本原 σ-LFSR 序列的线性复杂度研究

刘向辉　曾　光　韩文报
（解放军信息工程大学信息工程学院　郑州　450002）

摘　要：线性复杂度是衡量密钥流序列安全性的重要参数。该文考察了有限域上 n 级本原 σ - LFSR 序列的线性复杂度性质。首先得到了它的上下界并证明了界是紧致的，然后利用序列的根表示给出了计算本原 σ - LFSR 序列线性复杂度的方法。

关键词：序列密码；本原 σ - 线性反馈移位寄存器；线性复杂度；根表示
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2009)12-2897-04

Research on Linear Complexity of Primitive σ-LFSR Sequences

Liu Xiang-hui　Zeng Guang　Han Wen-bao
(*Information Engineering Institute*, *PLA Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: Linear complexity is an important parameter of sequences' security. In this paper, the linear complexity properties of primitive σ - LFSR sequences are studied. Firstly, the bounds of the linear complexity for one n stages primitive σ - LFSR sequence is given and it is proved that the bounds are tight; then, with the tool of root representation, a method to get the linear complexity of one primitive σ - LFSR sequence is obtained.

Key words: Stream cipher; Primitive σ - LFSR(Linear Feedback Shift Register); Linear complexity; Root representation

1　引言

序列密码一直被广泛应用于军事和通信领域，有限域上的递归序列具有良好的伪随机性，通常是人们研究的重点。随着现代计算机技术的飞速发展，许多应用要求序列密码能够适合快速软件实现，面向字运算的递归序列研究成为一个热门课题。

Tsaban 和 Vishne 于 2002 年提出了线性变换移位寄存器(TSR)[1, 2]的概念，它是一种基于字的移位寄存器。2004 年提出的 σ - LFSR [3]是对 TSR 的推广，它将易于现代 CPU 高效实现的循环移位操作和字 LFSR 结合而设计。文献[4]将多项式矩阵等理论应用到 σ - LFSR 的研究中，得到了它的状态图圈结构等基本定理和性质，并给出了一类形式简单适合快速软件实现的本原 σ - LFSR 的搜索算法。这些成果都丰富和发展了现代序列密码算法的研究。

在序列密码系统中，线性复杂度是衡量一条密钥流序列强度的重要参数。文献[5]指出，有限域 F_{2^m} 上的 n 级本原 σ - LFSR 序列的线性复杂度为 kn，其中 $1 \le k \le m$。大量实验表明，对于 F_{2^m} 上的所有 n 级本原 σ - LFSR，线性复杂度可以达到最大值，并且达到最大的序列占了多数。在实际应用中，不但要求序列具有大的周期，同时还需要其线性复杂度尽可能大。因此，对本原 σ - LFSR 序列的线性复杂度必须进行更加深刻的分析。

本文第 2 节设定了几个符号并给出必要的准备知识，第 3，4 节得到了主要结果，最后总结了全文。

2　符号及准备知识

首先给出几个符号。

$\underline{s} = s_0, s_1, \cdots$ 为域上序列，s_t 为第 t 时刻输出，$t = 0,1,\cdots$。$\underline{s}_i = s_{i,0}, s_{i,1}, \cdots$：表示序列 $\underline{s}$ 的第 i 条分位序列，$s_{i,t}$ 为第 t 时刻输出，$t = 0,1,\cdots$。$\underline{s}^f = s_0{}^f, s_1{}^f, \cdots$ 为以 $f(x)$ 为极小多项式的序列，$s_t{}^f$ 为第 t 时刻输出，$t = 0,1,\cdots$。$\boldsymbol{A}^{\mathrm{T}}$ 为矩阵或向量 $\boldsymbol{A}$ 的转置。$\mathrm{tr}_1^n(\alpha)$ 为从有限域 F_{2^n} 到其子域 F_2 上的迹函数，迹函数定义如文献[6]。$\mathrm{tr}_1^n(\alpha_0, \alpha_1, \cdots, \alpha_{m-1})^{\mathrm{T}}$ 为向量的迹函数 $(\mathrm{tr}_1^n(\alpha_0), \mathrm{tr}_1^n(\alpha_1), \cdots, \mathrm{tr}_1^n(\alpha_{m-1}))^{\mathrm{T}}$。$\mathbf{Vand}(\lambda_0, \lambda_1, \cdots, \lambda_{m-1})$ 为范德蒙矩阵。

