第 34 卷　第 18 期　　　　计　算　机　工　程　　　　2008 年 9 月
Vol.34　　*No.18*　　　　Computer Engineering　　　　September 2008

·安全技术·　　文章编号：1000—3428(2008)18—0179—02　　文献标识码：A　　中图分类号：TP311.12

Galois FCSR 的内部状态分析

薛　帅，戚文峰

(解放军信息工程大学应用数学系，郑州 450002)

摘　要：研究Galois FCSR状态序列的周期与互补性质及进位序列的互补性质。根据周期序列与有理数 2-adic表达之间的关系，证明l-序列的状态序列是准周期的，且其周期与l-序列的周期相同。分析以q为极小连接数的l-序列a的状态序列$s=(s_0, s_1,\cdots, s_n)$及进位序列$c=(c_0, c_1,\cdots, c_n)$，证明若s在t时刻进入周期，则$i\geq t$时，$s_i+s_{i+T/2}=\sum_{j=0}^{r-1}2^j$，$c_i+c_{i+T/2}=q-\sum_{j=0}^{r-1}2^j$，其中，$T=\mathrm{per}(a)$, $r=\lfloor \mathrm{lb}(q+1)\rfloor$。

关键词：周期互补序列；状态序列；进位序列

Inner State Analysis of Galois FCSR

XUE Shuai, QI Wen-feng

(Department of Applied Mathematics, PLA Information Engineering University, Zhengzhou 450002)

【**Abstract**】This paper investigates the period and complementarity property of Galois FCSR state-sequence, and the complementarity proterty of carry-sequence as well. By analyzing the relationship between a periodic sequence and the 2-adic expansion of a rational number, it is proved that the state-sequence of an l-sequence is eventually periodic and has the same period as that of the l-sequence. It analyzes an l-sequence a with minimum connection integer q, state-sequence $s=(s_0, s_1,\cdots, s_n)$ and carry-sequence $c=(c_0, c_1,\cdots, c_n)$, and proves that $s_i+s_{i+T/2}=\sum_{j=0}^{r-1}2^j$, $c_i+c_{i+T/2}=q-\sum_{j=0}^{r-1}2^j$ for $i\geq t$, where $T=\mathrm{per}(a)$, $r=\lfloor \mathrm{lb}(q+1)\rfloor$, and t is the time after which s is strictly periodic.

【**Key words**】periodic complementary sequence; state-sequence; carry-sequence

1　概述

带记忆反馈移位寄存器(Feedback with Carry Shift Register, FCSR)[1]是一种新的密钥流生成器，已成为序列密码领域的重要研究对象。

FCSR序列的伪随机特性和以FCSR为源序列生成器的流密码得到广泛发展(如作为欧洲密码标准候选方案的F-FCSR[2])。虽然FCSR输出序列研究具有重要意义，但从序列密码分析角度来看，FCSR结构仍有很多基础特性需要研究。FCSR序列中达到最大周期的序列称为l-序列，它有许多类似m-序列的优良密码性质[3-4]，因此，l-序列的FCSR结构成为研究重点。

设$a=(a_0, a_1,\cdots, a_n)$是一条二元序列，记序列a的 2-adic表示为$\alpha(a)=\sum_{i=0}^{\infty}a_i2^i$，则当且仅当$\alpha(a)$是分母为奇数的有理数时，序列$a$是准周期的，即

$$\alpha(a)=h/q$$

其中，q 为正奇数；h 为整数。

此时 q 是能产生序列 a 的 FCSR 的一个连接数，也称 q 是序列 a 的一个连接数。若 $\gcd(h, q)=1$，则 q 是序列 a 的最小连接数，它是产生序列 a 的最短 FCSR 的连接数。当且仅当$-q<h\leq 0$ 时，序列 a 是严格周期的。

