基于 RSA 模数的一类新型广义割圆序列的迹表示

陈智雄[1],刘华宁[2],杨 阳[3]
(1. 莆田学院福建省高校应用数学重点实验室,福建莆田 351100;2. 西北大学数学学院,陕西西安 710127;
3. 福建师范大学数学与信息学院,福建福州 350007)

摘 要: 针对最近研究的周期为 pq(两个不同的大素数的乘积)的一类广义割圆序列,通过计算该序列的离散傅里叶变换系数,从而确定了该序列的 Mattson-Solomon 多项式,并由此得到了序列的迹表示形式.

关键词: 流密码; RSA 模数; 广义割圆类; 广义割圆序列; Mattson-Solomon 多项式; 迹表示
中图分类号: TN918.4 **文献标识码:** A **文章编号:** 0372-2112 (2019)07-1512-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.07.015

Trace Representation of New Generalized Cyclotomic Sequences Based on RSA Moduli

CHEN Zhi-xiong[1], LIU Hua-ning[2], YANG Yang[3]
(1. *School of Mathematics and Financial, Putian University, Putian, Fujian* 351100, *China*;
2. *School of Mathematics, Northwest University, Xi' an, Shaanxi* 710127, *China*;
3. *School of Mathematics and Information, Fujian Normal University, Fuzhou, Fujian* 350007, *China*)

Abstract: For a new family of generalized cyclotomic sequences of period pq, a product of two large distinct primes, we calculate the discrete Fourier transform and hence determine Mattson-Solomon polynomial, which helps us to describe the sequences via trace functions.

Key words: stream cipher; RSA moduli; generalized cyclotomy; generalized cyclotomic sequence; Mattson-Solomon polynomial; trace representation

1 引言

在公钥密码学中,RSA 体制是一种应用广泛的公钥密码系统(可参阅 https://www.rsa.com/).它是在 20 世纪 70 年代由 Rivest,Shamir 与 Adleman 三位专家利用模 N 剩余类环设计的,其安全性基于大整数 N 的因式分解,这里的 N 是两个不同的大素数 p,q 的乘积,因此也称 N 为 RSA 模数.对于 RSA 模数的研究得到了密码设计者、密码分析者以及数学界研究人员的关注[1~4].

在流密码中,利用 RSA 模数来设计伪随机序列也一样得到高度的重视.研究人员讨论所生成序列的数学、密码学特性,如分布问题、相关性问题、复杂度问题等[5~17].我们首先对文献中基于 RSA 模数的伪随机序列做一个综述.

本文通篇假设 $N=pq$,其中 p,q 是两个不同的奇素数.根据中国剩余定理,存在模 p 和 q 公共原根.设 g 为这样的一个公共原根,并记 $g_p\equiv g(\mathrm{mod}p)$ 及 $g_q\equiv g(\mathrm{mod}q)$.另外设整数 x 满足

$$x\equiv g(\mathrm{mod}p),x\equiv 1(\mathrm{mod}q).$$

设 $d=\gcd(p-1,q-1)$,$e=(p-1)(q-1)/d$.在文献中,主要研究两类序列,一类称为 Whiteman 广义割圆序列,另一类称为 Ding-Helleseth 广义割圆序列.

从已有文献看,对任何可能的取值 d,在研究方法上有共通的地方.所以为简便起见,下面总假设 $d=\gcd(p-1,q-1)=2$,并设

$$P=\{p,2p,\cdots,(q-1)p\},Q=\{q,2q,\cdots,(p-1)q\},Q_0=Q\cup\{0\}.$$

Whiteman 广义割圆序列($s_n^{(1)}$)定义为:

$$s_n^{(1)}=\begin{cases}0, & \text{如果 } n(\mathrm{mod}N)\in W_0\cup Q_0,\\ 1, & \text{如果 } n(\mathrm{mod}N)\in W_1\cup P,\end{cases}$$

收稿日期:2018-05-18;修回日期:2019-03-07;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61772292,No.11571277);国家自然科学基金国际合作交流项目 NSFC-RFBR (No.61911530130);福建省自然科学基金(No.2018J01425);陕西省工业科技攻关项目(No.2016GY-077, No.2016GY-080)

其中集合 W_0, W_1 称为 Whiteman 广义割圆类,规定为

$$W_j = \{g^k x^j (\mathrm{mod} pq) : k = 0,1,\cdots,e-1\}, j = 0,1.$$

Ding-Helleseth 广义割圆序列 $(s_n^{(2)})$ 定义为:

$$s_n^{(2)} = \begin{cases} 0, & \text{如果 } n(\mathrm{mod}N) \in D_0 \cup Q_0, \\ 1, & \text{如果 } n(\mathrm{mod}N) \in D_1 \cup P, \end{cases}$$

其中集合 D_0, D_1 称为 Ding-Helleseth 广义割圆类,规定为

$$D_i = \{g^{2k+i} x^j (\mathrm{mod} pq) : k = 0,1,\cdots,e/2-1, j = 0,1\}.$$

对于 Whiteman 广义割圆序列与 Ding-Helleseth 广义割圆序列,从密码学的意义上研究结果相当丰富,如它们的相关性质[9,13,18]、线性复杂度性质[5,6,8,13,14,17,19]、迹表示[11,16,20]等.

