# 本原 σ-LFSR 序列的迹表示及其应用

张 猛 曾 光 韩文报 何开成
(解放军信息工程大学信息工程学院信息研究系 郑州 450002)

**摘 要**：σ-LFSR 是一基于字的 LFSR 模型，它的设计充分利用了现代 CPU 特点，可很好地应用于设计适合快速软件实现的序列密码算法中。而在实际应用中，本原 σ-LFSR 序列具有最核心的作用。该文分析了本原 σ-LFSR 序列的产生条件，利用其迭代关系式和有限域的迹函数，给出了它的具体表达式，从而得到本原 σ-LFSR 序列的迹表示；其次由本原 σ-LFSR 序列的迹表示，给出了一个 σ-LFSR 序列为本原的充要条件。它们为进一步研究本原 σ-LFSR 序列提供了新的工具。

**关键词**：序列密码；σ-LFSR 序列；迹表示；快速软件加密
**中图分类号**：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2009)04-0942-04

# Trace Representation of Primitive σ-LFSR Sequences and Its Application

Zhang Meng Zeng Guang Han Wen-bao He Kai-cheng
(*Department of Information Research*, *Information Engineering University*, *Zhengzhou* 450002, *China*)

**Abstract**: σ-LFSR is a kind of word-oriented LFSR with high efficiency and good cryptographic properties, especially suitable for modern processors. It can be used in stream cipher for fast software implementation. But in practicality, primitive σ-LFSR sequences are of the most importance. Firstly, by the iterative relationship of the primitive σ-LFSR sequences and the trace function in finite fields, the explicit expression of primitive σ-LFSR sequences is presented. Therefore the trace representation is gotten; then a sufficient and necessary condition is obtained due to the trace representation. It can be used to check whether a σ-LFSR sequence is primitive or not. They provide the new tool for further research of primitive σ-LFSR sequences.

**Key words**: Stream cipher; σ-LFSR sequences; Trace representation; Fast software encryption

## 1 引言

序列密码利用不断变化的加密变换对明文消息进行逐字符的加密。由于早先的 CPU 计算能力远远不能满足加密的需求，序列密码算法一般是由硬件做成密码设备或芯片实现。而现代 CPU 技术已经取得了突飞猛进的进展，其计算能力大为增强，密码算法的软件实现速度已大幅提高，序列密码算法的快速软件实现已有了广泛的应用平台。为此，国外著名学者 Preneel 在 1994 年 FSE(Fast Software Encryption Workshop)会议上提出：如何结合并行技术与现代处理器特点，设计基于字的高效安全的序列密码[1]。

2002 年 Tsaban 和 Vishne 提出了 TSR(Linear Transform Shift Register)的概念[2]。TSR 是一种基于字的 LFSR，它将现代处理器特点和字 LFSR 结合而设计，部分解决了 Preneel 的问题。作者分析了其达到最大周期的条件，并给出了一个最大周期 TSR 的搜索算法。随后 Dewar 和 Panario 发现了最大周期 TSR 成对出现的特点，并给出了详细的证明[3]。

近年来，适合软件快速实现的序列密码算法的研究愈来愈受关注。2005 年欧洲的 ECRYPT NoE eSTREAM[4]计划全面征集序列密码算法，在所有征集到的 34 个序列密码算法中有 22 个是作为适合软件快速实现而设计的。所以设计软件快速实现的序列密码算法已成为目前的一个研究热点。

在适合软件实现的现代序列密码中，如 Mugi[5]，Seal[6]，Scream[7]，Rabbit[8]，Helix[9]和 Snow[10,11] 等，可以发现这些序列密码的设计方式都是以字(如 32bit 或 64bit)为基本操作从而达到软件实现的高效，可见基于字的 LFSR 已经成了现代序列密码的重要组成部分，它为序列密码线性驱动部分的设计提供了新的选择。所以，对基于字的 LFSR 进行深入研究有重要的意义。

本文内容安排如下：第 2 节简介 σ-LFSR 模型，第 3 节给出本原 σ-LFSR 序列的迹表示，第 4 节利用迹表示给出一个 σ-LFSR 序列为本原的充要条件，文章的最后总结全文。

