SLCE 序列的 2-adic 复杂度

王艳，李顺波，薛改娜
（西安建筑科技大学理学院，陕西 西安 710055）

摘 要：针对 SLCE 序列的 2-adic 复杂度，首先利用分圆数获得此类序列的自相关函数值，根据 2-adic 复杂度与自相关函数的关系分析了序列 2-adic 复杂度取值特点，结合 SLCE 序列的自相关函数值与周期的最大公因子，给出了一个 SLCE 序列 2-adic 复杂度达到最大值的条件。结果表明很多有限域上的 SLCE 序列的 2-adic 复杂度可达到最大值。

关键词：序列密码；Sidelnikov-Lempel-Cohn-Eastman 序列；2-adic 复杂度；自相关性
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019143

2-adic complexity of SLCE sequence

WANG Yan, LI Shunbo, XUE Gaina
School of Science, Xi’ an University of Architecture and Technology, Xi’ an 710055, China

Abstract: Aiming at the 2-adic complexity of Sidelnikov-Lempel-Cohn-Eastman sequences, autocorrelation function value of this kind of sequence was obtained by using the cyclotomic number. Based on the relationship between 2-adic complexity and autocorrelation function, properties of 2-adic complexity value were analyzed. According to the greatest common divisor between the autocorrelation function value and the period of SLCE sequence, the condition that the 2-adic complexity of a SLCE sequence reaches its maximum value was given. The results show that 2-adic complexity of SLCE sequence on many finite field can reach the maximum value.

Key words: stream cipher, Sidelnikov-Lempel-Cohn-Eastman sequence, 2-adic complexity, autocorrelation

1 引言

周期伪随机序列在通信和密码领域有着广泛的应用。有关周期序列的自相关性、线性复杂度及 2-adic 复杂的研究一直是序列研究的热点。

周期序列可以由线性移位寄存器(LFSR，linear feedback shift register)生成，也可以由带进位的移位寄存器(FCSR，feedback with carry shift register)生成。生成序列的最短 LFSR 的级数称为该序列的线性复杂度，生成序列的最短 FCSR 的级数称为该序列的 2-adic 复杂度。由 B-M (Berlekamp-Massey)算法和有理逼近算法可知，获得连续 2 倍线性复杂度或 2 倍 2-adic 复杂度长的序列，便可以恢复生成该序列的 LFSR 或 FCSR，因此，周期序列的设计要求高线性复杂度、高 2-adic 复杂度。同时，序列的自相关性也是衡量序列的一个重要指标，好的序列应该有低的自相关值。

SLCE (Sidelnikov-Lempel-Cohn-Eastman) 序列是一类偶周期分圆序列，由 Sidelnikov[1]首次提出，故有文献称该类序列为 Sidelnikov 序列；Lempel、Cohn 和 Eastman[2]研究了该类序列的自相关性，使该序列受到关注，因而很多文献中以这 4 人的姓名首字母的缩写（SLCE）命名这种分圆序列。SLCE 序列的线性复杂度一度是一个难题，Kyureghyan 等[3]

收稿日期：2018−09−13；**修回日期**：2019−05−21
基金项目：西安建筑科技大学自然科学专项基金资助项目（No.1609718034）；国家自然科学基金资助项目（No.11471255）；西安建筑科技大学校人才基金资助项目（No.RC1221）
Foundation Items: The Natural Science Foundation of Xi’an University of Architectural Science and Technology (No.1609718034), The National Natural Science Foundation of China (No.11471255), The Talent Fund of Xi’an University of Architectural Science and Technology (No.RC1221)

发现 SLCE 序列的线性复杂度与一类分圆数的余数及 Jacobsthal 和有关，推进了此项研究工作。Helleseth 等[4-5]给出了 p=3,5,7 时，周期为 p^m-1 序列的线性复杂度；Meidl 等[6]利用分圆数确定了某些具体序列的线性复杂度。之后关于 SLCE 序列 1-错线性复杂度[7]、线性复杂度的界[8-9]、特征值[10]等研究陆续出现。基于这些研究，SLCE 序列的 2-adic 复杂度也成了一个有意义的问题，本文主要研究 SLCE 序列的 2-adic 复杂度。

2 基础知识

2.1 SLCE 序列

设 q 为奇素数 p 的幂，即 $q=p^m$，记 F_q 为 q 元有限域，α 为 F_q 的本原元，即 F_q 的乘法群 $F_q^*=F_q\setminus\{0\}$ 的生成元。定义 F_q^* 中的二次特征为

$$\eta(\beta)=\begin{cases}1, & \text{存在}\gamma\in F_q^*\text{使}\beta=\gamma^2\\ 0, & \beta=0\\ -1, & \text{其他}\end{cases}$$