最近,丁存生等为了研究编码的需要,通过对 Ding-Helleseth 广义割圆类进行重新分割,用于设计循环码[10]. 刘华宁等利用这种新的分类,研究了一类新的序列[14]. 设

$$V_0 = \{g^{2s} (\mathrm{mod} pq), g^{2s+1} x (\mathrm{mod} pq) : 0 \le s < e/2\},$$

$$V_1 = \{g^{2s+1} (\mathrm{mod} pq), g^{2s} x (\mathrm{mod} pq) : 0 \le s < e/2\}.$$

则新序列 $(s_n^{(3)})$ 定义为:

$$s_n^{(3)} = \begin{cases} 0, & \text{如果 } n(\mathrm{mod}N) \in V_0 \cup Q_0, \\ 1, & \text{如果 } n(\mathrm{mod}N) \in V_1 \cup P. \end{cases}$$

刘华宁等[14]计算了 $(s_n^{(3)})$ 的自相关值和线性复杂度. 由于该序列刚刚提出,从文献[14]看出该序列的性质还相当不错,而其它性质还有待继续挖掘,如序列的生成表示等. 考虑到迹表示是序列生成的一个重要方式,而且文献中报道过许多重要序列如 m-序列、Legendre 序列、Fermat 商序列等的迹表示[21,23~32],因此本文将讨论 $(s_n^{(3)})$ 的迹表示,采用的工具为序列的离散傅里叶变换.

设 $\mathbb{F}_2 = \{0,1\}$ 为二元域,$\overline{\mathbb{F}}_2$ 为 $\mathbb{F}_2$ 的代数闭包. 设 (s_u) 为 $\mathbb{F}_2$ 上周期为奇数 T 的二元序列. 假设 β 是有限域 $\overline{\mathbb{F}}_2$ 的一个 T 次本原单位根,则 (s_u) 的离散傅里叶变换系数定义为:

$$\rho_i = \sum_{0 \le u < T} s_u \beta^{-iu}, 0 \le i < T.$$

根据离散傅里叶逆变换,可以还原序列

$$s_u = \frac{1}{T} \sum_{0 \le i < T} \rho_i \beta^{iu}.$$

在编码理论中,称多项式 $G(X) = \frac{1}{T} \sum_{0 \le i < T} \rho_i X^i$ 为 Mattson-Solomon 多项式,即该多项式的系数对应序列 (s_u) 的离散傅里叶变换系数,特别地 $G(X)$ 在模 $X^T - 1$ 的情况下是唯一的. 文献[20]也称 $(G(X), \beta)$ 为二元序列 (s_u) 的定义对(defining pair). 与序列的离散傅里叶变换系数直接关联的重要密码学指标是它的线性复杂度 $LC((s_u))$,即为生成该序列的最短的线性反馈移位寄存器. Blahut 定理[22]刻画了它们的关系:

$$LC((s_u)) = |\{i : \rho_i \ne 0, 0 \le i < T\}|,$$

即非零的 ρ_i 的个数. 我们将首先计算序列 $(s_n^{(3)})$ 的离散傅里叶变换系数,再将该序列表示为迹函数的形式.

2　广义割圆类 V_0 和 V_1 的性质

在这一节,根据上文的定义我们证明一些必要的引理.

引理 1[14]　对整数 n,记符号 $nV_i = \{nv(\mathrm{mod} pq) : v \in V_i\}$,其中 $i = 0,1$. 当 $n \in V_0$ 时,

$$nV_0 = V_0, nV_1 = V_1.$$

而当 $n \in V_1$ 时,则有

$$nV_0 = V_1, nV_1 = V_0.$$

引理 2[14]　$2 \in V_0$ 当且仅当 $p \equiv \pm 1 (\mathrm{mod}8)$,$2 \in V_1$ 当且仅当 $p \equiv \pm 3 (\mathrm{mod}8)$.

引理 3[14]　设 $U(\mathrm{mod}m) = \{u(\mathrm{mod}m) : u \in U\}$. 则有

$$V_0(\mathrm{mod}q) = V_1(\mathrm{mod}q) = \{1,2,\cdots,q-1\},$$

且当 v 遍历 V_0(或 V_1)时,$v(\mathrm{mod}q)$ 遍历 $\{1,2,\cdots,q-1\}$ 中的每一个元素 $\frac{p-1}{2}$ 次.

设 Q_p 为模 p 剩余类环 $\mathbb{Z}_p$ 中平方剩余类构成的集合,N_p 为剩余类环 $\mathbb{Z}_p$ 中非平方剩余类构成的集合. 则有

$$V_0(\mathrm{mod}p) = Q_p, V_1(\mathrm{mod}p) = N_p.$$

此外当 v 遍历 V_0 时,$v(\mathrm{mod}p)$ 遍历 Q_p 中每个元素 $(q-1)$ 次;当 v 遍历 V_1 时,$v(\mathrm{mod}p)$ 遍历 N_p 中每个元素 $(q-1)$ 次.