## 2 σ-LFSR 模型

σ-LFSR 是一基于字的 LFSR 模型，它的设计充分利用了现代 CPU 的特点。本节简单介绍它的概念，具体可参见文献[12]–文献[14]。

为方便，本文在特征为 2 的域上讨论，本文的所有结论均可平推到特征为 $p$ 的域上。

2008-01-10 收到，2008-05-11 改回
国家 863 计划项目(2006AA01Z425)和国家自然科学基金(90704003)资助课题

σ 表示循环移位算子。循环移位具有良好的密码学性质，并且在软件上非常容易实现。σ -LFSR 设计的主要思想是 LFSR 中添加了 σ 算子，并把它与域上乘法算子结合在一起进行处理。

容易验证，σ 为线性空间 $F_{2^m}/F_2$ 上的一个线性变换。同时任给 $c\in F_{2^m}$，$c$ 可诱导出线性空间 $F_{2^m}/F_2$ 上的一个线性变换 $C$：$F_{2^m}\to F_{2^m}$ $C(\alpha)=c\alpha$，其中 $\alpha\in F_{2^m}$。则 $F_{2^m}[\sigma]$ 为线性空间 $F_{2^m}/F_2$ 上的所有线性变换集合[12]。

记 $F_2$ 上 $m\times m$ 阶矩阵环为 $\boldsymbol{M}_m(\boldsymbol{F}_2)$，由文献[13]，有

$$F_{2^m}[\sigma]\cong \boldsymbol{M}_m(\boldsymbol{F}_2) \tag{1}$$

**定义 1**　设 $c_0(\sigma),c_1(\sigma),\cdots,c_{n-1}(\sigma)\in F_{2^m}[\sigma]$，若 $F_{2^m}$ 上的序列 $s^\infty=s_0,s_1,s_2,\cdots$ 满足关系：

$$s_{i+n}=c_0(\sigma)s_i+c_1(\sigma)s_{i+1}+\cdots+c_{n-1}(\sigma)s_{i+n-1}$$

则称 $s^\infty$ 为 $F_{2^m}$ 上的 $n$ 级 σ-LFSR 序列，称多项式

$$F(x)=x^n+c_{n-1}(\sigma)x^{n-1}+\ldots+c_1(\sigma)x+c_0(\sigma)$$

为 $n$ 次 σ-多项式，它是 $s^\infty$ 的特征多项式。

注意到 $F_{2^m}$ 上 $n$ 级 σ -LFSR 序列 $s^\infty$ 的周期小于等于 $2^{mn}-1$，所以 $2^{mn}-1$ 是可能的最大周期。于是有下面的定义。

**定义 2**　如果 $s^\infty$ 为 $F_{2^m}$ 上的 $n$ 级 σ -LFSR 序列且周期为 $2^{mn}-1$，则称 $s^\infty$ 为本原 σ -LFSR 序列，称其次数最低的特征多项式为本原 σ -多项式。

从伪随机特性和资源利用率的角度看，在实际应用中，本原 σ -LFSR 序列是最重要的。

由式(1)，σ -LFSR 可看作矩阵环上的 LFSR，它是一种最广泛的线性变换寄存器模型。实际上，TSR 是 σ -LFSR 的特例。因为任意 σ -多项式 $F(x)=x^n+c_{n-1}(\sigma)x^{n-1}+\cdots+c_1(\sigma)x+c_0(\sigma)$ 均可对应到一个矩阵多项式，所以也有 $F(x)\in \boldsymbol{M}_m(\boldsymbol{F}_2)[x]$。

## 3　本原σ-LFSR 序列的迹表示

在序列问题中，若能将序列统一的表示为某种形式，对理解和研究它的各种性质无疑大有帮助，比如有限域上 LFSR 序列的迹表示、根表示等。本节利用迹函数给出本原 σ-LFSR 序列的迹表示。

迹函数是研究序列密码的重要工具，令迹函数 $\mathrm{tr}_1^n(\bullet)$ 表示从有限域 $F_{2^n}$ 到其子域 $F_2$ 的映射，定义为 $\mathrm{tr}_1^n(x)=\sum_{i=0}^{n-1}x^{2^i}$，有关迹函数的性质，见文献[15]。

