周期为 p^m 的广义割圆序列的线性复杂度

杜小妮[①②]　阎统江[③]　石永芳[④]
[①](西北师范大学数学与信息科学学院　兰州　730070)
[②](中国科学院研究生院信息安全国家重点实验室　北京　100049)
[③](中国石油大学数学与计算科学学院　东营　257061)
[④](甘肃联合大学数信学院　兰州　730000)

摘　要：该文将周期为 p^m (p 为奇素数，m 为正整数)广义割圆的研究推广到了任意阶的情形，构造了一类新序列，确定了该序列的极小多项式，指出线性复杂度可能的取值为 p^m-1， p^m， $(p^m-1)/2$ 和 $(p^m+1)/2$ 。并且指出，当选取的特征集满足一定条件时，对应序列的线性复杂度取值总是以上 4 种情形。结果表明，该类序列具有较好的线性复杂度性质。

关键词：流密码；广义割圆序列；线性复杂度；极小多项式
中图分类号：TN918.4　　**文献标识码**：A　　**文章编号**：1009-5896(2010)04-0821-04
DOI: 10.3724/SP.J.1146.2009.00430

Linear Complexity of Generalized Cyclotomic Sequences with Period p^m

Du Xiao-ni[①②]　Yan Tong-jiang[③]　Shi Yong-fang[④]
[①](*College of Mathematic and Information Science*, *Northwest Normal University*, *Lanzhou* 730070, *China*)
[②](*State Key Laboratory of Information Security*, *Graduate University of Chinese Academy of Sciences*, *Beijing* 100049, *China*)
[③](*Institute of Mathematics and Computer Science*, *China University of Petroleum*, *Dongying* 257061, *China*)
[④](*College of Mathematic and Information Science*, *Gansu Lianhe University*, *Lanzhou* 730070, *China*)

Abstract: In this paper, a new class of generalized cyclotomic sequences of period p^m (p odd prime and $m>1$) with arbitrary order is constructed and its minimal polynomial is determined. Hence the linear complexity of it is obtained. The possible values of its linear complexity are pointed out, which is p^m-1, p^m, $(p^m-1)/2$ and $(p^m+1)/2$. The research also indicate that linear complexity of the sequences always take the values as above when the corresponding characteristic sets satisfies certain conditions. The results show that most of these sequences have good linear complexity.

Key words: Stream cipher; Generalized cyclotomic sequences; Linear complexity; Minimal polynomial

1　引言

伪随机序列在序列密码、扩频通信等领域有着极为广泛的应用。线性复杂度是度量序列伪随机性质的一个重要的指标[1]。有限域 GF(q) 上周期为 M 的序列 $\{s_t\}=(s_0,s_1,\cdots,s_{M-1})$ 的线性复杂度 $L(s)$ 定义为满足函数 $s_j=c_1s_{j-1}+c_2s_{j-2}+\cdots+c_Ls_{j-L}$ 的最小 L，其中 $c_1,c_2,\cdots,c_L\in \mathrm{GF}(q)$, $j>L$。它也是生成 $\{s_t\}$ 的最短线性反馈移位寄存器的阶数[2]。记 $S(x)=s_0+s_1x+\cdots+s_{M-1}x^{M-1}$，则序列 $\{s_t\}$ 的线性复杂度和极小多项式 $m(x)$ 分别由下式给定

$$L=M-\deg\left(\gcd(x^M-1,S(x)\right) \tag{1}$$

$$m(x)=1+c_1x+\cdots+c_Lx^L=(x^M-1)/\gcd(x^M-1,S(x)) \tag{2}$$

为抵抗已知明文攻击，密钥流序列的线性复杂度必须足够大。根据Berlekamp-Massey算法，如果 $L(s)>M/2$ (M 是 $\{s_t\}$ 的周期)，则认为 $\{s_t\}$ 具有好的线性复杂度性质。