引理 4　设 2 模 pq 的阶为 ℓ,即 $\ell = \min\{r \in \mathbb{Z}^+ : 2^r \equiv 1 (\mathrm{mod} pq)\}$. 当 $2 \in V_0$ 且 $2 \equiv g^{2s_0+1} x (\mathrm{mod} pq)$,或者 $2 \in V_1$ 时,都有

(1) $4 \in V_0$,且 $4 \equiv g^{2k_0} (\mathrm{mod} pq)$,

(2) $2 | \ell$,且 4 模 pq 的阶为 $\ell/2$.

证明　当 $2 \in V_0$ 且 $2 \equiv g^{2s_0+1} x (\mathrm{mod} pq)$ 时,显然有 k_0 使得

$$4 = 2^2 \equiv g^{4s_0+2} x^2 (\mathrm{mod} pq).$$

因此必有 k_0 满足 $0 \le k_0 \le \frac{e}{2} - 1$ 以及 $4 \equiv g^{2k_0} (\mathrm{mod} pq)$. 从而 $4 \in V_0$. 又由 $2^\ell \equiv 1 (\mathrm{mod} pq)$ 可得 $g^{(2s_0+1)\ell} x^\ell \equiv 1 (\mathrm{mod} pq)$,因此 $e \mid (2s_0+1)\ell$ 以及 $2 | \ell$. 此时显然 4 模 pq 的阶为 $\frac{\ell}{2}$.

当 $2 \in V_1$ 时,不妨设

$$2 \equiv g^{s_0} x^{a_0} (\mathrm{mod} pq),$$

其中 $0 \le s_0 \le e-1, 0 \le a_0 \le 1, 2 \nmid s_0 + a_0$,可得

$$4 = 2^2 \equiv g^{2s_0} x^{2a_0} (\mathrm{mod} pq).$$

因此必有 k_0 满足 $0 \le k_0 \le \frac{e}{2} - 1$ 以及 $4 \equiv g^{2k_0}$

$(\mathrm{mod}pq)$. 从而 $4\in V_0$. 又由 $2^{\ell}\equiv 1(\mathrm{mod}pq)$ 可得 $g^{\ell s_0}x^{\ell a_0}\equiv 1(\mathrm{mod}pq)$,因此 $e\mid \ell s_0$ 以及 $2\mid \ell a_0$. 由此可得 $2\mid \ell$. 此时 4 模 pq 的阶为 $\ell/2$. 证毕.

定义多项式

$$h_0(X)=\sum_{n\in V_0}X^n, h_1(X)=\sum_{n\in V_1}X^n.$$

显然 $h_0(1)=h_1(1)=e=0$. 下面进一步考虑$h_0(X)$与 $h_1(X)$的性质.

引理5 设 α 是有限域$\mathbb{F}_2$的一个 pq 次本原单位根.

(1) $h_0(\alpha)+h_1(\alpha)=1$.

(2)当 $n\in P$ 时,有 $h_0(\alpha^n)=h_1(\alpha^n)=\dfrac{p-1}{2}$.

(3)当 $n\in Q$ 时,有 $h_0(\alpha^n)=h_1(\alpha^n)=0$.

(4) 当 $n\in V_0$ 时,有 $h_0(\alpha^n)=h_0(\alpha)$, $h_1(\alpha^n)=h_1(\alpha)$.

(5) 当 $n\in V_1$ 时,有 $h_0(\alpha^n)=h_1(\alpha)$, $h_1(\alpha^n)=h_0(\alpha)$.

证明

(1)显然有

$$h_0(\alpha)+h_1(\alpha)=\sum_{t=0}^{pq-1}\alpha^t-\sum_{t=0}^{p-1}\alpha^{tq}-\sum_{t=1}^{q-1}\alpha^{tp}=1.$$

(2)当 $n\in P$ 时,设 $n=ip$,其中 $1\le i<q$. 由引理 3 可得

$$h_0(\alpha^{ip})=h_1(\alpha^{ip})=\frac{p-1}{2}\cdot\sum_{t=1}^{q-1}\alpha^{tip}=\frac{p-1}{2}.$$

(3)当 $n\in Q$ 时,设 $n=iq$,其中 $1\le i<p$. 由引理3 可得

$$h_0(\alpha^{iq})=(q-1)\sum_{t\in Q_p}\alpha^{tiq}=0,$$

$$h_1(\alpha^{iq})=(q-1)\sum_{t\in N_p}\alpha^{tiq}=0.$$

(4)当 $n\in V_0$ 时,由引理 1 有

$$h_0(\alpha^n)=\sum_{t\in V_0}\alpha^{nt}=\sum_{t\in nV_0}\alpha^t=\sum_{t\in V_0}\alpha^t=h_0(\alpha),$$

$$h_1(\alpha^n)=\sum_{t\in V_1}\alpha^{nt}=\sum_{t\in nV_1}\alpha^t=\sum_{t\in V_1}\alpha^t=h_1(\alpha).$$

(5)当 $n\in V_1$ 时,由引理 1 同样可得

$$h_0(\alpha^n)=\sum_{t\in V_0}\alpha^{nt}=\sum_{t\in nV_0}\alpha^t=\sum_{t\in V_1}\alpha^t=h_1(\alpha),$$

$$h_1(\alpha^n)=\sum_{t\in V_1}\alpha^{nt}=\sum_{t\in nV_1}\alpha^t=\sum_{t\in V_0}\alpha^t=h_0(\alpha).$$

证毕.