设 $q=df+1$，$\langle\alpha^d\rangle$ 为由 α^d 生成的乘法子群，称陪集 $C_i^d=\alpha^i\langle\alpha^d\rangle, i=0,\cdots,d-1$ 为关于 F_q 的 d 阶分圆陪集。显然此处 C_i^d 依赖于 α 的选择，于是有 $F_q^*=\bigcup_{i=0}^{d-1}C_i^d$。

设 $C_{(l,m)}^d=(C_l^d+1)\cap C_m^d, l,m\in\{0,\cdots,d-1\}$，称常数 $(l,m)_d=\left|C_{(l,m)}^d\right|$ 为 F_q 的 d 阶分圆数。设 $D_{(l,m)}^d=C_l^d\cap(C_m^d-1), l,m\in\{0,\cdots,d-1\}$，由 $\left|D_{(l,m)}^d\right|=\left|C_l^d\cap(C_m^d-1)\right|=\left|(C_l^d+1)\cap C_m^d\right|$ 可知 $\left|D_{(l,m)}^d\right|=(l,m)_d$。关于 2 阶分圆数，有如下结果。

引理 1[11] 若 $q\equiv 1(\bmod 4)$，则有

$$(0,0)_2=\frac{q-5}{4},\ (0,1)_2=(1,0)_2=(1,1)_2=\frac{q-1}{4}$$

若 $q\equiv 3(\bmod 4)$，则有

$$(0,1)_2=\frac{q+1}{4},\ (0,0)_2=(1,0)_2=(1,1)_2=\frac{q-3}{4}$$

由前述记号，在 F_q^* 上定义周期为 $(q-1)$ 的 SLCE 序列 $\{s_i\}$ 如式(1)所示。

$$s_i=\begin{cases}1, & \eta(\alpha^i+1)=-1\\ 0, & \text{其他}\end{cases}\tag{1}$$

称序列 $\{s_i\}$ 为 SLCE 序列。这个定义等价于

$$s_i=\begin{cases}1, & \alpha^i\in D_{(0,1)}^2\cup D_{(1,1)}^2\\ 0, & \text{其他}\end{cases}\tag{2}$$

也等价于

$$s_i=\begin{cases}1, & \alpha^i\in\{\alpha^{2i+1}-1\}_{i=0}^{\frac{q-1}{2}-1}\\ 0, & \text{其他}\end{cases}\tag{3}$$

显然，$s_i=\frac{1}{2}(1-X(\alpha^i+1)-\eta(\alpha^i+1))$，且 $\{s_i\}$ 是平衡序列。其中，有

$$X(c)=\begin{cases}1, & c=0\\ 0, & \text{其他}\end{cases}\tag{4}$$

根据式(2)，在有限域 F_{31} 中取本原元 α=3，d=2，则有

$$C_0^2=3^0\left\langle 3^2\right\rangle=\{9, 19, 16, 20, 25, 8, 10, 28, 4, 5, 14, 2, 18, 7, 1\}$$

$$C_1^2=3^1\left\langle 3^2\right\rangle=\{27, 26, 17, 29, 13, 24, 30, 22, 12, 15, 11, 6, 23, 21, 3\}$$

进而可得一个周期为 30 的 SLCE 序列如式(5)所示。

$$\{s_i\}=1000\ 1100\ 1100\ 0101\ 1011\ 0111\ 0010\ 10\tag{5}$$

2.2 FCSR 和序列的 2-adic 复杂度

考虑到线性移位寄存器容易被攻击的问题，Klapper 等[12]提出了自带进位的反馈移位寄存器(FCSR)。FCSR 由 r 个系数 $q_i(i=1, 2,\cdots,r)\in(0,1)$，$q_r=1$，以及一个初始存储整数 m_{n-1}(可为任意整数)确定，结构如图 1 所示。

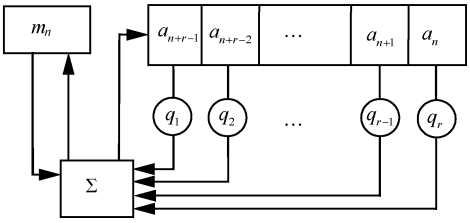

图 1 FCSR 结构

记 FCSR 的任意一个状态为 $(a_{n-1},a_{n-2},\cdots,a_i,\cdots,a_{n-r})$ $(a_i\in\{0,1\}, i=n-1,n-2,\cdots,n-r)$，存储整数为 m_{n-1}，其运算如下。

