IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 July 2022, accepted 21 August 2022, date of publication 25 August 2022, date of current version 23 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3201497

RESEARCH ARTICLE

Linear Complexity of New Binary Sequence Derived From Polynomial Quotients Modulo p in General Case and Their Generalizations

JIANG MA[1], JUN ZHANG[2], YANGUO JIA[1], AND XIUMIN SHEN[1]
[1]School of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China
[2]Tangshan Institute of Measurement Test, Tangshan Administration for Market Regulation, Tangshan 063000, China

Corresponding author: Yanguo Jia (jyg@ysu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61501395, in part by the Natural Science Foundation of Hebei Province under Grant F2020203043, in part by the Research Project for Science and Technology in Higher Education of Hebei under Grant QN2021144, and in part by the Science and Technology Research and Development Program of Qinhuangdao under Grant 202005A008.

ABSTRACT Pseudorandom sequences with large linear complexity have been widely applied in electronic countermeasures, mobile communication and cryptography. Linear complexity is considered as a primary security criterion to measure the unpredictability of pseudorandom sequences. This paper presents the linear complexity and minimal polynomial of a new family of binary sequences derived from polynomial quotients modulo an odd prime p in general case. The results indicate that the sequences have high linear complexity, which means they can resist the linear attack against pseudo-noise or stream ciphers. Moreover, we generalize the result to the polynomial quotients modulo a power of p in general case. Finally, we design a Gpqs stream cipher generator based on the generalized binary pseudorandom sequences to implement the sequences in hardware.

INDEX TERMS Pseudorandom sequences, electronic countermeasures, stream cipher, linear complexity, polynomial quotients.

I. INTRODUCTION

Pseudorandom sequences always have wide applications in engineering fields. From a cryptographic point of view, one good pseudorandom sequence should have high linear complexity, which is not less than half of the period of sequence. More recently, Fermat quotients and Euler quotients have been studied to construct a large number of pseudorandom sequences. Similar construction method is naturally generalized to polynomial quotient.

Let p be an odd prime, $f(x) \in \mathbb{Z}[x]$ a general polynomial with leading coefficient not divisible by p, where $\mathbb{Z}[x]$ denotes polynomial ring with integer coefficients. The polynomial quotient modulo p in general case is defined by

$$Q(u) \equiv \frac{f(u) - f_p(u)}{p} \bmod p,\ 0 \le Q(u) \le p-1, u \geqslant 0, \quad (1)$$

where $f_p(u) \equiv f(u) \bmod p$ [1].

For all integers u and k, under the condition that $f'(u)$ is not identically zero, it is easy to check that

$$Q(u + kp) \equiv Q(u) + kf'(u) \bmod p \quad (2)$$

where $f'(u)$ is defined to be the derivative of $f(u)$. Setting $k = p$ in (2), it is clear to see that $Q(u)$ is periodic with least period p^2 [2].

Chen and Winterhof first defined the Polynomial quotient modulo p in general case [1]. After that, cryptographic properties of pseudorandom sequences derived from polynomial quotient began to attract academic attention [3], [4], [5], [6]. Many number theoretic and cryptographic questions have

The associate editor coordinating the review of this manuscript and approving it for publication was Aneel Rahim.

been studied for polynomial quotients sequences [2], [7], [8], [9], [10]. It needs to be pointed out that most studies focused on special cases of $f(x)$ but rarely considered the general cases [7], [8], [9], [10], [11], [12], [13]. There are two families of binary sequences derived from polynomial quotients in general case to be discussed from the view point of cryptography [2]. One is the binary threshold sequences (e_u) defined as

$$e_u = \begin{cases} 0, & \text{if } 0 \leqslant Q(u)/p < 1/2, \\ 1, & \text{if } 1/2 \leqslant Q(u)/p < 1. \end{cases} \tag{3}$$

The other is the general polynomial quotient sequence (h_u) defined by

$$h_u = \begin{cases} 0, & \text{if } (\frac{Q(u)}{p}) = 1 or Q(u) = 0, \\ 1, & \text{otherwise.} \end{cases} \tag{4}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol [2]. The Legendre symbol is defined to be equal to ± 1 depending on whether a number is a quadratic residue modulo an odd prime.

