Estimate of Symmetric 2-adic Complexity of Ding - Helleseth Generalized Cyclotomic Sequences of Order Four With Period p^n

Vladimir Edemskiy
Department of Applied Mathematics and Information Science
Yaroslav-the-Wise Novgorod State University
Veliky Novgorod, Russia
vladimir.edemsky@novsu.ru

Oleg Churkin
Department of Applied Mathematics and Information Science
Yaroslav-the-Wise Novgorod State University
Veliky Novgorod, Russia
olegicho@yandex.ru

***Abstract*—In this paper, the symmetric 2-adic complexity of Ding-Helleseth generalized cyclotomic sequences of order four with period equal to a power of an odd prime is studied. The estimate of symmetric 2-adic complexity of these sequences is obtained. It is shown that above sequences have large symmetric 2-adic complexity.**

***Index Terms*—binary sequences, generalized cyclotomy, 2-adic complexity**

I. Introduction

Pseudorandom binary sequences are widely used in many areas of communication and cryptography. The use of cyclotomic classes and generalized cyclotomic classes to design sequences is a well-known method. Classical cyclotomy was first considered in detail by Gauss. Generalized cyclotomy, as a natural generalization of cyclotomy, was presented by Whiteman. Further, Ding and Helleseth proposed a generalized cyclotomy of order 2 with respect to odd modulo N [2]. This cyclotomy was generalized in series of papers. Later, Fan and Ge introduced a unified approach to study both of Whiteman and Ding-Helleseth generalized cyclotomy. There are a lot of papers devoted to study the properties of cyclotomic and generalized cyclotomic sequences.

In the application on cryptography, sequences, as candidates of key in stream cipher system, are needed to have big complexity. Linear complexity and 2-adic complexity of a sequence are defined as the length of the shortest linear feedback shift registers or feedback with carry shift registers respectively, which is able to generate the given sequence. The notation of 2-adic complexity of sequence was presented by Klapper and Goresky [9], [10]. Later Hu and Feng [8] proposed a new measure which they called symmetric 2-adic complexity. They also showed that symmetric 2-adic complexity is better than 2-adic complexity in measuring the security of a binary periodic sequence. Thus it is important to study 2-adic complexity of the known sequences and find binary sequences with large linear complexity and symmetric 2-adic complexity.

In this paper we consider the symmetric 2-adic compexity of Ding-Hellesth generalized sequences of order four with period equal to a power of an odd prime. The linear complexity of such sequences is studied in [4], [5], [16](see also references here). Comparing with the linear complexity, the 2-adic complexity of cyclotomic and generalized sequences has not been fully researched. The 2-adic complexity of the series of sequences with ideal autocorrelation or good autocorrelation were studied in [11], [12], [15], [17] (see also references here). Very recently, the 2-adic complexity of Ding-Helleseth sequence of order two with period p^2 was determined in [3], [14] for $p \not\equiv \pm 5 \pmod{24}$ and was estimated in [13] for p^n.

In this paper, we will obtain the estimate of symmetric 2-adic complexity of Ding-Helleseth binary sequence of order four with period p^n. The 2-adic complexity of these sequences was studied for $n = 1$ in [15] in a different way. Therefore, we will assume further that $n > 1$. Our results show that these sequences have high symmetric 2-adic complexity.

II. Ding-Helleseth sequences of order four with period p^n

We need some preliminary notations before we begin. First, we recall the definitions of generalized cyclotomic classes of Ding-Hellesth of order four and sequences for our case.

Let p be a prime, $p \equiv 1 \pmod 4$ and let $n \geq 1$ be an integer. Denote by g a primitive root modulo p^n. Then an order g equals $p^{n-1}(p-1)$.

For $k = 1, 2, \cdots, n$ we put by definition

$$D_j^{(p^k)} = \left\{ g^{j+4t} \pmod{p^k} \,|\, 0 \leq t < p^{k-1}(p-1)/4 \right\},\ j = 0, 1, 2, 3. \tag{1}$$

The cosets $D_j^{(p^k)}$, $j = 0, 1, 2, 3$ are called *Ding-Helleseth generalized cyclotomic classes* of order four with respect to p^k. It is clear by the definition that $|D_j^{(p^k)}| = p^{k-1}(p-1)/2$.