### 3.1 准备工作

首先引入几个符号。

记 $F_{2^m}$ 上的 σ-LFSR 序列全体为 $M$，则

$$M\triangleq\left\{\underline{a}=(a_0,a_1,a_2,\cdots,)\mid a_i\in F_{2^m}\right\}$$

对 $F(x)\in \boldsymbol{M}_m(\boldsymbol{F}_2)[x]$，定义

$$G(F(x))\triangleq\left\{\underline{a}\in M\mid F(x)\underline{a}=0\right\}$$

称 $G(F(x))$ 是 $F(x)$ 的零化空间。它实际上是 $F(x)$ 产生的所有序列集合，设 $n=\deg(F(x))$，则 $G(F(x))$ 可看作 $F_{2^m}$ 上的 $n$ 维线性空间。

设 $\boldsymbol{Y}=\left(y_{m-1},\cdots,y_1,y_0\right)^t\in F_{2^n}^m$，令 $\mathrm{tr}_1^n(\boldsymbol{Y})$ 表示 $\left(\mathrm{tr}_1^n(y_{m-1}),\cdots,\mathrm{tr}_1^n(y_1),\mathrm{tr}_1^n(y_0)\right)^t$。

设 $\boldsymbol{Y}=\left(y_{m-1},\cdots,y_1,y_0\right)^t\in F_{2^n}^m$，$\beta\in F_{2^n}$，令 $\boldsymbol{Y}\bullet\beta$ 表示 $\left(y_{m-1}\beta,\cdots,y_1\beta,y_0\beta\right)^t$。

**定义 3**　$s^\infty$ 是 $F_{2^m}$ 上的 σ-LFSR 序列，若把 $F_{2^m}$ 看作是 $F_2$ 上的 $m$ 维线性空间，设 $\alpha_0,\alpha_1,\cdots,\alpha_{m-1}$ 为 $F_{2^m}$ 在 $F_2$ 上的一组基，则 $s^\infty$ 可看作 $F_2$ 上的 $m$ 维向量序列，它可写成：

$$s^\infty=s_0^\infty\alpha_0+s_1^\infty\alpha_1+\cdots+s_{m-1}^\infty\alpha_{m-1} \tag{2}$$

称二元序列 $s_i^\infty$ 为 $s^\infty$ 的第 $i$ 个分位序列，其中 $0\le i\le m-1$。

**引理 1**[12]　设 $F_{2^m}$ 上 $n$ 级 σ-LFSR 以 $F(x)=x^n+c_{n-1}(\sigma)x^{n-1}+\cdots+c_1(\sigma)x+c_0(\sigma)$ 为特征多项式。设 $C_l=(c_l^{ij})_{m\times m}$ 为 $c_l(\sigma)$ 对应的矩阵，其中 $l=0,1,\cdots,n-1$，则 $F(x)$ 也可看作一多项式矩阵，即

$$F(x)=\left(f_{ij}(x)\right)_{m\times m}\in \boldsymbol{M}_m(F_2[x])$$

其中

$$f_{ij}(x)=\delta_{ij}x^n+\sum_{l=0}^{n-1}c_l^{ij}x^l\in F_2[x],\quad \delta_{ij}=\begin{cases}1, i=j\\ 0, i\ne j\end{cases}$$

则 σ-LFSR 为本原的当且仅当行列式 $|F(x)|$ 是 $F_2$ 上的 $mn$ 次本原多项式。

### 3.2　迹表示定理

**定理 1**　设 $F(x)=x^n+A_{n-1}x^{n-1}+\cdots+A_1x+A_0\in \boldsymbol{M}_m(\boldsymbol{F}_2)[x]$ 是本原 σ- 多项式，$\alpha$ 为 $|F(x)|$ 的根。将 $F(\alpha)$ 看作 $F_{2^{mn}}$ 上的 $m$ 阶矩阵，则

$$F(\alpha)\boldsymbol{X}=0 \tag{3}$$

为 $F_{2^{mn}}$ 上的 $m$ 元线性方程组。设 $\boldsymbol{Y}\in F_{2^{mn}}^m$ 为式(3)的一个非零解，记 $s_i=\mathrm{tr}_1^{mn}(\boldsymbol{Y}\cdot\alpha^i)$，$i=0,1,\cdots$，则序列 $s^\infty=(s_0,s_1,s_2,\cdots)\in G(F(x))$。