定义 1[3]　设 $\underline{s}$ 是 F_{2^m} 上的 σ-LFSR 序列，视 F_{2^m} 为 F_2 上的 m 维线性空间，$\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ 为其上一组基，则 $\underline{s}$ 可看作 F_2 上的 m 维向量序列，它可写成

$$\underline{s} = \underline{s}_0\alpha_0 + \underline{s}_1\alpha_1 + \cdots + \underline{s}_{m-1}\alpha_{m-1} \tag{1}$$

称二元序列 $\underline{s}_i$ 为 $\underline{s}$ 的第 i 条分位序列，其中 $0 \le i \le m-1$。

2008-12-15 收到，2009-04-27 改回
国家 863 计划项目(2006AA01Z425)和国家自然科学基金(90704003)资助课题

引理 1[3] 若 $\underline{s}$ 是 F_{2^m} 上的 n 级本原 σ-LFSR 序列，则其 m 条分位序列都为 F_2 上的 m-序列且具有相同的极小多项式，即为序列 $\underline{s}$ 极小多项式 $F(x)$的行列式$|F(x)|$。

设 F_{2^m} 上的 n 级本原 σ - LFSR 序列 $\underline{s}$ 极小多项式的行列式为 $g(x)$，它是 F_2 上的一个 mn 次本原多项式，α 为它的一个根。由有限域上 LFSR 序列的迹表示方法[7]，分位序列 $\underline{s}_i$ 的第 t 时刻输出 $s_{i,t}$ 具有表示：$s_{i,t}=\mathrm{tr}_1^{mn}(\beta_i\alpha^t)$，其中 $\beta_i\in F_{2^{mn}}, i=0,1,\cdots,m-1$。

引理 2[8] 设 $\underline{s}$ 是 F_{2^m} 上的序列，则它是 n 级本原 σ - LFSR 序列当且仅当满足

(1) $\underline{s}$ 的 m 条分位序列均为 F_2 上的 m-序列，且具有相同的极小多项式；

(2)设 $\alpha\in F_{2^{mn}}$ 为(1)中极小多项式的一个根，β_i 满足第 i 条分位序列的迹表示，则

$$A=\{\beta_0,\beta_0\alpha,\beta_0\alpha^2,\cdots,\beta_0\alpha^{n-1},\beta_1,\beta_1\alpha,\cdots,\beta_1\alpha^{n-1},\cdots,\beta_{m-1},\beta_{m-1}\alpha,\cdots,\beta_{m-1}\alpha^{n-1}\} \tag{2}$$

构成 $F_{2^{mn}}$ 在 F_2 上的一组基。

3 本原 σ - LFSR 线性复杂度的界

有限域 F_{2^m} 上的 n 级本原 σ - LFSR 序列的线性复杂度为 kn，其中 $1\le k\le m$，本节指出上界 mn 是紧致的。

引理 3[5] 有限域 F_{2^m} 上的 n 级本原 σ - LFSR 序列 $\underline{s}$ 的线性复杂度为 kn，其中 $1\le k\le m$。

显然，当 $\underline{s}$ 为 F_{2^m} 上的 n 级本原 LFSR 序列时，线性复杂度为 n。否则，其线性复杂度大于 n。下述定理 2 说明它可以达到最大值 mn。在此之前，首先证明如下定理。