We will denote by $\mathbb{Z}_{p^k}$ the ring of integers modulo p^k, and by $\mathbb{Z}_{p^k}^*$ the multiplicative group of $\mathbb{Z}_{p^k}$, namely, $\mathbb{Z}_{p^k}^* = \{x \in \mathbb{Z}_{p^k} \,|\, \gcd(x, p^k) = 1\}$. If A is a subset of $\mathbb{Z}_{p^k}$, then let us put by definition $bA = \{ba \mod p^k |\ a \in A\}$ and $b + A = \{(b + a) \mod p^k |\ a \in A\}$, where $b \in \mathbb{Z}$.

According to [2], we have partitions

$$\mathbb{Z}_{p^n}^* = D_0^{(p^n)} \cup D_1^{(p^n)} \cup D_2^{(p^n)} \cup D_3^{(p^n)}$$

and

$$\mathbb{Z}_{p^n} = \bigcup_{k=1}^{n} p^{n-k}\left(D_0^{(p^k)} \cup D_1^{(p^k)} \cup D_2^{(p^n)} \cup D_3^{(p^n)}\right) \cup \{0\}.$$

Let

$$C_0 = \bigcup_{k=1}^{n} p^{n-k}(D_0^{(p^k)} \cup D_1^{(p^k)}) \cup \{0\}$$

and

$$C_1 = \bigcup_{k=1}^{n} p^{n-k}(D_2^{(p^k)} \cup D_3^{(p^k)}).$$

Ding-Helleseth generalized cyclotomic sequences of order four $u^\infty = (u_0, u_1, u_2, \dots)$ with period p^n is defined as

$$u_i = \begin{cases} 0, & \text{if } i \pmod{p^n} \in C_0, \\ 1, & \text{if } i \pmod{p^n} \in C_1. \end{cases} \tag{2}$$

The linear complexity of these sequences was studied in [4]. Here we will estimate the symmetric 2-adic complexity of sequences defined by (2).

We end this section with a reminder of the method for computing 2-adic complexity. Let $s^\infty = \{s_0, s_1, \dots, s_N\}$ be a binary sequence with period N. Let $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$. According to [9] the 2-adic complexity of s^∞ can be defined as

$$\Phi(s^\infty) = \left\lfloor \log_2\left(\frac{2^N - 1}{\gcd(S(2), 2^N - 1)} + 1\right)\right\rfloor,$$

where $\lfloor x \rfloor$ is the greatest integer that is less than or equal to x.

The symmetric 2-adic complexity of s^∞ is defined by $\bar{\Phi}(s^\infty) = \min(\Phi(s^\infty), \Phi(\tilde{s}^\infty))$, where $\tilde{s}^\infty = (s_{N-1}, s_{N-2}, \dots, s_0)$ is the reciprocal sequence of s^∞. So, we must define the greatest common divisor of two numbers.

III. Subsidiary lemmas

In this section, we will first give some subsidiary lemmas, and then investigate 2-adic complexity of u^∞ defined in (2). The properties of generalized cyclotomic classes are well-known (see for example [2], [4]). The necessary for sequel properties are presented in the following lemma. Despite the simplicity, the proof is included here for completeness.

Lemma 1: Let $j = 0, 1, 2, 3$. With the notation as above, we have

(i) $D_j^{(p^n)} \pmod{p^l} = D_j^{(p^l)}$ for $l = 1, 2, \dots, n-1$;

(ii) If $b \in D_j^{(p^n)}$ then $(b + tp^l) \in D_j^{(p^n)}$ for $l = 1, 2, \dots, n-1$;

(iii) $D_j^{(p^n)} = \{b, b + p^l, \dots, b + (p^{n-l} - 1)p^l \mid b \in D_j^{(p^l)}\}$;

(iv) We have the partition $D_j^{(p^n)} = \bigcup_{t=0}^{p^{n-l}-1}\left(D_j^{(p^l)} + tp^l\right)$, $l = 1, 2, \dots, n-1$

(v) We have the partition

$$p^{n-k}D_j^{(p^k)} = \bigcup_{t=0}^{p^{k-l}-1}\left(p^{n-k}D_j^{(p^l)} + tp^{n-k+l}\right),$$

$k = 1, \dots, n$, $l = 1, \dots, k-1$.

Proof: (i) This statement follows from (1).

(ii) Since $b + tp^l \equiv b \pmod{p^l}$ we see that the second conclusion follows from (i) and (1).

(iii) According to (i) and (ii) any element from $\{b, b + p^l, \dots, b + (p^{n-l} - 1)p^l \mid b \in D_j^{(p^l)}\}$ belongs $D_j^{(p^n)}$ and a number of different elements of this set equals $p^{n-1}(p-1)$, i.e. it equals the order $D_j^{(p^n)}$.

