IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 9, 2020, accepted July 30, 2020, date of publication August 3, 2020, date of current version August 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3013956

Autocorrelation and Lower Bound on the 2-Adic Complexity of LSB Sequence of *p*-Ary *m*-Sequence

YUHUA SUN[1], QIUYAN WANG[2], TONGJIANG YAN[1], AND CHUN'E ZHAO[1]
[1]College of Science, China University of Petroleum, Qingdao 266555, China
[2]School of Computer Science and Technology, Tiangong University, Tianjin 300387, China

Corresponding author: Qiuyan Wang (wangyan198801@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61902429, in part by the Fundamental Research Funds for the Central Universities under Grant 19CX02058A, and in part by the Shandong Provincial Natural Science Foundation of China under Grant ZR2019MF070.

ABSTRACT LSB (Least Significant Bit) sequences are widely used as the initial inputs in some modern stream ciphers, such as the ZUC algorithm-the core of the 3GPP LTE International Encryption Standard. Therefore, analyzing the statistical properties (for example, autocorrelation, linear complexity and 2-adic complexity) of these sequences becomes an important research topic. In this article, we first reduce the autocorrelation distribution of the LSB sequence of a p-ary m-sequence with period $p^n - 1$ for any order $n \geq 2$ to the autocorrelation distribution of a corresponding Costas sequence with period $p - 1$, and from the computing of which by computer, we obtain the explicit autocorrelation distribution of the LSB sequence for each prime $p < 100$. In addition, we give a lower bound on the 2-adic complexity of each of these LSB sequences for all primes $p < 20$, which proves to be large enough to resist the analysis of RAA (Rational Approximation Algorithm) for FCSRs (Feedback with Carry Shift Registers). In particular, for a Mersenne prime $p = 2^k - 1$ (i.e., k is a prime such that p is also a prime), our results hold for all its bit-component sequences since they are shift equivalent to the LSB sequence.

INDEX TERMS p-ary m-sequence, LSB sequence, autocorrelation, 2-adic complexity.

I. INTRODUCTION

As important components of cipher systems, pseudo-random sequences have widely applications in cryptography. In order to prevent some malicious attacks, sequences as the key stream in a cipher system should have low similarity at different times and can not be regenerated by some simple registers, for example short Linear Feedback Shift Register (LFSR) and short Feedback with Carry Shift Register (FCSR), etc. Thus, autocorrelation distributions, linear complexity and 2-adic complexity of sequences become three important indexes to measure a cipher system, i.e., sequences used as a key stream should have low autocorrelation, high linear complexity and large 2-adic complexity.

Due to their ideal correlation property and other good performance measures such as highly efficient implementation, maximal length LFSR sequences (i.e., m-sequences) have been widely used in designing stream ciphers. However, since the linear complexity of these sequences is relatively low under the analysis of Berlekamp-Massey Algorithm (BMA), they can not be used by themselves. Therefore constructing nonlinear sequence generators with desirable good properties becomes a very important topic. As one class of promising nonlinear sequence generators, feedback with carry shift registers (FCSRs), were originally presented by Klapper and Goresky in 1997 [15]. At the same time, they introduced the notion of 2-adic complexity $\Phi_2(s)$ for a binary periodic sequence s, i.e., the length of the shortest FCSR which generates s. One direct result of this notion is that an m-sequence with period $N = 2^n - 1$ has maximal 2-adic complexity if $2^N - 1$ is a prime. Similar to BMA of LFSRs, Klapper and Goresky also proposed an algorithm, called Rational Approximation Algorithm (RAA), to determine the 2-adic complexity of s. They showed that, from the perspective of cryptography security, a desirable sequence should has both high linear complexity and high 2-adic complexity, namely,

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

greater than or equal to one half of the period. Although the linear complexity of many classes of sequences have been obtained (see [1], [2], [5], [8], [10], [13], [14], [16], [17], [22], [23], [25]), there are only a handful of papers on their 2-adic complexity. After Tian and Qi made a breakthrough, i.e., they proved that all binary m-sequences have maximal 2-adic complexity in [21], Xiong *et al.* presented a method to compute the 2-adic complexity of binary sequences by circulant matrixes in [26], [27]. They showed that all the known sequences with ideal 2-level autocorrelation and several other classes of sequences with optimal autocorrelation have maximum 2-adic complexity. Then Hu presented a simpler method in [12] to obtain the results of Xiong *et al.* by using exact autocorrelation distributions. Recently, Zhang *et al.* introduced a new method to determine the 2-adic complexity of a binary sequence by "Gauss periods" and "Gauss sum" over a ring Z_N of residue classes modulo an integer N [29]. More applications of these three methods can be found in [11], [18]–[20], [24], [28], in which the 2-adic complexity of Legendre sequences, Jacobi sequences, modified Jacobi sequences and a class of binary sequences with optimal autocorrelation was analyzed.

Since LSB sequences of p-ary m-sequences (see Definitions 1) can be easily implemented and have been tested to possess many good pseudo-random properties, some modern stream ciphers, such as the ZUC algorithm-the core of the 3GPP LTE International Encryption Standard, are designed by using them as the inputs [6], [7]. Earlier, Chan and Games [1] proved that these sequences have high linear complexity. However, the autocorrelation and the 2-adic complexity of them have still not been studied as far as we know. In this article, some analyses of these two properties of these sequences are given.

The rest of this article is organized as follows. We introduce notations and some well-known results in Section II. Some autocorrelation properties of LSB sequences of p-ary m-sequences, as well as the explicit autocorrelation distributions of Costas sequences with period $p-1$ for $p < 100$, are given in Section III. In Section IV, the lower bound on the 2-adic complexity of each of the LSB sequences of p-ary m-sequences for $p < 20$ and an open problem on the 2-adic complexity of the LSB sequence of a p-ary m-sequence for any prime p are presented. Finally, we give a conclusion in Section V.

II. PRELIMINARIES

Let N be a positive integer and $s = (s_0, s_1, \cdots, s_{N-1}, \cdots)$ be a binary sequence of period N. The autocorrelation of s is given by

$$AC_s(\tau) = \sum_{t=0}^{N-1} (-1)^{s_t + s_{t+\tau}}, \quad \tau = 0, 1, 2, \cdots, N-1.$$

The notion of the 2-adic complexity has been well defined by Klapper and Goresky [15] and they also presented a general formula of computing the 2-adic complexity of binary sequences. For simplicity, here we take this formula as its definition directly. Readers can refer to [15] or [26] for the formal definition.

Denote $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$ and take the polynomial function value $S(2)$ of $S(x)$ at the point 2. Let $\gcd(\star 1, \star 2)$ be the greatest common divisor of two integers $\star 1$ and $\star 2$. If we write

$$\frac{S(2)}{2^N - 1} = \frac{\frac{S(2)}{\gcd\left(S(2), 2^N - 1\right)}}{\frac{2^N - 1}{\gcd\left(S(2), 2^N - 1\right)}},$$

then the 2-adic complexity $\Phi_2(s)$ of the sequence s is determined by the following integer,

$$\Phi_2(s) = \left\lfloor \log_2 \frac{2^N - 1}{\gcd\left(S(2), 2^N - 1\right)} \right\rfloor, \tag{1}$$

where the symbol $\lfloor \star \rfloor$ denote the floor function, i.e., $\lfloor \star \rfloor$ is the greatest integer that is less than or equal to the number $\star$.

Let p be any odd prime, n be a positive integer, and α be a primitive element of $\mathbb{F}_{p^n}$. Then

$$a_t = \mathrm{Tr}(\alpha^t), \quad t = 0, 1, 2, \cdots, p^n - 2,$$

is a p-ary m-sequence, where $\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}$ is the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.

For each term a_t of the m-sequence $\{a_t\}_{t=0}^{p^n-2}$, we have the following 2-adic expansion

$$a_t = a_{t,0} + a_{t,1} \times 2 + a_{t,2} \times 2^2 + \cdots + a_{t,k-1} \times 2^{k-1},$$

where $a_{t,i} \in \{0, 1\}$, $i = 0, 1, \cdots, k-1$, $k = \lceil \log_2 p \rceil$ and $\lceil x \rceil$ is the least integer that is larger than or equal to x. Here, we identify the bit string $(a_{t,0}, a_{t,1}, \cdots, a_{t,k-1})$ of length k with the element a_t and the i-th element $a_{t,i-1}$ is called as the i-th bit-component of a_t. But the element $0 \in \mathbb{F}_p$ is written as p, i.e., 0 is identified with $(p_0, p_1, \cdots, p_{k-1})$, where the 2-adic expansion of p is $p_0 + p_1 \times 2 + \cdots + p_{k-1} \times 2^{k-1}$ (this is in accordance with the ZUC algorithm).

Definition 1: For a fixed $i \in \{1, 2, \cdots, k\}$, the sequence $\{a_{t,i-1}\}_{t=0}^{p^n-2}$ is called the i-th bit-component sequence of $\{a_t\}_{t=0}^{p^n-2}$. In particular, when $i = 0$, the bit-component sequence $\{a_{t,0}\}_{t=0}^{p^n-2}$ is called the Least Significant Bit sequence (the LSB sequence) of the m-sequence $\{a_t\}_{t=0}^{p^n-2}$ and we denote $\{s_t\}_{t=0}^{p^n-2} = \{a_{t,0}\}_{t=0}^{p^n-2}$ for convenience. In fact, it can also be expressed as

$$s_t = \begin{cases} \mathrm{Tr}(\alpha^t) \pmod 2, & \text{if } \mathrm{Tr}(\alpha^t) \in \mathbb{F}_p^*, \\ 1, & \text{if } \mathrm{Tr}(\alpha^t) = 0. \end{cases} \tag{2}$$

Definition 2: Denote $\beta = \alpha^{\frac{p^n-1}{p-1}}$, a primitive element of $\mathbb{F}_p$. The Costas sequence is defined as the sequence $\{b_j\}_{j=0}^{p-2}$ of period $p-1$ which is given by $b_j \equiv \beta^j \pmod 2$.