**证明**　首先分析式(3)解的结构。

因为 $\alpha$ 为 $|F(x)|$ 的根，所以矩阵 $F(\alpha)$ 降秩，故式(3)一定存在非零解。又因为 $F(x)$为本原 σ- 多项式，由引理 1，$|F(x)|$ 是 $F_2$ 上的 $mn$ 次本原多项式，所以 $|F(x)|$ 是 $\alpha$ 在 $F_2$ 上的极小多项式，而矩阵 $F(\alpha)$ 的任一个 $(m-1)$ 阶子阵的行列式至多为 $(m-1)n$ 次，它们一定不为零，所以它们均满秩，故矩阵 $F(\alpha)$ 的秩为 $(m-1)$。由此知式(3)有且仅有 $2^{mn}$ 个解，取其中一个非零解，记为 $\boldsymbol{Y}$。则式(3)的任一解可表为 $\boldsymbol{Y}\bullet\beta$，其中 $\beta\in F_{2^{mn}}$。

对任意 $k\ge 0$，有

$$\begin{aligned}
&s_{n+k}+A_{n-1}s_{n+k-1}+A_{n-2}s_{n+k-2}+\cdots+A_0s_k\\
&=\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\alpha^{n+k})+A_{n-1}\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\alpha^{n+k-1})\\
&\quad+A_{n-2}\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta\alpha^{n+k-2})+\cdots+A_0\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\alpha^k)\\
&=\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\alpha^{n+k}+A_{n-1}(\boldsymbol{Y}\bullet\alpha^{n+k-1})\\
&\quad+A_{n-2}(\boldsymbol{Y}\bullet\alpha^{n+k-2})+\cdots+A_0\boldsymbol{Y}\alpha^k)\\
&=\mathrm{tr}_1^{mn}(\,(\boldsymbol{Y}\bullet\alpha^n+A_{n-1}(\boldsymbol{Y}\bullet\alpha^{n-1})+A_{n-2}(\boldsymbol{Y}\bullet\alpha^{n-2})\\
&\quad+\cdots+A_0\boldsymbol{Y})\alpha^k\,)\\
&=\mathrm{tr}_1^{mn}(\,(F(\alpha)\boldsymbol{Y})\alpha^k\,)=\mathrm{tr}_1^{mn}(\boldsymbol{0})=\boldsymbol{0}
\end{aligned}$$

这说明 $s^\infty$ 满足 $F(x)$ 定义的迭代关系，因而 $s^\infty=(s_0,s_1,\cdots)\in G(F(x))$。 证毕

下面证明定理 1 的逆。

**定理 2** $F(x)$，$\alpha$，$\boldsymbol{Y}$ 定义如定理 1，则对任意 $s^\infty=(s_0,s_1,\cdots)\in G(F(x))$，都有一 $\beta\in F_{2^n}$，使得 $s_i=\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta\alpha^i)$，$i=0,1,2,\cdots$。

**证明** 因为 $\boldsymbol{Y}$ 为式(3)的解，所以 $\boldsymbol{Y}\bullet\beta$ 也是其解，由定理 1，有

$$(\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta\alpha),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta\alpha^2),\cdots)\in G(F(x))$$

下面只需证：当 $\beta$ 取遍 $F_{2^{mn}}$ 中所有元素时，序列

$$(\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta\alpha),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta\alpha^2),\cdots)$$

就给出了 $G_{F_{2^m}}(F(x))$ 中全部的序列。因为 $G_{F_{2^m}}(F(x))$ 中有 $2^{mn}$ 条序列，$F_{2^{mn}}$ 中有 $2^{mn}$ 个元素。所以只需证明：当 $\beta_1\neq\beta_2$ 时，

$$(\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta_1),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta_1\alpha),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta_1\alpha^2),\cdots)\neq(\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta_2),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta_2\alpha),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\beta_2\alpha^2),\cdots)$$