(iv) This statement follows from (iii).

(v) By (iv) we see that

$$p^{n-k}D_j^{(p^n)} = \bigcup_{t=0}^{p^{n-l}-1}\left(p^{n-k}D_j^{(p^l)} + tp^{n-k+l}\right) = \bigcup_{t=0}^{p^{k-l}-1}\left(p^{n-k}D_j^{(p^l)} + tp^{n-k+l}\right).$$

Since $p^{n-k}D_j^{(p^n)} = p^{n-k}D_j^{(p^k)}$ in $\mathbb{Z}_{p^n}$ this completes the proof of this lemma. ∎

Now we discuss the properties of generating sequence's polynomial.

Lemma 2: Let $m = 0, 1, \dots, n-1$ and $k = 1, \dots, n$. Then

$$\sum_{i \in p^{n-k}D_j^{(p^k)}} 2^i \pmod{\frac{2^{p^{m+1}}-1}{2^{p^m}-1}} = \begin{cases} 0, & \text{if } k > n-m, \\ p^{n-m-1}\sum\limits_{i \in D_j^{(p)}} 2^{p^m i}, & \text{if } k = n-m, \\ p^{k-1}(p-1)/4, & \text{if } k < n-m. \end{cases}$$

Proof: We consider three cases.

(i) Suppose $k > n-m$; then $n-k < m$ and by Lemma 1(v) for $l = m-n+k$ we obtain

$$\sum_{i \in p^{n-k}D_j^{(p^k)}} 2^i = \sum_{i \in p^{n-k}D_j^{(p^{m-n+k})}} \left(2^i + 2^{i+p^m} + \cdots + 2^{i+(p^{n-m}-1)p^m}\right)$$

and the statement of Lemma 2 (i) follows from the last equality.

(ii) Let $k = n-m$. In this case, by Lemma 1 (i) we get $p^{n-k}D_j^{(p^k)} \pmod{p^{m+1}} = p^m D_j^{(p^{n-m})} \pmod{p^{m+1}} = p^m D_j^{(p)} \pmod{p^{m+1}}$ and $|p^m D_j^{(p^{n-m})}| = p^{n-m-1}(p-1)/4$. Hence

$$\sum_{i \in p^{n-k}D_j^{(p^k)}} 2^i \pmod{2^{p^{m+1}} - 1} = p^{n-m-1}\sum_{i \in D_j^{(p)}} 2^{p^m i}.$$

(iii) If $k < n-m$ then $n-k \geq m+1$ and

$$\sum_{i \in p^{n-k}D_j^{(p^k)}} 2^i \pmod{2^{p^{m+1}} - 1} = \sum_{i \in D_j^{(p^k)}} 2^{p^{n-k} i} \pmod{2^{p^{m+1}} - 1} = |p^{n-k}D_j^{(p^k)}| = p^{k-1}(p-1)/2.$$

∎

The following lemma will be heavily used in our investigation of the 2-adic complexity of u^∞ in the next sections.

Lemma 3: Let u^∞ be defined by (2) and let $U(x)=\sum_{i=0}^{p^n-1}u_ix^i$ be a generating polynomial of u^∞. Then

$$U(2) \pmod{\frac{2^{p^{m+1}}-1}{2^{p^m}-1}} = \\ = p^{n-m-1}\sum_{i\in D_2^{(p)}\cup D_3^{(p)}} 2^{p^m i}+(p^{n-m-1}-1)/2$$

for $m=0,1,\ldots,n-1$.

Proof: By definition of $U(x)$ and (2) we see that

$$U(2)=\sum_{k=1}^{n}\sum_{i\in p^{n-k}(D_2^{(p^k)}\cup D_3^{(p^k)})}2^i.$$

Thus, using Lemma 2 we obtain this statement. ∎

So, we need to study the properties of sums $\sum_{i\in D_j^{(p)}}2^{p^m i}$. This will be done in the next section.

A. Generalized "Gauss sums"

In this subsection, we will use the generalization of notation of "Gauss periods" and "Gauss sums" presented in [17].

Let $a\neq 1$ and $\gcd(a,p)=1$. By definition put

$$\zeta_j(a)=\sum_{i\in D_j^{(p)}}a^i,\ j=0,1,2,3.$$

It is clear that $\zeta_j(a^b)\equiv\zeta_{j+k}(a) \pmod{a^p-1}$ for $b\in D_k^{(p)}$.

