New Construction of M-ary Sequence Families With Low Correlation From the Structure of Sidelnikov Sequences

Nam Yul Yu* and Guang Gong†

*Department of Electrical Engineering, Lakehead University

†Department of Electrical and Computer Engineering, University of Waterloo

Abstract

The main topics of this paper are the structure of Sidelnikov sequences and new construction of M-ary sequence families from the structure. For prime p and a positive integer m, it is shown that M-ary Sidelnikov sequences of period $p^{2m}-1$, if $M \mid p^m-1$, can be equivalently generated by the operation of elements in a finite field $\mathrm{GF}(p^m)$, including a p^m-ary m-sequence. The equivalent representation over $\mathrm{GF}(p^m)$ requires low complexity for implementing the Sidelnikov sequences of period $p^{2m}-1$. From the $(p^m-1)\times(p^m+1)$ array structure of the sequences, it is then found that a half of the column sequences and their constant multiples have low correlation enough to construct new M-ary sequence families of period p^m-1. In particular, new M-ary sequence families of period p^m-1 are constructed from the combination of the column sequence families and known Sidelnikov-based sequence families, where the new families have larger family sizes than the known ones with the same maximum correlation magnitudes. Finally, it is shown that the new M-ary sequence family of period p^m-1 and the maximum correlation magnitude $2\sqrt{p^m}+6$ asymptotically achieves $\sqrt{2}$ times the equality of the Sidelnikov's lower bound when $M=p^m-1$ for odd prime p.

Index Terms

Correlation, Polyphase sequences, Sequence family, Sidelnikov sequences, Weil bound.

I. Introduction

Sequences with low correlation find many applications in wireless communications for acquiring the correct timing information and distinguishing multiple users or channels with low mutual interference.

Also, sequences with variable alphabet size are suitable for adaptive modulation schemes, where variable data rates can be supported by wireless systems according to channel characteristics. In addition, a large number of distinct sequences are required for supporting as many distinct users or channels as possible.

Sidelnikov sequences introduced in [18] are polyphase sequences with low correlation and variable alphabet sizes, represented by multiplicative characters. For prime p and positive integers m and $M \mid p^m - 1$, M-ary *Sidelnikov sequences* of period $p^m - 1$ have the maximum out-of-phase autocorrelation magnitude of 4. The binary case of the sequences has been also discussed in [14]. Kim and Song [9] showed that the cross-correlation of an M-ary Sidelnikov sequence of period $p^m - 1$ and its constant multiple has the maximum magnitude of $\sqrt{p^m} + 3$.

To obtain a large number of distinct sequences, Sidelnikov sequences can be employed in constructing a polyphase sequence family. The efforts on the family have been initiated by Guohua and Quan's observation [3] on the correlation properties of the binary sequences obtained by the *shift-and-addition* of Legendre sequences of prime period p. In [17], Rushanan applied the Weil bound to theoretically prove that the correlation magnitude of the sequences is bounded by $2\sqrt{p}+5$. Inspired by [4] and [17], Kim *et al.* [10] then constructed M-ary sequence families from the shift and addition of Sidelnikov sequences. In [5], Han and Yang summarized the known constructions, and using the same technique $-$ shift and addition, they further constructed M-ary sequence families with larger size than the known ones, but the same maximum correlation magnitude. Recently, Yu and Gong [23] presented general constructions for some of known families by providing more efficient proofs on the maximum correlation magnitudes employing the refined Weil bound. They also generalized the constructions by the addition of multiple cyclic shifts of Sidelnikov sequences. For more details on this topic including *power residue sequences*, see [4], [5], [8], [9], [10], and [23].

This paper studies the structure of Sidelnikov sequences and presents new construction of polyphase sequence families from the structure. For prime p and a positive integer m, we show that M-ary Sidelnikov sequences of period $p^{2m} - 1$, if $M \mid p^m - 1$, can be equivalently generated by the operation of elements in a finite field $\mathrm{GF}(p^m)$, including a p^m-ary m-sequence of period $p^{2m}-1$. The equivalent representation over $\mathrm{GF}(p^m)$ requires low complexity for implementing the Sidelnikov sequences of period $p^{2m} - 1$. Investigating the $(p^m - 1) \times (p^m + 1)$ array structure of the sequences, we then discover that a half of the column sequences and their constant multiples have low correlation enough to construct new M-ary sequence families of period $p^m - 1$, where each family has the maximum correlation magnitude of $2\sqrt{p^m} + 2$ (for even M) and $3\sqrt{p^m} + 1$, respectively. Moreover, we construct new M-ary sequence families of period p^m-1 by combining the column sequence families with some known Sidelnikov-based

sequence families in [5] and [10]. The new sequence families provide larger family sizes than the known ones with the same maximum correlation magnitudes. Finally, we show that the new M-ary sequence family of period $p^m - 1$ and the maximum correlation magnitude $2\sqrt{p^m} + 6$ asymptotically achieves $\sqrt{2}$ times the equality of the Sidelnikov's lower bound [19] when $M = p^m - 1$ for odd prime p.

