第35卷　第18期　　计　算　机　工　程　　2009年9月
Vol.35　No.18　　Computer Engineering　　September 2009

·安全技术·　　文章编号：1000—3428(2009)18—0154—02　　文献标识码：A　　中图分类号：TN918.1

本原 σ-LFSR 的计数研究

刘向辉，张　猛，韩文报，曾　光

(解放军信息工程大学信息研究系，郑州 450002)

摘　要：针对 σ-LFSR 能够充分利用现代通用 CPU 且具有结构简单、适合软件快速实现的特点，利用本原 σ-LFSR 的距离向量和基判别定理，将本原 σ-LFSR 的计数问题转化为线性空间上基的问题，以此为基础，利用 F_2 上次数小于 n 的互素多项式的对数解决 F_4 上本原 σ-LFSR 的计数问题。

关键词：序列密码；本原 σ-LFSR；基判别定理；计数

Research on Counting of Primitive σ-LFSR

LIU Xiang-hui, ZHANG Meng, HAN Wen-bao, ZENG Guang

(Department of Information Research, PLA Information Engineering University, Zhengzhou 450002)

【**Abstract**】σ-LFSR is a kind of word-oriented Linear Feedback Shift Register(LFSR) with high efficiency and good cryptographic properties, especially its software implementation is efficient for modern processors. Through the coordinate sequences and base discriminance of primitive σ-LFSR, this paper converts the study of counting to the basis of liner space, and through the pairs of relatively prime polynomials on F_2 with degree smaller than n, the counting formula of primitive σ-LFSR on F_4 is obtained.

【**Key words**】stream cipher; primitive σ-LFSR; base discriminance; counting

1　概述

序列密码具有错误传播率低、实现简单、加解密速度快等优势，一直是密码学界研究的热点。它的一种方式是先产生具有良好性质的伪随机序列，再对其进行过滤加工以增加安全强度，源序列发生器是这种序列密码设计的基础。二元域上的线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)是其常用部件。传统的 LFSR 基于比特设计，适合硬件实现。然而，现代通用 CPU 是基于字运算的，这造成传统的序列密码算法在软件实现效率上大打折扣。为了充分利用 CPU 的性能，设计面向字运算的、适合软件实现的序列密码越来越受关注。

TSR(linear Transform Shift Register)[1]是一种基于字的 LFSR，它是将现代处理器特点和字 LFSR 相结合而设计的。2005 年，欧洲的 eSTREAM 计划全面征集序列密码算法，在征集到的 34 个序列密码算法中有 22 个是适合软件快速实现的。适合软件实现的现代序列密码算法，如 Ssc2, Panama, Mugi, Seal, Scream，都是以字为基本操作来达到软件高效实现的目的。而 Sober, Turing 和 Snow 等的源序列发生器就是基于字的有限域上的本原 LFSR 序列。可见，基于字的 LFSR 已经成为现代序列密码的重要组成部分，它为序列密码源驱动部分的设计提供了新的选择。

2　σ-LFSR 模型

循环移位是现代通用 CPU 的基本运算，它不仅实现快捷，而且具有良好的密码学性质，将其引入基于字的 LFSR 便是本文所研究的 σ-LFSR，其概念如下：

定义 1 设 $\alpha,\alpha^2,\cdots,\alpha^{2^{m-1}}$ 是线性空间 F_{2^m}/F_2 的一组正规基，并设 $\beta=k_0\alpha+k_1\alpha^2+\cdots+k_{m-1}\alpha^{2^{m-1}}\in F_{q^m}$, $k_0,k_1,\cdots,k_{m-1}\in F_2$，则 F_{2^m} 上的循环移位算子 σ 定义如下：

$$\sigma(\beta)=\sigma(k_0\alpha+k_1\alpha^2+\cdots+k_{m-1}\alpha^{2^{m-1}})\triangleq k_{m-1}\alpha+k_0\alpha^2+\cdots+k_{m-2}\alpha^{2^{m-1}}$$