The Costas sequence $\{b_j\}_{j=0}^{p-2}$ is actually the LSB sequence of the permutation $\{\beta^0, \beta^1, \ldots, \beta^{p-2}\}$ corresponding to a Welch Costas array determined by the primitive element β.

This sequence was first considered by J. P Costas in 1984 as permutation matrices with ambiguity functions taking only the values 0 and (possibly) 1, applied to the processing of radar and sonar signals. The basic algebraic construction of this sequence can be found in [9]. The sequence is closely related to APN functions and S-Box of block ciphers [4].

Definition 3: A function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is said to be balanced if the element 0 appears one less time than each nonzero element in $\mathbb{F}_p$ in the list $f(\alpha^0), f(\alpha^1), \cdots, f(\alpha^{p^n-2})$.

Definition 4: Let $f(x)$ be a function on $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Then the function $f(x)$ is called difference-balanced if $f(xz)-f(x)$ is balanced for any $z \in \mathbb{F}_{p^n}$ but $z \neq 1$.

Remark 1: It is well known that the trace function $\mathrm{Tr}(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is difference-balanced, which is in fact a linear function over $\mathbb{F}_p$.

III. AUTOCORRELATION PROPERTIES OF LSB SEQUENCES OF *p*-ARY *m*-SEQUENCES

Denote $N = p^n - 1$, $M = \frac{N}{p-1}$, and $\mathbb{Z}_N = \{0, 1, 2, \cdots, N-1\}$. For the rest of the paper, we always use them and other notations given in Section II unless otherwise specified.

Lemma 1: Let $n \geq 2$. Then, for $0 < \tau < N$ and $\tau \notin \{M\tau' \mid \tau' = 1, 2, \cdots, p-2\}$, the autocorrelation value $AC_s(\tau)$ of $\{s_t\}_{t=0}^{N-1}$ is given by $AC_s(\tau) = p^{n-2} - 1$.

Proof: For a fixed τ, denote

$$D_\tau = \{t \mid s_t \neq s_{t+\tau},\ t \in \mathbb{Z}_N\}.$$

s Then

$$AC_s(\tau) = |\mathbb{Z}_N \setminus D_\tau| - |D_\tau| = N - 2|D_\tau|, \tag{3}$$

where $|D_\tau|$ is the size of the collection D_τ. By (2), we get

$$\begin{aligned}
|D_\tau| &= \left|\{t \mid s_t \neq s_{t+\tau},\ t \in \mathbb{Z}_N\}\right| \qquad (4)\\
&= \left|\{t \in \mathbb{Z}_N \mid \mathrm{Tr}(\alpha^t), \mathrm{Tr}(\alpha^{t+\tau}) \in \mathbb{F}_p^*,\right.\\
&\quad \left.\mathrm{Tr}(\alpha^t) \equiv 1 \pmod 2, \mathrm{Tr}(\alpha^{t+\tau}) \equiv 0 \pmod 2\}\right|\\
&\quad + \left|\{t \in \mathbb{Z}_N \mid \mathrm{Tr}(\alpha^t), \mathrm{Tr}(\alpha^{t+\tau}) \in \mathbb{F}_p^*,\right.\\
&\quad \left.\mathrm{Tr}(\alpha^t) \equiv 0 \pmod 2, \mathrm{Tr}(\alpha^{t+\tau}) \equiv 1 \pmod 2\}\right|\\
&\quad + \left|\{t \mid \mathrm{Tr}(\alpha^t) = 0,\ \mathrm{Tr}(\alpha^{t+\tau}) \in \mathbb{F}_p^*\right.\\
&\quad \left.\text{and } \mathrm{Tr}(\alpha^{t+\tau}) = 0 \pmod 2,\ t \in \mathbb{Z}_N\}\right|\\
&\quad + \left|\{t \mid \mathrm{Tr}(\alpha^{t+\tau}) = 0,\ \mathrm{Tr}(\alpha^t) \in \mathbb{F}_p^*\right.\\
&\quad \left.\text{and } \mathrm{Tr}(\alpha^t) = 0 \pmod 2,\ t \in \mathbb{Z}_N\}\right|\\
&= \left|\{x \in \mathbb{F}_{p^n}^* \mid \mathrm{Tr}(x), \mathrm{Tr}(\alpha^\tau x) \in \mathbb{F}_p^*,\right.\\
&\quad \left.\mathrm{Tr}(x) \equiv 1 \pmod 2, \mathrm{Tr}(\alpha^\tau x) \equiv 0 \pmod 2\}\right| \qquad (5)\\
&\quad + \left|\{x \in \mathbb{F}_{p^n}^* \mid \mathrm{Tr}(x), \mathrm{Tr}(\alpha^\tau x) \in \mathbb{F}_p^*,\right.\\
&\quad \left.\mathrm{Tr}(x) \equiv 0 \pmod 2, \mathrm{Tr}(\alpha^\tau x) \equiv 1 \pmod 2\}\right| \qquad (6)\\
&\quad + \left|\{x \in \mathbb{F}_{p^n}^* \mid \mathrm{Tr}(x) = 0,\ \mathrm{Tr}(\alpha^\tau x) \in \mathbb{F}_p^*,\right.\\
&\quad \left.\text{and } \mathrm{Tr}(\alpha^\tau x) = 0 \pmod 2\}\right| \qquad (7)\\
&\quad + \left|\{x \in \mathbb{F}_{p^n}^* \mid \mathrm{Tr}(x) = 0,\ \mathrm{Tr}(x) \in \mathbb{F}_p^*,\right.\\
&\quad \left.\text{and } \mathrm{Tr}(x) = 0 \pmod 2\}\right|. \qquad (8)
\end{aligned}$$

Next, we determine the values of (5)-(8) respectively. From Definition 1, it is obvious that

$$\begin{aligned}
s_t \neq s_{t+\tau} &\Rightarrow \mathrm{Tr}(\alpha^t) - \mathrm{Tr}(\alpha^{t+\tau}) \neq 0\\
&\Rightarrow \mathrm{Tr}(x) - \mathrm{Tr}(\alpha^\tau x) \neq 0, \text{ where } x = \alpha^t.
\end{aligned}$$

By Remark 1 we know that the trace function $\mathrm{Tr}(x)$ is difference-balanced, namely, for each fixed $a \in \mathbb{F}_p^*$, the total number of x's in $\mathbb{F}_{p^n}^*$ satisfying

$$\mathrm{Tr}(x) - \mathrm{Tr}(\alpha^\tau x) = a$$

is p^{n-1}. And the number of x's to the equation

$$\mathrm{Tr}(x) - \mathrm{Tr}(\alpha^\tau x) = a$$

is actually the sum of the numbers of solutions x's to the following system of equations

$$\begin{cases} \mathrm{Tr}(x) = c + a, \\ \mathrm{Tr}(\alpha^\tau x) = c, \end{cases} \tag{9}$$

where c runs through $\mathbb{F}_p$. Notice that $\mathbb{F}_{p^n}$ is an n-dimensional vector space over $\mathbb{F}_p$. Let $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ be a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. For any element $x \in \mathbb{F}_{p^n}$, there exist n elements $x_i \in \mathbb{F}_p,\ i = 1, 2, \cdots, n$, such that $x = \sum_{i=1}^{n} x_i\alpha_i$. Then, for fixed $c + a \in \mathbb{F}_p$, $c \in \mathbb{F}_p$ and $\alpha^\tau \in \mathbb{F}_{p^n}$, Eq. (9) can be transformed into

$$\begin{cases} \sum_{i=1}^{n} \mathrm{Tr}(\alpha_i)x_i = c + a, \\ \sum_{i=1}^{n} \mathrm{Tr}(\alpha^\tau\alpha_i)x_i = c, \end{cases} \tag{10}$$

which is a linear equation system over $\mathbb{F}_p$ with n unknowns $x_i \in \mathbb{F}_p,\ i = 1, 2, \cdots, n$, and its coefficient matrix is

$$A = \begin{pmatrix} \mathrm{Tr}(\alpha_1) & \mathrm{Tr}(\alpha_2) & \cdots & \mathrm{Tr}(\alpha_n) \\ \mathrm{Tr}(\alpha^\tau\alpha_1) & \mathrm{Tr}(\alpha^\tau\alpha_2) & \cdots & \mathrm{Tr}(\alpha^\tau\alpha_n) \end{pmatrix}. \tag{11}$$

In fact, for $\alpha^\tau \notin \mathbb{F}_p^*$, i.e., $\tau \notin \{M\tau' \mid \tau' = 1, 2, \cdots, p-1\}$, the two rows in the above matrix A are linearly independent. Otherwise, there is an element $\delta \in \mathbb{F}_p$ such that $\mathrm{Tr}(\alpha^\tau\alpha_i) = \delta\mathrm{Tr}(\alpha_i)$ for each $i \in \{1, 2, \cdots, n\}$, i.e., $\mathrm{Tr}((\alpha^\tau - \delta)\alpha_i) = 0$ for each $i \in \{1, 2, \cdots, n\}$, which results in $\mathrm{Tr}((\alpha^\tau - \delta)\gamma)$ for each element $\gamma \in \mathbb{F}_{p^n}$ since $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ is a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. This is impossible since $\alpha^\tau - \delta \neq 0$. Therefore, the rank of the above matrix A in (11) is 2, which implies that there are p^{n-2} solutions in $\mathbb{F}_{p^n}$ to (9) for each $a \in \mathbb{F}_p^*$ and $c \in \mathbb{F}_p$.