The rest of this paper is organized as follows. In Section II, we give preliminaries for this work by describing definitions and concepts. Section III studies the structure of M-ary Sidelnikov sequences of period $p^{2m} - 1$ for $M \mid p^m - 1$, discussing the equivalent representation, the array structure, and correlations of the column sequences. In Section IV, we consider M-ary sequence families of period $p^m - 1$ by employing the column sequences described in Section III. Moreover, we combine the sequence families with known Sidelnikov-based families for constructing new M-ary sequence families with the same maximum correlation magnitudes as the known ones, but larger family sizes. Finally, we examine the asymptotic behavior of our new sequence family for odd prime p and $M = p^m - 1$, comparing it to the Sidelnikov bound. Concluding remarks are given in Section V.

II. Preliminaries

This section describes basic definitions and concepts for understanding the work in this paper. The following notations will be used throughout this paper.

- $\omega_M = e^{j\frac{2\pi}{M}}$ is a primitive M-th root of unity, where $j = \sqrt{-1}$.
- $\mathbb{F}_q = \mathrm{GF}(q)$ is a finite field with q elements and $\mathbb{F}_q^*$ denotes a multiplicative group of $\mathbb{F}_q$.
- $\mathbb{F}_q[x]$ is a polynomial ring over $\mathbb{F}_q$, where each coefficient of a polynomial $f(x) \in \mathbb{F}_q[x]$ is an element of $\mathbb{F}_q$.
- Let p be prime, and n and m be positive integers, where $m \mid n$. A *trace function* from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is defined by $\mathrm{Tr}_m^n(x)$, i.e.,

$$\mathrm{Tr}_m^n(x) = x + x^{p^m} + \cdots + x^{p^{m(\frac{n}{m}-1)}}, \quad x \in \mathbb{F}_{p^n}.$$

- For an element x in $\mathbb{F}_q$, a *logarithm* over $\mathbb{F}_q$ is defined by

$$\log_\alpha x = \begin{cases} t, & \text{if } x = \alpha^t,\ 0 \le t \le q-2, \\ 0, & \text{if } x = 0 \end{cases}$$

where α is a primitive element in $\mathbb{F}_q$.

A. Multiplicative characters

Let α be a primitive element of $\mathbb{F}_q$ and M a divisor of $q-1$, i.e., $M \mid q-1$. A *multiplicative character* [15] of $\mathbb{F}_q$ of order M is defined by

$$\psi(x) = \begin{cases} \exp\left(j\frac{2\pi t}{M}\right), & \text{if } x = \alpha^t,\ 0 \le t \le q-2 \\ 0, & \text{if } x = 0 \end{cases} \tag{1}$$

where it is the convention to assume $\psi(0) = 0$ [15]. If $M = 1$, then $\psi(\alpha^t) = 1$ for any integer t, which is trivial. Thus, we assume $M > 1$ for *nontrivial* multiplicative characters. For an integer $c,\ 1 \le c \le M-1$, $\psi^c(x) = \psi_1(x)$ is also a nontrivial multiplicative character with $2 \le \mathrm{ord}(\psi_1) \le M$, where $\mathrm{ord}(\psi_1)$ denotes the order of ψ_1, or the smallest positive integer d such that $\psi_1^d(x) = 1$ for all $x \in \mathbb{F}_q^*$. For the general definition of a multiplicative character, see Theorem 5.8 in [15].

From (1), it is straightforward to define the multiplicative character by a logarithm over finite fields.

Definition 1: A multiplicative character of $\mathbb{F}_q$ of order M is defined by

$$\psi(x) = \exp\left(j\frac{2\pi \log_\alpha x}{M}\right), \quad x \in \mathbb{F}_q \tag{2}$$

where $\psi(0) = 1$ by definition of the log operation.

In (2), note that $\psi(0) = 1$, which contradicts the conventional assumption in (1). In this paper, however, we keep the assumption of $\psi(0) = 1$ to maintain the definition of (2), which will be useful in representing Sidelnikov sequences in a simple form by multiplicative characters.

From basic log operations, multiplicative characters have some properties as follows.

a) $\psi(x^c) = \psi^c(x)$, where $x \in \mathbb{F}_q$ and c is constant,

b) $\psi(x)\psi(y) = \psi(xy)$, where $x, y \in \mathbb{F}_q^*$,

c) $\psi(x)\psi^{-1}(y) = \psi\left(\frac{x}{y}\right)$, where $x, y \in \mathbb{F}_q^*$

where we assume $0^c = 0$ for any constant c. Throughout this paper, $\psi(x)$ may be denoted as ψ if the context is clear.