定理 1 设 $f(x)$为 F_{2^m} 上 n 次本原多项式，α 为 $f(x)$的根，$\gamma_0,\gamma_1,\cdots,\gamma_{m-1}$ 为 F_{2^m} 在 F_2 上的一组基，$\underline{s}=s_0,s_1,\cdots$ 是由 $f(x)$生成的本原序列。在这组基下，视 $\underline{s}$ 为 F_2 上的向量序列，则存在 $\theta_f\in F_{2^{mn}}$ 使得 $s_t=\mathrm{tr}_1^{mn}(\delta_0\theta_f\alpha^t,\delta_1\theta_f\alpha^t,\cdots,\delta_{m-1}\theta_f\alpha^t)^{\mathrm{T}}$，$t=0,1,\cdots$，$\delta_0,\delta_1,\cdots,\delta_{m-1}$ 为 $\gamma_0,\gamma_1,\cdots,\gamma_{m-1}$ 的对偶基。

证明 设 $\underline{s}_i=s_{i,0},s_{i,1},\cdots$ 为 $\underline{s}$ 在基 $\gamma_0,\gamma_1,\cdots,\gamma_{m-1}$ 下的第 i 条分位序列，其中 $0\le i\le m-1$。于是可得 $s_t=s_{0,t}\gamma_0+s_{1,t}\gamma_1+\cdots+s_{m-1,t}\gamma_{m-1}$，$t=0,1,\cdots$。由本原序列的迹表示，存在 $\theta_f\in F_{2^{mn}}$ 使得 $s_t=\mathrm{Tr}_m^{mn}(\theta_f\alpha^t)$，即 $\mathrm{Tr}_m^{mn}(\theta_f\alpha^t)=s_{0,t}\gamma_0+s_{1,t}\gamma_1+\cdots+s_{m-1,t}\gamma_{m-1}$。由对偶基的定义，$s_{i,t}=\mathrm{Tr}_1^m(\delta_i\mathrm{Tr}_m^{mn}(\theta_f\alpha^t))=\mathrm{Tr}_1^{mn}(\delta_i\theta_f\alpha^t)$。于是，$s_t=(s_{0,t},s_{1,t},\cdots,s_{,t})^{\mathrm{T}}=\mathrm{tr}_1^{mn}(\delta_0\theta_f\alpha^t,\delta_1\theta_f\alpha^t,\cdots,\delta_{m-1}\theta_f\alpha^t)^{\mathrm{T}}$。当 θ_f 取遍 $F_{2^{mn}}$ 时，即为 $f(x)$ 生成的所有本原序列。 证毕

设 $g(x)=f_1(x)f_2(x)\cdots f_m(x)$ 为 F_2 上的 mn 次本原多项式，其中 $f_i(x)$ 为 F_{2^m} 上的 n 次本原多项式。设 $g(x)$ 的所有根为 $\alpha,\alpha^2,\cdots,\alpha^{2^{mn-1}}$，自然也可记为 $\alpha,\alpha^{1/2},\cdots,\alpha^{1/2^{mn-1}}$。这些根按照 $g(x)$的因子分为 m 类，不妨设 $\alpha^{1/2^{i-1}},\alpha^{1/2^{m+i-1}},\cdots,\alpha^{1/2^{(n-1)m+i-1}}$ 为 $f_i(x)$ 的根。根据定理 1，存在 $\theta_{f_i}\in F_{2^{mn}}$ 使得 $f_i(x)$ 的生成序列 $\underline{s}^{f_i}$ 的第 t 时刻输出具有表示 $s_t^{f_i}=\mathrm{tr}_1^{mn}(\delta_0\theta_{f_i}\alpha^t,\delta_1\theta_{f_i}\alpha^t,\cdots,\delta_{m-1}\theta_{f_i}\alpha^t)^{\mathrm{T}}$。考虑序列 $\underline{s}^{f_2}$ 的第 t 时刻输出 $s_t^{f_2}$，将迹表示展开可得