这是已知结论。 证毕

可见，本原 σ -LFSR 序列的迹表示在形式上与有限域上 m-序列的迹表示很相似，仅需在迹函数里加上方程组的解 $\boldsymbol{Y}$。

## 4 本原σ-LFSR 序列的充要条件

定理 1，定理 2 给出了本原 σ-LFSR 序列的一种表示法，这种表示在讨论本原 σ-LFSR 序列的某些问题时是有用的。本节利用它给出 σ-LFSR 序列为本原的充要条件。

**引理 2**[12] 若 $s^\infty$ 是 $F_{2^m}$ 上的 $n$ 级本原 σ-LFSR 序列，$F(x)$ 为它的 $n$ 次特征多项式，则 $s^\infty$ 的 $m$ 个分位序列均为 $F_2$ 上的 m-序列且极小多项式为 $|F(x)|$。

**定理 3** 设 $s^\infty$ 是 $F_{2^m}$ 上的序列，则它是 $n$ 级本原 σ-LFSR 序列当且仅当满足条件：

(1) $s^\infty$ 的 $m$ 条分位序列均为 $F_2$ 上的 m-序列，且极小多项式为 $F_2$ 上的 $mn$ 次本原多项式，设为 $g(x)$。

(2)设 $\alpha\in F_{2^{mn}}$ 为 $g(x)$ 的一个根，由条件(1)及有限域上 LFSR 序列的迹表示，$s^\infty$ 的任一分位序列 $s_i^\infty$ 可表为 $s_i^\infty=(\mathrm{tr}_1^{mn}(\beta_i),\mathrm{tr}_1^{mn}(\beta_i\alpha),\mathrm{tr}_1^{mn}(\beta_i\alpha^2),\cdots)$，其中 $\beta_i\in F_{2^{mn}}$，$i=0,1,\cdots,m-1$。则

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

构成 $F_{2^{mn}}$ 在 $F_2$ 上的一组基。

**证明** (必要性)若 $s^\infty$ 是本原的，由引理 2，条件(1)满足。

设 σ- 多项式 $F(x)\in M_m(F_2)[x]$ 为 $s^\infty$ 的极小多项式，则 $\deg(F(x))=n$。记条件(2)中的 $\beta_0,\beta_1,\cdots,\beta_{m-1}$ 为 $m$ 维向量 $\boldsymbol{Y}=(\beta_0,\beta_1,\cdots,\beta_{m-1})^{\mathrm{T}}$，则有

$$s^\infty=\left((\mathrm{tr}_1^{mn}(\boldsymbol{Y}),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\alpha),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\alpha^2),\cdots)\right)$$

由定理 2，$\boldsymbol{Y}$ 一定是 $F(\alpha)\boldsymbol{X}=0$ 的解。

将 $F(\alpha)$ 看作 $F_{2^{mn}}$ 上的 $m$ 阶矩阵，则 $F(\alpha)$ 可表为

$$F(\alpha)=\begin{pmatrix}f_{11}(\alpha) & \cdots & f_{1m}(\alpha)\\ \vdots & \ddots & \vdots\\ f_{m1}(\alpha) & \cdots & f_{mm}(\alpha)\end{pmatrix},\ \text{其中 } f_{ij}(x)\in F_2[x],$$

$$\deg(f_{ij})=\begin{cases}n, & i=j\\ <n, & i\neq j\end{cases}$$

因为 $\boldsymbol{Y}$ 为 $F(\alpha)\boldsymbol{X}=0$ 的解，有

$$\left.\begin{aligned}\sum_{j=1}^{m}f_{1j}(\alpha)\beta_{j-1}=0\\ \sum_{j=1}^{m}f_{2j}(\alpha)\beta_{j-1}=0\\ \vdots\\ \sum_{j=1}^{m}f_{mj}(\alpha)\beta_{j-1}=0\end{aligned}\right\}\tag{4}$$

将式(4)的 $m$ 个等式展开，并将 $\beta_i\alpha^n$ $(i=0,1,\cdots,m-1)$ 移到左边，可得

$$\left.\begin{aligned}\beta_0\alpha^n=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}k_{i,j}^{(0)}(\beta_j\alpha^i)\right)\\ \beta_1\alpha^n=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}k_{i,j}^{(1)}(\beta_j\alpha^i)\right)\\ \vdots\\ \beta_{m-1}\alpha^n=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}k_{i,j}^{(m-1)}(\beta_j\alpha^i)\right)\end{aligned}\right\}\tag{5}$$