If we take each element of $\mathbb{F}_p^* = \{1, 2, \cdots, p-1\}$ as an integer, then there are $\frac{p-1}{2}$ even integers, which implies there are $\frac{p-1}{2}$ c's in $\mathbb{F}_p^*$ such that $c \equiv 0 \pmod 2$. Furthermore,

for each fixed $c \equiv 0 \pmod 2$ in $\mathbb{F}_p^*$, if a runs through every element of $\mathbb{F}_p^*$, then $c+a$ runs through every element of $\mathbb{F}_p \backslash \{c\}$ and there are $\frac{p-1}{2}$ odd integers in $(\mathbb{F}_p \backslash \{c\}) \cap \mathbb{F}_p^*$, which tells us that there are $\frac{p-1}{2}$ a's such that $c + a \equiv 1 \pmod 2$ for each fixed $c \equiv 0 \pmod 2$ in $\mathbb{F}_p^*$. Then the value of (5) is equal to

$$\begin{aligned}&\Big|\{x \in \mathbb{F}_{p^n}^* \mid \mathrm{Tr}(x), \mathrm{Tr}(\alpha^\tau x) \in \mathbb{F}_p^*, \\ &\qquad \mathrm{Tr}(x) \equiv 1 \pmod 2, \mathrm{Tr}(\alpha^\tau x) \equiv 0 \pmod 2\}\Big| \\ &= p^{n-2} \times \frac{(p-1)^2}{4}.\end{aligned}$$

Similarly, the values of (6)-(8) are $p^{n-2} \times \frac{(p-1)^2}{4}$, $p^{n-2} \times \frac{p-1}{2}$, $p^{n-2} \times \frac{p-1}{2}$ respectively. The value of $|D_\tau|$ is the sum of the values of (5)-(8) by (4), i.e.,

$$\begin{aligned}|D_\tau| &= p^{n-2}\left(\frac{(p-1)^2}{4} + \frac{(p-1)^2}{4} + \frac{p-1}{2} + \frac{p-1}{2}\right) \\ &= \frac{p^n - p^{n-2}}{2}.\end{aligned}$$

Therefore, by (3),

$$\begin{aligned}AC_s(\tau) &= N - 2 \times \frac{p^n - p^{n-2}}{2} \\ &= p^n - 1 - (p^n - p^{n-2}) = p^{n-2} - 1.\end{aligned}$$

■

Lemma 2: For $\tau \in \{M\tau' \mid \tau' = 1, 2, \cdots, p-2\}$, the relation between the autocorrelation $AC_s(\tau)$ of the LSB sequence $\{s_t\}_{t=0}^{p^n-1}$ and the autocorrelation $AC_b(\tau')$ of the Costas sequence $\{b_j\}_{j=0}^{p-2}$ is given by

$$AC_s(\tau) = \big(AC_b(\tau') + 1\big)\, p^{n-1} - 1. \tag{12}$$

Proof: Recall that $\alpha^\tau = \beta^{\tau'} \in \mathbb{F}_p^*$ for $\tau \in \{M\tau' \mid \tau' = 1, 2, \cdots, p-2\}$ since $\beta = \alpha^M$. Then $\mathrm{Tr}(\alpha^\tau x) = \mathrm{Tr}(\beta^{\tau'} x) = \beta^{\tau'}\mathrm{Tr}(x)$ for $x \in \mathbb{F}_{p^n}^*$, i.e.,

$$\mathrm{Tr}(\alpha^\tau x) \in \mathbb{F}_p^* \Leftrightarrow \mathrm{Tr}(x) \in \mathbb{F}_p^*. \tag{13}$$

It is similar to the proof of Lemma 1 that

$$AC_s(\tau) = |\mathbb{Z}_N \setminus D_\tau| - |D_\tau| = N - 2|D_\tau|,$$

where $D_\tau = \{t \mid s_t \neq s_{t+\tau},\ t \in \mathbb{Z}_N\}$, and

$$\begin{aligned}s_t \neq s_{t+\tau} &\Rightarrow \mathrm{Tr}(x) - \mathrm{Tr}(\alpha^\tau x) \neq 0 \\ &\Rightarrow \mathrm{Tr}(x) \in \mathbb{F}_p^* \text{ and } \mathrm{Tr}(\alpha^\tau x) \in \mathbb{F}_p^*,\end{aligned} \tag{14}$$

where $x = \alpha^t$. Therefore,

$$\begin{aligned}|D_\tau| &= \Big|\{x \mid \mathrm{Tr}(x) \in \mathbb{F}_p^*,\ \mathrm{Tr}(x) \not\equiv \beta^{\tau'}\mathrm{Tr}(x) \pmod 2, \\ &\qquad x \in \mathbb{F}_{p^n}^*\}\Big| \\ &= p^{n-1} \times \Big|\{(c, \beta^{\tau'}c) \mid c \in \mathbb{F}_p^*, \\ &\qquad c \not\equiv \beta^{\tau'}c \pmod 2)\}\Big| \\ &= p^{n-1} \times \Big|\{j \mid \beta^j \not\equiv \beta^{j+\tau'} \pmod 2, \\ &\qquad j = 0, 1, \cdots, p-2\}\Big| \\ &= p^{n-1} \times |D'_{\tau'}|,\end{aligned} \tag{15}$$

where $D'_{\tau'} = \{j \mid \beta^j \not\equiv \beta^{j+\tau'} \pmod 2,\ j = 0, 1, \cdots, p-2\}$ and Eq. (15) holds because the equation $\mathrm{Tr}(x) = c$ has exact p^{n-1} solutions in $\mathbb{F}_{p^n}^*$ for each fixed $c \in \mathbb{F}_p^*$. Hence, we have

$$\begin{aligned}AC_s(\tau) &= N - 2|D_\tau| = (p^n - 1) - 2p^{n-1}|D'_{\tau'}| \\ &= (p - 2|D'_{\tau'}|)p^{n-1} - 1.\end{aligned} \tag{16}$$

Furthermore, since the autocorrelation of the Costas sequence $\{b_j\}_{j=0}^{p-2}$ is equal to

$$\begin{aligned}AC_b(\tau') &= \sum_{j=0}^{p-2}(-1)^{b_j - b_{j+\tau'}} = |\mathbb{Z}_{p-1} \setminus D'_{\tau'}| - |D'_{\tau'}| \\ &= p - 1 - 2|D'_{\tau'}|,\end{aligned} \tag{17}$$

the result follows. ■

Combining Lemmas 1 and 2, we have simplified the problem of computing the autocorrelation of the LSB sequence $\{s_t\}_{t=0}^{N-1}$ of period $p^n - 1$ for any positive integer $n \geq 2$ to the problem of computing the autocorrelation of the Costas sequence $\{b_j\}_{j=0}^{p-2}$ of period $p - 1$.

Lemma 3: Let the symbols be the same as above. We have the following results.

(1) For $1 \leq \tau' \leq \frac{p-3}{2}$, $AC_b(p-1-\tau') = AC_b(\tau')$.
(2) For $p \equiv 1 \pmod 4$ and $1 \leq \tau' \leq \frac{p-1}{4}$ or for $p \equiv 3 \pmod 4$ and $1 \leq \tau' \leq \frac{p-3}{4}$, $AC_b(\frac{p-1}{2} - \tau') = -AC_b(\tau')$. Particularly, when $p \equiv 1 \pmod 4$, $AC_b(\frac{p-1}{4}) = 0$.
(3) $AC_b(\frac{p-1}{2}) = -(p-1)$.

Proof: (1) By the discussion in Lemma 2, for a fixed $1 \leq \tau' \leq p-2$, the autocorrelation value $AC_b(\tau')$ depends on $|D_{\tau'}|$ which is in fact the number of c's in $\mathbb{F}_p^*$ such that the pair $(c, \beta^{\tau'}c)$ has different least significant bit (See (15)-(16)). Let $c' = \beta^{\tau'}c$ for $1 \leq \tau' \leq \frac{p-3}{2}$. Then $(c, \beta^{\tau'}c) = (\beta^{-\tau'}c', c') = (\beta^{p-1-\tau'}c', c')$. Since c' runs exactly through $\mathbb{F}_p^*$ when c runs through $\mathbb{F}_p^*$, we have $|D'_{\tau'}| = |D'_{p-1-\tau'}|$, which implies $AC_b(p-1-\tau') = AC_b(\tau')$ by (18).

(2) Since $-c$ is odd if c is even for $c \in \mathbb{F}_p^*$ and vice versa (Notice that p is odd and $-c = p - c$), we can derive $\Big|\{(-c, \beta^{\tau'}c) \mid c \in \mathbb{F}_p^*,\ -c \not\equiv \beta^{\tau'}c \pmod 2)\}\Big| = (p-1) - \Big|\{(c, \beta^{\tau'}c) \mid c \in \mathbb{F}_p^*,\ c \not\equiv \beta^{\tau'}c \pmod 2)\}\Big|$, which results in $-AC_b(\tau') = (p-1) - \Big|\{(-c, \beta^{\tau'}c) \mid c \in \mathbb{F}_p^*,\ -c \not\equiv \beta^{\tau'}c \pmod 2)\}\Big|$. Let $c' = \beta^{\tau'}c$. Then $(-c, \beta^{\tau'}c) = (\beta^{\frac{p-1}{2}-\tau'}c', c')$ from $\beta^{\frac{p-1}{2}} = -1$. By (18), we get $AC_b(\frac{p-1}{2} - \tau') = -AC_b(\tau')$. Particularly, for $p \equiv 1 \pmod 4$ and $\tau' = \frac{p-1}{4}$, we get $AC_b(\frac{p-1}{4}) = -AC_b(\frac{p-1}{4})$, which implies $AC_b(\frac{p-1}{4}) = 0$.

(3) Since the pair $(c, -c)$ always gives different LSBs for $c \in \mathbb{F}_p^*$, the result follows. ■

In convenience, we always use $AC_b(I) = (AC_b(i))_{i\in I}$, where

$$I = \begin{cases} \{1, 2, \cdots, \dfrac{p-5}{4}\}, & \text{for } p \equiv 1 \pmod 4; \\ \{1, 2, \cdots, \dfrac{p-3}{4}\}, & \text{for } p \equiv 3 \pmod 4. \end{cases} \tag{19}$$

We note that $I = \emptyset$ for $p = 3, 5$. Based on all the lemmas above, we obtain the following result.