$$\begin{aligned}s_t^{f_2}&=\mathrm{tr}_1^{mn}(\delta_0\theta_{f_2}(\alpha^{1/2})^t,\delta_1\theta_{f_2}(\alpha^{1/2})^t,\cdots,\delta_{m-1}\theta_{f_2}(\alpha^{1/2})^t)^{\mathrm{T}}\\&=\mathrm{tr}_1^{mn}((\delta_0\theta_{f_2})^2\alpha^t,(\delta_1\theta_{f_2})^2\alpha^t,\cdots,(\delta_{m-1}\theta_{f_2})^2\alpha^t)^{\mathrm{T}}\end{aligned} \tag{3}$$

同理 $f_i(x)$ 生成序列具有表示 $s_t^{f_i}=\mathrm{tr}_1^{mn}((\delta_0\theta_{f_i})^{2^{i-1}}\cdot\alpha^t,(\delta_1\theta_{f_i})^{2^{i-1}}\alpha^t,\cdots,(\delta_{m-1}\theta_{f_i})^{2^{i-1}}\alpha^t)^{\mathrm{T}}$，以上 $1\le i\le m$。

定理 2 在有限域 F_{2^m} 上的所有 n 级本原 σ - LFSR 序列中，必存在线性复杂度为 mn 的序列。

证明 从序列和的角度来证明这个结论。设 $\underline{s}$ 是有限域 F_{2^m} 上的 n 级本原 σ - LFSR 序列，$F(x)$为它的极小多项式。于是，$|F(x)|=f_1(x)f_2(x)\cdots f_m(x)$ 为这条序列在 F_{2^m} 上的零化多项式，从而可设 $\underline{s}=\underline{s}^{f_0}+\underline{s}^{f_1}+\cdots+\underline{s}^{f_{m-1}}$，其中 $\underline{s}^{f_1},\underline{s}^{f_2},\cdots,\underline{s}^{f_m}$ 分别以 $f_1(x),\ f_2(x),\cdots,f_m(x)$ 为极小多项式。又设 $\gamma_0,\gamma_1,\cdots,\gamma_{m-1}$ 为 F_{2^m} 在 F_2 上的一组基，$\delta_0,\delta_1,\cdots,\delta_{m-1}$ 为其对偶基。由式(3)及定理 1，必定存在 $\theta_{f_1},\theta_{f_2},\cdots,\theta_{f_m}\in F_{2^{mn}}$ 使得

$$\begin{aligned}s_t=s_t^{f_1}+s_t^{f_2}+\cdots+s_t^{f_m}=\mathrm{tr}_1^{mn}((&\delta_0\theta_{f_1}+\cdots\\&+(\delta_0\theta_{f_m})^{2^{m-1}})\alpha^t,(\delta_1\theta_{f_1}+\cdots+(\delta_1\theta_{f_m})^{2^{m-1}})\alpha^t,\\&\cdots,(\delta_{m-1}\theta_{f_1}+\cdots+(\delta_{m-1}\theta_{f_m})^{2^{m-1}})\alpha^t)^{\mathrm{T}}\end{aligned} \tag{4}$$

记 $\beta_0=\delta_0\theta_{f_1}+\cdots+(\delta_0\theta_{f_m})^{2^{m-1}},\cdots,\beta_{m-1}=\delta_{m-1}\theta_{f_1}+\cdots+(\delta_{m-1}\theta_{f_m})^{2^{m-1}}$。