其中 $k_{i,j}^{(l)}\in F_2$。

若把 $F_{2^{mn}}$ 看成 $F_2$ 上的线性空间，由式(5)，$(\beta_0\alpha^n,\beta_1\alpha^n,\cdots,\beta_{m-1}\alpha^n)$ 可由 $A$ 表出。

不妨取式(5)的第 1 个式子，为

$$\beta_0\alpha^n=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}k_{i,j}^{(0)}(\beta_j\alpha^i)\right)\tag{6}$$

将式(6)左右同乘以 $\alpha$，得

$$\beta_0\alpha^{n+1}=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}k_{i,j}^{(0)}(\beta_j\alpha^{i+1})\right)\tag{7}$$

因为 $(\beta_0\alpha^n,\beta_1\alpha^n,\cdots,\beta_{m-1}\alpha^n)$ 可由集合 $A$ 表出，再根据式(7)，知 $\beta_0\alpha^{n+1}$ 可由集合 $A$ 表出。

依次类推，$\beta_0\alpha^{n+2},\beta_0\alpha^{n+3},\cdots,\beta_0\alpha^{2^{mn}-2}$ 均可由集合 $A$ 表出，所以 $F_{2^{mn}}$ 上的所有元素均可由 $A$ 表出，故 $A$ 是 $F_{2^{mn}}$ 在 $F_2$ 上的一组基。

(充分性)记条件(2)中的 $\beta_0,\beta_1,\cdots,\beta_{m-1}$ 为 $m$ 维向量 $\boldsymbol{Y}=(\beta_0,\beta_1,\cdots,\beta_{m-1})^{\mathrm{T}}$，由条件(1)、条件(2)，有 $s^\infty=(\mathrm{tr}_1^{mn}(\boldsymbol{Y}),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\alpha),\mathrm{tr}_1^{mn}(\boldsymbol{Y}\bullet\alpha^2),\cdots)$

由条件(2)，集合 $A$ 构成 $F_{2^{mn}}$ 在 $F_2$ 上的一组基，则有

$$\left.\begin{aligned}
\beta_0\alpha^n &= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}k_{i,j}^{(0)}(\beta_j\alpha^i)\right)=\sum_{j=0}^{m-1}\left((\sum_{i=0}^{n-1}k_{i,j}^{(0)}\alpha^i)\beta_j\right)\\
\beta_1\alpha^n &= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}k_{i,j}^{(1)}(\beta_j\alpha^i)\right)=\sum_{j=0}^{m-1}\left((\sum_{i=0}^{n-1}k_{i,j}^{(1)}\alpha^i)\beta_j\right)\\
&\vdots\\
\beta_{m-1}\alpha^n &= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}k_{i,j}^{(m-1)}(\beta_j\alpha^i)\right)=\sum_{j=0}^{m-1}\left((\sum_{i=0}^{n-1}k_{i,j}^{(m-1)}\alpha^i)\beta_j\right)
\end{aligned}\right\}\quad(8)$$

记

$$f_{ij}(x)=\delta_{ij}x^n+\sum_{l=0}^{n-1}k_{l,j}^{(i)}x^l$$

其中 $\delta_{ij}=\begin{cases}1, & i=j\\ 0, & i\neq j\end{cases}$，$i,j=0,1,\cdots,m-1$。

构造多项式矩阵 $F(x)=(f_{ij}(x))_{m\times m}$。

由式(8)，得 $F(\alpha)\boldsymbol{Y}=0$。

因为 $\boldsymbol{Y}$ 非零，所以 $F(\alpha)\boldsymbol{X}=0$ 有非零解，这说明矩阵 $F(\alpha)$ 是降秩的，所以 $|F(\alpha)|=0$。

因为 $\alpha$ 是 $F_2$ 上 $mn$ 次本原元，所以 $|F(x)|$ 是 $F_2$ 上 $mn$ 次本原多项式。由引理 1，$F(x)$ 是 $n$ 次本原 σ- 多项式。由定理 1，$s^\infty\in G(F(x))$，所以 $s^\infty$ 是 $n$ 级本原 σ- LFSR 序列。

