本原 σ-LFSR 序列的若干性质*)

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

摘 要 σ-LFSR是一种基于字的LFSR模型,能充分利用现代CPU的特点,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。但从伪随机特性和资源利用率的角度看,实际应用的σ-LFSR序列必定是本原的。对本原σ-LFSR序列的性质作了较深入的分析,得到了其分位序列之间是线性无关的,并指出分位序列的极小多项式实际是状态转移矩阵的特征多项式;通过引入块Hankel矩阵,给出了一个求本原σ-LFSR序列极小多项式的算法;最后给出了σ-LFSR序列为本原的充要条件。

关键词 序列密码,本原σ-LFSR序列,分位序列,块Hankel矩阵

Several Properties on the Primitive σ-LFSR Sequences

ZHANG Meng HE Kai-cheng HAN Wen-bao ZENG Guang
(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. Proposed a thorough analysis on the properties of the primitive σ-LFSR sequences. Obtained the conclusion that the coordinate sequences of a primitive σ-LFSR sequence are linear independent, and the minimal polynomial of coordinate sequences is just the character polynomial of state transfer matrix. By introducing the block Hankel matrix, an algorithm to compute the minimal polynomial of a primitive σ-LFSR sequence was offered. At last, a sufficient and necessary condition was obtained which can be used to check whether a σ-LFSR sequence is primitive or not.

Keywords Stream cipher, Primitive σ-LFSR sequence, Coordinate sequence, Block Hankel matrix

1 引言

近年来,随着计算机技术的飞速发展,适合软件快速实现的序列密码算法的研究备受关注。在2005年欧洲的ECRYPT NoE eSTREAM[3]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。由此可以看出,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Ssc2, Panama, Mugi, Seal, Scream, Rabbit, Helix, Sober, Turing和Snow等,我们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节讨论本原σ-LFSR序列分位序列的性质,第4节给出一个求本原σ-LFSR序列极小多项式的算法,第5节得到σ-LFSR序列为本原的充要条件,最后总结全文。

2 σ-LFSR模型

σ-LFSR是一种基于字的LFSR模型,本节简单介绍它的概念,具体可参见文献[4-6]。

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。

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。

首先定义循环移位算子。

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,设

$\beta=k_0\alpha+k_1\alpha^2+\cdots+k_{m-1}\alpha^{m-1}\in F_{2^m}$, $k_0,k_1,\cdots,k_{m-1}\in F_2$

则F_{2^m}上的循环移位算子σ如下:

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

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[6]。

记F_2上$m\times m$阶矩阵环为$M_m(F_2)$,由文献[6],有

$$F_{2^m}[\sigma]\cong M_m(F_2) \tag{1}$$

*)基金项目:国家863高技术研究发展计划资助项目(2006AA01Z425),国家自然科学基金资助项目(90704003)。张 猛 硕士研究生,主要研究方向为信息安全;何开成 博士生,主要研究方向为信息安全;韩文报 教授,博士生导师,主要研究方向为信息安全;曾 光 博士生,主要研究方向为信息安全。

定义 2 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^∞ 为 F_{2^m} 上的 n 级 σ-LFSR 序列，称多项式

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

为 n 次 σ-多项式，它是 s^∞ 的特征多项式。

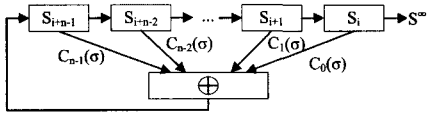

图 1 σ-LFSR 模型

注意到 F_{2^m} 上 n 级 σ-LFSRσ-LFSR 序列 s^∞ 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 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，称其次数最低的特征多项式为本原 σ-多项式。

由式(1)，任意 σ-多项式 $F(x)=x^n+c_{n-1}(\sigma)x^{n-1}+\cdots+c_1(\sigma)x+c_0(\sigma)$ 实际上是一个矩阵多项式，所以也有 $F(x)\in M_m(F_2)[x]$。