By definition, put $H=\zeta_0(a)+\zeta_2(a)-\zeta_1(a)-\zeta_3(a)$. Then $H(c)=\sum_{i\in\mathbb{Z}_q^*}\chi(i)c^i$ where χ is quadric character of $\mathbb{Z}_q^*$. The properties of H for $c=2$ were studied in [17]. In this case, we can also obtain the following statement in the same way as in [17].

Lemma 4: $H^2\equiv q \pmod{(c^q-1)/(c-1)}$.

Denote by $(i,j)=|(D_i^{(p)}+1)\cap D_j^{(p)}|$ the cyclotomic numbers of order four, $i,j\in\mathbb{N}$. The following statement is well-known for Gauss periods over finite fields (see for example [1]). It is also true for generalized Gauss periods over finite rings.

Lemma 5: Let $k,l=0,1,2,3$. Then

$$\zeta_l(a)\cdot\zeta_{l+k}(a)\equiv\sum_{f=0}^{3}(k,f)_4\zeta_{f+l}(a)+\delta \pmod{a^q-1},$$

where $\delta=\begin{cases}(p-1)/4, \text{ if } p\equiv 1 \pmod 8,\ k=0\\ \qquad\text{or } p\equiv 8 \pmod 8,\ k=2,\\ 0, \text{ otherwise.}\end{cases}$

Also we note that according to the definition we have

$$\zeta_0(a)+\zeta_1(a)+\zeta_2(a)+\zeta_3(a)=(a^p-1)/(a-1)-1.$$

Using the formulae for the cyclotomic numbers of order four from [6] and Lemma 5 we can obtain the following statement.

Lemma 6: Let $S(a)=\zeta_2(a)+\zeta_3(a)$, $\gcd(a,p)=1$ and $p=x^2+4y^2$. Then $S(a)$ and $S(a^{g^2})$ are satisfying the congruence

1) $X^2+4X\equiv 2yH-p-1 \pmod{(a^q-1)/(a-1)}$ for $q\equiv 5 \pmod 8$;
2) $X^2+4X\equiv 2yH+p-1 \pmod{(a^q-1)/(a-1)}$ for $q\equiv 1 \pmod 8$;

Using the new notations we can write that

$$U(2) \pmod{\frac{2^{p^{m+1}}-1}{2^{p^m}-1}} = p^{n-m-1}S(2^{p^m})+(p^{n-m-1}-1)/2 \tag{3}$$

for $m=0,1,\ldots,n-1$.

So, the studying of 2-adic complexity of above sequences is equivalent to the investigation of properties of generalized Gauss periods. We show in the following lemma that this is also true for symmetric 2-adic complexity.

Lemma 7: Let $\tilde{u}^\infty=(u_{p^n-1},u_{p^n-2},\ldots,u_0)$ be the reciprocal sequence of u^∞ defined by (2) and let $\widetilde{U}(x)\in\mathbb{Z}[x]$ be a generating polynomial of $\tilde{u}^\infty$. Then

$$2\widetilde{U}(2)\equiv\begin{cases}p^{n-m-1}S(2^{p^m}), & \text{if } q\equiv 1 \pmod 8\\ p^{n-m-1}S(2^{g^2p^m}), & \text{if } q\equiv 5 \pmod 8\end{cases} \\ +(p^{n-m-1}-1)/2 \pmod{\frac{2^{p^{m+1}}-1}{2^{p^m}-1}}.$$

Here $S(a)=\zeta_2(a)+\zeta_3(a)$ as in Lemma 5.

Proof: By definition we have $\widetilde{U}(x)=\sum_{i=0}^{p^n-1}u_{p^n-1-i}x^i$ and $2\widetilde{U}(2)=\sum_{i=1}^{p^n}u_{p^n-i}2^i$. We get $2\widetilde{U}(2)=\sum_{i=0}^{p^n-1}u_{-i}2^i-u_0+u_02^{p^n}$, hence

$$2\widetilde{U}(2)\equiv\sum_{i=0}^{p^n-1}u_{-i}2^i \pmod{2^{p^n}-1}.$$

Further, we consider two cases.

If $p\equiv 1 \pmod 8$ then $-1\in D_0^{(p)}$ and $u_i=u_{-i}$. In this case $2\widetilde{U}(2)\equiv U(2) \pmod{2^{p^n}-1}$.