Du *et al.* proved that the two sequences above have high linear complexity and extended the constructions to arbitrary d-ary sequences for prime $d \mid (p-1)$ with d a primitive root modulo p^2 [2]. In modular arithmetic, a number g is called a primitive root modulo n if and only if every number coprime to n is congruent to a power of g modulo n.

In this paper, we define a new binary sequence (s_u) derived from polynomial quotients in general case as

$$s_u = \begin{cases} 0, & \text{if } Q(u) \equiv 0 \bmod 2, \\ 1, & \text{if } Q(u) \equiv 1 \bmod 2. \end{cases} \tag{5}$$

Note that (s_u) is also p^2 periodical over the finite field $\mathbb{F}_2$. In fact, when $f(x) = x^w$, (s_u) is just the sequence defined by Zhao *et al.*, which is only a special case of this article [14]. Clearly that, the characteristic set of (s_u) is different from (e_u) and (h_u), and they belong to different sequences. We will investigate the minimal polynomial and linear complexity of (s_u). In addition, we extend the general polynomial quotients $Q(u)$ modulus p to $F(u)$ modulo p^r, a prime power.

We recall that the linear complexity $LC((a_u))$ of an N-periodic sequence (a_u) over the binary finite field $\mathbb{F}_2$ is the least order L of a linear recurrence relation over finite field $\mathbb{F}_2$ [7].

$$a_{u+L} + c_{L-1}a_{u+L-1} + \cdots + c_1 a_{u+1} + c_0 a_u = 0 \text{ for } u \geqslant 0, \tag{6}$$

which is satisfied by (a_u) and where $c_0 \neq 0$, $c_0 \cdots c_{L-1} \in \mathbb{F}_2$. The polynomial

$$a(x) = c_0 + c_1 x + c_2 x^2 \cdots + c_{N-1} x^{N-1} \in \mathbb{F}_2[x]. \tag{7}$$

is called the generating polynomial of (a_u).

The polynomial

$$m(x) = x^L + c_{L-1}x^{L-1} + \cdots + c_0 \in \mathbb{F}_2[x]. \tag{8}$$

is called the minimal polynomial of (a_u), which can be obtained by computing

$$m(x) = (x^N - 1)/\gcd(x^N - 1, a(x)). \tag{9}$$

and the linear complexity of (a_u) is

$$LC((a_u)) = \deg(m(x)) = N - \deg(\gcd(x^N - 1), a(x)). \tag{10}$$

See, e.g., [15], [16] for details.

II. THE MINIMAL POLYNOMIAL AND LINEAR COMPLEXITY

Note that a conjecture of Artin indicates that approximately 3/8 of all primes have 2 as a primitive root, and that it is very seldom that a primitive root modulo the prime p is not also a primitive root modulo p^2 [17], [18].

Lemma 1 [19]: Let p be an odd prime. If 2 is a primitive root modulo p^2, then 2 is also a primitive root modulo p^i for all $i \geqslant 1$. Consequently, the cyclotomic polynomials $\Phi_n(x)$ are irreducible in polynomial ring over a finite field $\mathbb{F}_2[x]$, where $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}$ and $\mu(\cdot)$ denotes Mobius function.

Theorem 1: Let (s_u) be the p^2-periodic binary sequence defined as in (5). If 2 is a primitive element modulo p^2, then the minimal polynomial of (s_u) is

$$m(x) = \begin{cases} \Phi_{p^2}(x), & \text{if } |D_1| = 0, \\ \Phi_p(x)\Phi_{p^2}(x), & \text{if } |D_1| \neq 0 \text{ is even}, \\ (x-1)\Phi_p(x)\Phi_{p^2}(x), & \text{if } |D_1| \text{ is odd}. \end{cases}$$

if $p \equiv 1 \bmod 4$, and

$$m(x) = \begin{cases} (1+x)\Phi_{p^2}(x), & \text{if } |D_0| = 0, \\ \Phi_p(x)\Phi_{p^2}(x), & \text{if } |D_0| \text{ is odd}, \\ (x-1)\Phi_p(x)\Phi_{p^2}(x), & \text{if } |D_0| \neq \text{ is even}. \end{cases}$$

if $p \equiv 3 \bmod 4$.

