Linear Complexity of a Family of Pseudorandom Discrete Logarithm Threshold Sequences

Chenhuang Wu[1,2], Xiaoni Du[3], and Zhengtao Jiang[4]
(Corresponding author: Chenhuang Wu)
School of Mathematics, Putian University[1]
Putian, Fujian 351100, P.R. China
School of Information Science and Technology, University of Science and Technology of China[2]
Hefei, Anhui 230000, P.R. China
(Email: ptuwch@163.com)
School of Mathematics and Information Science, Northwest Normal University[3]
Lanzhou, Gansu 730070, P.R. China
School of Computer Science, Communication University of China[4]
Chaoyang District, Beijing 100024, P.R. China
(Received Jan. 6, 2015; revised and accepted July 4 & Aug. 12, 2015)

Abstract

We discuss the linear complexity of a family of binary threshold sequence defined by the discrete logarithm of integers modulo a large prime. It is proved that the linear complexity is at least the half of their period and under some special conditions the linear complexity can achieve maximal.

Keywords: Binary threshold sequences, discrete logarithm, linear complexity

1 Introduction

A typical design approach to N-periodic sequences is application of cosets (or cyclotomic classes) via a subgroup of the group of invertible elements modulo N. Well-known basic examples are the Legendre and Jacobi sequences and their generalizations, which are related to discrete logarithm, see [4, 6, 8, 9, 10, 11, 12, 13] and references therein.

Let p be an odd prime. The *Legendre sequence* [9, 11, 16] $S_p = \{s_0, s_1, \ldots, s_{p-1}\}$ over the finite field $\mathbb{F}_2 = \{0, 1\}$ is defined as

$$s_u = \begin{cases} 0, & \text{if } \left(\frac{u}{p}\right) = 1 \text{ or } p|u, \\ 1, & \text{otherwise,} \end{cases} \qquad u \geq 0$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Let g be a (fixed) primitive root modulo p and $\mathrm{ind}(n)$ be the discrete logarithm of n modulo p (to the base g) so that

$$g^{\mathrm{ind}(n)} \equiv n \pmod{p}, \quad p \nmid n, \quad 1 \leq \mathrm{ind}(n) \leq p-1.$$

Then we get an equivalent definition of S_p:

$$s_u = \begin{cases} 0, & \text{if } \mathrm{ind}(u) \equiv 0 \pmod 2 \text{ or } p|u, \\ 1, & \text{otherwise,} \end{cases} \qquad u \geq 0.$$

Legendre sequences have strong pseudorandom properties: equidistribution, optimal correlation, high linear complexity and k-error linear complexity, see [1, 2, 8, 9, 11, 16].

In particular, Sárközy studied in [19] the following binary sequence $E_p = \{e_0, e_1, \ldots, e_{p-1}\}$, which is called *discrete logarithm threshold sequence* in [3], over $\mathbb{F}_2$ defined by

$$e_u = \begin{cases} 0, & \text{if } 1 \leq \mathrm{ind}(u) \leq (p-1)/2, \\ 1, & \text{if } (p+1)/2 \leq \mathrm{ind}(u) \leq p-1 \text{ or } u = 0. \end{cases} \tag{1}$$

Gyarmati later extended this construction in [15]. (Note that [15, 19] actually dealed with the sequences $E'_p = \{e'_0, \ldots, e'_{p-1}\} \in \{-1, 1\}^p$ defined by $e'_n = (-1)^{e_n}$, $0 \leq n \leq p-1$.)

Sárközy estimated the well-distribution measure and the correlation measure of order k (see [17] for the notions) for E_p in [19] and Brandstätter and Winterhof estimated a lower bound on linear complexity profile of E_p in terms of the correlation measure of order k in [3]. In this short article, we will view E_p as a p-periodic sequence and consider its *linear complexity* (see below for the notion) under some special conditions. Below we consider this problem in a general way.