近年来，广义割圆序列由于具有良好的线性复杂度而备受关注。该类序列的典型代表是周期为 pq (p,q 为素数)和周期为 p^m 的情形，其中 p,q 为奇素数，m 为正整数，关于该类序列主要的研究成果见参考文献[2–14]。

本文将考虑周期为 p^m 的广义割圆序列的线性复杂度，推广了现有的相关结论。假设 $AB=\{xy|x\in A,y\in B\}$，$xB=\{xy|y\in B\}$，$\mathrm{ord}_N(x)$ 表示 x 模 N 的阶。

2　周期为 p^m 的任意阶序列的构造

假设 p 为奇素数，整数 $m\ge 1$， d 满足 $2d\,|\,(p$

2009-03-30 收到，2009-10-19 改回
国家自然科学基金项目(60773003)，甘肃省自然科学基金项目(096RJZA124)，甘肃省科技攻关项目(2GS064-A52-035-03)，教育部科学技术研究重点项目(208148)，信息安全国家重点实验室开放基金和西北师范大学知识与科技创新工程项目资助课题
通信作者：杜小妮　ymLdxn@126.com

$-1)$。若 g 为 p^2 的本原元，$g_1 \equiv g(\bmod p)$，则 g 和 g_1 分别为 $p^e(e \geq 2)$ 和 p 的本原元。在本文中，假定 g 为 $p^m(m \geq 1)$ 的本原元。则根据中国剩余定理，有 $\mathrm{ord}_{p^m}(g) = \varphi(p^m) = p^{m-1}(p-1)$。

对任意的 n，$1 \leq n \leq m$，定义 $Z_{p^n}^* = (g)$，$D_0^{(n)} = (g^{2d})$，$D_i^{(n)} = g^i D_0^{(n)}$，$i = 1,2,\cdots,2d-1$，$R^{(n)} = \{0, p, 2p, \cdots, (p^{(n-1)}-1)p\} = pZ_{p^{n-1}}$，记 $R^{(1)} = \{0\}$。因此 $Z_{p^n} = (D_0^{(n)} \cup D_1^{(n)} \cup \cdots \cup D_{2d-1}^{(n)}) \cup R^{(n)} = Z_{p^n}^* \cup R^{(n)}$。由此可得到剩余类环 Z_{p^m} 的一个分割为

$$\begin{aligned} Z_{p^m} &= (D_0^{(m)} \cup D_1^{(m)} \cup \cdots \cup D_{2d-1}^{(m)}) \cup pZ_{p^{m-1}} \\ &= \left(D_0^{(m)} \cup pD_0^{(m-1)}\right) \cup \cdots \cup \left(D_{2d-1}^{(m)} \cup pD_{2d-1}^{(m-1)}\right) \\ &\quad \cup p^2 Z_{p^{m-2}} \\ &\quad \vdots \\ &= (\cup_{n=1}^{m} p^{m-n} D_0^{(n)}) \cup \cdots \cup (\cup_{n=1}^{m} p^{m-n} D_{2d-1}^{(n)}) \cup \{0\} \end{aligned}$$

假定 $D_i = \cup_{n=1}^{m} p^{m-n} D_i^{(n)}$，$i = 0,1,\cdots,2d-1$，则有 $\bigcup_{i=0}^{2d-1} D_i \cup \{0\} = Z_{p^m}$，且 $D_i \cap D_j = \varnothing$，$i \neq j$，$i, j = 0,1,\cdots,2d-1$，其中 $\varnothing$ 表示空集。