The corresponding linear complexity of (s_u) is

$$LC((s_u)) = \begin{cases} p^2 - p, & \text{if } |D_1| = 0, \\ p^2 - 1, & \text{if } |D_1| \neq 0 \text{ is even}, \\ p^2 & \text{if } |D_1| \text{ is odd}. \end{cases}$$

if $p \equiv 1 \bmod 4$, and

$$LC((s_u)) = \begin{cases} p^2 - p + 1, & \text{if } |D_0| = 0, \\ p^2 - 1, & \text{if } |D_0| \text{ is odd}, \\ p^2 & \text{if } |D_0| \neq 0 \text{ is even}. \end{cases}$$

if $p \equiv 3 \bmod 4$, where $|D_i|$ is the cardinality of D_i defined by

$$D_0 = \left\{u \mid 0 \leqslant u \leqslant p-1, f'(u) \equiv 0 \bmod p, Q(u) \equiv 0 \bmod 2\right\},$$
$$D_1 = \left\{u \mid 0 \leqslant u \leqslant p-1, f'(u) \equiv 0 \bmod p, Q(u) \equiv 1 \bmod 2\right\}.$$

Proof: Over the finite field $\mathbb{F}_2$, we have

$$x^{p^2} - 1 = (x-1)\Phi_p(x)\Phi_{p^2}(x),$$

where $\Phi_p(x) = \sum_{i=0}^{p-1} x^i \in \mathbb{F}_2[x], \Phi_{p^2}(x) = \sum_{i=0}^{p-1} x^{ip} \in \mathbb{F}_2[x]$. Let $m(x)$ be the minimal polynomial of (s_u), then $m(x)$ is a factor of $(x-1)\Phi_p(x)\Phi_{p^2}(x)$ by Lemma 1.

For any fixed u with $f'(u) \not\equiv 0 \bmod p$, when k ranges over $\{0, 1, 2, \cdots, p-1\}$, $Q(u+kp)$ takes on each element of $\{0, 1, 2, \cdots, p-1\}$, Thus $s_{u+kp} = 0$ for $(p+1)/2$ integers k and $s_{u+kp} = 1$ for $(p-1)/2$ integers k. We know $m(x) \nmid (x^p - 1)$, i.e., $m(x) \nmid (x-1)\Phi_p(x)$ since the period of (s_u) is $> p$. Also, we have $\sum_{k=0}^{p-1} s_{u+kp} = (p-1)/2$.
On the other hand, for any u with $f'(u) \equiv 0 \bmod p$, we have

$$\sum_{k=0}^{p-1} s_{u+kp} = \begin{cases} 0 \bmod 2, & \text{if } u \in D_0, \\ 1 \bmod 2, & \text{if } u \in D_1. \end{cases} \tag{11}$$

The proof can be given by the two cases of the values of p

1) $p \equiv 1 \bmod 4$

If $\forall u \notin D_1$, i.e., $|D_1| = 0$, we have $\sum_{k=0}^{p-1} s_{u+kp} \equiv 0 \bmod 2$ for any u.Thus $m(x) \mid \Phi_{p^2}(x)$ since $\Phi_{p^2}(x)$ is a characteristic polynomial of (s_u). That is, $m(x) = \Phi_{p^2}(x)$ since $\Phi_{p^2}(x)$ is irreducible over $\mathbb{F}_2(x)$. So the linear complexity of (s_u) is $LC((s_u)) = \deg(m(x)) = p^2 - p$.