Let $p - 1 = 2df$ for large prime p. The cyclotomic classes of order $2d$ give a partition of $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ defined by

$$D_l = \{g^{2di+l} \pmod{p} | i = 0, 1, \ldots, f-1\},$$

where $l = 0, 1, \ldots, 2d-1$. Then one can define binary sequences $\{e_u\}_{u\geq 0}$ of period p by setting

$$e_u = \begin{cases} 0, & \text{if } u \pmod p \in D_1 \cup \cdots \cup D_d, \\ 1, & \text{if } u \pmod p \in D_{d+1} \cup \cdots \cup D_{2d-1} \cup D_0, \\ 1, & \text{if } p|u, \end{cases} \tag{2}$$

where $u \geq 0$.

If $d = 1$, $\{e_u\}_{u\geq 0}$ is the complement of Legendre sequence. If $d = (p-1)/2$, $\{e_u\}_{u\geq 0}$ is the discrete logarithm threshold sequence E_p (viewing E_p as a p-periodic sequence) defined in Equation (1). The k-error linear complexity (over $\mathbb{F}_p$) of $\{e_u\}_{u\geq 0}$ was investigated in [1]. Certain pseudo-random measures of $\{e_u\}_{u\geq 0}$ were investigated in [6]. Below we consider the linear complexity (over $\mathbb{F}_2$) of $\{e_u\}_{u\geq 0}$ and hence obtain the linear complexity of E_p as a corollary in some special cases.

2 Linear Complexity

We recall that the *linear complexity* $L(\{s_t\}_{t\geq 0})$ of an N-periodic sequence $\{s_t\}_{t\geq 0}$ over $\mathbb{F}_2$ is the least order L of a linear recurrence relation over $\mathbb{F}_2$,

$$s_{t+L} = c_{L-1}s_{t+L-1} + \cdots + c_1 s_{t+1} + c_0 s_t \quad \text{for } t \geq 0$$

which is satisfied by $\{s_t\}_{t\geq 0}$ and where $c_0 = 1, c_1, \ldots, c_{L-1} \in \mathbb{F}_2$. The polynomial

$$M(x) = x^L + c_{L-1}x^{L-1} + \cdots + c_0 \in \mathbb{F}_2[x]$$

is called the *minimal polynomial* of $\{s_t\}_{t\geq 0}$. The *generating polynomial* of $\{s_t\}_{t\geq 0}$ is defined by

$$S(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1} \in \mathbb{F}_2[x].$$

It is easy to see that

$$M(x) = (x^N - 1)/\gcd\left(x^N - 1,\ S(x)\right),$$

hence

$$L(\{s_t\}_{t\geq 0}) = \deg(M(x)) = N - \deg\left(\gcd(x^N - 1,\ S(x))\right), \tag{3}$$

see, e.g. [18] for details.

Lemma 1. *Let $p - 1 = 2df$ and $a \in \mathbb{F}_p^*$, if $a \pmod p \in D_\ell$ for some $0 \leq \ell \leq 2d-1$, then we have*

$$aD_l = \{an \pmod p | n \in D_l\} = D_{l+\ell \pmod{2d}},$$

where $0 \leq l \leq 2d-1$.

Proof. Since $a \pmod p \in D_\ell$, there exists an integer $k_0 : 0 \leq k_0 < f$ such that $a \equiv g^{2dk_0+\ell} \pmod p$. Then we have

$$\begin{aligned} aD_l &= \left\{g^{2dk_0+\ell} \cdot g^{2dk+l} \pmod p |\ 0 \leq k < f\right\} \\ &= \left\{g^{2d(k_0+k)+(\ell+l)} \pmod p |\ 0 \leq k < f\right\} \\ &= D_{l+\ell \pmod{2d}}. \end{aligned}$$

□

For $0 \leq l \leq 2d-1$, define

$$D_l(x) = \sum_{n\in D_l} x^n \in \mathbb{F}_2[x]$$

and

$$U(x) = 1 + D_0(x) + D_{d+1}(x) + \cdots + D_{2d-1}(x), \tag{4}$$

which is the generating polynomial of $\{e_u\}_{u\geq 0}$ in Equation (2).

Lemma 2. *Let $p - 1 = 2df$ and $a \in \mathbb{F}_p^*$, if $a \pmod p \in D_\ell$ for some $0 \leq \ell \leq 2d-1$, then we have*

$$D_l(x^a) \equiv D_{l+\ell \pmod{2d}}(x) \pmod{x^p - 1},$$

where $0 \leq l \leq 2d-1$.