Now, let $p\equiv 5 \pmod 8$. In this case $-1\in D_2^{(p)}$ and we see that $-i\in p^mD_{(j+2)\bmod 2}^{(p^n)}$ if $i\in p^mD_j^{(p^n)}$. Thus

$$2\tilde{U}(2)=\sum_{k=0}^{n-1}\sum_{i\in p^{n-k}(D_0^{(p^k)}\cup D_1^{(p^k)})}2^i.$$

With similar arguments as above we obtain that $2\widetilde{U}(2)\equiv p^{n-m-1}\sum_{i\in D_0^{(p)}\cup D_1^{(p)}}2^{p^m i}+(p^{n-m-1}-1)/2\equiv p^{n-m-1}S(2^{g^2p^m})+(p^{n-m-1}-1)/2 \pmod{\frac{2^{p^{m+1}}-1}{2^{p^m}-1}}$. ∎

IV. Main result

Our main result is the following statement. Let n_0 be the greatest integer that is less than $(4n-3)/5$.

Theorem 8: Let u^∞ be a Ding-Helleseth generalized cyclotomic sequence defined by (2) and $n>1$. Then $\bar{\Phi}(u^\infty)\geq p^n-p^{n_0+1}$.

Proof: For the proof of this statement we will show that

$$\bar{\Phi}(u^\infty)\geq\left\lfloor\log_2\left(\frac{2^{p^n}-1}{2^{p^{n_0+1}}-1}+1\right)\right\rfloor.$$

We estimate of $\gcd\left(U(2),2^{p^n}-1\right)$ for this purpose.

It is clear that

$$2^{p^n}-1=\frac{2^{p^n}-1}{2^{p^{n-1}}-1}\cdot\ \ldots\ \cdot\frac{2^{p^2}-1}{2^p-1}\cdot(2^p-1).$$

Let d be a divisor of $\gcd\left(U(2),(2^{p^{m+1}}-1)/(2^{p^m}-1)\right)$. Then by Lemma 3 we obtain that d divides $p^{n-m-1}S(2^{p^m})-(p^{n-m-1})/2$ or $S(2^{p^m})\equiv p^{-n+m+1}(p^{n-m-1}-1)/2 \pmod d$.

We consider two cases.

(i) Let $p\equiv 5 \pmod 8$. Then by Lemma 6 we get $p^{2n-2m-1}+1\equiv 2yHp^{2n-2m-2} \pmod d$ or according to Lemma 4

$$p^{4n-4m-2}+2p^{2n-2m-1}+1\equiv 4y^2p^{4n-4m-3} \pmod d.$$

Since $p=x^2+4y^2$, it follows that

$$x^2p^{4n-4m-3}+2p^{2n-2m-1}+1\equiv 0 \pmod d.$$

Thus $d<p^{4n-4m-2}$. Further, d divides $(2^{p^{m+1}}-1)/(2^{p^m}-1)$, hence p^{m+1} divides $d-1$ and $d=1+hp^{m+1}$, $h\geq 1$ is an integer. We have $4n-4m-2>m+1$ or $m<(4n-3)/5$. So, if $m\geq(4n-3)/5$ then $\gcd\left(U(2),(2^{p^n}-1)/(2^{p^{m+1}}-1)\right)=1$ and

$$\Phi(u^\infty)\geq\left\lfloor\log_2\left(\frac{2^{p^n}-1}{2^{p^{n_0+1}}-1}+1\right)\right\rfloor$$

where n_0 is the greatest integer that is less than $(4n-3)/5$.

The inequality

$$\Phi(\tilde{u}^\infty)\geq\left\lfloor\log_2\left(\frac{2^{p^n}-1}{2^{p^{n_0+1}}-1}+1\right)\right\rfloor$$

we can prove in the same way using Lemma 7.

(ii) Let $p\equiv 1 \pmod 8$. In this case by Lemmas 6 and 7 we get $-p^{2n-2m-1}+1\equiv 2yHp^{2n-2m-2} \pmod d$ or according to Lemma 4

$$p^{4n-4m-2}-2p^{2n-2m-1}+1\equiv 4y^2p^{4n-4m-3} \pmod d.$$

Thus, in this case we can obtain the result in the same way as for $q\equiv 5 \pmod 8$.

■

It is clear that $n_0\leq n-1$ for $n>1$ and we have the following corollary from Theorem 8

Corollary 9: Let u^∞ be a Ding-Helleseth generalized cyclotomic sequence defined by (2). Then $\bar{\Phi}(u^\infty)\geq p^n-p^{n-1}$.