Theorem 1: Let the symbols be defined as before. For $0 < \tau < N$, the autocorrelation of the LSB sequence $\{s_t\}_{t=0}^{N-1}$ of a p-ary m-sequence $\{a_t\}_{t=0}^{N-1}$ is expressed as

$$AC_s(\tau) = \begin{cases} \big(1+AC_b(\tau')\big)p^{n-1} - 1, & \text{if } \tau \in S_1; \\ \big(1-AC_b(\tau')\big)p^{n-1} - 1, & \text{if } \tau \in S_2; \\ p^{n-1} - 1, & \text{if } p \equiv 1 \pmod 4 \\ & \text{and } \tau = \dfrac{p^n-1}{4}; \\ -(p-2)p^{n-1} - 1, & \text{if } \tau = \dfrac{p^n-1}{2}; \\ p^{n-2} - 1, & \text{otherwise}, \end{cases} \tag{20}$$

where

$$S_1 = \big\{M\tau',\ M(p-1-\tau') \mid \tau' \in I\big\},$$
$$S_2 = \big\{M(\frac{p-1}{2} - \tau'),\ M(\frac{p-1}{2} + \tau') \mid \tau' \in I\big\}.$$

In particular, the corresponding autocorrelations $AC_s(\tau)$ for $p = 3$ and $p = 5$ can be given directly by

$$AC_s(\tau) = \begin{cases} -3^{n-1} - 1, & \text{if } \tau = M, \\ 3^{n-2} - 1, & \text{otherwise}, \end{cases} \tag{21}$$

$$AC_s(\tau) = \begin{cases} 5^{n-1} - 1, & \text{if } \tau = M \text{ or } 3M, \\ -3 \times 5^{n-1} - 1, & \text{if } \tau = 2M, \\ 5^{n-2} - 1, & \text{otherwise} \end{cases} \tag{22}$$

respectively. ■

Example 1: By Matlab and Mathematica programs, let $n = 3$, we give the LSB sequence of period $p^n - 1$ for each prime $p < 20$ and have verified the results in Theorem 1. All these codes and the corresponding results have been organized into PDF files as data files.

Remark 2: For the autocorrelation function $AC_b(\tau')$ of the Costas sequence $\{b_j\}_{j=0}^{p-2}$ of period $p-1$, we have reduced its values from a set $\{AC_b(\tau)\}_{\tau=1}^{p-2}$ to a set $\{AC_b(\tau)|\tau \in I\}$. Hence the size of the problem is simplified to a quarter of the original size and it can be determined relatively more efficiently by computer. Indeed, we present the corresponding ordered array $AC_b(I)$ for all odd primes smaller than 100 in Table 1. Moreover, by plugging the values of $AC_b(I)$ in Table 1 for each prime $3 \le p < 100$ into the formula in Theorem 1, we can get the exact autocorrelation distribution of the LSB sequence of the corresponding p-ary m-sequence. Additionally, it can be observed from these examples that all the autocorrelation values satisfy $-\frac{p-1}{3} \le AC_b(\tau') \le \frac{p-1}{3}$ for

TABLE 1. Examples of $AC_b(I)$ for primes less than 100.

p	β	$AC_b(I)$
3	2	$\emptyset$
5	2,3	$\emptyset$
7	3,5	(2)
11	2,6,7,8	$(-2, 2)$
13	2,6,7,11	$(0, -4)$
17	3	$(4, 0, -4)$
19	2	$(-2, 2, -2, -6)$
23	5	$(2, -2, 2, -2, -6)$
29	2	$(0, -4, 0, -4, 8, 4)$
31	3	$(10, 6, 2, -2, -6, -2, 2)$
37	2	$(0, -4, 0, 4, -8, 4, 0, -12)$
41	6	$(4, -8, 4, 0, -12, 0, 4, 0, 4)$
43	3	$(14, 2, -2, -6, -2, 2, 6, 2, -2, 2)$
47	5	$(10, -2, -14, -2, 2, 6, 2, -2, -6, -2, 2)$
53	2	$(0, -4, 0, -4, 8, 4, 0, -4, -16, 4, 0, -4)$
59	2	$(-2, 2, -2, -6, -2, 10, -2, 18, -2, 2, -10, 2, -2, 2)$
61	2	$(0, -4, 0, -4, 0, 20, 0, -12, 0, -4, -8, 4, 0, -4)$
67	2	$(-2, 2, -2, 2, -2, -22, 6, 2, -2, -6, -2, 10, -2, -6, 14, 2)$
71	7	$(10, 6, 2, -10, 2, -2, -14, -2, -22, -2, 2, -2, 2, -2, 2, 6, -6)$
73	5	$(12, 0, -12, 0, 4, 24, 4, 0, -4, 0, 4, 8, 4, 0, -4, 0, 4)$
79	3	$(26, 6, 2, -2, -6, -2, -6, -2, 2, 6, 2, -2, -6, -10, 2, 14, 2, -2, 2)$
83	2	$(-2, 2, -2, -6, 6, -6, -2, 10, -2, 26, -2, 2, -2, -14, -2, 2, -2, 2, -2, 10)$
89	3	$(28, 8, 4, 8, 4, 8, 12, 0, -4, 0, 4, 0, -4, 0, -4, 0, 4, 16, 4, 0, -4)$
97	5	$(20, 0, -4, -8, 4, 0, 4, 0, -4, 8, 4, 0, 4, 0, 4, 0, -12, 0, 4, 0, -4, -32, -12)$

$\tau' \in \{1, 2, \cdots, p-2\}$ but $\tau' \ne \frac{p-1}{2}$. Finding out the complete and theoretical result of the autocorrelation distribution of the Costas sequence $\{b_j\}_{j=0}^{p-2}$ will be an interesting research problem, but due to our limited ability we can not resolve it in this article. So we sincerely invite those readers who are interested in this problem to participate in it.

Remark 3: Also, from Theorem 1, it seems that the autocorrelation values of the LSB sequences are high, comparing to the periods of these sequences, which is bad for the security of a key stream sequence. However, since the period of the bit-component sequence used in the ZUC algorithm-the core of the 3GPP LTE International Encryption Standard is huge (here $p = 2^{31} - 1$ and the period $N = p^{16} - 1$) and only a little part of the sequence is chosen to be as a key stream in the encryption process, then the high autocorrelation of the sequence has almost no negative impact on the security of the whole cipher system.

Theorem 2: Let $p = 2^k - 1$ be a Mersenne prime, and $\{a_{t,i-1}\}_{t=0}^{N-1}$ the i-th bit-component sequence of $\{a_t\}_{t=0}^{N-1}$. Then, for $2 \le i \le k$, the i-th bit-component sequence $\{a_{t,i-1}\}_{t=0}^{N-1}$ is a cyclic shift of the LSB sequence $\{s_t\}_{t=0}^{N-1}$.

Proof: Because $2 \in \mathbb{F}_p$, there exists some $1 \le j_0 \le p-2$ and $\tau_0 = \frac{p^n-1}{p-1} j_0$ such that $2 = \alpha^{\tau_0}$. Then

$$2a_t = 2\mathrm{Tr}(\alpha^t) = \mathrm{Tr}(\alpha^{t+\tau_0}) = a_{t+\tau_0},$$

which shows that $\{2a_t\}$ is the left cyclic shift of $\{a_t\}$ by τ_0. Moreover,

$$2a_t \bmod p = a_{t,k-1} + a_{t,0} \times 2 + \cdots + a_{t,k-2} \times 2^{k-1},$$

that is, the binary bit string of $2a_t$ is the left cyclic shift of the binary bit string of a_t by 1. Therefore, for $1 \le i \le k$,

the $((i \bmod k)+1)$-th bit-component sequence is the left cyclic shift of the i-th bit-component sequence by τ_0, which results in the conclusion. ■

IV. LOWER BOUND ON THE 2-ADIC COMPLEXITY OF EACH OF THESE LSB SEQUENCES FOR $p < 20$

First we describe the method of Hu [12] as the following lemma.

Lemma 4 [12]: Let $T(x) = \sum_{t=0}^{N-1} (-1)^{s_t} x^t \in \mathbb{Z}[x]$. Then

$$-2S(x)T(x^{-1}) \equiv N + \sum_{\tau=1}^{N-1} AC_s(\tau)x^{\tau} - T(x^{-1})\left(\sum_{t=0}^{N-1} x^t\right) \bmod \left(x^N - 1\right). \quad (23)$$

■

Lemma 5: Suppose that $n \geq 2$ is a positive integer and I is defined as in (19). Then we have

$$S(2)T(2^{-1}) \equiv -\frac{2^{\frac{N}{2}}-1}{2^M-1}\left(p-1\right)p^{n-2} \bmod \left(2^{\frac{N}{2}}-1\right), \quad (24)$$

$$S(2)T(2^{-1}) \equiv \left(\sum_{\tau' \in I} AC_b(\tau')\left(2^{M(\frac{p-1}{2}-\tau')} - 2^{M\tau'}\right) - (p-1)\right)p^{n-1} \bmod \left(2^{\frac{N}{2}}+1\right). \quad (25)$$