Proof. By Lemma 1 and the definition of $D_l(x)$, we have

$$\begin{aligned} D_l(x^a) &= \textstyle\sum_{n\in D_l} x^{an} \\ &= \textstyle\sum_{m\in aD_l} x^m \\ &\equiv D_{l+\ell \pmod{2d}}(x) \pmod{x^p - 1}. \end{aligned}$$

□

Lemma 3. *Let $p - 1 = 2df$ and $a \in \mathbb{F}_p^*$. For $U(x)$ in Equation (4), we have*

$$U(\beta^{ag^d}) = U(\beta^a) + 1,$$

where $\beta \in \overline{\mathbb{F}}_2$ is a primitive p-th root of unity.

Proof. Since $g^d \pmod p \in D_d$, using

$$D_0(\beta^a) + D_1(\beta^a) + \cdots + D_{2d-1}(\beta^a) = \sum_{i\in\mathbb{F}_p^*} \beta^{ai} = 1,$$

we have

$$\begin{aligned} & U(\beta^{ag^d}) \\ = \ & 1 + D_0(\beta^{ag^d}) + D_{d+1}(\beta^{ag^d}) + \cdots + D_{2d-1}(\beta^{ag^d}) \\ = \ & 1 + D_d(\beta^a) + D_1(\beta^a) + \cdots + D_{d-1}(\beta^a) \\ & \text{(by Lemma 2)} \\ = \ & 1 + 1 - D_0(\beta^a) - D_{d+1}(\beta^a) - \cdots - D_{2d-1}(\beta^a) \\ = \ & 1 + U(\beta^a). \end{aligned}$$

We note that the operations here (and hereafter) are performed in the algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$. □

Now we present main results of linear complexity of $\{e_u\}_{u\geq 0}$. According to Equation (3), we will consider below the number of $n : 0 \leq n < p$ such that $U(\beta^n) = 0$ for $\beta \in \overline{\mathbb{F}}_2$, which is a primitive p-th root of unity.

Proposition 1. *Let $p - 1 = 2df$ and $\{e_u\}_{u\geq 0}$ be defined in Equation (2). Then the linear complexity of $\{e_u\}_{u\geq 0}$ satisfies*

$$\frac{p-1}{2} + \epsilon(\frac{p+1}{2}) \leq L(\{e_u\}_{u\geq 0}) \leq p - 1 + \epsilon(\frac{p+1}{2}),$$

where $\epsilon(z) \in \{0, 1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Proof. As before, let $\beta \in \overline{\mathbb{F}}_2$ be a primitive p-th root of unity. If $U(\beta^n) = 0$ for some $n : 0 \le n < p$, we find that $U(\beta^{ng^d}) = 1$ by Lemma 3. We remark that the map $x \to xg^d$ on $\mathbb{F}_p^*$ is injective, so there are at most $(p-1)/2$ many $n \in \mathbb{F}_p^*$ such that $U(\beta^n) = 0$. Since there are exactly $(p+1)/2$ many 1's in one period of $\{e_u\}_{u\ge 0}$, we have $U(1) = (p+1)/2 \equiv 0 \pmod 2$ iff $\epsilon(\frac{p+1}{2}) = 0$. So in this case, we have the lower bound on linear complexity $L(\{e_u\}_{u\ge 0}) \ge (p-1)/2 + \epsilon(\frac{p+1}{2})$ and the upper bound $L(\{e_u\}_{u\ge 0}) \le p - 1 + \epsilon(\frac{p+1}{2})$ by Equation (3). □

For cryptographic applications, a sequence is required to have large linear complexity such that it can resist the Berlekamp-Massey algorithm. Below we discuss some special cases, under which the linear complexity of $\{e_u\}_{u\ge 0}$ is maximal.