定义[5]　设$q\in Z$为正奇数；$r=\lfloor \mathrm{lb}(q+1)\rfloor$;$q+1=q_12+q_22^2+\cdots+q_r2^r$, $q_i\in\{0, 1\}$且$q_r=1$。连接数为q的Galois FCSR如图 1 所示。其中，$\boxplus$表示整数带进位加法。$s_i, c_j\in\{0, 1\}$, $0\leq i\leq r-1$, $1\leq j\leq r-1$，分别表示Galois FCSR第i级状态寄存器和第j级进位寄存器。令$c_0=0$, $s=\sum_{i=0}^{r-1}s_i2^i$, $c=\sum_{i=0}^{r-1}c_i2^i$，称(s, c)为Galois FCSR的一个状态，Galois FCSR的运行方式如下：设Galois FCSR在时刻t的状态是$(s(t), c(t))$，其中，$s(t)=\sum_{i=0}^{r-1}s_i(t)2^i$; $c(t)=\sum_{i=0}^{r-1}c_i(t)2^i$。记$t+1$ 时刻Galois FCSR的状态为$(s(t+1), c(t+1))$，其中，$s=(s(0), s(1),\cdots, s(n))$为Galois FCSR的状态序列；$c=(c(0),c(1),\cdots, c(n))$为Galois FCSR的进位序列。当 $0\leq i\leq r-2$ 时，$s_i(t+1)=s_{i+1}(t)\oplus c_{i+1}(t)\oplus s_0(t)q_{i+1}$，$c_i(t+1)=s_{i+1}(t)c_{i+1}(t)\oplus s_{i+1}(t)s_0(t)q_{i+1}\oplus c_{i+1}(t)s_0(t)q_{i+1}$；当$i=r-1$ 时，$s_i(t+1)=s_0(t)$。

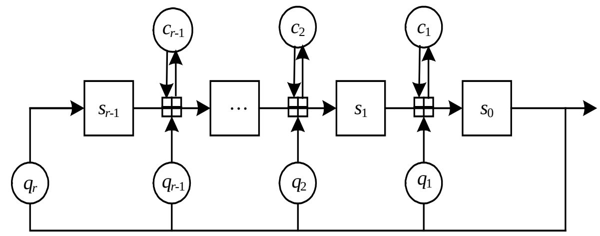

图 1　Galois FCSR 的结构

结论[5]　若已知连接数为q的r级Galois FCSR的状态寄存器和记忆寄存器初态分别是$(s_0, s_1,\cdots, s_{r-1})$和$(c_1, c_2,\cdots, c_{r-1})$，且有

$$h=s_0+(s_1+c_1)\cdot 2+ s_0+(s_1+c_1)\cdot 2^2+\cdots+(s_{r-1}+c_{r-1})\cdot 2^{r-1} \qquad (1)$$

则此Galois FCSR输出序列$b=(b_0, b_1,\cdots, b_n)$的有理表示为

基金项目：国家自然科学基金资助项目(60673081)；国家“863”计划基金资助项目(2006AA01Z417)

作者简介：薛　帅(1982－)，男，硕士研究生，主研方向：密码学；戚文峰，教授、博士生导师

收稿日期：2007-11-22　　**E-mail：**xue.shuai@163.com

$\alpha(b)=-h/q$。

若已知周期序列 b 的有理表示为$-h/q$，则序列 b 可由连接数为 q 的 Galois FCSR 生成，其初始赋值由式(1)确定。

2 Galois FCSR 的相关结论

引理 1[6](l-序列的周期互补性) 设a是以$q=p^e$为连接数的FCSR产生的l-序列，$T=\varphi(q)=p^{e-1}(p-1)$，则序列$a$在一个周期中的前一半恰好是后一半的补，即$a_{i+T/2}=a_i+1$。

定理 1(互补序列所对应有理表示的互补性) 设$a=(a_0, a_1,\cdots, a_n)$是周期为T的严格周期序列，它对应的有理表示为$-h/q$，序列$a'=(a_{T/2}, a_{1+T/2},\cdots, a_{n+T/2})$对应的有理表示为$-h'/q$。若对任意$i\geq 0$都满足$a_i+a_{i+T/2}=1$，则$h+h'=q$。