If $\exists\ u \in D_1$, i.e.,$|D_1| \neq 0$, we have $\sum_{k=0}^{p-1} s_{u+kp} = p \equiv 1 \bmod 2$ for $u \in D_1$. At the same time, by (11), we have $\sum_{k=0}^{p-1} s_{u+kp} + \sum_{k=0}^{p-1} s_{(u+1)+kp} = p \equiv 1 \bmod 2$ for any u. Hence $m(x) \nmid (1+x)\Phi_{p^2}(x)$. Now for all u we find that

$$\begin{aligned} \sum_{v=0}^{p^2-1} s_{u+v} &= \sum_{v=0}^{p^2-1} s_v = \sum_{v=0}^{p-1}\sum_{k=0}^{p-1} s_{v+kp} \\ &= \Big(\sum_{v\in D_1} + \sum_{\substack{v=0 \\ v\notin D_1}}\Big)\sum_{k=0}^{p-1} s_{v+kp} \\ &= |D_1|\,p \\ &= \begin{cases} 0 \bmod 2, & \text{if } |D_1| \text{ is even}, \\ 1 \bmod 2, & \text{if } |D_1| \text{ is odd}. \end{cases} \end{aligned}$$

for all u, which implies $m(x) \mid \Phi_p(x)\Phi_{p^2}(x)$ when $|D_1|$ is even, and $m(x) \mid (x^{p^2} - 1)$ when $|D_1|$ is odd. Then $LC((s_u)) = p^2 - 1$ when $|D_1|$ is even, and $LC((s_u)) = p^2$ when $|D_1|$ is odd.

2) $p \equiv 3 \bmod 4$

If $\forall u \notin D_0$, i.e., $|D_0| = 0$, we have $\sum_{k=0}^{p-1} s_{u+kp} = p \equiv 1 \bmod 2$ for any u, which implies that $m(x) \nmid \Phi_{p^2}(x)$. At the same time, by (11), we have $\sum_{k=0}^{p-1} s_{u+kp} + \sum_{k=0}^{p-1} s_{(u+1)+kp} = p + (p-1)/2 \equiv 0 \bmod 2$ for any u. Hence $m(x) \mid (1+x)\Phi_{p^2}(x)$, and $LC((s_u)) = \deg(m(x)) = p^2 - p + 1$.

If $\exists\ u \in D_0$, i.e.,$|D_0| \neq 0$, we have $\sum_{k=0}^{p-1} s_{u+kp} \equiv 0 \bmod 2$ only for $u \in D_0$. Now we find that

$$\begin{aligned} \sum_{v=0}^{p^2-1} s_{u+v} &= \sum_{v=0}^{p^2-1} s_v = \sum_{v=0}^{p-1}\sum_{k=0}^{p-1} s_{v+kp} \\ &= \Big(\sum_{v\in D_0} + \sum_{\substack{v=0 \\ v\notin D_0}}\Big)\sum_{k=0}^{p-1} s_{v+kp} \\ &= (p - |D_0|)p \\ &= \begin{cases} 0 \bmod 2, & \text{if } |D_0| \text{ is odd}, \\ 1 \bmod 2, & \text{if } |D_0| \text{ is even}. \end{cases} \end{aligned}$$

for all u, which implies $m(x) \mid \Phi_p(x)\Phi_{p^2}(x)$ when $|D_0|$ is odd, and $m(x) = x^{p^{p^2}} - 1$ when $|D_0|$ is even since $\Phi_p(x)$ and $\Phi_{p^2}(x)$ are irreducible in $\mathbb{F}_2(x)$ and neither of them is the characteristic polynomial of (s_u). Then $LC((s_u)) = p^2 - 1$ when $|D_0|$ is odd, and $LC((s_u)) = p^2$ when $|D_0|$ is even. The proof is completed.

In the following content, we will give two examples to confirm our main results.