Proposition 2. *Let $p - 1 = 2df$ and $\{e_u\}_{u\ge 0}$ be defined in Equation (2). If 2 is a primitive root modulo p, then the linear complexity of $\{e_u\}_{u\ge 0}$ satisfies*

$$L(\{e_u\}_{u\ge 0}) = p - 1 + \epsilon(\frac{p+1}{2}),$$

where $\epsilon(z) \in \{0, 1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Proof. When 2 is a primitive root modulo p, we see that $x^{p-1} + \cdots + x + 1$ is irreducible and $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. Since the minimal polynomial $M(x)$ of $\{e_u\}_{u\ge 0}$ satisfies $M(x)|(x^p - 1)$, there are only two choices for $M(x)$:

$$M(x) = x^p - 1 \quad \text{or} \quad M(x) = x^{p-1} + \cdots + x + 1.$$

On the other hand, we find that $\{e_u\}_{u\ge 0}$ satisfies the following recurrence relation

$$e_n + e_{n+1} + \cdots + e_{n+p-1} = (p+1)/2, \quad n \ge 0,$$

since again there are exactly $(p+1)/2$ many 1's in one period of $\{e_u\}_{u\ge 0}$. Hence $\epsilon(\frac{p+1}{2}) = 0$ implies $M(x) = x^{p-1} + \cdots + x + 1$ and $L(\{e_u\}_{u\ge 0}) = p - 1$, otherwise, $L(\{e_u\}_{u\ge 0}) = p$. □

When 2 is not a primitive root modulo p, it seems difficult to determine the linear complexity of $\{e_u\}_{u\ge 0}$, since now $x^{p-1} + \cdots + x + 1$ is reducible over $\mathbb{F}_2$. However, we have the following partial results.

Proposition 3. *Let $p - 1 = 2df$ and $\{e_u\}_{u\ge 0}$ be defined in Equation (2) and suppose that 2 is not a primitive root modulo p. If $2 \in D_0$ we have*

$$L(\{e_u\}_{u\ge 0}) = \frac{p-1}{2} + \epsilon(\frac{p+1}{2}).$$

And if $2 \in D_{\ell_0} \cup D_{2d-\ell_0}$ for some $1 \le \ell_0 \le d$ with $\ell_0|d$ or $\gcd(\ell_0, d) = 1$, we have

$$L(\{e_u\}_{u\ge 0}) = p - 1 + \epsilon(\frac{p+1}{2}),$$

where $\epsilon(z) \in \{0, 1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Proof. Let $\beta \in \overline{\mathbb{F}}_2$ be a primitive p-th root of unity. If $2 \in D_0$, then $U(\beta^a) \in \mathbb{F}_2$ for all $a \in \mathbb{F}_p^*$ from the fact $(U(\beta^a))^2 = U(\beta^{2a}) = U(\beta^a)$. So by Lemma 3 for any $a \in \mathbb{F}_p^*$ either $U(\beta^a) = 0$ or $U(\beta^{ag^d}) = 0$, and hence there are exactly $(p-1)/2$ many $a \in \mathbb{F}_p^*$ such that $U(\beta^a) = 0$, which implies the value of the linear complexity.

For the second statement, we need to show $U(\beta^a) \notin \mathbb{F}_2$ for all $a \in \mathbb{F}_p^*$. Suppose that $U(\beta^{a_0}) \in \mathbb{F}_2$ for some $a_0 \in \mathbb{F}_p^*$. Firstly let $2 \in D_{\ell_0}$. Using the equation $(U(\beta^{a_0}))^{2^{i+1}} = (U(\beta^{a_0}))^{2^i}$ for all $i \ge 0$, we get

$$\sum_{k=1}^{\ell_0} D_{k+i\ell_0}(\beta^{a_0}) = \sum_{k=d+1}^{d+\ell_0} D_{k+i\ell_0}(\beta^{a_0}), \tag{5}$$

here and hereafter, the subscripts of D are all modulo $2d$.

If $\gcd(\ell_0, d) = 1$, after adjusting the equations above, we get

$$\sum_{k=1+j}^{\ell_0+j} D_k(\beta^{a_0}) + \sum_{k=d+1+j}^{d+\ell_0+j} D_k(\beta^{a_0}) = 0$$

for $j = 0, 1, \ldots, d-1$. And hence we derive

$$\sum_{k=1+j}^{\ell_0+j} D_k(\beta) + \sum_{k=d+1+j}^{d+\ell_0+j} D_k(\beta) = 0$$

for $j = 0, 1, \ldots, d-1$. If $d = 1$, it contradicts to

$$D_0(\beta) + D_1(\beta) = 1.$$

For $d > 1$, let

$$F_j(x) = \sum_{k=1+j}^{\ell_0+j} D_k(x) + \sum_{k=d+1+j}^{d+\ell_0+j} D_k(x).$$