1) 计算 $\delta_n=\sum_{k=1}^{r}q_k a_{n-k}+m_{n-1}$。

2) 右移一位，输出最右端的 a_{n-r}。

3) 将 $a_n=\delta_n(\bmod 2)$ 放入 FCSR 最左端。

4) 令 $m_n=\frac{\delta_n-a_n}{2}=\left\lfloor\frac{\delta_n}{2}\right\rfloor$。

每一个最终周期序列都可以由一个 FCSR 产生。反过来，所有由 FCSR 生成的序列也都是最终

周期序列[12]。设 $\underline{x}$ 为最终周期序列，q 为生成 $\underline{x}$ 的 FCSR 的连接整数，则称 q 为 $\underline{x}$ 的极小连接整数，极小连接整数整除任意连接整数。FCSR 序列的周期完全由其极小连接整数确定。类似于线性复杂度，2-adic 复杂度衡量一个周期序列需要用多大周期的 FCSR 来生成，定义如下。

定义 1[12]　设 $s=\{s_i\}$ 为严格周期序列，$\sum_{i=0}^{\infty}s_i2^i=\frac{p}{q}$，其中，$q$ 为序列 s 的极小连接数，整数 p 满足 $\gcd(p,q)=1$，称实数 $\varphi(s)=\mathrm{lb}q$ 为序列 s 的 2-adic 复杂度。

2-adic 复杂度衡量一个二元序列由带进位的移位寄存器(FCSR)[12-13]生成的难度，它与线性复杂度没有必然联系。具有高线性复杂度的序列的 2-adic 复杂度可能会很低，反之亦然。Klapper 和 Goresky[12]提出了有理逼近算法，即对于一条固定序列，只要已知其约为 2-adic 复杂度个位置上的元素的 2 倍，就能唯一确定原序列。这就要求密钥序列必须具有高的 2-adic 复杂度，才能有效抵抗有理逼近攻击。

设 s 为严格周期序列，记 $S(x)=\sum_{i=0}^{N-1}s_ix^i\in Z[x]$，则有 $\sum_{i=0}^{\infty}s_i2^i=\frac{S(2)}{2^N-1}$，故

$$\varphi(s)=\mathrm{lb}(2^N-1)-\mathrm{lb}\gcd(S(2),2^N-1)$$

当 $\gcd(S(2),2^N-1)=1$ 时，$\varphi(s)$ 达到最大值 $\mathrm{lb}(2^N-1)\approx N$。

巧合的是，$2^N-1=M_N$ 恰为第 N 个 Mersenne 数，当 M_N 为 Mersenne 素数时，有 $\gcd(S(2),2^N-1)=1$，即序列 s 的极小连接整数为 Mersenne 素数时，其 2-adic 复杂度达到最大。迄今，已发现的 Mersenne 素数有 51 个，分别为 N=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1 279, 2 203, 2 281, 3 217, 4 253, 4 423, 9 689, 9 941, 11 213, 19 937, 21 701, 23 209, 44 497, 86 243, 110 503, 132 049, 216 091, 756 839, 859 433, 1 257 787, 1 398 269, 2 976 221, 3 021 377, 6 972 593, 13 466 917, 20 996 011, 24 036 583, 25 964 951, 30 402 457, 32 582 657, 37 156 667, 42 643 801, 43 112 609, 57 885 161, 74 207 281, 77 232 917, 82 589 933。由于第 N 个 Mersenne 数为素数的必要条件是 N 为素数，因而对素数周期序列，当周期 N 满足 2^N-1 为素数时，序列 2-adic 复杂度达到最大。

对一般周期序列，2-adic 复杂度由 $\gcd(S(2),2^N-1)$ 确定，这依赖于序列本身的性质。Tian 等[13]研究了 m 序列的 2-adic 复杂度，利用 m 序列极小多项式的特征，推导出 m 序列可以达到最大 2-adic 复杂度。Xiong 等[14]通过对周期序列的循环行列式非奇异性的研究，指出任何周期为 N 的理想二值自相关序列的 2-adic 复杂度就是 N，该结果覆盖了文献[13]的结果。Hu 等[15]对文献[14]的结果给出了一个简化的证明，给出了获得周期序列 2-adic 复杂度的新方法。