显然，σ 为线性空间 F_{2^m}/F_2 上的一个线性变换。同时任意 $c\in F_{2^m}$ 可以诱导出线性空间 F_{2^m}/F_2 上的一个线性变换：$C:F_{2^m}\to F_{2^m}$, $C(\alpha)=c\alpha$，$\alpha\in F_{2^m}$。从线性变换的角度出发，将循环移位算子 σ 添加到 F_{2^m} 中得到一个新的代数结构 $F_{2^m}[\sigma]$。可以验证，$F_{2^m}[\sigma]$ 为 F_{2^m}/F_2 上的所有线性变换集合。记 F_2 上 $m\times m$ 阶矩阵环为 $M_m(F_2)$，则有 $F_{2^m}[\sigma]\cong M_m(F_2)$。

定义 2 设 n 是一个正整数，$c_0(\sigma),c_1(\sigma),\cdots,c_{n-1}(\sigma)$ 是 $F_{2^m}[\sigma]$ 上的元素。若 F_{2^m} 上的序列 $s^\infty=s_0,s_1,s_2,\cdots$ 满足关系：$s_{i+n}=c_0(\sigma)s_i+c_1(\sigma)s_{i+1}+\cdots+c_{n-1}(\sigma)s_{i+n-1}$, $i=0,1,2,\cdots$，则称 s^∞ 为 F_{2^m} 上的 n 级 σ-LFSR 序列，多项式 $F(x)=x^n+c_{n-1}(\sigma)x^{n-1}+\cdots+c_1(\sigma)x+c_0(\sigma)$ 为 σ-LFSR 序列 s^∞ 的特征多项式，简称为 σ-多项式，如图 1 所示。

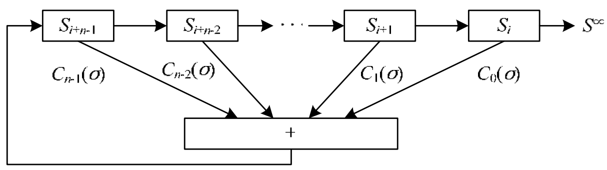

图 1　σ-LFSR 模型

定义 3 如果 s^∞ 为 F_{2^m} 上的 n 级 σ-LFSR 序列且周期为 $2^{mn}-1$，则称 s^∞ 为本原 σ-LFSR 序列，称其特征多项式为本原 σ-多项式。

基金项目：国家“863”计划基金资助项目(2006AA01Z425)；国家自然科学基金资助项目(90704003)

作者简介：刘向辉(1984－)，男，硕士研究生，主研方向：序列密码；张　猛，硕士研究生；韩文报，教授、博士生导师；曾　光，博士研究生

收稿日期：2009-01-20　　**E-mail：**lxhkz2002@163.com

3 本原 σ-LFSR 的计数问题转化

有限域 F_{2^m} 上本原 σ-LFSR 的计数是一个基础问题，但还未得到很好的解决，仅仅有一个猜想。本节利用 σ-LFSR 的分位序列和基判别定理，将计数问题转化为线性空间 F_{2^m}/F_2 上基的问题。

猜想[2] 设 F_{2^m} 上 n 次本原 σ-LFSR 个数为 $N(m,n)$，则有

$$N(m,n)=\frac{|GL_m(F_2)|}{2^m-1}\cdot\frac{\varphi(2^{mn}-1)}{mn}\cdot 2^{m(m-1)(n-1)}$$

其中，$|GL_m(F_2)|=\prod_{i=0}^{m-1}(2^m-2^i)$，表示 F_2 上 $m\times m$ 阶可逆矩阵的个数；$\varphi(2^{mn}-1)$ 为欧拉函数，$\frac{\varphi(2^{mn}-1)}{mn}$ 表示 F_2 上 mn 次本原多项式的个数。

3.1 准备工作

σ-LFSR 分位序列和距离向量的概念如下：

定义 4 设 s^∞ 是 F_{2^m} 上的σ-LFSR 序列，把 F_{2^m} 看作 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^∞ 可看作 F_2 上的 m 维向量序列，可写成：$s^\infty=s_0^\infty\alpha_0+s_1^\infty\alpha_1+\cdots+s_{m-1}^\infty\alpha_{m-1}$，称二元序列 s_i^∞ 为 s^∞ 的第 i 个分位序列，其中，$0\le i\le m-1$。