不妨设 $\delta_0=1,\delta_1=\lambda,\cdots,\delta_{m-1}=\lambda^{m-1}$，$\lambda$ 为 F_{2^m} 中本原元，同时令 $\theta_1=\theta_{f_1},\theta_2=\theta_{f_2}^2,\cdots,\theta_m=\theta_{f_m}^{2^{m-1}}$，于是可得

$$\begin{cases}\theta_1+\theta_2+\cdots+\theta_m=\beta_0\\ \lambda\theta_1+\lambda^2\theta_2+\cdots+\lambda^{2^{m-1}}\theta_m=\beta_1\\ \quad\vdots\\ \lambda^{m-1}\theta_1+(\lambda^2)^{m-1}\theta_2+\cdots+(\lambda^{2^{m-1}})^{m-1}\theta_m=\beta_{m-1}\end{cases} \tag{5}$$

亦即

$$\mathbf{Vand}(\lambda,\lambda^2,\cdots,\lambda^{2^{m-1}})\begin{bmatrix}\theta_1\\ \theta_2\\ \vdots\\ \theta_m\end{bmatrix}=\begin{bmatrix}\beta_0\\ \beta_1\\ \vdots\\ \beta_{m-1}\end{bmatrix} \tag{6}$$

现只需说明存在一组 $\beta_0,\beta_1,\cdots,\beta_{m-1}$ 使得由其确定的 σ - LFSR 序列是本原的，同时由式(6)所求 $\theta_1,\theta_2,\cdots,\theta_m$ 全部非 0 即可。由于 λ 为 F_{2^m} 中本原元，故可设 $\lambda=\alpha^{2^{mn}-1/2^m-1}$，取 $\beta_0=1,\beta_1=\alpha^n,\cdots,\beta_{m-1}=\alpha^{(m-1)n}$，显然由其做成的集合式(2)构成 $F_{2^{mn}}$ 在 F_2 上的一组基，由引理 2，$\beta_0,\beta_1,\cdots,\beta_{m-1}$ 确定的 σ - LFSR 序列是本原的。此时可解得 $\theta_1\neq 0,\theta_2\neq 0,\cdots,\theta_m\neq 0$，即 $\underline{s}^{f_0}\neq\underline{0},\underline{s}^{f_1}\neq\underline{0},\cdots,\underline{s}^{f_{m-1}}\neq\underline{0}$。故 $\underline{s}$ 为 F_{2^m} 上 m 条极小多项式不同的本原序列之和，其极小多项式即为 m 个本原多项式的乘积，从而序列 $\underline{s}$ 线性复杂度为 mn。　　证毕

在式(6)中，若取 $\beta_0=1,\beta_1=\lambda,\cdots,\beta_{m-1}=\lambda^{m-1}$，则序列线性复杂度为 n，它的极小多项式即为 $f_1(x)$。若取 $\beta_1=1,\beta_2=\lambda^2,\cdots,\beta_m=(\lambda^2)^{m-1}$，它的极小多项式即为 $f_2(x)$。

4　本原 σ - LFSR 线性复杂度的计算

本节利用序列的根表示来计算本原 σ - LFSR 序列的线性复杂度。下面首先给出引理 4，常称之为有限域上 LFSR 序列的根表示定理。

引理 4[7]　设 $g(x)\in F_{2^m}[x]$ 是一个 n 次无重因子多项式，$g(0)\neq 0$，且 $\alpha_0,\alpha_1,\cdots,\alpha_{n-1}$ 为其所有根，则对于 $g(x)$ 生成的序列 $\underline{s}=s_0,s_1,\cdots$，存在唯一一组 $w_0,w_1,\cdots,w_{n-1}\in F_{2^{mn}}$ 使得 $s_t=w_0{\alpha_0}^t+\cdots+w_{n-1}\cdot\alpha_{n-1}^t$，$t=0,1,\cdots$。此时，$g(x)$ 为 $\underline{s}$ 的极小多项式当且仅当所有 $w_i\neq 0$。

对于有限域 F_{2^m} 上的 n 级本原 σ - LFSR 序列 $\underline{s}=s_0,s_1,\cdots$，设其极小多项式的行列式为 $g(x)=f_1(x)f_2(x)\cdots f_m(x)$。视它为 LFSR 序列，则 $g(x)$ 为其特征多项式且无重因子，由引理 4，$\underline{s}$ 具有根表示。而本原 σ - LFSR 序列的分位序列是 m-序列，自然具有根表示，现在从分位序列来考虑 $\underline{s}$ 的根表示。

