文章编号:1001 - 2486(2003)05 - 0103 - 06

一类基于 m 序列的非线性序列生成器*

黄建忠,李　超,项攀攀
(国防科技大学理学院,湖南 长沙　410073)

摘　要:构造了一类非线性序列生成器,其生成的序列周期长,线性复杂度高,且可控制。分析表明在满足一定条件下,它具有很高的安全性,适于做密钥流生成器。

关键词:线性复杂度;周期;密码分析;序列密码
中图分类号:TN918　　**文献标识码**:A

A Class of Nonlinear Sequence Generators Base on m Sequence

HUANG Jian-zhong, LI Chao, XIANG Pan-pan
(College of Science, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: A class of nonlinear sequence generators of long period and high linear complexity are constructed. It is shown that linear complexity and period can be determind. And they are safe if some conditions are given. So they can be used as the key sequence generators.

Key words: linear complexity; period; analysis of cryptology; sequence cryptology

近20年来,序列密码作为密码学的一个重要分支,得到了广泛的研究和分析。如何构造线性复杂度高、周期大的密钥流序列,对于序列密码体制的研究和应用具有重要意义。密钥流序列由密钥流生成器产生,常见的有:(非)线性反馈移位寄存器、前馈序列产生器、非线性组合序列产生器、钟控序列生成器等。本文对一类适于做密钥流生成器的非线性序列生成器的构造和分析进行了研究。

1　预备知识

在非线性序列生成器的构造之前,先给出本文需要用到的一些定义和结论。

定义1　设 M, q 均是正整数,q 为奇数,而 $m_{t_0}(0 \leqslant t_0 < q-1)$ 是一组非负整数。任给 $t \in N$,当 $t = t_0 + kq$ 时,定义:$m_t = m_{t_0+kq} = m_{t_0} + kM$,其中 $k \in N$,则称 $\{m_t\}$ 是模 M,周期为 q 的下标函数,简称下标函数。而 M 称为 $\{m_t\}$ 的模,q 称为 $\{m_t\}$ 的周期。

定义2　设 $\{m_t\}$ 是模 M,周期为 q 的下标函数,$\{y_t\}$ 是二元周期序列,令:$u_t = y_{m_t}, 0 \leqslant t < \infty$,称 $\{u_t\}$ 是 $\{y_t\}$ 相应于 $\{m_t\}$ 的下标序列,简称下标序列。

定义3　设 s^∞ 是 $GF(q)$ 上周期为 p 的序列,定义 s^∞ 的重量复杂度和球体复杂度分别为:

$$WC_u(s^\infty) = \min_{W_H(t^p)=u,\, per(t^\infty)=p} L(S^\infty + t^\infty), \quad SC_u(s^\infty) = \min_{0 \leqslant W_H(t^p) \leqslant u,\, per(t^\infty)=p} L(S^\infty + t^\infty)$$

其中 t^p 表示 t^∞ 的第一个周期段。

引理1[3]　设 $f(x) = c_0 + c_1 x + \cdots + c_n x^n (c_0 = 1, c_n = 1)$ 是 $GF(2)$ 上的 n 次既约多项式,而 β 为 $f(x)$ 在 $GF(2^n)$ 中的一个根。对于 $\{a_k\} \in G(f)$,如果 $\{a_k\}$ 的 s - 采样序列 $\{a_{sk}\}$ 为非零序列,则 $\{a_{sk}\}$ 的极小多项式即为 β^s 的极小多项式 $f_s(x)$,并且 $p(\{a_{sk}\}) = p(f_s)$。由于 $p(f)$ 即为 β 之级,而 $p(f_s)$ 即为

* 收稿日期:2003 - 04 - 08
基金项目:东南大学移动通信国家重点实验室开放基金项目(A0101);国防科技大学基础研究基金项目(JC02 - 02 - 007)
作者简介:黄建忠(1973—),男,助理研究员,硕士生。

β^r 之级，因此，$p(\{a_{sk}\}) = p(f_s) = \frac{p(f)}{(p(f),s)} = \frac{p(\{a_k\})}{(p(\{a_k\}),s)}$。

引理 2[3] 设$\{a_k\}$是周期为 p 的m序列，则$\{a_k\}$的 s - 采样序列$\{a_{sk}\}$仍是周期为 p 的m序列的充要条件是$(p,s) = 1$。