引理6 设 α 是有限域$\mathbb{F}_2$的一个 pq 次本原单位根,$\omega\in\mathbb{F}_4\backslash\mathbb{F}_2$.

(1)当 $2\in V_0$ 时,$h_0(\alpha)=0$ 且 $h_1(\alpha)=1$,或 $h_0(\alpha)=1$ 且 $h_1(\alpha)=0$.

(2)当 $2\in V_1$ 时,$h_0(\alpha)=\omega$ 且 $h_1(\alpha)=1+\omega$,或 $h_0(\alpha)=1+\omega$ 且 $h_1(\alpha)=\omega$.

证明

(1) 当 $2\in V_0$ 时,由引理 1,对于 $i=0,1$,有 $(h_i(\alpha))^2=h_i(\alpha^2)=h_i(\alpha)$. 因此 $h_i(\alpha)\in\mathbb{F}_2$,再由引理 5(1)即得相关结果.

(2)当 $2\in V_1$ 时,由引理 1,对于 $i=0,1$,有 $(h_i(\alpha))^2=h_i(\alpha^2)=h_{(i+1)(\mathrm{mod}2)}(\alpha)$. 再根据引理 5(1)可得$(h_i(\alpha))^2=1+h_i(\alpha)$,从而 $h_i(\alpha)\in\mathbb{F}_4\backslash\mathbb{F}_2$,即得相关结果. 证毕.

引理 7 设 α 是有限域$\mathbb{F}_2$的一个 pq 次本原单位根.

(1)设 $H(X)=h_0(\alpha)h_0(X)+h_1(\alpha)h_1(X)$. 则有

$$H(\alpha^n)=\begin{cases}1, & \text{如果 } n(\mathrm{mod}N)\in V_0,\\ 0, & \text{如果 } n(\mathrm{mod}N)\in V_1.\end{cases}$$

(2)设 $\overline{H}(X)=h_0(\alpha)h_1(X)+h_1(\alpha)h_0(X)$. 则有

$$\overline{H}(\alpha^n)=\begin{cases}0, & \text{如果 } n(\mathrm{mod}N)\in V_0,\\ 1, & \text{如果 } n(\mathrm{mod}N)\in V_1.\end{cases}$$

证明 (1)当 $n\in V_0$ 时,可得

$$\begin{aligned}H(\alpha^n)&=h_0(\alpha)h_0(\alpha^n)+h_1(\alpha)h_1(\alpha^n)\\&=(h_0(\alpha)+h_1(\alpha))^2=1.\end{aligned}$$

而当 $n\in V_1$ 时,有

$$\begin{aligned}H(\alpha^n)&=h_0(\alpha)h_0(\alpha^n)+h_1(\alpha)h_1(\alpha^n)\\&=h_0(\alpha)h_1(\alpha)+h_1(\alpha)h_0(\alpha)=0.\end{aligned}$$

(2)的证明类似. 证毕.

3 离散傅里叶变换

根据引理 2 与 6,我们给出第一个结论.

定理1 对于 $p\equiv\pm1(\mathrm{mod}8)$,设 α 是有限域$\mathbb{F}_2$中的一个 pq 次本原单位根且满足 $h_0(\alpha)=0$. 我们有

(1)如果 $p\equiv1(\mathrm{mod}8)$,则序列$(s_n^{(3)})$的 Mattson-Solomon 多项式为

$$G(X)=h_1(X)+\sum_{t=1}^{q-1}X^{tp}.$$

(2)如果 $p\equiv-1(\mathrm{mod}8)$,则序列$(s_n^{(3)})$的 Mattson-Solomon 多项式为

$$G(X)=h_0(X).$$

证明 下面只证(1),同理可得(2).

当 $n=0$ 时,有 $G(\alpha^0)=G(1)=h_1(1)+(q-1)=e+q-1=0=s_0$.

当 $n\in P$ 时,由引理5(2)可得

$$G(\alpha^n)=h_1(\alpha^n)+\sum_{t=1}^{q-1}\alpha^{tpn}=\frac{p-1}{2}+1=\frac{p+1}{2}.$$

注意到 $p\equiv1(\mathrm{mod}8)$,因此 $G(\alpha^n)=1=s_n$.