设 $\alpha_0,\alpha_1,\cdots,\alpha_{mn-1}$ 为多项式 $g(x)$ 的所有根，并设 $\underline{s_i}=s_{i,0},s_{i,1},\cdots$ 为 $\underline{s}$ 的第 i 条分位序列，由引理 4，存在唯一一组 $w_{i,0},w_{i,1},\cdots,w_{i,mn-1}\in F_{2^{mn}}$ 使得 $s_{i,t}=w_{i,0}{\alpha_0}^t+\cdots+w_{i,mn-1}\alpha_{mn-1}^t$，于是本原 σ - LFSR 序列具有如下根表示定理。

定理 3　设线性空间 F_{2^m}/F_2 的一组基为 $\gamma_0,\gamma_1,\cdots,\gamma_{m-1}$，$g(x)=f_1(x)f_2(x)\cdots f_m(x)$ 为 F_{2^m} 上 n 级本原 σ - LFSR 序列 $\underline{s}=s_0,s_1,\cdots$ 极小多项式的行列式。$\alpha_0,\alpha_1,\cdots,\alpha_{mn-1}$ 为 $g(x)$ 的所有根，$\omega_{i,0},\omega_{i,1},\cdots,\omega_{i,mn-1}$ 满足分位序列的根表示，其中 $i=0,1,\cdots,m-1$。则序列 $\underline{s}$ 具有唯一表示：

$$\begin{aligned}s_t=&(w_{0,0}\gamma_0+\cdots+w_{m-1,0}\gamma_{m-1}){\alpha_0}^t+\cdots+\\&(w_{0,mn-1}\gamma_0+\cdots+w_{m-1,mn-1}\gamma_{m-1})\alpha_{mn-1}^t\end{aligned}\tag{7}$$

证明　将分位序列的根表示形式代入计算即可。　　证毕

为方便，记 $\eta_0\triangleq w_{0,0}\gamma_0+\cdots+w_{m-1,0}\gamma_{m-1},\cdots,\eta_{mn-1}\triangleq w_{0,mn-1}\gamma_0+\cdots+w_{m-1,mn-1}\gamma_{m-1}$。

定理 4　设线性空间 F_{2^m}/F_2 的一组基为 $\gamma_0,\gamma_1,\ldots,\gamma_{m-1}$，$\underline{s}$ 为有限域 F_{2^m} 上的 n 级本原 σ - LFSR 序列，$\underline{s_i}$ 满足第 i 条分位序列的迹表示，即引理 2 中条件(2)。则 $\underline{s}$ 线性复杂度为 kn 当且仅当 $\theta_0=\beta_0\gamma_0+\cdots+\beta_{m-1}\gamma_{m-1}$，$\theta_1=\beta_0\gamma_0^{2^{mn-1}}+\cdots+\beta_{m-1}\gamma_m^{2^{mn-1}},\cdots,\theta_{m-1}=\beta_0\gamma_0^{2^{mn-(m-1)}}+\cdots+\beta_{m-1}\gamma_{m-1}^{2^{mn-(m-1)}}$ 这 m 个元素中有 k 个不等于 0。