Example 1: Let $p = 5, f(x) = 4x^3 + 3x^2 + 5x + 6$. Then $p \equiv 1 \bmod 4$, and 2 is a primitive root modulo 25. The least period of the binary sequence (s_u) is 25. $|D_0| = 0, |D_1| = 1$ is odd.

The sequence (s_u) in one period is

$$\{1,1,\ 1,\ 1,\ 0,\ 1,1,\ 1,\ 1,1,\ 0,\ 1,0,\ 0,\ 1,\ 0,1,\ 0,\ 0,0,\ 0,1,\ 0,0,\ 0\}.$$

The minimal polynomial of the sequence (s_u) over $\mathbb{F}_2$ is $x^{25} - 1$.

And so the linear complexity of this sequence is exactly $25 = p^2$.

Example 2: Let $p = 11, f(x) = 2x^7 + 3x^5 + 4x^3 + 7x^2 + 4x + 9$. Then $p \equiv 3 \bmod 4$, and 2 is a primitive root modulo 121. The least period of the binary sequence (s_u) is $p^2 = 121$. $|D_0| = 0, |D_1| = 0$.

The sequence (s_u) in one period is

$\{0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0,$
$1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0,$
$1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1,$
$0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0,$
$0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0\}.$

The minimal polynomial of the sequence (s_u) over $\mathbb{F}_2$ is $x^{111}+x^{110}+x^{100}+x^{99}+x^{89}+x^{88}+x^{78}+x^{77}+x^{67}+x^{66}+x^{56}+x^{55}+x^{45}+x^{44}+x^{34}+x^{33}+x^{23}+x^{22}+x^{12}+x^{11}+x+1$. And so the linear complexity of this sequence is exactly equal to $111 = p^2 - p + 1$.

With the help of programming software, more examples have been tested. In fact, all possible values of linear complexity of (s_u) could be taken when the polynomial $f(x)$ is properly chosen. The results are consistent with the Theorem 1 in this paper.

III. GENERALIZATION TO THE POLYNOMIAL QUOTIENT IN GENERAL CASE

For an odd prime p, integers $r > 0$, and $f(x)$ a polynomial over $\mathbb{Z}[x]$, the polynomial quotient modulo p^r in general case is defined by

$$F(u) \equiv \frac{f(u) - f_{p^r}(u)}{p^r} \bmod p^r, \quad 0 \le F(u) \le p^r - 1, \tag{12}$$

for all u, where $f_{p^r}(u) \equiv f(u) \bmod p^r$. Clearly that $F(u)$ is just the function in (1) when $r = 1$. For all integers u and k, under the condition that $f'(u)$ is not identically zero, it is easy

to check that

$$F(u+kp^r) \equiv F(u) + kp^{r-1}f'(u) \bmod p^r \tag{13}$$

where $f'(u)$ is defined to be the derivative of $f(u)$. Setting $k = p$ in (13), under the condition that $f'(u)$ is not identically zero, it is clear to see that $F(u)$ is periodic with least period p^{r+1}. Then we define the binary sequence (f_u) by

$$f_u = \begin{cases} 0, & \text{if } F(u) \equiv 0 \bmod 2, \\ 1, & \text{if } F(u) \equiv 1 \bmod 2. \end{cases} \tag{14}$$

Theorem 2: Let (f_u) be the p^{r+1}-periodic binary sequence defined as in (14). If 2 is a primitive element modulo p^2, then there exists $H = \{0, 1, 2, \cdots, r-1\}$ such that the minimal polynomial of (f_u) is

$$m(x) = \Phi_{p^{r+1}}(x) \prod_{i \in H} \Phi_{p^i}(x),$$

and the corresponding linear complexity of (f_u) is

$$LC((f_u)) = p^{r+1} - p^r + \sum_{i \in H} p^i(p-1)$$

Proof: The multiplicative order of 2 mod p^i is $p^{i-1}(p-1)$ since 2 is a primitive element modulo p^2. Thus the cyclotomic polynomial $\Phi_{p^i}(x)$ is irreducible over in $\mathbb{F}_2[x]$.