令 $C_0 = D_0 \cup D_1 \cup \cdots \cup D_{d-1}$，$C_1 = D_d \cup D_{d+1} \cup \cdots \cup D_{2d-1}$。构造周期为 p^m 的二元广义割圆序列如下

$$s(t) = \begin{cases} 0, & t \in C_0 \\ 1, & \text{其它} \end{cases} \tag{3}$$

由定义可以看出，该序列为平衡序列。此时称集合 $C_1 \cup \{0\}$ 为序列的特征集。

显然，当参数 $m = 1$ 且 $d = 1$ 时，序列 $s(t)$ 即为 Lengdre序列[7]，关于其伪随机性质的研究已经较为完善。对于参数 $m = 1$ 且 $d = 3$，$m = 2$ 且 $d = 1$，$m = 2$ 且 $d = 2$ 和 $m = 3$ 且 $d = 1$ 时序列的线性复杂度和自相关性质等伪随机性质，见参考文献[8–11]；当参数 $m \geq 2$ 且 $d = 1$ 时，Yan[12]和Kim[13]等人分别于2007年和2008年确定了该类序列的线性复杂度。这些研究结果表明，序列 $\{s(t)\}$ 具有很好的密码学性质。

下面我们确定序列 $\{s(t)\}$ 的线性复杂度。

3 序列的线性复杂度

定义 $B_i = \bigcup_{d+i}^{2d-1+i} D_i$，显然 $B_0 = C_1$，$B_d = C_0$。其中 D，B 的下标均模 $2d$。

引理 1 对任意的 $a \in D_i^{(n)}$，$i, j = 0,1,\cdots,2d-1$，有下式成立

(1) $aD_j^{(n)} = D_{i+j}^{(n)}$; (2) $aD_j = D_{i+j}$; (3) $aB_j = B_{i+j}$。

证明 (1)的证明和文献[3]中的证明类似，此处不再重复。

(2)由 $D_i^{(n)}$ 的定义可知，$D_i^{(1)} \subset D_i^{(2)} \subset \cdots \subset D_i^{(m)}$，$D_i^{(n)} \bmod p^l = D_i^{(l)}$ 若 $l \leq n$，$D_i^{(n)} \bmod p^l = D_i^{(n)} \subset D_i^{(l)}$ 若 $l > n$。

因此，根据(1)有

$$\begin{aligned} aD_j &= a \cup_{k=1}^{m} p^{m-k} D_j^{(k)} = \cup_{k=1}^{m} p^{m-k} aD_j^{(k)} \\ &= \cup_{k=1}^{m} p^{m-k} D_{i+j}^{(k)} = D_{i+j}, \quad i, j = 0,1,\cdots,2d-1 \end{aligned}$$

(3)根据(2)有

$$\begin{aligned} aB_j &= a\bigcup_{d+j}^{2d-1+j} D_i = \bigcup_{d+j}^{2d-1+j} aD_i \\ &= \bigcup_{d+j}^{2d-1+j} D_{i+j} = B_{i+j} \end{aligned}$$

证毕

定义 $B_i(x) = \sum_{i \in B_i} x^i + 1$，$j = 0,1,\cdots,2d-1$。则 $B_0(x) = \sum_{i \in B_0} x^i + 1 = \sum_{i \in C_1} x^i + 1$ 是序列 $\{s(t)\}$ 的生成多项式。令 α 表示有限域 $\mathrm{GF}(2^m)$ 上的 N 次本原单位根，这里 $\mathrm{GF}(2^m)$ 是 $x^N - 1$ 的分裂域，$m = \mathrm{ord}_N(2)$。

引理 2 $B_i(\alpha) + B_{d+i}(\alpha) = 1$，$i = 0,1,\cdots,d-1$。

证明 因为 $0 = \alpha^{p^m} - 1 = (\alpha - 1)(1 + \alpha + \alpha^2 + \cdots + \alpha^{p^m - 1})$。由 α 的定义有 $\alpha + \alpha^2 + \cdots + \alpha^{p^m-1} = \sum_{i \in B_i} \alpha^i + \sum_{i \in B_i + d} \alpha^i = B_i(\alpha) + B_{d+i}(\alpha) = 1$。 证毕

引理 3[3] 剩余类方程 $ax \equiv b \pmod m$，$a \not\equiv 0 \pmod m$ 是可解的当且仅当 $\gcd(a, m) \mid b$。