证毕

## 5　结束语

$\sigma$- LFSR 序列生成速度快，同时具有良好的密码学性质[12,13]，较好地适应了现代序列密码与现代 CPU 的发展方向，为序列密码驱动部分的设计提供了更多的选择。本文给出了本原 σ- LFSR 序列的迹表示，并利用这种表示给出了一个本原 σ- LFSR 序列的充要条件，它们为进一步研究本原 σ- LFSR 序列的各种问题(如计数及采样)提供了新的工具。随着字 LFSR 的流行与处理器的发展，我们希望 $\sigma$- LFSR 序列能在密码设计中得到越来越广泛的应用。

## 参 考 文 献


[1] Preneel B. Introduction to the proceedings of the fast software encryption 1994 workshop[C]. Lecture Notes in Computer Science, Leuven Belgium, 1995, 1008: 1–5.

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

[3] Dewar M and Panario D. Linear Transformation Shift Registers[J]. *IEEE Trans. on Inform. Theory*, 2003, 49(8): 2047–2052.

[4] ECRYPT, eSTREAM: ECRYPT Stream Cipher Project, IST-2002-507932, Available at http://www.ecrypt.eu.org/stream/.

[5] Watanabe P, Furuya S and Yoshida H, *et al*.. A new keystream generator MUGI[C]. Fast Software Encryption 2002 workshop, Lecture Notes in Computer Science, Leuven Belgium, 2003, 2365: 179–194.

[6] Rogaway P and Coppersmith D. A software-optimized encryption algorithm[C]. Fast Software Encryption 1993 Workshop, Lecture Notes in Computer Science, Cambridge UK, 1994, 809: 53–63.

[7] Coppersmith D, Halevi S, and Jutla C. Scream: A Software-Efficient Stream Cipher[C]. Fast Software Encryption 2002 Wokshop, Lecture Notes in Computer Science, Leuven Belgium, 2003, 2365: 195–209.

[8] Boesgaard M, Vesterager M, and Pedersen T, *et al*.. Rabbit: A new high-performance stream cipher[C]. Fast Software Encryption 2003 Wokshop, Lecture Notes in Computer Science, Lund Sweden, 2004, 2887: 307–329.

[9] Ferguson N, Whiting D, and Schneier B, *et al*.. Helix: Fast encryption and authentication in a single cryptographic primitive[C]. Fast Software Encryption 2003 Wokshop, Lecture Notes in Computer Science, Lund Sweden, 2004, 2887: 330–346.

[10] Ekdahl P and Hohansson T. Snow—A new stream cipher. Proceedings of the first open NESSIE workshop, Heverlee Belgium, 2000.

[11] Ekdahl P and Hohansson T. A new version of the stream cipher snow[C]. Selected Areas in Cryptography 2002 workshop. Lecture Notes in Computer Science, Newfoundland Canada, 2003, 2595: 47–61.

[12] Zeng Guang, Han Wen-bao, and He Kai-cheng. High Efficiency Feedback Shift Register: σ -LFSR. Cryptology ePrint Archive, Report 2007/114 http://eprint.iacr.org/ 2007: 2–5.

[13] 曾光，何开成，韩文报. 一类三项式形式适合软件实现的 σ-LFSR[J]. 中国科学 E 辑: 信息科学, 2007, 37(2): 209–222.
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.

[14] 张猛，韩文报. σ-LFSR 的分类研究[C]. 密码学进展——ChinaCrypt'2007-中国密码学会 2007 年会论文集, 中国，成都, 2007: 27–35.
Zhang Meng and Han Wen-bao. On the Classification of σ-LFSR[C]. Progress on cryptography——ChinaCrypt'2007, China, Chengdu, 2007: 27–35.

[15] Lidi R and Niederreiter H. Introduction to Finite Fields and Their Applications[M]. Great Britain: Cambridge University Press, 1986: 54–63.



张　猛：　男，1982 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，博士生，研究方向为序列密码.

韩文报：　男，1963 年生，教授，博士生导师，主要研究方向为信息安全.

何开成：　男，1972 年生，博士生，研究方向为信息安全.