阵 $A_{m\times n}$和 $b_{m\times 1}$，求满足 $AX\leqslant b$ 的整数解 $X=(x_1,\cdots,x_n)^T$。如果变量个数 n 固定，则 Kannan 算法的运行时间为 $O(n^{9n}L\log L)$。其中 L 表示输入数据的长度。这里 $L=mn\log(a+2)$，其中 a 表示矩阵 $A_{m\times n}$和 $b_{m\times 1}$系数中最大的绝对值数。

显然，如果 z_1,z_2,z_3,z_4 是由式(*)产生的，则必为式(1)的解。一般说来解不是唯一的。以下研究使解唯一的条件。

令 $B_M=\{0\leqslant a\leqslant M-1:\exists\ (u,v),0\leqslant u<L=2^m,|v|<L$，且 u,v 不同时为零，

$$|av+bu\ \mathrm{mod}\ M|<L,|(a^2+b)v+abu\ \mathrm{mod}\ M|<L\}$$

$$S_M=\{0,1,2,\cdots,M-1\}-B_M$$

易知，如果 $a\in S_M$ 则式(1)至多产生一个解，且有解时 Kannan 算法可以找到该解。

显然 $a\notin S_M$ 当且仅当 $a\in B_M$ 当且仅当下列整数规划问题有整数解(u,v,p_1,p_2)且 $uv\neq 0$。

$$\begin{cases} 0\leqslant u<L \\ |v|<L \\ -L<av+bu+p_1M<L \\ -L<(a_2+b)v+abu+p_2M<L \end{cases} \qquad (2)$$

算法 1

(1) 输入 a,b,c,M,y_1,y_2,y_3,y_4，检验 a 是否属于 S_M，即用 Kannan 算法判定整数规划问题(2)是否有整数解。

(2) 如果 $a\in S_M$，则用 Kannan 算法解式(1)，得到一个正确(唯一)解，否则算法无效。

下面估计$|B_M|$。给定一组(u,v)，以下总假设 $0<u<L,0<|v|<L$。

令

$$B_{(u,v)}=\{0\leqslant a\leqslant M-1:\ |av+bu\ \mathrm{mod}\ M|<L,\ |(a^2+b)v+abu\ \mathrm{mod}\ M|<L\}$$

$$B_{(o,v)}=\{0\leqslant a\leqslant M-1:\ |av\ \mathrm{mod}\ M|<L,\ |(a^2+b)v\ \mathrm{mod}\ M|<L\}$$