证明　设 $\underline{s}$ 分位序列的极小多项式为 $g(x)$，$\alpha_0,\alpha_1,\cdots,\alpha_{mn-1}$ 为其所有根，于是它具有定理 3 中式(7)所示根表示形式，由引理 4 判断 $\underline{s}$ 的极小多项式只需判断 $\eta_0,\eta_1,\cdots,\eta_{mn-1}$ 是否为 0 即可。显然，$g(x)=f_1(x)f_2(x)\cdots f_m(x)$，在 $g(x)$ 的所有根中，不妨设 $\alpha_0=\alpha,\cdots,\alpha_{n-1}=\alpha^{2^{m(n-1)}}$ 为 $f_1(x)$ 的根，$\alpha_n=\alpha^2,\cdots,\alpha_{2n-1}=\alpha^{2^{m(n-1)+1}}$ 为 $f_2(x)$ 的根，$\cdots$，$\alpha_{(m-1)n}=\alpha^{2^{m-1}},\cdots,\alpha_{mn-1}=\alpha^{2^{mn-1}}$ 为 $f_m(x)$ 的根，其中 α 为 $g(x)$ 的根。于是，由本原序列根表示定理的证明过程可得

$$\begin{aligned}s_t&=\eta_0{\alpha_0}^t+\eta_1{\alpha_1}^t+\cdots+\eta_{mn-1}\alpha_{mn-1}^t\\&=\mathrm{Tr}_1^{mn}(\eta_0{\alpha_0}^t)+\mathrm{Tr}_1^{mn}(\eta_n{\alpha_n}^t)+\cdots\\&\quad+Tr_1^{mn}(\eta_{(m-1)n}\alpha_{(m-1)n}^t)\end{aligned}\tag{8}$$

由式(8)显然可知：$\eta_{in},\eta_{in+1},\cdots,\eta_{in+n-1}$ 这 n 个值是否为 0 是等价的，其中 $i=0,1,\cdots,m-1$。从而确定序列的线性复杂度只需要判断 $\eta_0,\eta_n,\eta_{2n},\cdots,\eta_{(m-1)n}$ 的值是否为 0 即可。同样由 $\underline{s}$ 分位序列 $\underline{s_i}$ 根表示的过程可知：$w_{i,0}=\beta_i$ 且 $w_{i,n}=(w_{i,0})^2=\beta_i^2,w_{i,2n}=\beta_i^4,\cdots,w_{i,(m-1)n}=\beta_i^{2^{m-1}}$，其中 $i=0,1,\cdots,m-1$。由此可得

$$\left.\begin{aligned}\eta_0&=\beta_0\gamma_0+\cdots+\beta_{m-1}\gamma_{m-1}\\\eta_n&=\beta_0^2\gamma_0+\cdots+\beta_{m-1}^2\gamma_{m-1}\\&\vdots\\\eta_{(m-1)n}&=\beta_0^{2^{(m-1)}}\gamma_0+\cdots+\beta_{m-1}^{2^{(m-1)}}\gamma_{m-1}\end{aligned}\right\}\tag{9}$$

对式(9)两边分别 $2^{mn},2^{mn-1},\cdots,2^{mn-(m-1)}$ 次方可得

$$\left.\begin{aligned}\eta_0&=\beta_0\gamma_0+\cdots+\beta_{m-1}\gamma_{m-1}\\\eta_n^{2^{mn-1}}&=\beta_0\gamma_0^{2^{mn-1}}+\cdots+\beta_{m-1}\gamma_{m-1}^{2^{mn-1}}\\&\vdots\\\eta_{(m-1)n}^{2^{mn-(m-1)}}&=\beta_0\gamma_0^{2^{mn-(m-1)}}+\cdots+\beta_{m-1}\gamma_{m-1}^{2^{mn-(m-1)}}\end{aligned}\right\}\tag{10}$$

记 $\theta_0\triangleq\eta_0,\theta_1\triangleq\eta_n^{2^{mn-1}},\cdots,\theta_{m-1}\triangleq\eta_{(m-1)n}^{2^{mn-(m-1)}}$，结论成立。　　证毕