当 $n\in Q$ 时,由引理5(3) 可得

$$G(\alpha^n)=h_1(\alpha^n)+\sum_{t=1}^{q-1}\alpha^{tpn}=0+(q-1)=0=s_n.$$

当 $n\in V_0$ 时,由引理5(4) 有

$$G(\alpha^n)=h_1(\alpha^n)+\sum_{t=1}^{q-1}\alpha^{ntp}=h_1(\alpha)+1=0=s_n.$$

当 $n\in V_1$ 时,由引理5(5) 有

$$G(\alpha^n)=h_1(\alpha^n)+\sum_{t=1}^{q-1}\alpha^{ntp}=h_0(\alpha)+1=1=s_n.$$

综上可得 $G(X)$ 是序列 $(s_n^{(3)})$ 关于 α 的 Mattson-Solomon 多项式. 证毕.

类似地,我们得到当 $p\equiv\pm3\pmod 8$ 时序列 $(s_n^{(3)})$ 的 \ Mattson-Solomon 多项式.

定理 2　对于 $p\equiv\pm3\pmod 8$,设 α 是有限域 $\overline{\mathbb{F}}_2$ 中的一个 pq 次本原单位根且满足 $h_0(\alpha)=\omega\in\mathbb{F}_4\backslash\mathbb{F}_2$. 我们有

(1) 如果 $p\equiv3\pmod 8$,则序列 $(s_n^{(3)})$ 的 Mattson-Solomon 多项式为

$$G(X)=\omega h_1(X)+(1+\omega)h_0(X).$$

(2) 如果 $p\equiv-3\pmod 8$,则序列 $(s_n^{(3)})$ 的 Mattson-Solomon 多项式为

$$G(X)=\omega h_0(X)+(1+\omega)h_1(X)+\sum_{t=1}^{q-1}X^{tp}.$$

在第 1 节中我们已经指出,根据 Blahut 定理,序列 $(s_n^{(3)})$ 的线性复杂度即为 $G(X)$ 中非零项的数目. 因此可得在文献[14]中证明的 $(s_n^{(3)})$ 的线性复杂度的值:

$$LC((s_n^{(3)}))=\begin{cases}\dfrac{pq+q-p-1}{2}, & \text{当 } p\equiv1\pmod 8,\\ \dfrac{pq-q-p+1}{2}, & \text{当 } p\equiv-1\pmod 8,\\ pq-q-p+1, & \text{当 } p\equiv3\pmod 8,\\ pq-p, & \text{当 } p\equiv-3\pmod 8.\end{cases}$$

下一节,我们根据上述两个定理讨论序列 $(s_n^{(3)})$ 的迹表示.

4　迹表示

本节我们将序列 $(s_n^{(3)})$ 的 Mattson-Solomon 多项式 $G(X)$ 表示为迹函数的形式.

从有限域 $\mathbb{F}_{2^r}$ 到有限域 $\mathbb{F}_{2^s}$ 的迹函数定义为

$$\mathrm{Tr}_k^n(x)=x+x^{2^k}+x^{2^{2k}}+\cdots+x^{2^{(n/k-1)k}}.$$

对于 $a,b\in\mathbb{F}_{2^s}$ 及 $x,y\in\mathbb{F}_{2^r}$,有 $\mathrm{Tr}_k^n(ax+by)=a\,\mathrm{Tr}_k^n(x)+b\,\mathrm{Tr}_k^n(y)$. 迹函数是表示序列的一个重要方式. 例如周期为 2^n-1 的 $m-$序列 (s_u) 的迹表示为:

$$s_u=\mathrm{Tr}_1^n(a\beta^u),$$

其中 β 为 2^n-1 阶本原根. 关于序列的迹表示的研究,已有非常丰富的文献[11,16,20,21,23~28,30~32].

下面我们重新对 $\mathbb{Z}_q^*$,V_0 及 V_1 进行分类. 设 2 模 q 的阶为 ℓ_q,即

$$\ell_q=\min\{a\in\mathbb{Z}^+:2^a\equiv1\pmod q\}.$$

由 2 模 q 生成的集合记为

$$\langle2\rangle_q=\{2^j\pmod q:0\le j<\ell_q\}.$$

对任意整数 a,记 $a\langle2\rangle_q=\{a2^j\pmod q:0\le j<\ell_q\}$.

则 $\mathbb{Z}_q^*$ 可以分解为

$$\mathbb{Z}_q^*=\langle2\rangle_q\cup g_q\langle2\rangle_q\cup\cdots\cup g_q^{(q-1)/\ell_q-1}\langle2\rangle_q.$$

于是根据 $\mathrm{Tr}_1^{\ell_q}(X)\equiv\sum_{t\in\langle2\rangle_q}X^t\pmod{X^q-1}$,有

$$\sum_{t=1}^{q-1}X^t\equiv\sum_{i=0}^{(q-1)/\ell_q-1}\mathrm{Tr}_1^{\ell_q}(X^{g_q^i})\pmod{X^q-1}.$$

设 2 模 pq 的阶为 ℓ,即

$$\ell=\min\{r\in\mathbb{Z}^+:2^r\equiv1\pmod{pq}\}.$$

由 2 模 pq 生成的集合记为

$$\langle2\rangle=\{2^j\pmod{pq}:0\le j<\ell\}.$$

对任意整数 a,记 $a\langle2\rangle=\{a2^j\pmod{pq}:0\le j<\ell\}$.