For any fixed u with $\gcd(u, p) = 1$, by (13) we have

$$F(u+kp^r) = \left\{F(u), F(u)+p^{r-1}, \cdots, F(u)+(p-1)p^{r-1}\right\}$$

if k runs through the set $\{0, 1, \cdots, p-1\}$. Then,

when $F(u)$ is even, it follows that

$$f_u + f_{u+p^r} + \cdots + f_{u+(p-1)p^r} = \frac{p-1}{2}.$$

when $F(u)$ is odd, it follows that

$$f_u + f_{u+p^r} + \cdots + f_{u+(p-1)p^r} = \frac{p+1}{2}.$$

So there always exists u such that $f_u + f_{u+p^r} + \cdots + f_{u+(p-1)p^r} \neq 0$, which implies that $\Phi_{p^{r+1}}(x) \mid m(x)$ and $m(x) \neq \Phi_{p^{r+1}}(x)$. We know $m(x) \mid x^{p^{r+1}} - 1$ and the cyclotomic polynomial $\Phi_{p^i}(x)$ is irreducible over in $\mathbb{F}_2[x]$. Thus there exists nonempty set $H \subseteq \{0, 1, 2, \cdots, r-1\}$ such that the minimal polynomial of (f_u) is

$$m(x) = \Phi_{p^{r+1}}(x) \prod_{i \in H} \Phi_{p^i}(x),$$

and the corresponding linear complexity of (f_u) is

$$LC((f_u)) = p^{r+1} - p^r + \sum_{i \in H} p^i(p-1).$$

The proof is completed.

The following example helps to confirm our main results.

Example 3: Let $p = 5$, $r = 2$, $f(x) = 4x^3 + 3x^2 + 5x + 6$, $f_{p^r}(x) = f(x)^{(\varphi(p^r)+r)}$ meets the condition that $f(x)^r \equiv f_{p^r}(x) \bmod p^r$, where $\varphi(x)$ denote Euler's function. Then 2 is a primitive root modulo 25. The least period of the binary sequence (s_u) is $p^3 = 125$. The sequence (s_u) in one period is

$\{0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0\}$.

The minimal polynomial of the sequence (s_u) over $\mathbb{F}_2$ is

$$\begin{aligned} m(x) = {} & x^{120} + x^{115} + x^{110} + x^{105} + x^{100} + x^{95} + x^{90} + x^{85} \\ & + x^{80} + x^{75} + x^{70} + x^{65} + x^{60} + x^{55} + x^{50} + x^{45} \\ & + x^{40} + x^{35} + x^{30} + x^{25} + x^{20} + x^{15} + x^{10} + x^5 + 1. \end{aligned}$$

And so the linear complexity of this sequence is exactly equal to $120 = p^3 - p^2 + p(p-1)$.

IV. IMPLEMENTATION AND APPLICATION IN STREAM CIPHER SYSTEM

After Shannon proved the absolute security of the one-time pad in theory, the research on stream ciphers has been triggered. Pseudorandom sequences have been the kernel of stream ciphers. By generalizing to the polynomial quotient modulo p^r in general case, we can obtain lots of pseudorandom sequences with high linear complexity [16]. We will apply them to stream cipher system as follows.

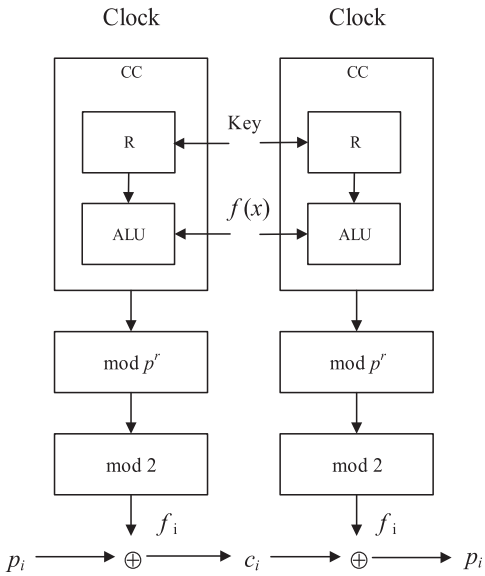


FIGURE 1. The implementation and application of Gpqs stream cipher generator.