Proof: We only present the proof for the case of $p \equiv 3 \pmod 4$ and the other case is similar. Substituting (20) in Theorem 1 into (23) in Lemma 4, we have

$$\begin{aligned}
&-2S(x)T(x^{-1}) \\
&\equiv N + \sum_{\tau \neq M\tau', \tau'=1,2,\cdots,p-2} \left(p^{n-2}-1\right)x^{\tau} \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \left[\left(1+AC_b(\tau')\right)p^{n-1} - 1\right]x^{M\tau'} \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \left[\left(1-AC_b(\tau')\right)p^{n-1} - 1\right]x^{M(\frac{p-1}{2}-\tau')} \\
&\quad + \left[-(p-2)p^{n-1} - 1\right]x^{\frac{N}{2}} \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \left[\left(1-AC_b(\tau')\right)p^{n-1} - 1\right]x^{M(\frac{p-1}{2}+\tau')} \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \left[\left(1+AC_b(\tau')\right)p^{n-1} - 1\right]x^{M(p-1-\tau')} \\
&\quad - T\left(x^{-1}\right)\left(\sum_{t=0}^{N-1} x^t\right) \bmod \left(x^N-1\right) \\
&\equiv N - \left(p^{n-2}-1\right) + \sum_{\tau=0}^{N-1} \left(p^{n-2}-1\right)x^{\tau} \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \left[\left(1+AC_b(\tau')\right)p^{n-1} - p^{n-2}\right]x^{M\tau'} \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \left[\left(1-AC_b(\tau')\right)p^{n-1} - p^{n-2}\right]x^{M(\frac{p-1}{2}-\tau')} \\
&\quad + \left[-\left(p-2\right)p^{n-1} - p^{n-2}\right]x^{\frac{N}{2}} \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \left[\left(1-AC_b(\tau')\right)p^{n-1} - p^{n-2}\right]x^{M(\frac{p-1}{2}+\tau')} \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \left[\left(1+AC_b(\tau')\right)p^{n-1} - p^{n-2}\right]x^{M(p-1-\tau')} \\
&\quad - T\left(x^{-1}\right)\left(\sum_{t=0}^{N-1} x^t\right) \bmod \left(x^N-1\right) \\
&\equiv \Bigg\{ \sum_{\tau'=1}^{\frac{p-3}{4}} \Bigg[\left(\left(1+AC_b(\tau')\right)p-1\right)x^{M\tau'} \\
&\quad + \left(\left(1-AC_b(\tau')\right)p-1\right)x^{M(\frac{p-1}{2}+\tau')}\Bigg] \\
&\quad + \sum_{\tau'=1}^{\frac{p-3}{4}} \Bigg[\left(\left(1-AC_b(\tau')\right)p-1\right)x^{M(\frac{p-1}{2}-\tau')} \\
&\quad + \left(\left(1+AC_b(\tau')\right)p-1\right)x^{M(p-1-\tau')}\Bigg]\Bigg\}p^{n-2} \\
&\quad + \left(p^2-1\right)p^{n-2} - \left(p-1\right)^2 p^{n-2}x^{\frac{N}{2}} \\
&\quad - \left(p^{n-2}-1+T(x^{-1})\right)\left(\sum_{t=0}^{N-1} x^t\right) \bmod \left(x^N-1\right).
\end{aligned} \quad (26)$$

Furthermore, we note that $x^{M\times\frac{p-1}{2}} = x^{\frac{N}{2}} \equiv 1 \bmod (x^{\frac{N}{2}}-1)$ and $x^{\frac{N}{2}} \equiv -1 \bmod (x^{\frac{N}{2}}+1)$. Substituting x for 2, the desirable results can be derived. ■

In the sequel, we also need the following result from the elementary number theory.

Lemma 6: (1) Let p be an odd prime and n be a positive integer. Then $p \mid (2^{p^n-1}-1)$. Further, $p^e \mid (2^{p^n-1}-1)$ if and only if $p^e \mid (2^{p-1}-1)$ for $e \geq 2$ (An odd prime p satisfying $p^2 \mid (2^{p-1}-1)$ is called a Wieferich prime. It is shown in [3] that there are only two Wieferich primes 1093 and 3511 up to 6.7×10^{15}. Additionally, by direct computation, we get $p^3 \nmid (2^{p-1}-1)$ for $p = 1093, 3511$).

(2) A Mersenne prime $p = 2^k - 1$ is not a Wieferich prime. Furthermore, for an odd prime k, we have $p \mid (2^{\frac{p^n-1}{2}}-1)$, $p^2 \nmid (2^{\frac{p^n-1}{2}}-1)$, $p \nmid (2^{\frac{p^n-1}{2}}+1)$.

Proof: (1) Due to $(p-1) \mid (p^n-1)$, we have $(2^{p-1}-1) \mid (2^{p^n-1}-1)$. By Fermat's little Theorem we know that

$p \mid (2^{p-1}-1) \Rightarrow p \mid (2^{p^n-1}-1)$. Further, by Euler's theorem, we have $p^e \mid (2^{p^{e-1}(p-1)}-1)$ since Euler's phi Function value $\phi(p^e) = p^{e-1}(p-1)$. And $p^n - 1 = (p-1)(p^{n-1}+p^{n-2}+\cdots+p+1) \equiv (p^{e-2}+p^{e-3}+\cdots+1)(p-1) \bmod (p^{e-1}(p-1))$, which implies that $p^e \mid (2^{p^n}-1) \Rightarrow p^e \mid (2^{(p^{e-2}+p^{e-3}+\cdots+1)(p-1)}-1)$. Therefore, $p^e \mid \gcd(2^{p^{e-1}(p-1)}-1, 2^{(p^{e-2}+p^{e-3}+\cdots+1)(p-1)}-1)$ if $p^e \mid (2^{p^n-1}-1)$, i.e.,

$$p^e \mid (2^{\gcd(p^{e-1}(p-1),(p^{e-2}+p^{e-3}+\cdots+1)(p-1))}-1).$$

Note that

$$\gcd(p^{e-1}(p-1), (p^{e-2}+p^{e-3}+\cdots+1)(p-1)) = p-1.$$

The result follows.

(2) Notice that $k=2$ or k is an odd prime for a Mersenne prime $p = 2^k - 1$. If $k=2$, i.e., $p=3$, then p is not a Wieferich prime from the conclusion in [3]. If k is an odd prime for $p = 2^k-1$, we get $k \mid (p-1)$ by $p \mid (2^{p-1}-1)$. Suppose $p^2 \mid (2^{p-1}-1)$, i.e.,

$$\left(2^k-1\right)^2 \mid \left[\left(2^k-1\right)\left(2^{(\frac{p-1}{k}-1)k}+\cdots+2^k+1\right)\right],$$

which implies

$$(2^k-1) \mid (2^{(\frac{p-1}{k}-1)k}+2^{(\frac{p-1}{k}-2)k}+\cdots+2^k+1). \quad (27)$$

But we know

$$2^{(\frac{p-1}{k}-1)k}+2^{(\frac{p-1}{k}-2)k}+\cdots+2^k+1 \equiv \frac{p-1}{k} \equiv \frac{2(2^{k-1}-1)}{k} \bmod (2^k-1) \quad (28)$$

and $\gcd\left(2(2^{k-1}-1), 2^k-1\right) = 1$, i.e.,

$$\gcd(2^k-1, 2^{(\frac{p-1}{k}-1)k}+2^{(\frac{p-1}{k}-2)k}+\cdots+2^k+1) = 1,$$

a contradiction to (27). Hence p is not a Wieferich prime. Furthermore, since $k \mid (2^{k-1}-1)$, $2^{k-1}-1 = \frac{p-1}{2}$ and $\frac{p-1}{2} \mid \frac{p^n-1}{2}$, we get $k \mid \frac{p^n-1}{2}$ and $(2^k-1) \mid (2^{\frac{p^n-1}{2}}-1)$, i.e., $p \mid (2^{\frac{p^n-1}{2}}-1)$. Moreover, $p^2 \nmid (2^N-1)$ implies $p^2 \nmid (2^{\frac{N}{2}}-1)$ and $p \mid (2^{\frac{p^n-1}{2}}-1)$ results in $p \nmid (2^{\frac{p^n-1}{2}}+1)$. ■

In convenience, we denote

$$g(p,2^M) = \sum_{\tau' \in I} AC_b(\tau')\left(2^{M(\frac{p-1}{2}-\tau')}-2^{M\tau'}\right)-(p-1). \quad (29)$$

Lemma 7: Let the notations be the same as above and let $\delta := \mathrm{Ord}_p(2)$ be the multiplicative order of 2 modular p. Suppose that $n \geq 2$ is a positive integer. Then we have the following two results:

(1)

$$\gcd\left(S(2)T(2^{-1}), 2^{\frac{N}{2}}-1\right) = \begin{cases} \gcd\left((p-1)p^{n-2}, 2^M-1\right)\dfrac{2^{\frac{N}{2}}-1}{2^M-1}, \\ \qquad \text{if } n \equiv 0 \pmod{\delta}, n \neq 2, \\ \gcd\left(p-1, 2^M-1\right)\dfrac{2^{\frac{N}{2}}-1}{2^M-1}, \\ \qquad \text{if } n \not\equiv 0 \pmod{\delta} \text{ or } n = 2, \end{cases} \quad (30)$$

$$\gcd\left(S(2)T(2^{-1}), 2^{\frac{N}{2}}+1\right) = \begin{cases} \gcd\left(g(p,2^M)p^{n-1}, 2^{\frac{N}{2}}+1\right), & \delta \nmid \dfrac{p-1}{2} \text{ and } n \textit{ is} \text{ odd}, \\ \gcd\left(g(p,2^M), 2^{\frac{N}{2}}+1\right), & \delta \mid \dfrac{p-1}{2} \text{ or } n \text{ is even}. \end{cases} \quad (31)$$

(2) If $p = 2^k - 1 > 5$ is a Mersenne prime, then

$$\gcd\left(S(2)T(2^{-1}), 2^{\frac{N}{2}}-1\right) = \begin{cases} \gcd\left(p-1, 2^M-1\right)\dfrac{2^{\frac{N}{2}}-1}{2^M-1}p, \\ \qquad \text{if } n \equiv 0 \pmod{\delta} \text{ but } n \neq 2, \\ \gcd\left(p-1, 2^M-1\right)\dfrac{2^{\frac{N}{2}}-1}{2^M-1}, \\ \qquad \text{if } n \not\equiv 0 \pmod{\delta} \text{ or } n = 2, \end{cases} \quad (32)$$

$$\gcd\left(S(2)T(2^{-1}), 2^{\frac{N}{2}}+1\right) = \begin{cases} \gcd\left(g(p,2^M)p, 2^{\frac{N}{2}}+1\right), & \delta \nmid \dfrac{p-1}{2} \text{ and } n \text{ is odd}, \\ \gcd\left(g(p,2^M), 2^{\frac{N}{2}}+1\right), & \delta \mid \dfrac{p-1}{2} \text{ or } n \text{ is even}. \end{cases} \quad (33)$$

Proof: (1) From (24), we get

$$\gcd\left(S(2)T(2^{-1}), 2^{\frac{N}{2}}-1\right) = \frac{2^{\frac{N}{2}}-1}{2^M-1}\gcd\left((p-1)p^{n-2}, 2^M-1\right).$$

Note that $2^{p^i} \equiv 2 \pmod{p}$ for any nonnegative integer i by Fermat's Little Theorem. Since

$$M = \frac{N}{p-1} = p^{n-1}+p^{n-2}+\cdots+p+1,$$

we get

$$2^M = 2^{p^{n-1}+p^{n-2}+\cdots+p+1} \equiv 2^n \pmod{p}.$$

By the definition of δ, we know that $2^M - 1 \equiv 0 \pmod{p}$ if $n \equiv 0 \pmod{\delta}$, otherwise, $2^M - 1 \not\equiv 0 \pmod{p}$, Eq. (30) holds.