引理 3[3] 设$\{a_k\}$是周期为 p 的m序列，且有正整数 s_1, s_2，使$(p,s_1) = 1, (p,s_2) = 1$。则m序列$\{a_{t_1 k}\}$与$\{a_{t_2 k}\}$平移等价的充要条件是存在整数 $r(0 \leqslant r \leqslant n-1)$，使得 $s_2 \equiv 2^r s_1 (\mathrm{mod} p)$ 成立。

由有限域的知识知，二元域上 n 次本原多项式的个数有$\phi(2^n - 1)/n$个，其中 $\phi(\cdot)$ 为 Euler 函数。而上面的引理告诉我们，要得到周期为 $p = 2^n - 1$ 的全部彼此移位不等价的m序列，只须先找出一个周期为 p 的m序列，然后从它的每一个陪集中选一个代表元素作为采样间隔，这样就得到同周期且两两彼此移位不等价的m序列组。随着 n 的增大，$\phi(2^n - 1)/n$ 个数也大大增加。这样为构造非线性序列生成器提供了充分的保证。

2 构造与结论

2.1 构造描述

构造的非线性序列生成器示意图如图 1 所示。

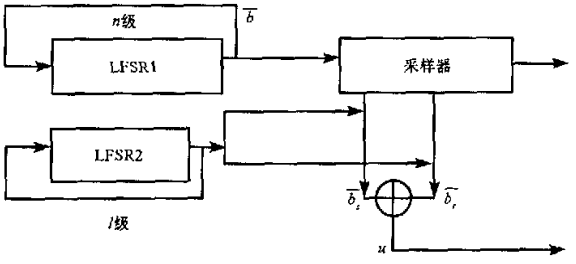

图 1 非线性序列生成器

Fig.1 Nonlinear sequence generators

图 1 中，LFSR1 为 n 级m序列；LFSR2 为 $l(l \geqslant n)$ 级m序列，其输出连续 h 比特中前 z 比特(本文 z 取 1 比特) 用来控制采样序列；前 x 比特用来控制采样序列移位的位数，用 $bc = \sum_{i=0}^{x-1} x_i 2^i + 1$ 表示，其中 x_i 表示 x 比特中第 i 比特的值。具体来说就是假定 $\bar{b}_s, \bar{b}_r$ 分别为 LFSR1 的 s, r 采样 n 级m序列，且互不平移等价，已经预先选择确定。若 LFSR2 输出 h 比特中 z 比特值为 1，则 $\bar{b}_s$ 移位 bc 位；否则 $\bar{b}_r$ 移位 bc 位。$\bar{b}_s, \bar{b}_r$ 的移位输出之和作为非线性序列 u 的输出。

若用 $b_s(t), b_r(t)$ 表示采样序列 $\bar{b}_s, \bar{b}_r$ 在 t 时刻的输出值，$x(t)$ 表示 x 比特在 t 时刻的状态值，$z(t)$ 表示 z 比特在时刻 t 的状态值，则非线性序列 u 在 t 时刻的输出可表示如下：

$$u(h,t) = u(x,z,t) = \begin{cases} b_s(i+t) \oplus b_r(t), (1 \leqslant i \leqslant x(t)+1), z(t) = 1 \\ b_r(i+t) \oplus b_s(t), (1 \leqslant i \leqslant x(t)+1), z(t) = 0 \end{cases} \tag{1}$$

2.2 周期和线性复杂度

先给出几个需要用到的定理。为方便起见，用符号 $\gcd(a,b) = c$ 表示 a, b 的最大公因子为 c，以下同。

引理 4 设$\{m_t\}$是模 M 周期为 q 的下标函数，$\{y_t\}$是 n 级m序列，$\gcd(M, 2^n - 1) = d$，$\{u_t\}$是相应的下标序列，其周期为 T，线性复杂度为 L。则有 $dT \mid q(2^n - 1), (2^n - 1) \mid Td, L \leqslant qn$。

证明： 设 $f(x) = \prod_{i=0}^{n-1} (x - \alpha^{2^i})$ 为$\{y_t\}$的极小多项式，其中 α 是其一个本原根；再设 $h(x)$ 为$\{y_t\}$