引理 4 对任意正整数 d，$1 \leq i \leq d-1$，方程 $ix \equiv d \pmod{2d}$ 关于变量 x 是可解的。

证明与文献[14]中的证明类似，此处不再重复。

引理 5 $2 \in D_0$ 当且仅当 $B_0(\alpha) \in \{0,1\}$。

证明 因为 $\gcd(2, p) = 1$，且 $p > 2$，显然存在 i，$0 \leq i \leq 2d-1$，使得 $2 \in D_i$。因为 $\gcd(2, p) = 1$，且 $p > 2$，显然 $2 \in D_i^{(1)} \subset D_i^{(2)} \subset \cdots \subset D_i^{(m)}$。

充分性： 如果 $2 \notin D_0$，根据引理 4，存在 x_i 满足方程 $ix \equiv d \pmod{2d}$。因此，对任意的 $j = 1,\cdots, d-1$，有

$$B_{j+ix_i}(\alpha) = B_{j+d}(\alpha) = B_j(\alpha) + 1 \tag{4}$$

因此，根据式(4)和引理 4，有

$$B_{j+(x_i-1)i}^2(\alpha) = B_{j+ix_i}(\alpha) = B_{j+d}(\alpha) = B_j(\alpha) + 1$$

从而，$B_j(\alpha) \notin \{0,1\}$，$j = 1,\cdots,d-1$。根据这个事实，有 $B_d(\alpha) + B_0(\alpha) = 1$，因此，$B_0(\alpha) \notin \{0,1\}$。

必要性： 若 $2 \in D_0$，根据引理 3，$B_0(\alpha^2) = B_0(\alpha)$，因为 $\alpha \in \mathrm{GF}(2^m)$，则有 $(B_0(\alpha))^2 = B_0(\alpha^2)$。从而 $(B_0(\alpha))^2 = B_0(\alpha)$。因此 $B_0(\alpha) \in \{0,1\}$。 证毕

定理 1 如果 $2 \notin D_0$，则序列的线性复杂度和极小多项式分别为

$$L(s) = \begin{cases} p^m, & m\text{为偶数, 或者}m\text{为奇数且}(p \equiv -3 (\bmod\ 8) \text{ 或者 } p \equiv 1 (\bmod\ 8)) \\ p^m - 1, & m\text{为奇数且}(p \equiv 3 (\bmod\ 8) \text{或者 } p \equiv -1 (\bmod\ 8)) \end{cases}$$

$$m(x)=\begin{cases}x^{p^m}-1, & m\text{为偶数 或者}m\text{为奇数且}(p\equiv -3(\bmod\ 8)\text{或者}p\equiv 1(\bmod\ 8))\\ (x^{p^m}-1)/(x-1), & m\text{为奇数且}(p\equiv 3\ (\bmod\ 8)\text{或者}p\equiv -1\ (\bmod\ 8))\end{cases}$$

证明　因为 $B_0(\alpha^0)=1$ 当且仅当：(1) m 为偶数；或(2)　m 为奇数，且 $p\equiv -3\ (\bmod\ 8)$ 或者 $p\equiv 1\ (\bmod\ 8)$ 成立。从而根据引理 5 可知 $\gcd(x^{p^m}-1, B_0(x))=1$，根据式(1)和式(2)有 $m(x)=\dfrac{x^{p^m}-1}{\gcd(x^{p^m}-1,B_0(x))}=x^{p^m}-1$　。　$L(s)=\deg(m(x))=p^m$。　证毕

$B_0(\alpha^0)=0$ 当且仅当 m 为奇数，且 $p\equiv 3\ (\bmod\ 8)$ 或 $p\equiv -1\ (\bmod\ 8)$ 成立，从而根据引理 5 和等式(1)和式(2)可知，$\gcd(x^{p^m}-1,B_0(x))=x-1$，$m(x)=\dfrac{x^{p^m}-1}{x-1}$。$L(s)=p^m-1$。