3 本原 σ-LFSR 序列分位序列的性质

定义 4 s^∞ 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^∞ 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^∞ 为 s^∞ 的第 i 个分位序列，其中 $0\leqslant i\leqslant m-1$。

定理 1[5] 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-序列且极小多项式相同。

为进一步研究分位序列的性质，做下列定义。

定义 5 设 $s^\infty=s_0,s_1,s_2,\cdots$ 是 F_{2^m} 上的 σ-LFSR 序列，引入块 Hankel 矩阵

$$H_i^{(n)}=\begin{pmatrix} s_{i+n-1} & s_{i+n-1} & \cdots & s_{i+mn+n-2} \\ \vdots & \vdots & \cdots & \vdots \\ s_{i+1} & s_{i+2} & \cdots & s_{i+mn} \\ s_i & s_{i+1} & \cdots & s_{i+mn-1} \end{pmatrix}_{mn\times mn}$$

易见，$H_i^{(n)}\in M_{mn}(F_2)$，称 $H_i^{(n)}$ 为 s^∞ 的第 i 个 n 级状态矩阵。

定理 2 给出了本原 σ-LFSR 序列分位序列间的关系。

定理 2 设 F_{2^m} 上的序列 s^∞ 是一个 n 级本原 σ-LFSR 序列，则 s^∞ 的 m 个分位序列线性无关。

在给出它的证明前，先证明一个引理。

引理 1 设 A 为 F_2 上的 n 阶可逆矩阵，且 A 的阶为 $e=2^n-1$，$\alpha\in F_2^n$ 为一个 n 维非零向量，令

$$B=(\alpha,A\alpha,A^2\alpha,\cdots,A^{n-1}\alpha)_{n\times n}$$

则 B 是可逆矩阵。

证明：(反证)若 B 不可逆，则存在 $0\leqslant i_1<i_2<\cdots<i_k\leqslant n-1$，$1\leqslant k\leqslant n$，使得 $A^{i_1}\alpha+A^{i_2}\alpha+\cdots+A^{i_k}\alpha=0$，所以有

$$(A^{i_1}+A^{i_2}+\cdots+A^{i_k})\alpha=0 \tag{3}$$

下面说明 $A^{i_1}+A^{i_2}+\cdots+A^{i_k}$ 必为 A 的某个方幂。

因为 A 为最大周期的，所以其极小多项式为 $f(x)=|xE-A|$，$\deg(f(x))=n$，则对任意 i，存在 $q(x),r(x)\in F_2(x)$，使得 $A^i=f(A)q(A)+r(A)=r(A)$，其中 $\deg(r(x))<n$。又对任意 $i\neq j$ 且 $i,j\in[0,2^n-2]$，有 $A^i\neq A^j$。由此知，当 i 遍历 $[0,2^n-2]$，A^i 恰好遍历小于 n 次的非零矩阵多项式 $r(A)$。所以必存在 $l\in[0,2^n-2]$，使得 $A^l=A^{i_1}+A^{i_2}+\cdots+A^{i_k}$。

将 A^l 代入(3)式，有 $A^l\alpha=0$，A^l 是满秩的，所以有 $\alpha=0$，这与 α 是非零向量矛盾，问题得证。

定理 2 的证明：设 $F(x)=x^n+A_{n-1}x^{n-1}+\cdots+A_1x+A_0\in M_m(F_2)[x]$ 是 s^∞ 的特征多项式，它对应的状态转移矩阵为

$$T=\begin{pmatrix} A_{n-1} & A_{n-2} & \cdots & \cdots & A_0 \\ E_m & 0 & 0 & 0 & 0 \\ 0 & \ddots & \cdots & \vdots & \\ 0 & 0 & E_m & 0 & 0 \\ 0 & 0 & 0 & E_m & 0 \end{pmatrix}_{mn\times mn}$$