第一种情况:当 $2\in V_0$ 且 $2\equiv g^{2k_0}\pmod{pq}$ 时,V_0 与 V_1 可以表示为

$$\begin{aligned}V_0&=\langle2\rangle\cup g^2\langle2\rangle\cup\cdots\cup g^{e/\ell-2}\langle2\rangle\\&\quad\cup gx\langle2\rangle\cup g^3x\langle2\rangle\cup\cdots\cup g^{e/\ell-1}x\langle2\rangle,\\V_1&=g\langle2\rangle\cup g^3\langle2\rangle\cup\cdots\cup g^{e/\ell-1}\langle2\rangle\\&\quad\cup g^2x\langle2\rangle\cup g^4x\langle2\rangle\cup\cdots\cup g^{e/\ell-2}x\langle2\rangle.\end{aligned}$$

由 $\mathrm{Tr}_1^\ell(X)\equiv\sum_{t\in\langle2\rangle}X^t\pmod{X^{pq}-1}$,可将 $h_0(X)$ 与 $h_1(X)$ 表示为:

$$h_0(X)\equiv\sum_{i=0}^{e/(2\ell)-1}\mathrm{Tr}_1^\ell(X^{g^{2i}})+\sum_{i=0}^{e/(2\ell)-1}\mathrm{Tr}_1^\ell(X^{xg^{2i+1}})\pmod{X^{pq}-1},$$

$$h_1(X)\equiv\sum_{i=0}^{e/(2\ell)-1}\mathrm{Tr}_1^\ell(X^{g^{2i+1}})+\sum_{i=0}^{e/(2\ell)-1}\mathrm{Tr}_1^\ell(X^{xg^{2i}})\pmod{X^{pq}-1}.$$

第二种情况:当 $2\in V_0$ 且 $2\equiv g^{2s_0+1}x\pmod{pq}$,或者 $2\in V_1$ 时,由引理 4 可得 $4\in V_0$,且 $4\equiv g^{2k_0}\pmod{pq}$,以及 4 模 pq 的阶为 $\frac{\ell}{2}$. 记 $\langle4\rangle=\{4^j\pmod{pq}:0\le j<\ell/2\}$,则 V_0 与 V_1 可表示为

$$\begin{aligned}V_0&=\langle4\rangle\cup g^2\langle4\rangle\cup\cdots\cup g^{2e/\ell-2}\langle4\rangle\cup gx\\&\quad\langle4\rangle\cup g^3x\langle4\rangle\cup\cdots\cup g^{2e/\ell-1}x\langle4\rangle,\\V_1&=g\langle4\rangle\cup g^3\langle4\rangle\cup\cdots\cup g^{2e/\ell-1}\langle4\rangle\cup g^2x\\&\quad\langle4\rangle\cup g^4x\langle4\rangle\cup\cdots\cup g^{2e/\ell-2}x\langle4\rangle.\end{aligned}$$

从而

$$h_0(X)\equiv\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(X^{g^{2i}})+\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(X^{xg^{2i+1}})\pmod{X^{pq}-1},$$

$$h_1(X)\equiv\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(X^{g^{2i+1}})+\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(X^{xg^{2i}})\pmod{X^{pq}-1}.$$

结合上述的讨论,我们得到以下关于序列 $(s_n^{(3)})$ 的迹表示.

定理 3　对于 $p\equiv\pm1\pmod 8$,设 α 是有限域 $\overline{\mathbb{F}}_2$ 中的一个 pq 次本原单位根且满足 $h_0(\alpha)=0$. 设 2 模 q 的阶为 ℓ_q,2 模 pq 的阶为 ℓ,并设 $2\equiv g^{2k_0}\pmod{pq}$. 我们有

(1) 如果 $p\equiv1\pmod 8$,则序列 $(s_n^{(3)})$ 的迹表示为

$$s_n=\sum_{i=0}^{e/(2\ell)-1}\mathrm{Tr}_1^\ell(\alpha^{ng^{2i+1}})+\sum_{i=0}^{e/(2\ell)-1}\mathrm{Tr}_1^\ell(\alpha^{nxg^{2i}})$$

$$+\sum_{i=0}^{(q-1)/\ell_q-1}\mathrm{Tr}_1^{\ell_q}(\alpha^{npg_q^i}).$$

(2) 如果 $p\equiv -1(\mathrm{mod}8)$,则序列 $(s_n^{(3)})$ 的迹表示为

$$s_n=\sum_{i=0}^{e/(2\ell)-1}\mathrm{Tr}_1^{\ell}(\alpha^{ng^{2i}})+\sum_{i=0}^{e/(2\ell)-1}\mathrm{Tr}_1^{\ell}(\alpha^{nxg^{2i+1}}).$$