下面考虑 $2\in D_0$ 的情形。对文献[3]的结论稍作变动，可有如下的引理。

引理 6　(1) $\sum\limits_{i\in p^{m-1}D_0^{(1)}}\theta^i+\cdots+\sum\limits_{i\in p^{m-1}D_{2d-1}^{(1)}}\theta^i=1$；

(2) 若 $l=2,\cdots,m$，$\sum\limits_{i\in p^{m-l}D_0^{(l)}}\theta^i+\cdots+\sum\limits_{i\in p^{m-l}D_{2(d-1)}^{(l)}}\theta^i=\sum\limits_{i\in p^{m-l}D_1^{(l)}}\theta^i+\cdots+\sum\limits_{i\in p^{m-l}D_{2d-1}^{(l)}}\theta^i=0$。

注意到对任意的 $l=1,2,\cdots,m$，　$k=0,1,\cdots,2d-1$ 以及任意的正整数 i，若 i 满足 $n-l+i\le m-1$，　有

$$p^i\cdot p^{m-l}D_k^{(l)}\ (\bmod p^m)\equiv p^{m-l+i}D_k^{(l-i)}\ (\bmod p^m),$$

$$|\,p^i\cdot p^{m-l}D_k^{(l)}\ (\bmod p^m)\,|=p^i\,|\,p^{m-l+i}D_k^{(l-i)}\ (\bmod p^m)\,|$$

若 i 满足 $n-l+i\ge m$，有 $p^i\cdot p^{m-l}D_k^{(l)}(\bmod p^m)\equiv 0\ (\bmod p^m)$。

若 $a\in\bigcup_{j=0}^{2d-1}p^{m-l}D_j^{(l)}$，显然存在某个 $b\in Z_{p^k}^*=\bigcup_{j=0}^{2d-1}D_j^{(l)}$，　使得 $a=p^{m-l}b$。因此

$$\begin{aligned}B_0(\theta^a)&=\sum_{j=d}^{2d-1}\left(\sum_{t\in D_j^{(m)}}\theta^{at}+\cdots+\sum_{t\in p^{m-1}D_j^{(1)}}\theta^{at}\right)+1\\&=\sum_{j=d}^{2d-1}\left(\sum_{t\in p^{m-l}D_j^{(m)}}\theta^{bt}+\sum_{t\in p^{m-l+1}D_j^{(m-1)}}\theta^{bt}+\cdots+\sum_{t\in p^{m-l}\bullet p^{m-1}D_j^{(1)}}\theta^{bt}\right)+1\\&=p^{m-l}\sum_{j=d}^{2d-1}\left(\sum_{t\in p^{m-l}D_j^{(l)}}+\sum_{t\in p^{m-l+1}D_j^{(l-1)}}+\cdots+\sum_{t\in p^{m-1}D_j^{(1)}}\right)\theta^{bt}+\sum_{j=d}^{2d-1}\left(\sum_{t\in p^lD_j^{(m-l)}}+\cdots+\sum_{t\in p^{m-1}D_j^{(1)}}\right)\theta^{0\cdot t}+1\\&=p^{m-l}\sum_{j=d}^{2d-1}\left(\sum_{t\in p^{m-l}D_j^{(l)}}+\sum_{t\in p^{m-l+1}D_j^{(l-1)}}+\cdots+\sum_{t\in p^{m-1}D_j^{(1)}}\right)\theta^{bt}+\frac{p^{m-l}+1}{2}\end{aligned}$$