的 M - 采样序列的极小多项式。

(Ⅰ)当 $d=1$ 时,此时命题即为文献[1]的定理1。

(Ⅱ)当 $d>1$ 时,则由引理2知 $h(x)$ 不是 n 级m序列。设其级数为 m,周期为 e,则由引理1知,$m<n$,$e=(2^n-1)/d$。由多项式的根表示,我们有 $h(x)=\prod_{i=0}^{m-1}(x-\alpha^{M2^i})$。则此时下标序列 $\{u_t\}$ 的生成多项式 $h(x^q)=\prod_{i=0}^{m-1}(x^q-\alpha^{M2^i})$。其余证明过程类似于(Ⅰ)的证明,即有:$T\mid qe$,$(2^n-1)\mid Td$,$L\leqslant qm$。

引理5[1] 设 $\{m_t\}$ 是模 M 周期为 q 的下标函数,$\{y_t\}$ 的极小多项式 $f(x)$ 满足:(1)$f(x)$ 的指数为 p,阶为 n;(2)$\gcd((q,2^n-1)/p)=1$,q 的素因子亦为 2^n-1 的素因子;(3)$\gcd(M,p)=1$。则下标序列 $\{u_t\}$ 的周期 $T=qp$,线性复杂度 $L=qn$。

引理6[2] 设 $s_1^\infty,\cdots,s_k^\infty$ 为 $GF(q)$ 上的 k 个周期序列,且 $r_{s1}(x)/f_{s1}(x),\cdots,r_{sk}(x)/f_{sk}(x)$ 分别为它们生成函数的既约有理分式表示;再设 $t^\infty=\sum_{i=1}^{k}s_i^\infty$ 为这 k 个序列的和序列。命:$g(x)=\sum_{j=1}^{k}r_{sj}(x)\prod_{i\neq j}f_{si}(x)$,$f(x)=\prod_{i=1}^{k}f_{si}(x)$,则有:

(1) $f_t(x)=f(x)/\gcd(f(x),g(x))$;

(2) $per(t^\infty)=ord(f/\gcd(f,g))\leqslant lcm[per(s_1^\infty),\cdots,per(s_k^\infty)]$,其中等号当 $f_{s1},\cdots,f_{sk}$ 两两互素时成立;

(3) $L(t^\infty)\leqslant\sum_{i=1}^{k}L(s_i^\infty)$,当且仅当 $f_{s1},\cdots,f_{sk}$ 两两互素时等号成立。

由定义2及(1)式易知本文构造的非线性序列为两个下标序列(不妨设为 $\{u_t\}$、$\{v_t\}$)之和序列,其中下标序列是 n 级m序列(不妨设为 $\{y_t\}$)相应于下标函数 $\{m_t\}$ 的下标序列,而下标函数 $\{m_t\}$ 由 l 级m序列和参数 h 所确定。以下总假设 $\{m_t\}$ 的周期为 q,模为 M。

引理7 n,l,x,z,M,q 如前所述,则 $q=2^l-1+\sum_{i=1}^{x}2^{l-2+i}$,$M=2^{l-1}+\sum_{i=1}^{x}2^{l-3+i}$。

证明: (Ⅰ)首先考虑 $x=1$ 时的情形。

我们知道在 l 级m序列的一个周期段 2^l-1 内1有 2^{l-1} 个,0有 $2^{l-1}-1$ 个;而在连续的 2^l-1 比特中,00有 $2^{l-2}-1$ 个,01、10、11有 2^{l-2} 个(见文献[5])。则由(1)式及定义1,有:

$$q=2\cdot 2^{l-2}+2\cdot 2^{l-2}+1\cdot 2^{l-2}+1\cdot(2^{l-2}-1)=2^l-1+2^{l-1}$$

可见,$\{m_t\}$ 的周期比 l 级m序列的周期大 2^{l-1}。同时由定义1知 M 实际上就是在周期 q 内 $\{m_t\}$ 走的次数。而由于在m序列的一个周期段内,1总比0多一个。故 $\{m_t\}$ 走的次数比停的次数多1,也就是有下面关系式:

$$q=2M-1 \tag{2}$$

从而有:

$$M=2^{l-1}+2^{l-2}$$

(Ⅱ)$x>1$ 时,我们不妨把连续的 2^l-1 个 x 比特状态,写成如下矩阵形式:

$$\begin{pmatrix} a_{1,x-1} & & a_{1,0} \\ & \ddots & \\ a_{2^l-1,x-1} & & a_{2^l-1,0} \end{pmatrix}$$