定理 4 对于 $p\equiv\pm 1(\mathrm{mod}8)$,设 α 是有限域 $\mathbb{F}_2$ 中的一个 pq 次本原单位根且满足 $h_0(\alpha)=0$. 设 2 模 q 的阶为 ℓ_q,2 模 pq 的阶为 ℓ,并设 $2\equiv g^{2k_0+1}x(\mathrm{mod}pq)$. 我们有

(1) 如果 $p\equiv 1(\mathrm{mod}8)$,则序列 $(s_n^{(3)})$ 的迹表示为

$$s_n=\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{ng^{2i+1}})+\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{nxg^{2i}})+\sum_{i=0}^{(q-1)/\ell_q-1}\mathrm{Tr}_1^{\ell_q}(\alpha^{npg_q^i})$$

(2) 果 $p\equiv -1(\mathrm{mod}8)$,则序列 $(s_n^{(3)})$ 的迹表示为

$$s_n=\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{ng^{2i}})+\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{nxg^{2i+1}}).$$

定理 5 对于 $p\equiv\pm 3(\mathrm{mod}8)$,设 α 是有限域 $\mathbb{F}_2$ 中的一个 pq 次本原单位根且满足 $h_0(\alpha)=\omega\in\mathbb{F}_4\backslash\mathbb{F}_2$. 设 2 模 q 的阶为 ℓ_q,2 模 pq 的阶为 ℓ. 我们有

(1) 如果 $p\equiv 3(\mathrm{mod}8)$,则序列 $(s_n^{(3)})$ 的迹表示为

$$s_n=\omega\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{ng^{2i+1}})+\omega\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{nxg^{2i}})+(1+\omega)\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{ng^{2i}})+(1+\omega)\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{nxg^{2i+1}}).$$

(2) 如果 $p\equiv -3(\mathrm{mod}8)$,则序列 $(s_n^{(3)})$ 的迹表示为

$$s_n=\omega\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{ng^{2i}})+\omega\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{nxg^{2i+1}})+(1+\omega)\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{ng^{2i+1}})+(1+\omega)\sum_{i=0}^{e/\ell-1}\mathrm{Tr}_2^{\ell/2}(\alpha^{nxg^{2i}})+\sum_{i=0}^{(q-1)/\ell_q-1}\mathrm{Tr}_1^{\ell_q}(\alpha^{npg_q^i}).$$

5 结论

本文中,我们针对最近由刘华宁等利用 RSA 模数设计的一类新序列,给出了迹表示,对探析此类序列的密码学性质有积极的意义. 文献[14]已经研究了序列的线性复杂度及相关性,但其他性质,如线性复杂度轮廓、k-错线性复杂度等也是重要的密码学指标,因此进一步挖掘这些性质也是相当有意义的. 另外,从文献[14]知,这类序列具有六值自相关值,因此可以讨论该序列的 2-adic 复杂度.

参考文献

[1] Graham S, Shparlinski I. On RSA moduli with almost half of the bits prescribed[J]. Discrete Applied Mathematics, 2008, 156(16): 3150 – 3154.

[2] Shparlinski I. On the uniformity of distribution of the RSA pairs[J]. Mathematics of Computation, 2001, 70(234): 801 – 808.

[3] Shparlinski I. On RSA moduli with prescribed bit patterns [J]. Designs, Codes and Cryptography, 2006, 39(1): 113 – 122.

[4] Whiteman A. A family of difference sets[J]. Illinois Journal of Mathematics, 1962, 6: 107 – 121.

[5] Bai E, Fu X, Xiao G. On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq}[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2005, 88: 392 – 395.

[6] Bai E, Liu X, Xiao G. Linear complexity of new generalized cyclotomic sequences of order two of length pq[J]. IEEE Transactions on Information Theory, 2005, 51: 1849 – 1853.

[7] 常祖领,周玉倩,柯品惠. 一类新的 *pqr* 长 2 阶广义分圆序列的线性复杂度[J]. 电子学报, 2015, 43(1): 166 – 170.
Chang Zuling, Zhou Yuqian, Ke Pinhui. Linear complexity of new generalized cyclotomic sequences of order two and length *pqr*[J]. Acta Electronica Sinica, 2015, 43(1): 166 – 170. (in Chinese)

[8] Ding C. Linear complexity of generalized cyclotomic binary sequences of order 2[J]. Finite Fields and Their Applications, 1997, 3: 159 – 174.

[9] Ding C. Autocorrelation values of generalized cyclotomic sequences of order two[J]. IEEE Transactions on Information Theory, 1998, 44: 1699 – 1702.

[10] Ding C. Cyclotomic constructions of cyclic codes with length being the product of two primes[J]. IEEE Transactions on Information Theory, 2012, 58(4): 2231 – 2236.

[11] Du X, Yan T, Xiao G. Trace representation of some generalized cyclotomic sequences of length *pq*[J]. Information Sciences, 2008, 178(16): 3307 – 3316.