当 $b\in D_i^{(l)}$，根据引理 1，有 $bD_j^{(n)}=D_{i+j}^{(n)}\ (\bmod p^n)$，$bp^{m-n}D_j^{(n)}=p^{m-n}D_{i+j}^{(n)}$，$n=1,2,\cdots,l$，$i,j=0,1,\cdots 2d-1$。所以

$$B_0(\theta^a)=p^{m-l}\sum_{j=d}^{2d-1}\left(\sum_{t\in p^{m-l}D_{i+j}^{(l)}}+\sum_{t\in p^{m-l+1}D_{i+j}^{(l-1)}}+\cdots+\sum_{t\in p^{m-1}D_{i+j}^{(1)}}\right)\cdot\theta^t+\frac{p^{m-l}+1}{2}$$

因此，依据引理 1，若 $s\in D_d^{(l)}$，有

$$B_0(\theta^{as})=p^{m-l}\sum_{j=0}^{d-1}\left(\sum_{t\in p^{m-l}D_{i+j}^{(l)}}+\sum_{t\in p^{m-l+1}D_{i+j}^{(l-1)}}+\cdots+\sum_{t\in p^{m-1}D_{i+j}^{(1)}}\right)\cdot\theta^t+\frac{p^{m-l}+1}{2}=B_d(\theta^a)$$

根据引理 2 和引理 6，$a\in Z_{p^m}\setminus\{0\}$，有 $B_0(\theta^a)+B_d(\theta^a)=1$，因而当 a 取遍 $\bigcup_{i=0}^{2d-1}D_i$ 中的所有元素时，$B_0(\theta^a)=0$ 当且仅当 a 跑遍其中的 d 个 D_i，即恰好有 d 个 D_i 中的元素 a 使得 $B_0(\theta^a)=0$。因而，$B_0(\theta^a)=0$ 和 $B_0(\theta^a)=1$ 出现的次数相等，均为 $(p^m-1)/2$。定义集合 $T=\{l\,|\,B_0(\theta^a)=0, a\in D_l,\ l=0,1,\cdots,2d-1\}$ $S=\{0,1,\cdots,2d-1\}\setminus T$，显然 $|\,S\,|=|\,T\,|=d$。

定理 2　如果 $2\in D_0$，则序列的线性复杂度和极小多项式分别为

$$L(s)=\begin{cases}\dfrac{p^m+1}{2}, & m\text{为偶数, 或者}m\text{为奇数且}\ p\equiv 1\ (\bmod\ 8)\\ \dfrac{p^m-1}{2}, & m\text{为奇数且}\ p\equiv -1\ (\bmod\ 8)\end{cases}$$

$$m(x)=\begin{cases}(x-1)\prod_{a\in\cup_{i\in S}D_i}(x-\theta^a),\ m\text{为偶数},\\ \quad \text{或者}m\text{为奇数且}p\equiv 1(\bmod\ 8)\\ \prod_{a\in\cup_{i\in S}D_i}(x-\theta^a),\ m\text{为奇数且}\\ \quad p\equiv -1(\bmod\ 8)\end{cases}$$

证明 因为 $B_0(\alpha^0)=1$ 当且仅当 (1) m 为偶数，或(2) m 为奇数且 $p\equiv 1\ (\bmod\ 8)$ 成立。从而依据引理 6 和上面的讨论可知， $B_0(\theta^a)=0$ 当且仅当 $a\in\cup_{i\in T}D_i$。因此，

$$\gcd(x^{p^m}-1,\ B_0(x))=\prod_{a\in\cup_{i\in T}D_i}(x-\theta^a),$$

$$m(x)=(x-1)\prod_{a\in\cup_{i\in S}D_i}(x-\theta^a),\ \ L(s)=\frac{p^m+1}{2}$$

若 m 为奇数且 $p\equiv -1\ (\bmod\ 8)$， 则 $B_0(\alpha^0)=0$。类似地，有

$\gcd(x^{p^m}-1,B_0(x))=(x-1)\prod_{a\in\cup_{i\in T}D_i}(x-\theta^a)$, $m(x)=\prod_{a\in\cup_{i\in S}D_i}(x-\theta^a)$。 $L(s)=\dfrac{p^m-1}{2}$。 证毕