不妨设 F_{2^m} 在 F_2 上的一组基为 $1,\lambda,\cdots,\lambda^{m-1}$，$\lambda$ 为

F_{2^m} 上的本原元，则有

$$\left.\begin{aligned}\theta_0 &= \beta_0 + \cdots + \beta_{m-1}\lambda^{m-1}\\ \theta_1 &= \beta_0 + \cdots + \beta_{m-1}\lambda^{(m-1)2^{mn-1}}\\ &\vdots\\ \theta_{m-1} &= \beta_0 + \cdots + \beta_{m-1}\lambda^{(m-1)2^{mn-(m-1)}}\end{aligned}\right\} \tag{11}$$

亦即

$$\begin{bmatrix}\theta_0\\ \theta_1\\ \vdots\\ \theta_{m-1}\end{bmatrix} = \mathbf{Vand}(\lambda, \lambda^{2^{mn-1}}, \cdots, \lambda^{2^{mn-(m-1)}})^{\mathrm{T}} \begin{bmatrix}\beta_0\\ \beta_1\\ \vdots\\ \beta_{m-1}\end{bmatrix} \tag{12}$$

因此，给定一条本原 σ - LFSR 序列，只需计算式(12)中矩阵的乘积，然后根据 $\theta_0, \theta_1, \cdots, \theta_{m-1}$ 这 m 个值是否为 0 即可确定其线性复杂度。实际上，此时也确定了该本原 σ - LFSR 序列的极小多项式。

5 结束语

σ - LFSR 基于字设计，适合软件快速实现，为现代序列密码驱动部分的设计提供了更多的选择。线性复杂度是 σ - LFSR 序列的重要密码学性质。本文考察了本原 σ - LFSR 序列的线性复杂度性质，分析了其特点，给出了一个计算本原 σ - LFSR 序列线性复杂度的方法，为在序列密码系统中选取合适的密钥流序列提供了理论依据。

参 考 文 献

[1] Tsaban B and Vishne U. Efficient linear feedback shift registers with maximal period[J]. *Finite Fields and Their Applications*, 2002, 8(2): 256–267.

[2] Dewar Michael and Panario Daniel. Linear transformation shift registers[J]. *IEEE Transactions on Information Theory*, 2003, 49(8): 2047–2052.

[3] Zeng Guang, Han Wen-bao, and He Kai-cheng. High efficiency feedback shift register: σ-LFSR [EB/OL]. Cryptology ePrint Archive, Report 2007/114, http://eprint.iacr.org/2007.

[4] Zeng Guang, He Kai-cheng, and Han Wen-bao. A trinomial type of σ-LFSR oriented toward software implementation. *Science in China Series F*: *Information Sciences*, 2007, 50(3): 359–372.

[5] 曾光. σ- 线性反馈移位寄存器及其在密码学中的应用[D]. [博士论文], 解放军信息工程大学, 2008.

Zeng Guang. σ- Linear feedback shift registers and their applications in cryptography[D]. [Ph.D. dissertation], PLA Information Engineering University, 2008.

[6] Lidi Rudolf and Niederreiter Harald. Finite fields[M]. New Jersey: Addison-Wesley Publishing Company, 1983: 54–62.

[7] 丁石孙. 线性移位寄存器序列[M]. 上海: 上海科学技术出版社, 1982: 31–35.

Ding Shi-sun. Linear Feedback Shift Register Sequences[M]. Shanghai: Shanghai Scientific and Technical Publishers, 1982: 31–35.

[8] 张猛, 曾光, 韩文报, 何开成. 本原 σ-LFSR 序列的迹表示及其应用[J]. 电子与信息学报, 2009, 31(4): 942–945.

Zhang Meng, Zeng Guang, Han Wen-bao, and He Kai-cheng. Trace representation of primitive σ-LFSR sequences and its application[J]. *Journal of Electronics & Information Technology*, 2009, 31(4): 942–945.

刘向辉： 男，1984 年生，硕士生，研究方向为序列密码分析与设计.

曾 光： 男，1980 年生，讲师，研究方向为序列密码.

韩文报： 男，1963 年生，教授，博士生导师，研究方向为密码学和信息安全.