Similarly, since $2^{\frac{N}{2}} = (2^M)^{\frac{p-1}{2}} \equiv 2^{\frac{n(p-1)}{2}} \pmod{p}$ and $2^{p-1} \equiv 1 \pmod{p}$ by Fermat Little Theorem, we can get $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ if $\delta \nmid \frac{p-1}{2}$. Combining (25), we know that the Eq. (31) holds.

(2) The proof is similar to the above. ■

Corollary 1: Let $\mathrm{ind}(p)$ be the largest integer e satisfying $p^e \mid (2^{p-1}-1)$ for a prime p. Suppose $n \geq 2$. Then we have

$$\gcd\left(S(2), 2^N-1\right) \leq \gcd\left(S(2)T(2^{-1}), 2^N-1\right) \leq \frac{2^{\frac{N}{2}}-1}{2^M-1} \times p^{\mathrm{ind}(p)} \times \gcd(p-1, 2^M-1) \times \gcd\left(g(p,2^M), 2^{\frac{N}{2}}+1\right). \quad (34)$$

Proof: It is obvious that

$$\gcd\big(S(2), 2^N - 1\big) \le \gcd\big(S(2)T(2^{-1}), 2^N - 1\big).$$

Since $\gcd\big(2^{\frac{N}{2}} - 1, 2^{\frac{N}{2}} + 1\big) = 1$, then $\gcd\big(S(2)T(2^{-1}), 2^N - 1\big) = \gcd\big(S(2)T(2^{-1}), 2^{\frac{N}{2}} - 1\big) \times \gcd\big(S(2)T(2^{-1}), 2^{\frac{N}{2}} + 1\big)$. Observing (30)-(33), the reason why each of them is divided into two cases is because of the uncertainty of $\gcd\big(p^{n-2}, 2^M - 1\big)$ or $\gcd\big(p^{n-1}, 2^{\frac{N}{2}} + 1\big)$ which is essentially the uncertainty of $\gcd\big(p^{n-1}, 2^N - 1\big)$. By Lemma 6, this problem can be converted to the value of ind(p). The result follows. ■

Remark 4: Firstly, it is obvious that the integer ind(p) in the above Corollary 1 only depends on the property of the prime p. By Fermat's little Theorem, we know ind$(p) \ge 1$. On the other hand, from Lemma 6, up to now, for all primes $p \le 6.7 \times 10^{15}$ we have ind$(p) \le 2$ and there are only two Wieferich primes 1093 and 3511 with ind$(p) = 2$ among them. Therefore, the probability of ind$(p) = 2$ is very small and the probability of ind$(p) \ge 3$ is almost 0. Secondly, $2^M - 1$ is far greater than $p - 1$ for $n \ge 2$, the size of the value $\gcd(p - 1, 2^M - 1)$ depends on the factorization of $p - 1$ which in fact depends on the property of the prime p. Thus, combining the discussion here and the result of the above Corollary 1, the upper bound of the value $\gcd\big(S(2), 2^N - 1\big)$ depends on some properties of the prime p and the value of (34).

For $p = 3, 5$, we can easily get the following Theorem 3.

Theorem 3: Let $\{s_t\}_{t=0}^{N-1}$ be the LSB sequence of a p-ary m-sequence of order $n \ge 2$. Then the 2-adic complexity $\Phi_2(s)$ is bounded by $\Phi_2(s) \ge N - 3$ for $p = 3$ and $\Phi_2(s) \ge \frac{3N}{4} - 4$ for $p = 5$.

Proof: Note $\frac{2^{\frac{N}{2}}-1}{2^M-1} = 1$ for $p = 3$ and $\frac{2^{\frac{N}{2}}-1}{2^M-1} = 2^{\frac{N}{4}} + 1$ for $p = 5$. Further, ind$(p) = 1$, $\gcd(p - 1, 2^M - 1) = 1$, and $I = \emptyset$ for both $p = 3$ and $p = 5$. Therefore, from Corollary 1, $\gcd\big(S(2), 2^N - 1\big) \le 3$ for $p = 3$ and $\gcd\big(S(2), 2^N - 1\big) \le 5(2^{\frac{N}{4}} + 1)$ for $p = 5$. From (1), the results follow. ■

In fact, we can also derive an upper bound on the value $\gcd\big(S(2), 2^N - 1\big)$ and the corresponding lower bound on the 2-adic complexity of the LSB sequence for $p = 7, 11, 13, 17, 19$ respectively. In order to avoid repetition, here we only give the whole proof for $p = 19$ and we list the results for $p = 7, 11, 13, 17$. We also skip and present them in Table 2. In convenience, we give the following notation.

Suppose $\frac{p-1}{2} = 2^l(2k_1 + 1)$ for some two integers $l \ge 0$ and $k_1 \ge 0$. Then we have

$$\begin{aligned} &2^{\frac{N}{2}} + 1 = 2^{\frac{p-1}{2}M} + 1 \\ &= (2^{2^lM} + 1)(2^{(2k_1)2^lM} - 2^{(2k_1-1)2^lM} + \cdots - 2^{2^lM} + 1). \end{aligned}$$

Now, denote

$$h(p, 2^M) = 2^{(2k_1)2^lM} - 2^{(2k_1-1)2^lM} + \cdots - 2^{2^lM} + 1.$$

Theorem 4: Let $p = 7$, $n \ge 2$ be a positive integer, and $\{s_t\}_{t=0}^{N-1}$ be the LSB sequence of any 7-ary m-sequence of order n. Then we have

$$\begin{aligned} &\frac{2^{\frac{N}{2}} - 1}{2^M - 1} = 2^{\frac{N}{3}} + 2^{\frac{N}{6}} + 1, \\ &\text{ind}(p) = 1, \\ &\gcd(p - 1, 2^M - 1) \le 3, \\ &\gcd\big(g(p, 2^M), 2^{\frac{N}{2}} + 1\big) = 1. \end{aligned} \tag{35}$$

Thus the 2-adic complexity $\Phi_2(s)$ of $\{s_t\}_{t=0}^{N-1}$ satisfies $\Phi_2(s) \ge \frac{2N}{3} - 6$. ■

Theorem 5: Let $p = 11$, $n \ge 2$ be a positive integer, and $\{s_t\}_{t=0}^{N-1}$ be the LSB sequence of any 11-ary m-sequence of order n. Then we have

$$\begin{aligned} &\frac{2^{\frac{N}{2}} - 1}{2^M - 1} = 2^{\frac{2N}{5}} + 2^{\frac{3N}{10}} + 2^{\frac{N}{5}} + 2^{\frac{N}{10}} + 1, \\ &\text{ind}(p) = 1, \\ &\gcd(p - 1, 2^M - 1) \le 5, \\ &\gcd\big(g(p, 2^M), 2^{\frac{N}{2}} + 1\big) = 1 \text{ for even } n. \end{aligned}$$

And for odd n, we have $\gcd\big(g(p, 2^M), 2^M + 1\big) = 3$ and $\gcd\big(g(p, 2^M), h(p, 2^M)\big) = 1$, i.e., $\gcd\big(g(p, 2^M), 2^{\frac{N}{2}} + 1\big) = 3$. Thus, by (1) and corollary 1, the lower bound on the 2-adic complexity $\Phi_2(s)$ of $\{s_t\}_{t=0}^{N-1}$ is given by $\Phi_2(s) \ge \frac{3N}{5} - 9$. ■

Theorem 6: Let $p = 13$, $n \ge 2$ be a positive integer, and α be a primitive element of $\mathbb{F}_{13^n}$ such that $\beta = \alpha^M = 2, 6, 7$ or 11. Let $\{s_t\}_{t=0}^{N-1}$ be the LSB sequence of the 13-ary m-sequence defined by α. Then we have

$$\begin{aligned} &\frac{2^{\frac{N}{2}} - 1}{2^M - 1} = 2^{\frac{5N}{12}} + 2^{\frac{N}{3}} + 2^{\frac{N}{4}} + 2^{\frac{N}{6}} + 2^{\frac{N}{12}} + 1, \\ &\text{ind}(p) = 1, \\ &\gcd(p - 1, 2^M - 1) \le 3, \\ &\gcd\big(g(p, 2^M), 2^{\frac{N}{2}} + 1\big) = 1 \text{ for even } n. \end{aligned}$$

And for odd n, we have $\gcd\big(g(p, 2^M), 2^{2M} + 1\big) = 5$ and $\gcd\big(g(p, 2^M), h(p, 2^M)\big) = 1$, i.e., $\gcd\big(g(p, 2^M), 2^{\frac{N}{2}} + 1\big) = 5$. Thus, by (1) and corollary 1, the 2-adic complexity $\Phi_2(s)$ of $\{s_t\}_{t=0}^{N-1}$ satisfies $\Phi_2(s) \ge \frac{7N}{12} - 9$. ■

Theorem 7: Let $p = 17$, $n \ge 2$ be a positive integer, and α be a primitive element of $\mathbb{F}_{17^n}$ such that $\beta = \alpha^M = 3$. Let $\{s_t\}_{t=0}^{N-1}$ be the LSB sequence of the 17-ary m-sequence defined by α. Then we have

$$\begin{aligned} &\frac{2^{\frac{N}{2}} - 1}{2^M - 1} = 2^{\frac{7N}{16}} + 2^{\frac{3N}{8}} + 2^{\frac{5N}{16}} + 2^{\frac{N}{4}} + 2^{\frac{3N}{16}} + 2^{\frac{N}{8}} + 2^{\frac{N}{16}} + 1, \\ &\text{ind}(p) = 1, \\ &\gcd(p - 1, 2^M - 1) = 1, \\ &\gcd\big(g(p, 2^M), 2^{\frac{N}{2}} + 1\big) = 1. \end{aligned}$$

Thus, by (1) and corollary 1, the 2-adic complexity $\Phi_2(s)$ of $\{s_t\}_{t=0}^{N-1}$ satisfies $\Phi_2(s) \ge \frac{9N}{16} - 6$. ■

Theorem 8: Let $p = 19$, $n \ge 2$ be a positive integer, and α be a primitive element of $\mathbb{F}_{19^n}$ such that $\beta = \alpha^M = 2$. Let $\{s_t\}_{t=0}^{N-1}$ be the LSB sequence of the 19-ary m-sequence

defined by α. Then the lower bound on the 2-adic complexity $\Phi_2(s)$ of $\{s_t\}_{t=0}^{N-1}$ is given by $\Phi_2(s) \geq \frac{5N}{9} - 12$.