证明：由$-h/q=\sum_{i=0}^{\infty} a_i 2^i$, $-h'/q=\sum_{i=0}^{\infty} a_{i+T/2}2^i$可得

$$(-h/q)+(-h'/q)=\sum_{i=0}^{\infty}(a_i+a_{i+T/2})2^i=\sum_{i=0}^{\infty}2^i=-1$$，即$h+h'=q$。

根据文献[2]关于 Galois FCSR 状态寄存器比特序列有理表示的有关结论可以证明，当 Galois FCSR 产生 l-序列时，其每级状态寄存器比特产生的序列都是准周期 l-序列。

引理 2[2] 设$s_i=(s_i(t))_{t\geq 0}$, $0\leq i\leq r-1$ 是以连接数为q的Galois FCSR的第i级状态寄存器产生的序列，则存在整数h_i，使序列s_i的有理表示为$-h_i/q$，其中，$h_{r-1}=-qs_{r-1}(0)+2h_0$；当$q_i=0$时，$h_{i-1}=-qs_{i-1}(0)+2h_i$, $1\leq i\leq r-2$；当$q_i=1$时，$h_{i-1}=-q(s_{i-1}(0)+2c_{i-1}(0))+2(h_i+h_0)$, $1\leq i\leq r-2$。

推论 若连接数为q的Galois FCSR生成l-序列，则每级状态寄存器产生的序列$s_i=(s_i(t))_{t\geq 0}$, $0\leq i\leq r-1$都是准周期的l-序列，且其连接数为q的因子。

证明：记第i级状态寄存器输出序列s_i的有理表示为$-h_i/q$, $0\leq i\leq r-1$，因为Galois FCSR的输出序列为l-序列s_0，所以$0<h_0<q$且$\gcd(h_0, q)=1$。由引理 2 可知

$$h_{r-1}=-qs_{r-1}(0)+2h_0 \tag{2}$$

当 $2\leq i\leq r-1$ 时，若$q_i=0$，则

$$h_{i-1}=-qs_{i-1}(0)+2h_i \tag{3}$$

若$q_i=1$，则

$$h_{i-1}=-q(s_{i-1}(0)+2c_{i-1}(0))+2(h_i+h_0) \tag{4}$$

下文将证明$h_j\neq 0 \pmod q$, $1\leq j\leq r-1$，即证明$s_i\neq 0=(0, 0,\cdots, 0)$且$s_i$周期部分非全 1 序列。

由式(2)可知$h_{r-1}\equiv 2h_0 \bmod q$，又因为$\gcd(h_0,q)=1$，所以$h_{r-1}\neq 0 \bmod q$。

若 $1\leq k\leq r-2$，由式(3)、式(4)可知

$$h_k=q_{k+1}[-q(s_{i-1}(0)+2c_{i-1}(0))+2(h_i+h_0)]-(q_{k+1}-1)[-qs_{i-1}(0)+2h_i]$$

简化后可得整数 m 满足

$$h_k=mq+2h_{k+1}+2q_{k+1}h_0 \qquad 1\leq k\leq r-2 \tag{5}$$

由式(5)、式(2)可得整数 n 满足

$$h_k=nq+(2^{r-k}+2^{r-k-1}q_{r-1}+\cdots+2q_{k+1})h_0=nq+2^{-k}(2^r+2^{r-1}q_{r-1}+\cdots+2^{k+1}q_{k+1})h_0$$

从而可得

$$h_k\equiv 2^{-k}(2^r+2^{r-1}q_{r-1}+\cdots+2^{k+1}q_{k+1})h_0 \bmod q \tag{6}$$

因为 $0<2^r+2^{r-1}q_{r-1}+\cdots+2^{k+1}q_{k+1}<q$，又$\gcd(h_0, q)=1$, $\gcd(2, q)=1$，所以由式(6)可知$h_k\neq 0 \pmod q$, $1\leq k\leq r-2$。

记h_j'/q'表示h_j/q的既约分数，其中，$1\leq j\leq r-1$，则$q'|q$且$\gcd(h_j', q')=1$。设$q=p^e$，则存在e_j, $1\leq e_j\leq e$，使$q'=p^{e_j}$，可得a_j是以$q'=p^{e_j}$为连接数的准周期l-序列。