[12] 柯品惠,李瑞芳,张胜元. 一类新的周期为 $p^{m+1}q^{n+1}$ 的二元广义分圆序列的线性复杂度[J]. 电子学报, 2014, 42(5): 1009 – 1013.
Ke Pinhui, Li Ruifang, Zhang Shengyuan. The linear complexity of a new class of generalized cyclotomic binary sequences of length $p^{m+1}q^{n+1}$[J]. Acta Electronica Sinica, 2014, 42(5): 1009 – 1013. (in Chinese)

[13] Li S, Chen Z, Sun R, et al. On the randomness of generalized cyclotomic sequences of order two and length pq[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A: 2037 – 2041.

[14] 刘华宁,陈晓林. 一类新的广义割圆序列的线性复杂度

及其自相关值[J]. 数学学报,2019,62(2):233 – 246.
Liu Huaning, Chen Xiaolin. Autocorrelation values and linear complexity of new generalized cyclotomic sequences [J]. Acta Mathematica Sinica Chinese Series, 2019, 62(2):233 – 246. (in Chinese)

[15] 刘龙飞,杨凯,杨晓元. 新的周期为 p^m 的 $GF(h)$ 上广义割圆序列的线性复杂度[J]. 通信学报,2017,38(9):39 – 45.
Liu Longfei, Yang Kai, Yang Xiaoyuan. On the linear complexity of a new generalized cyclotomic sequence with length p^m over $GF(h)$ [J]. Journal on Communications, 2017,38(9):39 – 45. (in Chinese)

[16] Qi M, Xiong S, Yuan J, et al. Trace representation over F_r of binary Jacobi sequences with period pq [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, 98-A(3):912 – 917.

[17] Yan T, Du X, Xiao G, et al. Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2^k [J]. Information Sciences, 2009, 179(7):1019 – 1023.

[18] Hu L, Yue Q. Autocorrelation value of Whiteman generalized cyclotomic sequence[J]. Journal of Mathematical Research with Applications, 2012, 32(4):415 – 422.

[19] Hu L, Yue Q, Wang M. The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$ [J]. IEEE Transactions on Information Theory, 2012, 58(8):5534 – 5543.

[20] Dai Z, Gong G, Song H. A trace representation of binary Jacobi sequences [J]. Discrete Mathematics, 2009, 309(6):1517 – 1527.

[21] 杜小妮,李芝霞,万韫琦,李晓丹. 基于费马商的 r 元序列的迹表示[J]. 电子学报,2017,45(10):2439 – 2442.
Du Xiaoni, Li Zhixia, Wan Yunqi, et al. Trace representation of r-ary sequences derived from Fermat quotients[J]. Acta Electronica Sinica, 2017, 45(10):2439 – 2442. (in Chinese)

[22] Blahut R. Transform techniques for error control codes [J]. IBM Journal of Research and Development, 1979, 23(3):299 – 315.

[23] Chen Z. Trace representation and linear complexity of binary sequences derived from Fermat quotients [J]. SCIENCE CHINA Information Sciences, 2014, 57(11): 1 – 10.

[24] Chen Z. Linear complexity and trace representation of quaternary sequences over $\mathbb{Z}_4$ based on generalized cyclotomic classes modulo pq [J]. Cryptography and Communications, 2017, 9(4):445 – 458.

[25] Chen Z, Du X, Marzouk R. Trace representation of pseudorandom binary sequences derived from Euler quotients [J]. Applicable Algebra in Engineering, Communication and Computing, 2015, 26(6):555 – 570.

[26] Dai Z, Gong G, Song H, et al. Trace representation and linear complexity of binary e-th power residue sequences of period p [J]. IEEE Transactions Information Theory, 2011, 57(3):1530 – 1547.

[27] Du X, Chen Z. Trace representation of binary generalized cyclotomic sequences with length p^m [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, 94-A(2):761 – 765.

[28] Du X, Chen Z, Shi A, et al. Trace representation of a new class of sextic residue sequences of period p = 3 (mod8) [J]. IEICE Transactions, 2009, 92-A(2):668 – 670.

[29] Helleseth T, Kim S, No J. Linear complexity over F_p and trace representation of Lempel-Cohn-Eastman sequences [J]. IEEE Transactions Information Theory, 2003, 49(6): 1548 – 1552.

[30] Kim J, Song H. Trace representation of Legendre sequences[J]. Designs, Codes and Cryptography, 2001, 24(3):343 – 348.

[31] No J, Lee H, Chung H, et al. Trace representation of Legendre sequences of Mersenne prime period [J]. IEEE Transactions Information Theory, 1996, 42(6): 2254 – 2255.

[32] Qi M, Xiong S, Yuan J, et al. A simpler trace representation of Legendre sequences [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, 98-A(4):1026 – 1031.

作者简介

陈智雄　男,生于 1972 年,福建莆田人. 2006 年毕业于西安电子科技大学,密码学博士. 现为莆田学院教授、硕士生导师、福建省高校应用数学重点实验室主任,中国密码学会高级会员. 主要研究方向为序列密码.
E-mail:ptczx@126.com

刘华宁　男,生于 1979 年,湖南永州人. 2007 年毕业于西北大学,理学博士. 现为西北大学教授、博士生导师. 主要研究方向为伪随机数列.
E-mail:hnliu@nwu.edu.cn