A stream cipher generator derived from polynomial quotients with period p^{r+1} can be implemented in Fig.1, where CC denote cyclic counter that count the numbers $\{0, 1, 2, \cdots, p^{r+1}-1\}$ cyclically, and within CC, there are registers to store the current counted number and arithmetic logic unit(ALU) to computer polynomial quotients [20]. We name the generator as Gpqs stream cipher generator. The initial value of the register form the key of this generator. The polynomial $f(x)$ is defined in section 3. The f_i denotes pseudorandom sequence, the p_i denotes plaintext stream, the c_i denotes ciphertext stream, and the symbol $\oplus$ denotes XOR.

By the choices of different polynomials and the power of p, the Gpqs stream cipher generator can generate lots of pseudorandom sequences with high linear complexity.

V. CONCLUSION

In this work, we firstly define a family of new binary sequence derived from polynomial quotients modulo an odd prime p in general case, then determine the linear complexity and the minimal polynomial of the sequences under the condition that 2 is a primitive element modulo p^2. By the Berlekamp-Massey algorithm, the linear complexity of pseudorandom sequence must be greater than the half of its period [21]. The results show that the sequences have high linear complexity to resist the attack of Berlekamp-Massey algorithm. It can be seen that Zhao *et al.*'s conclusion is only a special case of our results [14]. Furthermore, we generalize the results to the polynomial quotients modulo a power of p in general case for the first time. We give the general expression of the linear complexity and the minimal polynomial of the sequences under the condition that 2 is a primitive element modulo p^2. The results indicate that the generalized sequences still have high linear complexity. In addition, we show the implementation and application of the generalized sequences in stream cipher system. It is interesting to study pseudorandom properties of these sequences when 2 is not a primitive element modulo p^2.

ACKNOWLEDGMENT

The authors would like to thank the editors and the anonymous reviewers for their constructive suggestions, which greatly improve the presentation quality of this paper.

REFERENCES

[1] Z. X. Chen and A. Winterhof, "Additive character sums of polynomial quotients," in *Proc. 10th Int. Conf. Finite Fields Their Appl.*, vol. 579. Ghent, Belgium: American Mathematical Society, 2012, pp. 67–73.

[2] X. Du, J. Zhang, and C. Wu, "Linear complexity of pseudorandom sequences derived from polynomial quotients: General cases," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E97.A, no. 4, pp. 970–974, 2014.

[3] I. E. Shparlinski and A. Winterhof, "Distribution of values of polynomial fermat quotients," *Finite Fields Their Appl.*, vol. 19, no. 1, pp. 93–104, Jan. 2013.

[4] Z. Ye, P. Ke, and Z. Chen, "Further results on pseudorandom binary sequences derived from Fermat–Euler quotients," in *Proc. 10th Int. Conf. Inf., Commun. Signal Process. (ICICS)*, Dec. 2015, pp. 1–4, doi: 10.1109/ICICS.2015.7459968.

[5] D. Gomez and A. Winterhof, "Multiplicative character sums of Fermat quotients and pseudorandom sequences," *Periodica Math. Hungarica*, vol. 64, no. 2, pp. 161–168, 2012.

[6] Z. Chen and A. Winterhof, "Polynomial quotients: Interpolation, value sets and Waring's problem," *Acta Arithmetica*, vol. 170, no. 2, pp. 121–134, 2015.

[7] X. Du, A. Klapper, and Z. Chen, "Linear complexity of pseudorandom sequences generated by fermat quotients and their generalizations," *Inf. Process. Lett.*, vol. 112, no. 6, pp. 233–237, Mar. 2012.

[8] Z. X. Chen and D. Gómez-Pérez, "Linear complexity of binary cequences derived from polynomial quotients," in *Proc. Int. Conf. Sequences Their Appl.* Berlin, Germany: Springer, 2012, pp. 181–189.