则有 $T(s_{n-1},\cdots,s_1,s_0)^t=(s_n,s_{n-1},\cdots,s_1)^t$。

记 mn 维向量 $X_0=(s_{n-1},s_{n-2},\cdots,s_1,s_0)^t$，由定义 5 知

$$H_0^{(n)}=(X_0,TX_0,T^2X_0,\cdots,T^{mn-2}X_0)_{mn\times mn}$$

因为 T 的周期为 $2^{mn}-1$，由引理 1，得 $H_0^{(n)}$ 是可逆矩阵，所以 $H_0^{(n)}$ 的最后 m 行线性无关，即 s^∞ 的 m 个分位序列线性无关。

定理 3 说明了 s^∞ 分位序列的极小多项式与状态转移矩阵的关系。

定理 3 设 F_{2^m} 上的 σ-LFSR 序列 s^∞ 是 n 级本原的。设 T 是它的状态转移矩阵，$g(x)=x^{mn}+b_1x^{mn-1}+\cdots+b_{mn-1}x+1\in F_2[x]$ 是其分位序列的极小多项式，则 $g(x)=|\lambda E-T|$，即 $g(x)$ 是 T 的特征多项式。

证明：因为 s^∞ 是 n 级本原的，由定义 5，任意 mn 维向量 X 一定等于 s^∞ 某个 n 级状态矩阵的第一列，不妨设为第 i 个，记为 $H_i^{(n)}$。则有 $T\cdot H_i^{(n)}=H_{i+1}^{(n)}$。记

$$H_i^{(n)}=(X,X_{i+1},\cdots,X_{i+mn-1})$$

$$H_{i+1}^{(n)}=(X_{i+1},X_{i+2},\cdots,X_{i+mn})$$

由递归关系，有 $X_{i+mn}=b_1X_{i+mn-1}+\cdots+b_{mn-1}X_{i+1}+X$，即

$$T^{mn}\cdot X=b_1T^{mn-1}\cdot X+\cdots+b_{mn-1}T\cdot X+X$$

$$(T^{mn}+b_1T^{mn-1}+\cdots+b_{mn-1}T+1)X=0$$

由 X 的任意性，得

$$T^{mn}+b_1T^{mn-1}+\cdots+b_{mn-1}T+1=0,\text{即 } g(T)=0。$$

可见 $g(x)$ 是 T 的 mn 次零化多项式。因为 s^∞ 是 n 级本原的，所以 T 达到最大周期，即 $ord(T)=2^{mn}-1$，所以 T 的 mn 次零化多项式唯一，故一定有 $g(x)=|\lambda E-T|$。

定义 6 对于任一 σ-LFSR 序列 $s^\infty\in F_{2^m}^\infty$，记能够产生它的次数最低的 σ-多项式为 $F(x)$，则 $F(x)$ 称为 s^∞ 的极小多项式，显然有 $F(x)\in M_m(F_2)[x]$。

4 本原 σ-LFSR 序列极小多项式的计算

实际中最有用的 σ-LFSR 序列是本原的。如果知道了一个本原 σ-LFSR 序列，能否求出它的极小多项式呢？本节利用上节定义的状态矩阵解决这个问题。

算法 1 计算本原 σ-LFSR 序列的极小多项式

设 $s^\infty=s_0,s_1,s_2,\cdots$ 是 F_{2^m} 上的本原 σ-LFSR 序列，求 s^∞ 极小多项式的算法描述如下：

Step1 利用 BM 算法求出 s^∞ 第一条分位序列的极小多项式，得到其次数 d，则 $n=d/m$。

Step2 根据定义 5，构造 s^∞ 的第一个和第二个 n 级状态矩阵 $H_0^{(n)}$ 和 $H_1^{(n)}$。

Step3　计算 $T=H_1^{(n)}(H_0^{(n)})^{-1}$，由 $H_i^{(n)}$ 的形式知 T 一定形如 $\begin{pmatrix} A_{n-1} & A_{n-2} & \cdots & \cdots A_0 & \\ E_m & 0 & 0 & 0 & 0 \\ 0 & \ddots & \cdots & \vdots & \\ 0 & 0 & E_m & 0 & 0 \\ 0 & 0 & 0 & E_m & 0 \end{pmatrix}_{mn\times mn}$，则 s^∞ 的极小多项式为 $F(x)=x^n+A_{n-1}x^{n-1}+\cdots+A_1x+A_0$。显然，$F(x)\in M_m(F_2)[x]$，并且这样的多项式是唯一的。