则从纵向看每一列元素均遍历 l 级m序列的一个周期,且各列之间平移等价。

由(Ⅰ)的证明我们知道 $\{m_t\}$ 的周期比 l 级m序列的周期大 2^{l-1},即矩阵第一列(按从右至左的顺序)遍历一个周期后 $\{m_t\}$ 要多走 2^{l-1} 次。则依题意,第二列跑遍一个周期后 $\{m_t\}$ 要多走 $2\cdot 2^{l-1}$ 次,类似地,第 i 列跑遍一个周期后 $\{m_t\}$ 要多走 $2^{i-1}\cdot 2^{l-1}$ 次。故 $\{m_t\}$ 的周期:

$$q = 2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i} \tag{3}$$

再由(2)式,则有:

$$M = 2^{l-1} + \sum_{i=1}^{x} 2^{l-3+i} \tag{4}$$

定理1 $n,l,x,z,M,q,\{u_t\},\{v_t\}$ 如前所述。若 $\gcd(M,2^n-1)=1$,则非线性序列的周期 $T \mid (2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})(2^n-1)$,且 $(2^n-1) \mid T$,线性复杂度 $L \leqslant 2n(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})$。

证明: (Ⅰ)先证明 z 比特取固定值0(或1)时的情况,此时的非线性序列为一条下标序列 $\{u_t\}$(或 $\{v_t\}$)。由引理7,我们有:

$$q = 2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i}, M = 2^{l-1} + \sum_{i=1}^{x} 2^{l-3+i}$$

直接利用引理4即有:

$$T \mid (2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})(2^n-1), (2^n-1) \mid T, L \leqslant n(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i}) \tag{5}$$

(Ⅱ)当 z 变动时,此时的非线性序列为两条下标序列 $\{u_t\}$、$\{v_t\}$ 之和。由于两条采样序列均为 n 级m序列,因此由(*I*)的证明知下标序列 $\{u_t\}$、$\{v_t\}$ 的周期和线性复杂度均满足(5)式。再由引理6即得:

$$T \mid (2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})(2^n-1), (2^n-1) \mid T, L \leqslant 2n(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})$$

定理2 $n,l,x,z,M,q,\{u_t\},\{v_t\}$ 如前所述。若满足:(1)q 的素因子都是 2^n-1 的素因子;(2)$\gcd(M,2^n-1)=1$;(3)设 $\{u_t\},\{v_t\}$ 的极小多项式分别为 $g(x),h(x)$,且 $\gcd(g(x),h(x))=1$。则非线性序列的周期 $T = (2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})(2^n-1)$,线性复杂度 $L = 2n(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})$。

证明: 由题设条件(a)、(b)知,引理5的条件满足,故此时 $\{u_t\}$、$\{v_t\}$ 的周期均为 $(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})(2^n-1)$,线性复杂度均为 $n(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})$。

又由条件(3)知,引理6的条件满足,故有:

$$T = (2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i})(2^n-1), L = 2n(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i}) \tag{6}$$

定理3 n,l,x,z 如前所述,$n=l$;LFSR2的两个采样m序列的本原多项式分别为 $f_s(x),f_r(x)$;假定 x 比特状态为固定值 $g(g \geqslant 1)$,记 $h = \gcd(g,2^n-1)$,且当 $g>1$ 时满足两个条件:(1)$\gcd\left(g, \frac{2^{n(2^n-1)}-1}{(2^n-1)^2}\right) = 1$;(2)$g$ 的所有素因子是 $2^{n(2^n-1)}-1$ 的素因子。若 $f_s(x),f_r(x)$ 互反,则非线性序列的周期 $T=(2^n-1)^2 g/h$,线性复杂度 $L = n(2^n-1)g$;否则非线性序列的周期 $T=(2^n-1)^2 g/h$,线性复杂度 $L = 2n(2^n-1)g$。