Proof: Firstly, for $p = 19$, we have $M = \frac{p^n-1}{p-1} = \frac{19^n-1}{18}$ and $\frac{N}{2} = \frac{p-1}{2}M = 9M$, then

$$\frac{2^{\frac{N}{2}}-1}{2^M-1} = 2^{\frac{4N}{9}} + 2^{\frac{7N}{18}} + 2^{\frac{N}{3}} + 2^{\frac{5N}{18}} + 2^{\frac{2N}{9}} + 2^{\frac{N}{6}} + 2^{\frac{N}{9}} + 2^{\frac{N}{18}} + 1, \quad (36)$$

Secondly, by Remark 4,

$$\mathrm{ind}(p) = 1. \quad (37)$$

Thirdly, since $2^M - 1$ is odd, it is easy to see

$$\begin{aligned}\gcd(p-1, 2^M-1) &= \gcd(18, 2^M-1)\\ &= \gcd(9, 2^M-1) \quad (38)\end{aligned}$$

Finally, we determine the value of $\gcd\Big(g(p, 2^M), 2^{\frac{N}{2}}+1\Big)$. From Table 1 we can get

$$g(p, 2^M) = -2\Big(2^{8M} - 2^{7M} + 2^{6M} + 3\cdot 2^{5M} - 3\cdot 2^{4M} - 2^{3M} + 2^{2M} - 2^M + 9\Big).$$

Denote

$$g_1(p, 2^M) = 2^{8M} - 2^{7M} + 2^{6M} + 3\cdot 2^{5M} - 3\cdot 2^{4M} - 2^{3M} + 2^{2M} - 2^M + 9. \quad (39)$$

Since $2^{\frac{N}{2}} + 1$ is odd, then

$$\gcd\Big(g(p, 2^M), 2^{\frac{N}{2}}+1\Big) = \gcd\Big(g_1(p, 2^M), 2^{\frac{N}{2}}+1\Big) \quad (40)$$

Notice that

$$\begin{aligned}2^{\frac{N}{2}} + 1 &= 2^{9M} + 1 = (2^{3M}+1)(2^{6M} - 2^{3M} + 1)\\ &= (2^M+1)(2^{2M} - 2^M + 1)(2^{6M} - 2^{3M} + 1) \quad (41)\end{aligned}$$

Now, we compute

$$\gcd\Big(g_1(p, 2^M), 2^M + 1\Big), \quad (42)$$

$$\gcd\Big(g_1(p, 2^M), 2^{2M} - 2^M + 1\Big), \quad (43)$$

$$\gcd\Big(g_1(p, 2^M), 2^{6M} - 2^{3M} + 1\Big) \quad (44)$$

respectively. By (39) and direct computation, we know

$$g_1(p, 2^M) \equiv 9 \bmod (2^M + 1).$$

From Euclid algorithm, this implies

$$\gcd\Big(g_1(p, 2^M), 2^M + 1\Big) = \gcd\Big(9, 2^M + 1\Big). \quad (45)$$

Similarly, direct computation derives

$$g_1(p, 2^M) \equiv 12 \bmod (2^{2M} - 2^M + 1).$$

Therefore,

$$\begin{aligned}&\gcd\Big(g_1(p, 2^M), 2^{2M} - 2^M + 1\Big)\\ &= \gcd\Big(12, 2^{2M} - 2^M + 1\Big)\\ &= \gcd\Big(3, 2^{2M} - 2^M + 1\Big). \quad (46)\end{aligned}$$

Next, by Euclid algorithm and direct calculation, we can get

$$\begin{aligned}&g_1(p, 2^M) \equiv 4(2^{5M} - 2^{4M} + 2) \bmod (2^{6M} - 2^{3M} + 1).\\ &2^{6M} - 2^{3M} + 1 \equiv 2^{4M} - 2^{3M} - 2\cdot 2^M - 1 \bmod (2^{5M} - 2^{4M} + 2).\\ &2^{5M} - 2^{4M} + 2 \equiv 2\cdot 2^{2M} + 2^M + 2 \bmod (2^{4M} - 2^{3M} - 2\cdot 2^M - 1).\\ &4(2^{4M} - 2^{3M} - 2\cdot 2^M - 1) \equiv 2^{2M} - 2^M - 2 \bmod (2\cdot 2^{2M} + 2^M + 2).\\ &2\cdot 2^{2M} + 2^M + 2 \equiv 3\cdot 2^M + 6 \bmod (2^{2M} - 2^M - 2).\\ &3(2^{2M} - 2^M - 2) \equiv 12 \bmod (3\cdot 2^M + 6),\end{aligned}$$

then from the above series of congruences we get

$$\gcd\Big(g_1(p, 2^M), 2^{6M} - 2^{3M} + 1\Big) \mid 12.$$

But $2^{6M} - 2^{3M} + 1$ is odd, so we have

$$\gcd\Big(g_1(p, 2^M), 2^{6M} - 2^{3M} + 1\Big) \leq 3. \quad (47)$$

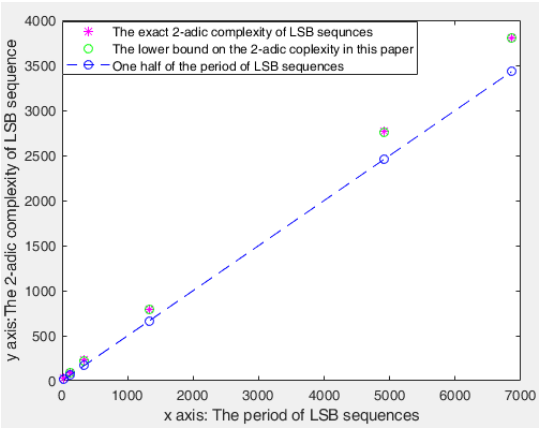
Since $\gcd(2^M - 1, 2^M + 1) = 1$, we know that the values of (38) and (45) can not be larger than 1 at the same time. Combining the above (36)-(47) and corollary 1, we know that

$$\gcd\big(S(2), 2^N - 1\big) \leq 19\times 9\times 3\times 3\Big(2^{\frac{4N}{9}} + 2^{\frac{7N}{18}} + 2^{\frac{N}{3}} + 2^{\frac{5N}{18}} + 2^{\frac{2N}{9}} + 2^{\frac{N}{6}} + 2^{\frac{N}{9}} + 2^{\frac{N}{18}} + 1\Big)$$

which implies $\Phi_2(s) \geq \frac{5N}{9} - 12$ by (1). ■

Example 2: By Matlab and Mathematica programs, let $n = 3$, we give the LSB sequence of period $p^n - 1$ for each prime $p < 20$ and have verified the results in Lemma 7, Corollary 1 and Theorems 3-8. All these codes and the corresponding results have been organized into PDF files as data files.

In the following, we present a figure to explain the significance of the lower bound on the 2-adic complexity of each LSB sequence in this article. From the figure, we can see the lower bound is almost equal to the exact 2-adic complexity of each LSB sequence obtained by direct computation. Further, both the lower bound and the exact 2-adic complexity are larger than one half of the period of each LSB sequence.



A comparison of the exact 2-adic complexity, the lower bounds and one half of the periods of LSB sequences

Remark 5: In the process of computing the lower bound on the 2-adic complexity of each LSB sequence of the above six classes, we always suppose $n \geq 2$. In fact, it can be testified by simply calculation that all the lower bounds also hold for $n = 1$.

Remark 6: The final conclusion of Remark 4 tells us that the upper bound of the value $\gcd\big(S(2), 2^N - 1\big)$ depends on some properties of the prime p and the value of (34). Further, in (34), both $g(p, 2^M)$ and $2^{\frac{N}{2}} + 1 = 2^{\frac{p-1}{2}M} + 1$ can be regarded as polynomials with respect to 2^M, where the coefficients of the former depends on the prime p and the coefficients of the latter is certain. From the results of Theorems 4-7 and the proof of Theorem 8, the greatest common divisor of these two polynomials with respect to 2^M is a number which has nothing to do with 2^M but is different for every different prime p. But due to our limited ability, we can not give a unified representation for infinitely many primes. So we give a conjecture according to those above characteristics. And in order to observe the laws of the 2-adic complexity of the LSB sequence in each of Theorems 3-8, we list the Table 2, from which it is obvious that, for $n \geq 2$, the main part in the expression of the lower bound of the 2-adic complexity of the LSB sequence (all the bit-component sequences for a Mersenne prime) of the p-ary m-sequence for each $p \leq 19$ have a unified form, i.e., $\frac{N}{2} + \frac{N}{p-1}$, which are large enough to resist the RAA.