证明：由定理 1，若 s^∞ 是一个 n 级本原 σ-LFSR 序列，则其任意一个分位序列均为 F_2 上 mn 级的 m-序列。所以通过 Step1 可计算出 s^∞ 极小多项式的次数 n。

设 s^∞ 的特征多项式为 $F(x)=x^n+A_{n-1}x^{n-1}+\cdots+A_1x+A_0$，其对应的状态转移矩阵为

$$T=\begin{pmatrix} A_{n-1} & A_{n-2} & \cdots & \cdots & A_0 \\ E_m & 0 & 0 & 0 & 0 \\ 0 & \ddots & \cdots & \vdots & \\ 0 & 0 & E_m & 0 & 0 \\ 0 & 0 & 0 & E_m & 0 \end{pmatrix}_{mn\times mn}$$

按照 σ-LFSR 序列的产生方式，对 s^∞ 的任两个 n 级状态矩阵 $H_i^{(n)}$ 和 $H_{i+1}^{(n)}$，均有 $TH_i^{(n)}=H_{i+1}^{(n)}$，Step2 中取 $H_0^{(n)}$ 和 $H_1^{(n)}$。根据定理 1 的证明，知 $H_0^{(n)}$ 和 $H_1^{(n)}$ 都是可逆矩阵，所以一定有 $T=H_1^{(n)}(H_0^{(n)})^{-1}$。

同时，根据 T 的计算方式知，它由 $H_0^{(n)}$ 和 $H_1^{(n)}$ 唯一确定，而 $H_0^{(n)}$ 和 $H_1^{(n)}$ 是由 s^∞ 唯一确定的，所以 T 唯一。这说明本原 σ-LFSR 序列的极小多项式唯一。

5　本原 σ-LFSR 的判别

上节给出了一个求本原 σ-LFSR 序列极小多项式的方法。自然还会提出一个问题：对给定的 σ-LFSR 序列 s^∞，如何判断它是否本原呢？

定理 2 给出了本原 σ-LFSR 序列的一条性质。可惜的是，不能根据它来判断 σ-LFSR 序列是否本原。因为经测试发现，定理 2 仅仅是一个必要条件。

本节将利用算法 1，给出一个 σ-LFSR 序列为本原的充要条件。

定理 4　设 $s^\infty=s_0,s_1,s_2,\cdots$ 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

(I) s^∞ 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 $g(x)$；

(II) s^∞ 的第一个状态矩阵 $H_0^{(n)}$ 可逆。

证明：(必要性)若 s^∞ 是本原的，由定理 1，(I)满足。由定理 2 的证明知(II)也满足。

(充分性)由条件(I)知 s^∞ 是 F_{2^m} 上的周期序列，且周期为 $2^{mn}-1$。要证明 s^∞ 是 n 级本原 σ-LFSR 序列，只需说明存在一个 n 次 σ-多项式生成它。

因 $H_0^{(n)}$ 可逆，可构造 mn 阶矩阵 $T=H_1^{(n)}\cdot(H_0^{(n)})^{-1}\in M_{mn}(F_2)$，下面证明 T 就是 s^∞ 的状态转移矩阵。