For any $n \in D_i$, $0 \le i \le 2d-1$, we derive

$$\begin{aligned} F_j(\beta^n) &= \sum_{k=1+j}^{\ell_0+j} D_k(\beta^n) + \sum_{k=d+1+j}^{d+\ell_0+j} D_k(\beta^n) \\ &= \sum_{k=1+j}^{\ell_0+j} D_{k+i}(\beta) + \sum_{k=d+1+j}^{d+\ell_0+j} D_{k+i}(\beta) \\ &= F_{j+i}(\beta) = 0 \end{aligned}$$

for $j = 0, 1, \ldots, d-1$. That is to say, each $F_j(x)$ has at least $p-1$ many roots. But we remark that $p - 1 = g^{(p-1)/2} = g^{df} \in D_0 \cup D_d$, which implies that there exists at least one $F_j(x)$ such that its degree is smaller than $p-1$, a contradiction.

If $\ell_0|d$, from Equation (5) we will get

$$\sum_{k=0}^{2d-1} D_k(\beta^{a_0}) = 0,$$

which contradicts to $\sum_{i\in\mathbb{F}_p^*} \beta^{ai} = 1$.

Secondly, let $2 \in D_{2d-\ell_0}$. Using

$$\sum_{i \in \mathbb{F}_p^*} \beta^{ai} = \sum_{k=0}^{2d-1} D_k(\beta^a) = 1$$

for all $a \in \mathbb{F}_p^*$, we derive a similar argument as above. □

In order to control the generation of $\{e_u\}_{u\geq 0}$ easily, we present the following corollary for special d.

Corollary 1. *Let $p-1 = 2df$ and $\{e_u\}_{u\geq 0}$ be defined in Equation (2). If d is a prime, then the linear complexity of $\{e_u\}_{u\geq 0}$ satisfies*

$$L(\{e_u\}_{u\geq 0}) = \begin{cases} p-1+\epsilon(\frac{p+1}{2}), & \text{if } 2 \notin D_0, \\ \frac{p-1}{2}+\epsilon(\frac{p+1}{2}), & \text{if } 2 \in D_0, \end{cases}$$

where $\epsilon(z) \in \{0,1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Certain related binary sequences have been investigated in the references. As special cases of Corollary 1, the following cyclotomic sequence of order 4, which is a complement of $\{e_u\}_{u\geq 0}$ (in this case, $d=2$), see [8, Chapter 8] or [1], is defined as

$$f_u = \begin{cases} 0, & \text{if } u \pmod p \in \{0\} \cup D_0 \cup D_3, \\ 1, & \text{if } u \pmod p \in D_1 \cup D_2, \end{cases} \qquad u \geq 0,$$

and the cyclotomic sequence of order 6, see [14], is defined as

$$h_u = \begin{cases} 0, & \text{if } u \pmod p \in \{0\} \cup D_1 \cup D_2 \cup D_3, \\ 1, & \text{if } u \pmod p \in D_4 \cup D_5 \cup D_0, \end{cases} \quad u \geq 0$$

which is a slight modification of $\{e_u\}_{u\geq 0}$ (in this case, $d=3$). The idea of this article can help us to determine the linear complexity of $\{f_u\}_{u\geq 0}$ and $\{h_u\}_{u\geq 0}$.

Corollary 2. *Let $p-1 = 2df$ and $\{e_u\}_{u\geq 0}$ be defined in Equation (2). If $d=4$, then the linear complexity of $\{e_u\}_{u\geq 0}$ satisfies*

$$L(\{e_u\}_{u\geq 0}) = \begin{cases} p-1+\epsilon(\frac{p+1}{2}), & \text{if } 2 \notin D_0, \\ \frac{p-1}{2}+\epsilon(\frac{p+1}{2}), & \text{if } 2 \in D_0, \end{cases}$$

where $\epsilon(z) \in \{0,1\}$ with $\epsilon(z) \equiv z \pmod 2$.