Remark 1: If $q\equiv 5 \pmod 8$ then by Lemma 4 and the proof of this theorem we see that

$$\Phi(\tilde{u}^\infty)=\left\lfloor\log_2\left((2^{p^n}-1)/d+1\right)\right\rfloor$$

where

$$d=\prod_{m=0}^{n_0}\gcd\left(\frac{2^{p^{m+1}}-1}{2^{p^m}-1},x^2p^{4n-4m-3}+2p^{2n-2m-1}+1\right).$$

For $q\equiv 1 \pmod 8$ we have that

$$\Phi(\tilde{u}^\infty)\geq\left\lfloor\log_2\left((2^{p^n}-1)/d+1\right)\right\rfloor$$

where

$$d=\prod_{m=0}^{n_0}\gcd\left(\frac{2^{p^{m+1}}-1}{2^{p^m}-1},x^2p^{4n-4m-3}-2p^{2n-2m-1}+1\right).$$

Theorem 8 shows that Ding-Helleseth generalized cyclotomic sequences of order four with period p^n have high symmetric 2-adic complexity.

V. Conclusion

We showed that Ding-Helleseth generalized cyclotomic binary sequences of order four with period equal to a power of an odd prime have high symmetric 2-adic complexity. Thus, 2-adic complexity of these sequences is good enough to resist the attack by the rational approximation algorithm.

References

[1] T. Cusick, C. Ding, A. Renvall, Stream Ciphers and Number Theory, Gulf Professional Publishing, 2004.

[2] C. Ding, and T. Helleseth, "New generalized cyclotomy and its applications," Finite Fields Appl., vol. 4, pp.140 – 166, 1998.

[3] Du X., Zhao L., and Niu Z., "2-Adic Complexity of Two Classes of Generalized Cyclotomic Binary Sequences with Order 4," IEICE TRANS. FUNDAMENTALS, vol.E102A, No.11, pp. 1566–1570, November 2019.

[4] V. Edemskiy, "About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}," Designs, Codes and Cryptography, vol.61(3), pp. 251–260, 2011.

[5] Y.J. Kim, and H.Y. Song, "Linear Complexity of Prime n-Square Sequences," In: IEEE International Symposium on Information Theory, Toronto, Canada, pp. 2405–2408, 2008.

[6] M. Hall, Combinatorial Theory, Wiley, New York, 1975

[7] H. Hu, "Comments on "a new method to compute the 2-adic complexity of binary sequences". IEEE Trans. Inform. Theory, vol. 60, pp. 5803–5804, 2014.

[8] H. Hu, and D. Feng, "On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences," IEEE Trans. Inf. Theory, vol. 54(2), pp. 874–883, 2008.

[9] A. Klapper, and M. Goresky. "Cryptanalysis based on 2-adic rational approxiamtion," In: CRYPTO 1995, LNCS, vol. 963, pp. 262–273, 1995.

[10] A. Klapper, and M. Goresky. "Feedback shift registers, 2-adic span, and combiners with memory," Journal of Cryptology, vol. 10, pp. 111–147, 1997.

[11] Y. Sun, Q. Wang, and T. Yan. "The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation," Cryptography and Communications, vol. 10 (3), pp. 467–477, 2018.

[12] Y. Sun, T. Yan,and Z. Chen. "The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude," Cryptogr. Commun., vol.12, pp. 675-683, 2020.

[13] Y. Sun, Q. Wang, T. Yan, and C. Zhao, A lower bound om the 2- adic compelxity of Ding-Helleseth generalized cyclotomic sequence of period p^n, arXiv preprint arXiv:1704.05544, 2017.

[14] Z. Xiao, X. Zeng, and Z. Sun, "2-Adic complexity of two classes of generalized cyclotomic binary sequences,"Internationl Journal of Foundations of Comput. Sci., vol. 27 (7), pp. 879–893, 2016.

[15] H. Xiong, L. Qu, and C. Li, "A new method to compute the 2-adic complexity of binary sequences," IEEE Trans. Inform. Theory, vol.60, pp. 2399–2406, 2014.

[16] T. Yan, S. Li, and Xiao, "On the linear complexity of generalized cyclotomic sequences with the period p^m," Applied Mathematics Letter, vol. 21, pp. 187–193, 2008.

[17] L. Zhang, J. Zhang, M. Yang, and K. Feng, "On the 2-Adic Complexity of the Ding-Helleseth-Martinsen Binary Sequences," IEEE Trans. Inform. Theory, 2020. DOI: 10.1109/TIT.2020.2964171.