定理 1[2] 若 s^∞ 是 F_{2^m} 上的 n 级本原σ-LFSR 序列，则其 m 个分位序列都为 F_2 上的 m-序列且具有相同的极小多项式。

设 s^∞ 为有限域 F_{2^m} 上的σ-LFSR 序列，若其分位序列都是 F_2 上的 m-序列且具有相同的极小多项式，则 s^∞ 可表示为

$$s^\infty=\begin{pmatrix}\underline{a}\\ L^{d_1}\underline{a}\\ \cdots\\ L^{d_{m-1}}\underline{a}\end{pmatrix}$$

其中，$\underline{a}$ 是 mn 级的 m-序列；$L^k\underline{a}$ 表示将 $\underline{a}$ 左移 k 位。

以 $\underline{a}$ 为基准序列，定义 s^∞ 的距离向量为 $\boldsymbol{D}_m=(0,d_1,d_2\cdots,d_{m-1})$。本原$\sigma$-LFSR 序列有距离向量 $\boldsymbol{D}_m$ 且完全由其 σ-多项式 $F(x)$ 决定，它是一个特征量。

定义迹函数 $tr_1^n(\bullet)$ 为 $tr_1^n(x)=\sum_{i=0}^{n-1}x^{2^i}$，它是从有限域 F_{2^n} 到其子域 F_2 的映射。本原 σ-LFSR 的基判别定理如下：

定理 2[3] 设 s^∞ 是 F_{2^m} 上的序列，则它是 n 级本原σ-LFSR 序列，当且仅当满足以下条件：

(1) s^∞ 的 m 条分位序列均为 F_2 上 m-序列，且极小多项式为 F_2 上的 mn 次本原多项式。

(2)设 $\alpha\in F_{2^{mn}}$ 为条件(1)中本原多项式的一个根，由有限域上 LFSR 序列的迹表示，s^∞ 的任一分位序列 s_i^∞ 可表示为 $s_i^\infty=(tr_1^{mn}(\beta_i),tr_1^{mn}(\beta_i\alpha),tr_1^{mn}(\beta_i\alpha^2),\cdots)$，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。

3.2 问题转化

因为距离向量是本原 σ-LFSR 的特征量，所以可通过它研究计数问题。根据文献[4]，对于有限域 F_{2^m} 上的 n 次本原 σ-LFSR，可按 F_2 上的 mn 次本原多项式进行分类：若 $g(x)\in F_2[x]$ 为 mn 次本原多项式，则 F_{2^m} 上所有行列式为 $g(x)$ 的 n 级本原 σ-LFSR 为一类，称之为 F_{2^m} 上的 n 级本原 $g(x)$-类。

从 F_{2^m} 上 n 级本原 $g(x)$-类所含元素的个数考虑问题，以下所述的本原 σ-LFSR 都在同一类中。显然，F_{2^m} 上的 n 级本原 $g(x)$-类中的本原 σ-LFSR 序列和它们的距离向量是一一对应的。若 s^∞ 是 F_{2^m} 上的 σ-LFSR 序列，其分位序列都是 F_2 上的 m-序列且具有相同的极小多项式 $g(x)$，设其距离向量为 $\boldsymbol{D}_m=(0,d_1,d_2\cdots,d_{m-1})$。于是，由有限域上 LFSR 序列的迹表示，$s^\infty$ 的任一分位序列 s_i^∞ 可表示为：$s_i^\infty=(tr_1^{mn}(\beta_i),tr_1^{mn}(\beta_i\alpha),tr_1^{mn}(\beta_i\alpha^2),\cdots)$，其中，$\beta_i\in F_{2^{mn}}$，$i=0,1,\cdots,m-1$。由定理 2，$s^\infty$ 是 n 级本原σ-LFSR 序列，当且仅当集合 $A=\{\beta_0,\beta_0\alpha,\cdots,\beta_0\alpha^{n-1},\beta_1,\beta_1\alpha,\cdots,\beta_1\alpha^{n-1},\cdots,\beta_{m-1},\beta_{m-1}\alpha,\cdots,\beta_{m-1}\alpha^{n-1}\}$ 构成 $F_{2^{mn}}$ 在 F_2 上的一组基，显然，$\beta_0^{-1}\cdot A$ 也构成 $F_{2^{mn}}$ 在 F_2 上的一组基。而根据分位序列平移等价性，必有 $\beta_i=\beta_0\alpha^{d_i}$，$i=1,2,\cdots,m-1$，于是得出如下推论：