证明: (Ⅰ)先证 $g=1$ 时的情形。此时的非线性序列相当于两个"停走"发生器[8]之和序列,不妨设其为 $\{u_t\}$、$\{v_t\}$。此时 $\{u_t\}$、$\{v_t\}$ 的母函数可表示成如下既约有理形[2]:

$$u^{\infty}(x) = g_r(x)/f_r^*(x^{2^n-1}), v^{\infty}(x) = g_s(x)/f_s(x^{2^n-1})$$

其中 f^* 表示 f 的互反多项式;且 $ord(f_s(x^{2^n-1})) = ord(f_r^*(x^{2^n-1})) = (2^n-1)^2$。则:

$$(u+v)^{\infty}(x) = \frac{g_r(x)f_s(x^{2^n-1}) + g_s(x)f_r^*(x^{2^n-1})}{f_s(x^{2^n-1})f_r^*(x^{2^n-1})}$$

由于 $u^{\infty}(x),v^{\infty}(x)$ 既约,故 $\gcd(g_r(x),f_r^*(x^{2^n-1}))=1, \gcd(g_s(x),f_s(x^{2^n-1}))=1$。

若 $f_s(x),f_r(x)$ 不互反,则显然有 $f_s(x^{2^n-1}) \neq f_r^*(x^{2^n-1})$。此时易知 $(u+v)^{\infty}(x)$ 亦为既约有理形,

从而 $f_r(x^{2^n-1})f_r^*(x^{2^n-1})$ 为非线性序列的极小多项式,其周期 $T=(2^n-1)^2$,线性复杂度 $L=2n(2^n-1)$。

否则,此时 $(u+v)^m(x)=\dfrac{g_r(x)+g_s(x)}{f_t(x^{2^n-1})}$ 为既约有理形,从而 $f_t(x^{2^n-1})$ 为非线性序列的极小多项式,其周期 $T=(2^n-1)^2$,线性复杂度 $L=n(2^n-1)$。

(Ⅱ)当 $g>1$ 时,把序列 $\{u_t\}$ 写成 g 列宽的矩阵,则每一列都是一个由 $f_r(x)$ 的 g - 采样产生的序列。设其极小多项式为 $f_{ug}(x)$,则 $\{u_t\}$ 的生成多项式为 $f_{ug}(x^g)$。类似地可得 $\{v_t\}$ 的生成多项式为 $f_{vg}(x^g)$。其余证明过程类似(Ⅰ),只需应用引理1和Dickson引理[4]的结论即可得证。

从上面几个定理可以看出,非线性序列生成器的周期和线性复杂度与两个LFSR的级数、h 比特状态都有关,并随之增加而呈指数增长。且由(6)式知其周期和线性复杂度是可以控制的。

3 密码分析

假设级数为 n 的本原多项式有 R_n 个,周期为 T_n;级数为 l 的本原多项式有 R_l 个,周期为 T_l;令 $y=\phi(2^n-1)/n$,则从 y 个分园陪集中选择两条采样序列有 C_y^2 种可能;现假定 x 已知,则本文构造的非线性序列的密钥量 $=T_nR_nT_lR_lC_y^2$。例如取 $n=l=64$,则其密钥量超过 2^{128} 这种数量级,若去穷举攻击,则几乎不可能。

为了考察非线性序列的安全性,不妨退一步,看看限制 x,z 的变化时,非线性序列的安全性如何。当 z 固定时,这是一种极端退化情形,此时输出序列仍为m序列,因此没有安全性可言;当 x 固定,z 变化时,此时有定理3的结论。且当两个采样序列的反馈多项式互反时,此时非线性序列生成器退化为 $KM\overline{M}$ 生成器[9]。文献[10]指出只要 K,M 的级数相等,则它是安全的,是一种理想的伪随机序列生成器。由此可见,在退化情形,只要 z 不固定;或者当 x 固定,z 变化时,让两个LFSR的级数取相等,则非线性序列仍然是安全的。

3.1 DC攻击

DC[6]攻击这种思想是Siegenthler于1983年提出的,主要针对非线性组合流密码。它是一种唯密文攻击,通过计算LFSRi的输出序列与密文序列之间的相关度来提取LFSRi子密钥的信息。它对级数较小的LFSR才有可能成功。