3　SLCE 序列的自相关性

设 $\{s_i\},i=0,1,\cdots,n-1$，为二元序列，称函数

$$\mathrm{AC}(\tau)=\sum_{i=0}^{n-1}(-1)^{s_i+s_{i+\tau}},\tau=0,1,\cdots,n-1$$

为该序列的自相关函数。周期为 n 的序列 $\{s_i\}$ 的自相关函数可用差集表示为[16]

$$\mathrm{AC}(\tau)=n-4(|C|-|(\tau+C)\cap C|),$$

其中，集合 $C=\{i\,|\,s_i=1,i=0,1,\cdots,n-1\}$ 为序列 $\{s_i\}$ 的支撑集。

由于 SLCE 序列为周期为 $(q-1)$ 的平衡序列，其自相关函数满足

$$\mathrm{AC}(\tau)=q-4\left(\frac{q-1}{2}-|(\tau+C)\cap C|\right)\qquad(6)$$

自相关函数值反映了序列在移位 τ 后，与原序列的接近程度。实际应用中希望序列的自相关函数值尽可能小。

设 q 为奇素数的幂，即 $q=p^m$，记 F_q 为 q 元有限域，α 乘法群 $F_q^*=F_q\setminus\{0\}$ 的本原元。记

$$A_1=\{\tau\,|\,(\alpha^\tau-1)^{-1}\in D_0,\ \alpha^\tau(\alpha^\tau-1)^{-1}\in D_0\}$$
$$A_2=\{\tau\,|\,(\alpha^\tau-1)^{-1}\in D_0,\ \alpha^\tau(\alpha^\tau-1)^{-1}\in D_1\}$$
$$A_3=\{\tau\,|\,(\alpha^\tau-1)^{-1}\in D_1,\ \alpha^\tau(\alpha^\tau-1)^{-1}\in D_0\}$$
$$A_4=\{\tau\,|\,(\alpha^\tau-1)^{-1}\in D_1,\ \alpha^\tau(\alpha^\tau-1)^{-1}\in D_1\}$$

定理 1　设 $\{s_i\}$ 是周期为 $(q-1)$ 的 SLCE 序列，则

1) 当 $q\equiv1(\mathrm{mod}\,4)$ 时，

$$\mathrm{AC}(\tau)=\begin{cases}0, & \tau\in A_1\cup A_2\cup A_3\\ -4, & \tau\in A_4\end{cases}$$

2) 当 $q\equiv3(\mathrm{mod}\,4)$ 时，

$$\mathrm{AC}(\tau)=\begin{cases}-2, & \tau\in A_1\cup A_2\cup A_4\\ 2, & \tau\in A_3\end{cases}$$

证明　根据式(1)，需计算 $|(\tau+C)\cap C|$，定义 $\alpha^C=\{\alpha^i:i\in C\}=D_1-1$，及 $\alpha^{C+\tau}=\alpha^\tau(D_1-1)$，则有

$$|(\tau+C)\cap C|=|\alpha^{\tau}\cap\alpha^{\tau+C}|=$$

$$|(D_1-1)\cap\alpha^{\tau}(D_1-1)|=|(D_1+\alpha^{\tau}-1)\cap\alpha^{\tau}D_1|=$$

$$|((\alpha^{\tau}-1)^{-1}D_1+1)\cap\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1$$

由引理 1 和式(1)可得

1) 当 $q\equiv 1(\bmod 4)$ 时，若 $\tau\in A_1\cup A_2\cup A_3$，则有

$(\alpha^{\tau}-1)^{-1}D_1\in D_1$，$\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1\in D_1$

或者 $(\alpha^{\tau}-1)^{-1}D_1\in D_1$，$\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1\in D_0$

或者 $(\alpha^{\tau}-1)^{-1}D_1\in D_0$，$\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1\in D_1$

对应的 $|(\tau+C)\cap C|$ 分别等于二阶分圆数 $(1,1)_2$、$(1,0)_2$ 和 $(0,1)_2$，且都等于 $\frac{q-1}{4}$。根据式(6)有

$$\mathrm{AC}(\tau)=q-1-4\left(\frac{q-1}{2}-\frac{q-5}{4}\right)=0$$

若 $\tau\in A_4$，则有

$(\alpha^{\tau}-1)^{-1}D_1\in D_0$，$\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1\in D_0$

$$|(\tau+C)\cap C|=(0,0)_2=\frac{q-5}{4}$$

于是

$$\mathrm{AC}(\tau)=q-1-4\left(\frac{q-1}{2}-\frac{q-5}{4}\right)=-4$$

2) 当 $q\equiv 3(\bmod 4)$ 时，若 $\tau\in A_1\cup A_2\cup A_4$，则有

$(\alpha^{\tau}-1)^{-1}D_1\in D_1$，$\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1\in D_1$