Unfortunately, for other composite d, the argument is more complicated. With notations as in Proposition 3, when $1 < \gcd(\ell_0, d) < \ell_0$ experiments show that linear complexity might take other values except $p-1+\epsilon(\frac{p+1}{2})$ and $\frac{p-1}{2}+\epsilon(\frac{p+1}{2})$, see Table 1. In fact, let $\mathtt{ord}_p(2)$ be the order of 2 modulo p. When 2 is not a primitive root of p, from the fact that $x^{p-1}+\cdots+x+1$ can be written as the product of $\frac{p-1}{\mathtt{ord}_p(2)}$ many irreducible polynomials of degree $\mathtt{ord}_p(2)$ over $\mathbb{F}_2$, see e.g. [8], the linear complexity of $\{e_u\}_{u\geq 0}$ is of the form $\frac{p-1}{2}+k\cdot\mathtt{ord}_p(2)+\epsilon(\frac{p+1}{2})$ with some integer $0 \leq k \leq \frac{p-1}{2\cdot\mathtt{ord}_p(2)}$.

Table 1: Linear complexity of $\{e_u\}_{u\geq 0}$ for some p and d with $1 < \gcd(\ell_0, d) < \ell_0$

p	g	d	$L(\{e_u\}_{u\geq 0})$	ℓ_0	$\mathtt{ord}_p(2)$
31	3	15	25	6	5
73	5	12	55	8	9
127	3	63	119	54	7
151	6	15	120	10	15
241	7	15	193	6	10
337	10	12	253	8	12
337	10	24	293	16	21
601	7	60	551	48	25
631	3	21	540	14	45
881	3	40	826	16	55
911	17	65	819	20	91

Corollary 3. *Let E_p be the discrete logarithm threshold sequence (of period p) with the first period defined in Equation (1). Then the linear complexity of E_p satisfies*

$$L(E_p) \geq \frac{p-1}{2} + \epsilon(\frac{p+1}{2}).$$

In particular,

$$L(E_p) = p-1+\epsilon(\frac{p+1}{2})$$

if $(p-1)/2$ is prime or 2 is a primitive root modulo p.

There exist primes p such that $L(E_p) \neq p-1+\epsilon(\frac{p+1}{2})$ when $(p-1)/2$ is not a prime number. For example, in Table 1, $p=241$, we have $(p-1)/2 = 120$ and $L(E_p) = 193 \neq p-1+\epsilon(\frac{p+1}{2})$.

3 Concluding Remarks

In this work, we have shown that the linear complexity of a family of discrete logarithm threshold sequences of period p is at least the half of their period, which can resist the B-M attack. We also gave some special conditions under which the linear complexity can achieve maximal.

We remark that we only concentrate on the threshold sequences in terms of the discrete logarithm of integers modulo p. Recently a family of binary threshold sequences of period p^2 has been defined by using Fermat quotient and its generalizations, such sequences are related to discrete logarithm of integers modulo p^2 [5, 7, 22].

The idea of this work can also help us to deal with binary threshold sequences defined by the discrete logarithm of integers modulo p^r for $r \geq 3$. Actually Ref.[14] deals with the case of any $r \geq 2$ and $d=3$. Of course, it is interesting to study binary threshold sequences in terms of the discrete logarithm of integers modulo pq, thanks to the Jacobi sequence and its generalizations investigated in the literature [6, 10, 12, 20, 21].

Acknowledgements

The authors wish to thank Zhixiong Chen for helpful discussions. C.H.W. was partially supported by the National Natural Science Foundation of China under grant No.61373140, and the Natural Science Foundation of Fujian Province No.2015J01662. X.N.D. was partially supported by the National Natural Science Foundation of China under grant 61462077. Z.T.J. was partially supported by the National Natural Science Foundation of China(61103199), and the Engineering Program Project of CUC(3132015XNG1541).

References

[1] H. Aly, W. Meidl and A. Winterhof, "On the k-error linear complexity of cyclotomic sequences", *Journal of Mathematical Cryptology*, vol. 1, no. 3, pp. 283–296, 2007.

[2] H. Aly and A. Winterhof, "On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidel'nikov sequences", *Designs, Codes and Cryptography*, vol. 40, no. 3, pp. 369–374, 2006.