为了说明问题,我们做了许多模拟试验,用生成的非线性序列 u 与LFSR1、LFSR2产生的m序列作符合,统计其符合优势。因为DC攻击能否成功的关键是看符合率,若偏离50%较多的话,有望成功;否则很难成功。但统计结果表明符合率均接近50%,因此要想从 u 中提取LFSR1和LFSR2的信息是很难的。即本文构造的非线性序列能抵抗DC攻击。表1是随机抽取出的部分试验结果,表示 x 分别取1、2和3时产生的非线性序列 u 与两个LFSR之间的符合率,其中两个LFSR均为7级m序列。

表1 u 与 *LFSR1*、*LFSR2* 的符合率

Tab.1 The correlation between u and LFSRi($i=1,2$)

符合率	LFSR1	LFSR2
$X=1$	0.497382	0.497712
$X=2$	0.499716	0.498729
$X=3$	0.499610	0.498952

3.2 BAA攻击

BAA攻击[12]实质为最佳仿射逼近分析的推广,是丁存生等于1987年提出的。其思想是利用有关密码系统的信息构造一个新的级数不超过 $\sum r_i$ 的线性反馈移存器,以它来近似代替原密码系统生成器。

本质上是用低复杂度去逼近高复杂度序列。能否成功得看最大谱值的大小。若足够大，可望成功。若不够大，还得花足够的计算代价去构造出产生密钥流序列的 LFSR。在分析本文的非线性序列之前，先给出其重量复杂度和球体复杂度的下界。

引理 8[2] 设 s^∞ 是 $GF(q)$ 上周期为奇数的序列，则：

$$WC_k(s^\infty) \geqslant [N/k] - \deg(f_s), SC_k(s^\infty) \geqslant [N/k] - \deg(f_s)$$

其中 f_s 为序列 s^∞ 的极小多项式，N 不一定是最小周期。

定理 4 在满足定理 2 条件情况下，有：

$$WC_k(s^\infty) \geqslant \left[\left(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i}\right)(2^n - 1)/k\right] - 2n\left(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i}\right)$$

$$SC_k(s^\infty) \geqslant \left[\left(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i}\right)(2^n - 1)/k\right] - 2n\left(2^l - 1 + \sum_{i=1}^{x} 2^{l-2+i}\right)$$

证明： 由引理 8 和定理 2 易证(略)。

这个定理告诉我们，只要 $k < \lfloor (2^n - 1)/4n \rfloor$，则在非线性序列每个周期段的对应位置上任意改变不超过 k 个比特，都不会使序列的复杂度降低。也就是说，这种序列的线性复杂度稳定性在流密码学意义下较为理想，从而 BBA 攻击很难见效。

4 结 论

构造了一类非线性序列生成器，具有可控制的周期和线性复杂度。分析表明，只要 LFSR 的级数和参数 h 满足一定条件，则其周期和线性复杂度可以达到很大，且具备较强的抵抗 DC 攻击和 BBA 攻击的能力，因而它是安全的，适于做密钥流序列。

参 考 文 献：

[1] 李献刚，王增法，肖国镇.一类伪随机采样序列的复杂度[J].通信学报，1990，11(2)：1 - 6.

[2] 丁存生，肖国镇.流密码学及其应用[M].北京：国防工业出版社，1994.

[3] 肖国镇，梁传甲，王育民.伪随机序列及其应用[M].北京：国防工业出版社，1985.

[4] Dickson. Linear Groups with an Exposition of Galois Field Theory[M]. Springer, 1990(Dover Publ, 1958).

[5] 万哲先.代数与编码[M].北京：科学出版社，1976.

[6] Siegenthaler T. Decrypting a Class of Stream Ciphers Using Ciphertext only[J]. IEEE Trans. Computers, Jan. 1985, C - 34(1)：81 - 85.

[7] Lidl R, Niederreiter H. Finite Field[M]. Addisonwesley Publishing Company, 1983.

[8] Bell T, Piper F C. The Stop-and-go Generator[A]. Advances in Cryptology-proceedings of EUROCRYPT84. Springer Lecture Notes in Computer Science, 209：88 - 92, 1984.

[9] Gunther C G. A Generator of Psedorandom Sequences with Clock Controlled Linear Feedback Shift Registers[A]. EUROCRYPT87, Extended Abstract, 1987.

[10] 郭宝安.钟控序列分析[J].通信学报，1990，11(6)：50 - 56.