或者 $(\alpha^{\tau}-1)^{-1}D_1\in D_1$，$\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1\in D_0$

或者 $(\alpha^{\tau}-1)^{-1}D_1\in D_0$，$\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1\in D_0$

对应的 $|(\tau+C)\cap C|$ 分别等于 $(1,1)_2$、$(1,0)_2$ 和 $(0,0)_2$，且都等于 $\frac{q-3}{4}$。根据式(6)有

$$\mathrm{AC}(\tau)=q-1-4\left(\frac{q-1}{2}-\frac{q-3}{4}\right)=-2$$

若 $\tau\in A_3$，则有

$(\alpha^{\tau}-1)^{-1}D_1\in D_0$，$\alpha^{\tau}(\alpha^{\tau}-1)^{-1}D_1\in D_1$

$$|(\tau+C)\cap C|=(0,1)_2=\frac{q+1}{4}$$

于是

$$\mathrm{AC}(\tau)=q-1-4\left(\frac{q-1}{2}-\frac{q+1}{4}\right)=2$$

证毕。

定理 1 表明 SLCE 序列是 3 值自相关序列。

推论 1 设 $\{s_i\}$ 是周期为 $q-1$ 的 SLCE 序列，则

1) 当 $q\equiv 1(\bmod 4)$ 时，在 $\tau=1,2,\cdots,q-2$ 中有 $\frac{q-1}{4}$ 个数使 $\mathrm{AC}(\tau)=-4$。

2) 当 $q\equiv 3(\bmod 4)$ 时，在 $\tau=1,2,\cdots,q-2$ 中有 $\frac{q-3}{4}$ 的数使 $\mathrm{AC}(\tau)=2$。

由分圆数的取法可证明推论 1。

定义 2 若序列 $\{s_i\}$、$\{t_j\}$ 均为周期为 N 的序列，并且在一个周期上有 $s_i=t_{N-1-i}, i=0,1,\cdots,N-1$，则称 $\{s_i\}$、$\{t_j\}$ 为互反序列。

定理 2 记 φ 为欧拉函数，域 F_q 中共有 $\varphi(q-1)$ 个 SLCE 序列，并成对为互反序列。

证明 由 F_q 中本原元的个数为 $\varphi(q-1)$ 可得，由于在有限域中，当 α 为本原元时，α^{-1} 也为本原元，故 $\varphi(q-1)$ 个本原元成对出现。由于对本原元 α，$\alpha^i\in\alpha\langle\alpha^2\rangle-1$ 时，$\alpha^{-i}=\alpha^{q-1-i}\in\alpha^{-1}\langle\alpha^2\rangle-1$，故 α^{-1} 生成序列的第 i 个元与 α 生成序列的第 $(q-1-i)$ 个元一样，即为互反序列。

证毕。

定理 3 设 $\{s_i\}$ 是周期为 $(q-1)$ 的 SLCE 序列，则

1) 当 $q\equiv 1(\bmod 4)$ 时，F_q 上的全部 SLCE 序列共有 $\frac{\varphi(q-1)}{4}$ 个自相关谱。

2) 当 $q\equiv 3(\bmod 4)$ 时，F_q 上的全部 SLCE 序列共有 $\frac{\varphi(q-1)}{2}$ 个自相关谱。

证明 记 α 为 F_q 的一个本原元，当 $q\equiv 1(\bmod 4)$ 时，$-\alpha$ 也是 F_q 的一个本原元，且有 $\langle(-a)^2\rangle=\langle a^2\rangle$，故 α 与 $-\alpha$ 生成序列的自相关谱相同。又由自相关函数的对称性及 α 与 α^{-1} 生成序列为互反序列可知，α 与 α^{-1} 生成序列的自相关谱相同。于是 α、$-\alpha$、α^{-1}、$-\alpha^{-1}$ 生成的序列同自相关谱。并且由其他本原元生成序列不同可得，当 $q\equiv 1(\bmod 4)$ 时，F_q 上的全部 SLCE 序列共有 $\frac{\varphi(q-1)}{4}$ 个自相关谱。

当 $q\equiv 3(\bmod 4)$ 时，对本原元 α、$-\alpha$ 不是本原元，由前述知，此时 F_q 上的全部 SLCE 序列共有 $\frac{\varphi(q-1)}{2}$ 个自相关谱。