TABLE 2. Examples of $\Phi_2(s)$ for $p < 20$.

p	β	the lower bound on the 2-adic complexity $\Phi_2(s)$
3	2	$\Phi_2(s) \geq N - 3 = \frac{N}{2} + \frac{N}{p-1} - 3$
5	2,3	$\Phi_2(s) \geq \frac{3N}{4} - 5 = \frac{N}{2} + \frac{N}{p-1} - 4$
7	3,5	$\Phi_2(s) \geq \frac{2N}{3} - 7 = \frac{N}{2} + \frac{N}{p-1} - 6$
11	2,6,7,8	$\Phi_2(s) \geq \frac{3N}{5} - 8 = \frac{N}{2} + \frac{N}{p-1} - 9$
13	2,6,7,11	$\Phi_2(s) \geq \frac{7N}{12} - 4 = \frac{N}{2} + \frac{N}{p-1} - 9$
17	3	$\Phi_2(s) \geq \frac{9N}{16} - 7 = \frac{N}{2} + \frac{N}{p-1} - 6$
19	2	$\Phi_2(s) \geq \frac{5N}{9} - 15 = \frac{N}{2} + \frac{N}{p-1} - 12$

Conjecture 1: Let the symbols be the same as those in Corollary 1. Then there exists a fixed constant $C_{1,p}$ which has nothing to do with 2^M (i.e., it has nothing to do with the size of n) for each prime p such that $\gcd\Big(g(p, 2^M), 2^{\frac{N}{2}} + 1\Big) = C_{1,p}$. Thus, by Corollary 1, the conclusion of Remarks 4 and 6, there exists a constant C_p such that the 2-adic complexity $\Phi_2(s)$ of $\{s_t\}_{t=0}^{N-1}$ is lower bounded by $\frac{p+1}{2(p-1)}N - C_p$ which is larger than $\frac{N}{2}$, where the constant number C_p depends only on p. ■

V. CONCLUSION

In this article, we first turned the problem of determining the autocorrelation distribution of the LSB sequence of a p-ary m-sequence with period $p^n - 1$ for any order $n \geq 2$ into the problem of calculating the autocorrelation distribution of a corresponding Costas sequence with period $p - 1$ directly by computer. As examples, we list the explicit autocorrelation distributions of costas sequences for all primes $p < 100$ in a table. Further, by means of these examples, the 2-adic complexity of all Costas sequences for $p < 20$ were analyzed, which indicates that these sequences can resist the analysis of RAA (Rational Approximation Algorithm) for FCSRs (Feedback with Carry Shift Registers). Finally, a conjecture on the lower bound of the 2-adic complexity of the LSB sequences of all p-ary m-sequences is proposed.

It should be pointed out that the problems discussed in this article originate from the core of the 3GPP LTE International Encryption Standard, i.e., ZUC algorithm, which is in fact being proposed as 5G mobile communication encryption standard. The main reason why the algorithm is still safe after so many years is that it destroys the theoretical structures of binary and nonbinary fields themselves. Hence, it is difficult for us within our capabilities to give a completely theoretical proof of Conjecture 1. We sincerely invite those experts who are interested in it to participate in this work.

ACKNOWLEDGMENT

The authors would like to thank editors and the anonymous reviewers for giving them very useful suggestions which help them to improve the quality of the paper.

DATA AVAILABILITY

The code and the results of the programs of the examples in this article have been uploaded to the submission system.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] A. H. Chan and R. A. Games, "On the linear span of binary sequences obtained from finite geometries," in *Advances Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 263. 1987, pp. 405–417.

[2] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 693–698, May 1998.

[3] F. Dorais and D. Klyve, "A Wieferich prime search up to 6.7×10^{15}," *J. Integer Sequences*, vol. 14, no. 9, pp. 1–14, 2011.

[4] K. Drakakis, V. Requena, and G. McGuire, "On the nonlinearity of exponential Welch Costas functions," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1230–1238, Mar. 2010.

[5] V. Edemskiy and A. Palvinskiy, "The linear complexity of binary sequences of length 2P with optimal three-level autocorrelation," *Inf. Process. Lett.*, vol. 116, no. 2, pp. 153–156, Feb. 2016.

[6] *ETSL/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-ELA3, Version: 1.6*, document 2, ZUC Specification, 2011.

[7] *ETSL/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3, Version: 1.6*, document 1, 128-EEA3 and 128-EIA3 Specification, 2011.

[8] T. Etzion, "Linear complexity of de Bruijn sequences-old and new results," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 693–698, Mar. 1999.

[9] S. W. Golomb, "Algebraic constructions for Costas arrays," *J. Combinat. Theory A*, vol. 37, no. 1, pp. 13–21, Jul. 1984.

[10] T. Helleseth, J. E. Mathiassen, M. Maas, and T. Segers, "Linear complexity over $\mathbb{F}_p$ of Sidel'nikov sequences," in *Proc. ISIT*, 2004, p. 122.

[11] R. Hofer and A. Winterhof, "On the 2-adic complexity of the two-prime generator," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5957–5960, Aug. 2018.

[12] H. Hu, "Comments on 'a new method to compute the 2-adic complexity of binary sequences,'" *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5803–5804, Sep. 2014.

[13] L. Hu, Q. Yue, and M. Wang, "The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5534–5543, Apr. 2012.

[14] Y. S. Kim, J. W. Jang, S. H. Kim, and J. S. No, "Linear complexity of quaternary sequences constructed from binary Legendre sequences," in *Proc. ISITA*, 2012, pp. 611–614.

[15] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *J. Cryptol.*, vol. 10, no. 2, pp. 111–147, Mar. 1997.

[16] N. Li and X. Tang, "On the linear complexity of binary sequences of period 4*N* with optimal autocorrelation value/magnitude," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7597–7604, Nov. 2011.

[17] R. A. Rueppel, "Linear complexity and random sequences," in *Advances in Cryptology—EUROCRYPT*. 1986, pp. 167–188.

[18] 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," *Cryptogr. Commun.*, vol. 10, no. 3, pp. 467–477, May 2018.

[19] Y. Sun, Q. Wang, and T. Yan, "A lower bound on the 2-adic complexity of the modified Jacobi sequence," *Cryptogr. Commun.*, vol. 11, no. 2, pp. 337–349, Mar. 2019.

[20] Y. Sun, T. Yan, Z. Chen, and L. Wang, "The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude," *Cryptogr. Commun.*, to be published, doi: 10.1007/s12095-019-00411-4.

[21] T. Tian and W.-F. Qi, "2-adic complexity of binary *m*-sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 450–454, Dec. 2010.

[22] Q. Wang and X. Du, "The linear complexity of binary sequences with optimal autocorrelation," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6388–6397, Dec. 2010.

[23] Q. Wang, Y. Jiang, and D. Lin, "Linear complexity of binary generalized cyclotomic sequences over GF(q)," *J. Complex.*, vol. 31, no. 5, pp. 731–740, 2015.

[24] Z. Xiao, X. Zeng, and Z. Sun, "2-adic complexity of two classes of generalized cyclotomic binary sequences," *Int. J. Found. Comput. Sci.*, vol. 27, no. 7, pp. 879–893, Nov. 2016.

[25] H. Xiong, L. Qu, C. Li, and S. Fu, "Linear complexity of binary sequences with interleaved structure," *IET Commun.*, vol. 7, no. 15, pp. 1688–1696, Oct. 2013.

[26] H. Xiong, L. Qu, and C. Li, "A new method to compute the 2-adic complexity of binary sequences," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2399–2406, Apr. 2014.

[27] H. Xiong, L. Qu, and C. Li, "2-adic complexity of binary sequences with interleaved structure," *Finite Fields Appl.*, vol. 33, pp. 14–28, May 2015.

[28] M. Yang, L. Zhang, and K. Feng, "On the 2-adic complexity of a class of binary sequences of period 4*P* with optimal autocorrelation magnitude," *CoRR*, 2019.

[29] L. Zhang, J. Zhang, M. Yang, and K. Feng, "On the 2-adic complexity of the Ding-Helleseth-Martinsen binary sequences," *IEEE Trans. Inf. Theory*, vol. 66, no. 7, pp. 4613–4620, Jul. 2020, doi: 10.1109/TIT.2020.2964171.

YUHUA SUN was born in Shandong, China, in 1979. She received the M.S. degree in mathematics from Tongji University, Shanghai, in 2004, and the Ph.D. degree in cryptography from Xidian University, Xi'an, Shanxi, in 2013.

She is the author of more than 20 articles. Her research interests include cryptography, coding theory, and information theory. She holds a patent.

Dr. Sun was a recipient of the Youth Program of National Natural Science Foundation of China. She is a Reviewer of the IEEE TRANSACTIONS ON INFORMATION THEORY, *Finite Fields and Their Applications*, *Cryptography and Communications*, and so on.

QIUYAN WANG was born in 1987. She received the degree from the Shandong University of Technology, China, in 2009, the M.S. degree in mathematics from Capital Normal University, Beijing, in 2012, and the Ph.D. degree in information security from the University of Chinese Academy of Sciences, in 2016.

Her education has a background in computer science and mathematics. She is the author of more than 20 articles. Her research interests include cryptography, coding theory, and information theory. She was a recipient of the Youth Program of National Natural Science Foundation of China.

TONGJIANG YAN was born in Shandong, China, in 1973. He received the degree from the Department of Mathematics, Huaibei Coal Industry Teachers College, China, in 1996, the M.S. degree in mathematics from Northeast Normal University, Lanzhou, China, in 1999, and the Ph.D. degree from Xidian University, in 2007.

He is the author of more than 60 articles. His research interests include cryptography, coding theory, and information theory. He holds a patent.

Dr. Yan was a recipient of the General Fund of National Natural Science of China. He is a Reviewer of the IEEE TRANSACTIONS ON INFORMATION THEORY, *Finite Field and Their Applications*, *Cryptography and Communications*, and so on.

CHUN'E ZHAO was born in Shandong, China, in 1981. She received the M.S. degree in mathematics from Anhui University and the Ph.D. degree from Xidian University.

She is the author of more than ten articles. Her research interests include cryptography, coding theory, and information theory.