定理 2 若连接数为q的Galois FCSR生成l-序列，那么它的状态序列$s=(s(0), s(1),\cdots, s(n))$是准周期序列，其周期$\mathrm{per}(s)=\varphi(q)$。若周期为$s$，则$s(t)+s(t+\varphi(q)/2)=\sum_{i=0}^{r-1}2^i$。

证明：设序列$s_i=(s_i(t))_{t\geq 0}$在$t_0\geq N_i(0\leq i\leq r-1, N_0=0)$时进入周期状态，则当$t_1\geq r\cdot\max_{0\leq i\leq r-1}\{N_i\}$时，$s$进入周期状态。由状态序列的定义可知$s=\sum_{i=0}^{r-1}2^i s_i$。

设$q=p^e$，由推论可知

$\mathrm{per}(s_i)=\varphi(p^{ei})$, $1\leq e_i\leq e$, $1\leq i\leq r-1$

因为$\varphi(p^{ei})|\varphi(p^e)$，所以

$\mathrm{per}(s)\leq\varphi(q)$

又因为$\mathrm{per}(s)\geq\mathrm{per}(s \bmod 2)=\mathrm{per}(s_0)=\varphi(q)$，所以

$\mathrm{per}(s)=\varphi(q)$

对任意$t\geq t_1$，有

$$s(t)+s(t+\varphi(q)/2)=\sum_{i=0}^{r-1}s_i(t)2^i+\sum_{i=0}^{r-1}s_i(t+\varphi(q)/2)2^i=\sum_{i=0}^{r-1}(s_i(t)+s_i(t+\varphi(q)/2))2^i$$

因为$\mathrm{per}(s_i)=\varphi(p^{ei})$, $1\leq e_i\leq e$, $e_0=e$, $0\leq i\leq r-1$，所以

$s_i(t)+s_i(t+\varphi(q)/2)=s_i(t)+s_i(t+p^{e-ei}\varphi(p^{ei})/2)$

又因为p^{e-ei}为奇数，且由引理 1 可知，s_i在周期状态具有周期互补性，根据推论可得$s_i(t)+s_i(t+p^{e-ei}\varphi(p^l)/2)=s_i(t)+s_i(t+\varphi(p^l)/2)=1$，所以

$$s(t)+s(t+\varphi(q)/2)=\sum_{i=0}^{r-1}2^i$$

定理 3 设以 q 为连接数的 Galois FCSR 生成 l-序列，周期为 T，记$(s(t), c(t))$表示 Galois FCSR 在时刻 t 的状态，则当 Galois FCSR 状态序列进入周期循环时，有

$$c(t)+c(t+T/2)=q-\sum_{i=0}^{r-1}2^i$$

证明：设$t\geq t_0$时，Galois FCSR状态序列进入周期循环，时刻t输出序列对应的有理表示为$-h(t)/q$，则由定理 1 可知

$$h(t)=\sum_{i=0}^{r-1}s_i(t)2^i+\sum_{i=0}^{r-1}c_i(t)2^i=s(t)+c(t)$$

$h(t+T/2)=s(t+T/2)+c(t+T/2)$

根据定理 1 有 $h(t)+h(t+T/2)=q$，可得

$s(t)+s(t+T/2)+c(t)+c(t+T/2)=q$

根据定理 2 有$s(t)+s(t+T/2)=\sum_{i=0}^{r-1}2^i$，可得

$$c(t)+c(t+T/2)=q-\sum_{i=0}^{r-1}2^i$$

3 结束语

本文对状态序列 s 和进位序列 c 的分析可以作为 F-FCSR 类似序列分析的部分依据。如果把生成 l-序列的 Galois FCSR 看作一个序列生成器，则其每个状态寄存器产生的序列都是准周期 l-序列，这可以作为以 q 或 q 因子为连接数的大量 l-序列的一种生成方式。由于 Galois FCSR 被越来越多地应用于流密码设计中，因此需要分析其内部状态。本文只给出了有关 l-序列的部分结论，其他情况的 Galois FCSR 内部状态有待进一步研究。

(下转第 183 页)