证毕。

下面研究 SLCE 序列的 2-adic 复杂度。

4 SLCE 序列的 2-adic 复杂度

定理 4 设 $\{s_i\}$ 是周期为 $(q-1)$ 的 SLCE 序列，则

1) 当 $q\equiv 1(\bmod 4)$ 时，$\gcd(S(2),2^{q-1}-1)=$

$\gcd(\frac{q-1}{4}-\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}} 2^\tau, 2^{q-1}-1)$。

2) 当 $q\equiv 3(\bmod 4)$ 时，$\gcd(S(2),2^{q-1}-1)=\gcd(\frac{q+1}{4}+\sum_{\tau\in \mathrm{AC}_\tau^{(2)}} 2^\tau, 2^{q-1}-1)$。

其中，$\mathrm{AC}_\tau^{(k)}=\{\tau|\mathrm{AC}(\tau)=k\}$。

证明　设 $\{s_i\}$ 为 SLCE 序列，记 $Z[x]$ 多项式为

$$P(x)=\sum_{i=0}^{q-2}(-1)^{s_i}x^i$$

则有

$$P(x)P(x^{-1})=\left(\sum_{i=0}^{q-2}(-1)^{s_i}x^i\right)\left(\sum_{j=0}^{q-2}(-1)^{s_j}x^{-j}\right)=\sum_{i=0}^{q-2}\sum_{j=0}^{q-2}(-1)^{s_i+s_j}x^{i-j}\equiv q-1+\sum_{\tau=1}^{q-2}\sum_{j=0}^{q-2}(-1)^{s_{j+\tau}+s_j}x^\tau \bmod(x^{q-1}-1)\equiv q-1+\sum_{\tau=1}^{q-2}\mathrm{AC}(\tau)x^\tau \bmod(x^{q-1}-1)$$

当 $x=2$ 时，有

$$P(2)P(2^{-1})\equiv q-1+\sum_{\tau=1}^{q-2}\mathrm{AC}(\tau)2^\tau \bmod(2^{q-1}-1)\equiv q-1+\sum_{\tau=1}^{q-2}\mathrm{AC}(\tau)2^\tau \bmod(2^{q-1}-1)$$

又由

$$P(2)=\sum_{i=0}^{q-2}(-1)^{s_i}2^i=\sum_{i=0}^{q-2}(1-2s_i)2^i=2^{q-1}-1-2S(2)$$

知 $P(2)\equiv -2S(2) \bmod(2^{q-1}-1)$，从而

$$-2S(2)P(2^{-1})\equiv q-1+\sum_{\tau=1}^{q-2}\mathrm{AC}(\tau)2^\tau \bmod(2^{q-1}-1)$$

即

$$k(2^{q-1}-1)-2P(2^{-1})S(2)=q-1+\sum_{\tau=1}^{q-2}\mathrm{AC}(\tau)2^\tau$$

其中，k 为整数。于是

$$\gcd(S(2),2^{q-1}-1)=\gcd(q-1+\sum_{\tau=1}^{q-2}\mathrm{AC}(\tau)2^\tau,2^{q-1}-1) \quad (7)$$

1) $q\equiv 1(\bmod 4)$ 时，$\mathrm{AC}_\tau^{(-4)}=\{\tau|\mathrm{AC}(\tau)=-4\}$，于是

$$q-1+\sum_{\tau=1}^{q-2}C(\tau)2^\tau\equiv q-1+(-4)\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}}2^\tau \bmod(2^{q-1}-1)\equiv \frac{q-1}{4}-\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}}2^\tau \bmod(2^{q-1}-1)$$

$$\gcd(S(2),2^{q-1}-1)=\gcd(\frac{q-1}{4}-\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}}2^\tau,2^{q-1}-1)$$

2) $q\equiv 3(\bmod 4)$ 时，$\mathrm{AC}_\tau^{(2)}=\{\tau|\mathrm{AC}_s(\tau)=2\}$，$\mathrm{AC}_\tau^{(-2)}=\{\tau|\mathrm{AC}(\tau)=-2\}$，于是

$$P(2)P(2^{-1})\equiv q-1+2\sum_{\tau\in \mathrm{AC}_\tau^{(2)}}2^\tau-2\sum_{\tau\in \mathrm{AC}_\tau^{(-2)}}2^\tau \bmod(2^{q-1}-1)\equiv q-1+2\sum_{\tau\in \mathrm{AC}_\tau^{(2)}}2^\tau-(-2)\sum_{\tau\in \mathrm{AC}_\tau^{(-2)}}2^\tau+(-2)\sum_{\tau=1}^{q-2}2^\tau \bmod(2^{q-1}-1)\equiv q-1+4\sum_{\tau\in \mathrm{AC}_\tau^{(2)}}2^\tau+(-2)(2^{q-1}-2) \bmod(2^{q-1}-1)\equiv q-1+2+4\sum_{\tau\in \mathrm{AC}_\tau^{(2)}}2^\tau \bmod(2^{q-1}-1)\equiv \frac{q+1}{4}+\sum_{\tau\in \mathrm{AC}_\tau^{(2)}}2^\tau \bmod(2^{q-1}-1)$$