[3] N. Brandstätter and A. Winterhof, "Linear complexity profile of binary sequences with small correlation measure", *Periodica Mathematica Hungarica*, vol. 52, no. 2, pp. 1–8, 2006.

[4] A. Çeşmelioğlu and W. Meidl, "A General Approach to Construction and Determination of the Linear Complexity of Sequences Based on Cosets", in *Sequences and Their Applications (SETA'10)*, LNCS 6338, pp. 125–138, Springer, 2010.

[5] Z. Chen and X. Du, "On the linear complexity of binary threshold sequences derived from Fermat quotients", *Designs, Codes and Cryptography,* vol. 67, no. 3, pp. 317–323, 2013.

[6] Z. Chen, X. Du and G. Xiao, "Sequences Related to Legendre/Jacobi Sequences", *Information Sciences*, vol. 177, no. 21, pp. 4820–4831, 2007.

[7] Z. Chen, A. Ostafe and A. Winterhof, "Structure of pseudorandom numbers derived from Fermat quotients", *International Workshop on the Arithmetic of Finite Fields (WAIFI'10)*, LNCS 6087, pp. 73–85, Springer, 2010.

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

[9] C. Ding, "Pattern distribution of Legendre sequences", *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1693–1698, 1998.

[10] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2", *Finite Fields and Their Applications*, no. 3, pp. 159–174, 1997.

[11] C. Ding, T. Helleseth and W. Shan, "On the linear complexity of Legendre sequence", *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, 1998.

[12] C. Ding, "Autocorrelation values of generalized cyclotomic sequences of order two", *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1699–1702, 1998.

[13] C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, Springer-Verlag, Berlin, 1991.

[14] X. Du and Z. Chen, "A Generalization of the Hall's Sextic Residue Sequences", *Information Sciences*, vol. 222, pp. 784–794, 2013.

[15] K. Gyarmati, "On a family of pseudorandom binary sequences", *Periodica Mathematica Hungarica*, vol. 49, no. 2, pp. 45–63, 2004.

[16] J. H. Kim and H. Y. Song, "Trace representation of Legendre sequences", *Designs, Codes and Cryptography*, vol. 24, no. 3, pp. 343–348, 2001.

[17] C. Mauduit and A. Sárközy, "On Finite Pseudorandom Binary Sequences I: Measures of Pseudorandomness, the Legendre Symbol", *Acta Arithmetica*, vol. 82, no. 12, pp. 365–377, 1997.

[18] H. Niederreiter, "Linear complexity and related complexity measures for sequences", *Progress in Cryptology (INDOCRYPT'03)*, LNCS 2904, pp. 1–17, Springer, 2010.

[19] A. Sárközy, "A finite pseudorandom binary sequence", *Studia Scientiarum Mathematicarum Hungarica*, vol. 38, no. 1–4, pp. 377–384, 2001.

[20] T. Yan, "New Binary Sequences of Period pq with Low Values of Correlation and Large Linear Complexity", *International Journal of Network Security*, vol. 10, no. 3, pp. 185–189, 2010.

[21] T. Yan, X. Du, S. Li and G. Xiao, "Trace representations and multi-rate constructions of two classes of generalized cyclotomic sequences", *International Journal of Network Security*, vol. 7, no. 2, pp. 269–272, 2008.

[22] C. Wu, Z. Chen and X. Du, "Binary Threshold Sequences Derived from Carmichael Quotients with Even Numbers Modulus", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E95-A, no. 7, pp. 1197–1199, 2012.

Chenhuang Wu was born in 1981. He received the M.S. degree in mathematics from Minnan Normal University in 2007. Now he is an associate professor of Putian University. His research interests include stream cipher, elliptic curve cryptography and digital signatures.

Xiaoni Du was born in 1972. She received the M.S degree in computer science from Lanzhou University in 2000 and Ph.D. degree in cryptography from Xidian University, China, in 2008, respectively. Now she is a professor of Northwest Normal University. Her research interests include cryptology and information security.

Zhengtao Jiang was born in 1976. He got doctor degree in 2005, and now he is an associate professor working for Department of Computer Science, Communication

University of China. His research interest include: Information security, Public opinion analysis, Computational advertising.