设

$$H_i^{(n)}=\begin{pmatrix} s_{i+n-1} & s_{i+n-1} & \cdots & s_{i+mn+n-2} \\ \vdots & \vdots & \cdots & \vdots \\ s_{i+1} & s_{i+2} & \cdots & s_{i+mn} \\ s_i & s_{i+1} & \cdots & s_{i+mn-1} \end{pmatrix}_{mn\times mn}=(X_i,X_{i+1},X_{i+2},\cdots,X_{i+mn-1})_{mn\times mn}$$

根据 T 的定义，有 $T\cdot H_0^{(n)}=H_1^{(n)}$，所以有

$T\cdot X_i=X_{i+1}$，$i=0,1,\cdots,mn-1$

设分位序列的极小多项式 $g(x)$ 为 $g(x)=x^{mn}+b_1x^{mn-1}+\cdots+b_{mn-1}x+1$，由条件(I)，得

$X_{mn}=b_1X_{mn-1}+b_2X_{mn-2}+\cdots+b_{mn-1}X_1+X_0$

两边同作用 T，得

$$\begin{aligned} T\cdot X_{mn}&=b_1T\cdot X_{mn-1}+b_2T\cdot X_{mn-2}+\cdots+b_{mn-1}T\cdot X_1+T\cdot X_0\\ &=b_1X_{mn}+b_2X_{mn-1}+\cdots+b_{mn-1}X_2+X_1\\ &=X_{mn+1}\end{aligned}$$

依此类推，可得

$T\cdot X_i=X_{i+1}$，对任意 $i\geqslant 0$

这说明 T 恰好是 s^∞ 的状态转移矩阵，所以存在相应的 n 次 σ-多项式生成 s^∞，故 s^∞ 是 n 级本原 σ-LFSR 序列。

结束语　σ-LFSR 序列生成速度快，同时具有良好的密码学性质[5,6]。本文对本原 σ-LFSR 序列的性质做了研究，进一步刻画了其分位序列的性质，同时给出了计算本原 σ-LFSR 序列极小多项式的方法，最后给出一个充要条件，解决了本原 σ-LFSR 序列的判断问题。随着字 LFSR 的流行与处理器的发展，我们希望 σ-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] Golomb S W. Shift Register Sequences. San Francisco: Holden-Day, 1967

[2] Preneel B. Introduction to the Proceedings of the Fast Software Encryption 1994 Workshop // Lecture Notes in Computer Science. Vol. 1008, 1995: 1-5

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

[4] 沈勇，何开成，韩文报. F_4 上的 σ-线性反馈移位寄存器 // 国家自然科学基金委员会“网络与信息安全重大研究计划”2004 年学术论文集. 2004

[5] Zeng Guang, Han Wenbao, He Kaicheng. High Efficiency Feedback Shift Register: σ-LFSR. Cryptology ePrint Archive, Report 2007/114. http://eprint.iacr.org/, 2007

[6] 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

[7] Lidi R, Niederreiter H. Finite Fields[M]. Addison-Wesley, 1983

[8] Rogaway P, Coppersmith D. A software-optimized encryption algorithm // Fast Software Encryption 1993 Workshop. LNCS. Berlin Heiderberg: Springer-Verlag, 1994, 809: 53-63

[9] Coppersmith D, Halevi S, Jutla C. Scream: A Software-efficient Stream Cipher[A] // Fast Software Encryption (FSE)2002(Lecture Notes in Computer Science Vol. 2365)[C]. Leuven, Belgium: Springer Verlag, 2002: 195-209

[10] Berbain C, Billet O, et al. Sosemanuk: a fast software-oriented stream cipher. ECRYPT Stream Cipher Project, 2007

[11] Jansen C J A. Streamcipher design: Make your LFSRs jump! The State of the Art of Stream Ciphers // Workshop Record. Brugge, Belgium, 2004: 94-108

[12] Tsaban B, Vishne U. Efficient Linear Feedback Shift Registers with Maximal Period. Finite Fields Appl., 2002, 8: 256-267

[13] Dewar M, Panario D. Linear Transformation Shift Registers[J]. IEEE Trans. Inform. Theory, 2003, 49: 2047-2052