[9] Z. Chen and X. Du, "On the linear complexity of binary threshold sequences derived from fermat quotients," *Des., Codes Cryptogr.*, vol. 67, no. 3, pp. 317–323, Jun. 2013.

[10] C. E. Zhao, T. J. Yan, and Q. H. Niu, "Linear complexity of the balanced polynomial quotients sequences," in *Proc. 3rd Int. Conf. Circuits Syst.* San Francisco, CA, USA, Oct. 2018, Art. no. 01014, doi: 10.1051/MATECCONF/201822801014.

[11] Z. Chen, "Trace representation and linear complexity of binary sequences derived from fermat quotients," *Sci. China Inf. Sci.*, vol. 57, no. 11, pp. 1–10, Nov. 2014.

[12] Z. Chen, "Linear complexity of Legendre-polynomial quotients," *IET Inf. Secur.*, vol. 12, no. 5, pp. 414–418, Sep. 2018.

[13] L. P. Zhao, X. N. Du, and C. H. Wu, "Trace representation of the sequences derived from polynomial quotient," in *Proc. 4th Int. Conf. Cloud Comput. Secur.* Haikou, China, Jun. 2018, pp. 26–38.

[14] C. Zhao, W. Ma, T. Yan, and Y. Sun, "Linear complexity of least significant bit of polynomial quotients," *Chin. J. Electron.*, vol. 26, no. 3, pp. 573–578, May 2017.

[15] A. Winterhof, "Linear complexity and related complexity measures," in *Selected Topics in Information and Coding Theory*. Singapore: World Scientific, 2010, pp. 3–40.

[16] T. W. Cusick, C. S. Ding, and A. Renvall, *Stream Ciphers Number Theory*. Amsterdam, The Netherlands: Elsevier, North-Holland Mathematical Library, 1998.

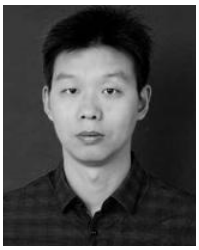
[17] R. Lidl and H. Niederreiter, *Finite Fields*. New York, NY, USA: Cambridge Univ. Press, 1997.

[18] R. Sárközy, "Unsolved problems in number theory," *Periodica Math. Hungarica*, to be published.

[19] W. Meidl, "How many bits have to be changed to decrease the linear complexity?" *Des., Codes Cryptogr.*, vol. 33, no. 2, pp. 109–122, Sep. 2004.

[20] Y. Asimi and A. Asimi, "A synchronous stream cipher generator based on quadratic fields (SSCQF)," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 12, pp. 151–160, 2015.

[21] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 1, pp. 122–127, Jan. 1969.



JIANG MA was born in Henan, China, in 1984. He received the master's degree in computer Software and theory from South China Normal University, in 2009. He is currently pursuing the Ph.D. degree in computer science and technology with Yanshan University. His research interests include coding theory, cryptography, and stream cipher.

JUN ZHANG was born in Hebei, China, in 1985. She received the B.S. degree in electronic information engineering from the Hebei Normal University of Science and Technology, China, in 2009. She is currently a Senior Engineer with the Tangshan Institute of Measurement Test, Tangshan Administration for Market Regulation. Her research interest includes signal and information processing.

YANGUO JIA was born in Hebei, China, in 1971. He received the master's and Ph.D. degrees from Yanshan University, China, in 1999 and 2006, respectively. He is currently working as a Professor with the School of Information Science and Engineering, Yanshan University. His research interests include coding theory, cryptography, spread spectrum sequence design, and software engineering.

XIUMIN SHEN was born in Hebei, China, in 1982. She received the B.S., M.S., and Ph.D. degrees in computer science and technology from Yanshan University, in 2004, 2007, and 2018, respectively. She is currently a Lecturer with the School of Information Science and Engineering, Yanshan University. Her research interests include sequence design and coding theory.