推论 设 s^∞ 是 F_{2^m} 上的序列，则它是 n 级本原σ-LFSR 序列，当且仅当满足如下条件：

(1) s^∞ 的 m 条分位序列均为 F_2 上 m-序列，且极小多项式为 F_2 上的 mn 次本原多项式。

(2) 设 $\alpha\in F_{2^{mn}}$ 为条件(1)中本原多项式的一个根，$\boldsymbol{D}_m=(0,d_1,d_2\cdots,d_{m-1})$ 为距离向量，则

$$A=\{1,\alpha,\cdots,\alpha^{n-1},\alpha^{d_1},\alpha^{d_1+1},\cdots,\alpha^{d_1+n-1},\cdots,\alpha^{d_{m-1}},\alpha^{d_{m-1}+1},\cdots,\alpha^{d_{m-1}+n-1}\}$$

构成 $F_{2^{mn}}$ 在 F_2 上的一组基。

由上述推论，求解 $F_{2^{mn}}$ 上 n 级本原 $g(x)$-类所含元素的个数等价于如下问题：对于距离向量 $\boldsymbol{D}_m=(0,d_1,d_2,\cdots,d_{m-1})$，当 $d_i(i=1,2,\cdots,m-1)$ 遍历 $[0,2^{mn}-2]$ 时，对应的 A 能构成 $F_{2^{mn}}$ 在 F_2 上的一组基的个数。

4 F_4 上本原 σ-LFSR 的计数公式

虽然 F_{2^m} 上本原 σ-LFSR 的计数问题可以转化为 3.2 节所述问题，但对于域 $F_{2^m},m\ge 3$，该问题并没有很好的解决方法。本文利用 F_2 上次数小于 n 的互素多项式的对数给出了 F_4 上的本原 σ-LFSR 计数公式。

设 $g(x)$ 是 F_2 上的任一 $2n$ 次本原多项式，α 是 $g(x)$ 的根。如 3.2 节所述，F_4 上 n 级本原 $g(x)$-类所含元素的个数可转化为如下问题：当 k 遍历 $[0,2^{2n}-2]$ 时，使 $A=\{1,\alpha,\cdots,\alpha^{n-1};\alpha^k,\alpha^{k+1},\cdots,\alpha^{k+n-1}\}$ 为 $F_{2^{2n}}$ 在 F_2 上的一组基的个数。

要解决这个问题，需要先给出 F_2 上次数小于 n 的互素多项式的对数。Benjamin 和 Bennett 利用 Euclid 算法给出了如下公式：

定理 3[5] F_2 上次数小于 n 的互素多项式对数为 $2^{2n-1}+1$。

定理 4 设 α 为 $F_{2^{2n}}$ 上的非零元，$(f_1(x),f_2(x))$ 和 $(g_1(x),g_2(x))$ 为 $F_2[x]$ 中 2 个不同的次数小于 n 的互素对，则有 $f_1(\alpha)/f_2(\alpha)\ne g_1(\alpha)/g_2(\alpha)$。

证明：假设 $f_1(\alpha)/f_2(\alpha)=g_1(\alpha)/g_2(\alpha)$，则有

$$f_1(\alpha)g_2(\alpha)+f_2(\alpha)g_1(\alpha)=0$$

显然，$\deg(f_1(x)g_2(x)+f_2(x)g_1(x))<2n$，因为 α 的极小多项式是 $2n$ 次的，所以必有

$$f_1(x)g_2(x)+f_2(x)g_1(x)=0\Rightarrow f_1(x)g_2(x)=f_2(x)g_1(x)$$

又因为 $(f_1(x),f_2(x))=1$，$(g_1(x),g_2(x))=1$，所以 $f_1(x)=g_1(x)$，$f_2(x)=g_2(x)$。结论得证。

定理 5 F_4 上 n 级本原 σ-LFSR 的个数为 $\frac{\varphi(2^{2n}-1)}{2n}2^{2n-1}$。

(下转第 158 页)