4 结论

本文对周期为 p^m 任意阶的广义割圆序列的线性复杂度进行了研究。结果表明：(1)该类序列的线性复杂度最小为 $(p^m-1)/2$，最大可达到 p^m， 且该类序列为平衡序列。除了参数同时满足 $2\in D_0$，m 为奇数且 $p\equiv -1\ (\bmod\ 8)$ 外，序列的线性复杂度均大于 $(p^m+1)/2$，因此，根据B-M算法，获取该序列的任何一段子序列都不能用该算法恢复出全部序列。(2)该结果与文献[7−13]的线性复杂度取值完全符合。 并且通过定理1的证明以及引理3，引理6可以看出：若定义集合 $\{0,1,\cdots,2d-1\}$ 中的任意 d 个元素构成的子集为 T，且若多项式 $B_T(x)=\sum_{t\in\cup_{i\in X}D_i}x^t+1$ 满足 $B_T(\alpha)+B_{T+d}(\alpha)=1$，则序列

$$s(t)=\begin{cases}0,\ \ t\in\cup_{i\in X}D_i\\ 1,\ \ \text{其它}\end{cases}\tag{4}$$

的线性复杂度结果取值有 p^m-1，p^m，$(p^m-1)/2$ 和 $(p^m+1)/2$ 4 种情形，与本文所给出的结论一致。

参 考 文 献

[1] Golomb S W. Shift Register Sequences[M]. Holden-Day, CA, San Francisco, 1967. Revised edition: Aegean Park, CA, Laguna Hills, 1982, Chapter 2.

[2] Ding C. Binary cyclotomic generators [C]. Fast Software Encryption: Berlin: Springer-Veralg, 1995, LNCS 1008: 20−60.

[3] Cusick T W, Ding C, and Renvall A. Stream Ciphers and Number Theory[M]. Elsevier, Amsterdam, 1998, Chapter 3−8.

[4] Ding C and Helleseth T. New generalized cyclotomy and its application[J]. *Finite Fields Applications*, 1998, 4(2): 140−166.

[5] Chen Z and Li S. Some notes on generalized cyclotomic sequences of length pq[J]. *Journal of Computer Science and Technology*, 2008, 23(5): 843−850.

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

[7] Ding C, Helleseth T, and Shan W J. On the linear complexity of Legendre sequence[J]. *IEEE Transaction on Information Theory*, 1998, 44(3): 1276−1278.

[8] Yan T, Huang B, and Xiao G. Cryptographic properties of some binary generalized cyclotomic sequences with the length p^2 [J]. *Information Sciences*, 2008, 178(4): 807−815.

[9] Du X, Chen Z, Shi A, and Sun R. Trace representation of a new class of sextic sequences of period p=3(mod8) [J]. *IEICE Transaction on Fundamentals*, 2009, E92-A(2): 668−670.

[10] Yan T, Sun R, and Xiao G. Autocorrelation and linear complexity of the new generalized cyclotomic sequences[J]. *IEICE Transaction on Fundamentals*, 2007, E90-A(4): 857−864.

[11] Kim Y J, Jin S Y, and Song H Y. Linear complexity and autocorrelation of prime cube sequences[C]. AAECC 2007, Springer-Verlag Berlin Heidelberg 2007, LNCS 4851: 188−197.

[12] Yan T, Li S, and Xiao G. On the linear complexity of generalized cyclotomic sequences with the period p^m [J]. *Applied Mathematics Letters*, 2008, 21(2): 187−193.

[13] Kim Y J and Song H Y. Linear complexity of prime n-square sequences[C]. ISIT 2008, Toronto, Canada, July 6−11, 2008: 2405−2408.

[14] Yan T, Du X, and Xiao G. Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2^k [J]. Information Sciences, Doi:10.1016/j.ins. 2008. 11. 006.

杜小昵： 女，1972年生，副教授，研究方向为密码学和信息安全.

闫统江： 男，1974年生，副教授，研究方向为密码学和信息安全.