由 $P(2)\equiv -2S(2) \bmod(2^{q-1}-1)$ 可得

$$\gcd(S(2),2^{q-1}-1)=\gcd\left(\frac{q+1}{4}+\sum_{\tau\in \mathrm{AC}_\tau^{(2)}}2^\tau,2^{q-1}-1\right)$$

证毕。

推论 2　设 $s=\{s_i\}$ 是周期为 $q-1$ 的 SLCE 序列，记 $\mathrm{AC}_\tau^{(k)}=\{\tau|\mathrm{AC}(\tau)=k\}$，有

1) 若 $q\equiv 1(\bmod 4)$ 且

$$\gcd\left(\frac{q-1}{4}-\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}}2^\tau,2^{q-1}-1\right)=1$$

则 s 的 2-adic 复杂度 $\varphi(s)$ 达到最大值。

2) 若 $q\equiv 3(\bmod 4)$，且

$$\gcd\left(\frac{q+1}{4}+\sum_{\tau\in \mathrm{AC}_\tau^{(2)}}2^\tau,2^{q-1}-1\right)=1$$

则 s 的 2-adic 复杂度 $\varphi(s)$ 达到最大值。

推论 2 的证明由定理 4 易得。

进一步，当 $q\equiv 1(\bmod 4)$ 时，有

$$2^{q-1}-1=2^{4k}-1=(2^4-1)(2^{4(k-1)}+2^{4(k-2)}+\cdots+2^4+1)$$

故当 3、5 或 15 整除 $(\frac{q-1}{4}-\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}}2^\tau)$ 时，$\gcd(\frac{q-1}{4}-\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}}2^\tau,2^{q-1}-1)$ 有因子 3、5 或 15。

当 $q\equiv 3(\bmod 4)$ 时，有

$$2^{q-1}-1=2^{4k+2}-1=(2^2-1)(2^{2\times 2k}+2^{2(2k-1)}+\ldots+2^2+1)$$

故当 $3\left|\frac{q-1}{4}-\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}}2^\tau\right.$ 时，$\gcd(\frac{q-1}{4}-\sum_{\tau\in \mathrm{AC}_\tau^{(-4)}}2^\tau,2^{q-1}-1)$ 有因子 3。

例 $q=43$ 时，F_{43} 上的本原元分别对应 3, 29, 5, 26, 12, 18, 19, 34, 20, 28, 30, 33。由本原元 3 生成的 SLCE 序列为 1,0,0,1,1,1,1,0,1,1,0,0,1,0,1,0,0,1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1。 $C_\tau^{(2)}=\{1,3,5,11,19,23,31,37,39,41\}$，且有

$$\gcd(S(2),2^N-1)=\gcd(11-\sum_{\tau\in AC_\tau^{(2)}}2^\tau,2^{42}-1)=1 \quad (8)$$

由本原元 5 生成的 SLCE 序列为 1,0,1,0,0,1,0,0, 0,0,0,0,1,1,1,0,0,1,1,0,1,0,1,1,1,0,0,1,1,0,1,1,0,1,0,1,0, 0,0,1,1,1, $C_\tau^{(2)}=\{5,11,13,15,17,25,27,29,31,37\}$，且有式(8)成立。

由本原元 26 生成的 SLCE 序列为 1,1,1,1,0,0,0, 1,0,1,0,1,1,0,1,1,0,0,1,1,1,0,1,0,1,1,0,0,1,1,1,0,0,0,0,0, 0,1,0,0,1,0, $C_\tau^{(2)}=\{5,11,13,15,17,25,27,29,31,37\}$，且有式(8)成立。

由本原元 29 生成的 SLCE 序列为 1,1,0,0,1,0,1, 1,1,0,0,1,1,1,1,1,0,0,0,0,0,0,0,1,0,1,0,0,1,0,1,0,0,1,1,0, 1,1,1,1,0,0], $C_\tau^{(2)}=\{5,11,13,15,17,25,27,29,31,37\}$，且有式(8)成立。

由 Magma 验证发现，F_{43} 中的所有 SLCE 序列都达到最大 2-adic 复杂度。类似地，F_7、F_{19}、F_{31}、F_{47} 等域上的 SLCE 序列都可达到最大 2-adic 复杂度。但 F_{3^3}、F_{17}、F_{7^2}、F_{61} 等域上的 SLCE 序列都满足 $\gcd(S(2),2^N-1)=3$。尽管没有达到最大 2-adic 复杂度，但由 $\mathrm{lb}\dfrac{2^N-1}{3}\geqslant N-2$ 可知，在 $N>4$ 时，这样的 SLCE 序列仍有很高的 2-adic 复杂度。

5 结束语

SLCE 序列已被证明具有高线性复杂度，其 2-adic 复杂度取值成为有意义的问题。本文通过 SLCE 序列的自相关函数值研究了其 2-adic 复杂度，给出了 SLCE 序列可以达到最大 2-adic 复杂度的一个充分条件，并举例证明确实存在大量能达到条件的 SLCE 序列，这些 SLCE 序列能够抵抗有理逼近攻击，结合 SLCE 序列高线性复杂度[3-6]可知，这些 SLCE 序列是密码学意义上的好的伪随机序列。

参考文献：

[1] SIDELNIKOV V M. Some *k*-valued pseudo-random and nearly equidistant code[J]. Problems of Information Transmission, 1969, 5(1): 16-22.

[2] LEMPEL A, COHN M, EASTMAN W L. A class of balanced binary sequences with optimal autocorrelation properties[J]. IEEE Transactions on Information Theory,1977, 23(1): 38-42.

[3] KYUREGHYAN G M, POTT A. On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences[J]. Designs Codes & Cryptography, 2003, 49(1-3): 149-164.

[4] HELLESETH H, KIM S H, NO J S. Linear complexity over F_p and trace representation of Lembel-Cohn-Eastman sequences[J]. IEEE Transactions on Information Theory, 2003,49(6): 1548-1552.

[5] HELLESETH H, MAAS M, MATHIASSN J E, et al. Linear complexity over F_p of Sidel'nikov sequences[J]. IEEE Transactions on Information Theory, 2004, 50(10):2468-2472.

[6] MEIDL W, WINTERHOF A. Some notes on the linear complexity of Sidel'nikov-Lempel-Cohn-Eastman sequences[J]. Designs Codes & Cryptography, 2006, 38(2):159-178.

[7] EUN Y C, SONG H Y, KYUREGHYAN G M. One-error linear complexity over F_p of Sidelnikov sequences[C]// International Conference on Algorithmic Applications in Management. Springer, 2004, 154-165.

[8] GARAEV M Z, LUCA F, SHPARLINSKI I E, et al. On the lower bound of the linear complexity over F_p of Sidelnikov sequences[J]. IEEE Transactions on Information Theory, 2006, 52(7):3299-3304.

[9] SU M. On the linear complexity of Legendre-Sidelnikov sequences[J]. Designs Codes & Cryptography, 2015, 74(3):703-717.

[10] SABAN A, MILLAR G. Character values of the Sidelnikov-Lempel-Cohn-Eastman sequences[J]. Cryptography & Communications, 2016, 9(6):1-18.

[11] MYERSON G. Period polynomials and Gauss sums for finite fields[J]. ACTA Arithmetica, 1981, 39(3):251-264.

[12] KLAPPER A, GORESKY M. Feedback shift registers, 2-adic span, and combiners with memory[J]. Journal of Cryptology, 1997, 10(2):111-147.

[13] TIAN T, QI W F. Adic complexity of binary-sequences[J]. IEEE Transactions on Information Theory , 2010, 56(1):450-454.

[14] XIONG H, QU L, LI C. A new method to compute the 2-adic complexity of binary sequences[J]. IEEE Transactions on Information Theory, 2014, 60(4):2399-2406.

[15] HU H G. Comments on "a new method to compute the 2-adic complexity of binary sequences" [J]. IEEE Transactions on Information Theory, 2014, 60 (9): 5803-5804.

[16] DING C S. Stream ciphers and number theory [M]. Amsterdam: Elsevier, 2004: 113-114.

[作者简介]

王艳（1982− ），女，陕西三原人，博士，西安建筑科技大学副教授，主要研究方向为序列密码。

李顺波（1979− ），男，陕西周至人，博士，西安建筑科技大学副教授，主要研究方向为数字签名和序列密码。

薛改娜（1992− ），女，陕西渭南人，西安建筑科技大学硕士生，主要研究方向为序列密码。