B. Sidelnikov sequences

Sidelnikov [18] introduced a polyphase sequence with low periodic autocorrelation. We present its definition by a logarithm as well as the original one.

Definition 2: Let $\mathbb{F}_q$ be a finite field with $q = p^m$ and M a divisor of $q-1$, i.e., $M \mid q-1$, where p is prime and m is a positive integer. Let α be a primitive element in $\mathbb{F}_q$. Let $D_k = \{\alpha^{Mi+k} - 1 \mid 0 \le i < \frac{q-1}{M}\}$

for $0 \le k \le M-1$. The M-ary Sidelnikov sequence $\mathbf{s} = \{s(t) \mid 0 \le t \le q-2\}$ of period $q-1$ is defined by

$$s(t) = \begin{cases} 0, & \text{if } \alpha^t = -1 \\ k, & \text{if } \alpha^t \in D_k. \end{cases}$$

Equivalently, $s(t)$ is defined by

$$s(t) \equiv \log_\alpha(\alpha^t + 1) \mod M, \quad 0 \le t \le q-2. \tag{3}$$

By (2) and (3), the modulated sequence of $s(t)$ is represented by

$$\omega_M^{s(t)} = \psi(\alpha^t + 1), \quad 0 \le t \le q-2 \tag{4}$$

where $\psi(0) = 1$. (4) represents Sidelnikov sequences in a simple form by multiplicative characters, without the indicator function $I(x)$ used in [5] and [10].

Given the notations in Definition 2, we consider the polynomial representations of Sidelnikov sequences. Let $s(t)$ be an M-ary Sidelnikov sequence of period $q-1$. With a polynomial $S(x) = x+1$ in $\mathbb{F}_q$,

$$s(t) \equiv \log_\alpha S(\alpha^t) \mod M, \quad \omega_M^{s(t)} = \psi\left(S(\alpha^t)\right)$$

where $0 \le t \le q-2$. In this case, $s(t)$ is said to have the *polynomial representation* $S(x)$.

C. Correlations and sequence families

Let $\mathbf{a} = \{a(t)\}$ and $\mathbf{b} = \{b(t)\}$ be M-ary sequences of period L, where $0 \le t \le L-1$. A (periodic) correlation of sequences $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{t=0}^{L-1} \omega_M^{a(t)-b(t+\tau)}, \quad 0 \le \tau \le L-1$$

where the indices are computed modulo L. If $\mathbf{a}$ and $\mathbf{b}$ are *cyclically equivalent*, i.e., $a(t) = b(t+l)$ for all t's and an integer l, then $C_{\mathbf{a},\mathbf{b}}(\tau)$ becomes the *autocorrelation* of $\mathbf{a}$. Otherwise, if $\mathbf{a}$ and $\mathbf{b}$ are *cyclically distinct*, then $C_{\mathbf{a},\mathbf{b}}(\tau)$ is the *cross-correlation* of $\mathbf{a}$ and $\mathbf{b}$.

Let $\mathcal{S} = \{\mathbf{s}^{(0)}, \cdots, \mathbf{s}^{(N-1)}\}$ be a set of N cyclically distinct M-ary sequences of period L, and $C_{\max}(\mathcal{S})$ be defined by

$$C_{\max}(\mathcal{S}) = \max \left| C_{\mathbf{s}^{(i)},\mathbf{s}^{(j)}}(\tau) \right| \text{ for any } 0 \le \tau \le L-1,\ 0 \le i,j \le N-1$$

where $\tau \ne 0$ if $i = j$. Clearly, $C_{\max}(\mathcal{S})$ is the maximum of all nontrivial auto- and cross-correlations of pairs of sequences in $\mathcal{S}$. Then, the set $\mathcal{S}$ is called an *M-ary sequence family* of period L, where N is the *family size* and $C_{\max}(\mathcal{S})$ is the *maximum correlation magnitude* of $\mathcal{S}$. The sequence family $\mathcal{S}$ is

said to have *low correlation* if $C_{\max}(\mathcal{S}) \leq v\sqrt{L} + \epsilon$ for small constants v and ϵ. For more details on correlation and sequence families, see [1] and [7].

D. The Weil bound

The Weil bound [22] gives the upper bound on the magnitude of character sums (or exponential sums). It has been widely employed in determining the maximum correlation magnitude of a sequence family since the correlation of sequences is ultimately equivalent to a character sum. For the applications of exponential sums to sequence and coding theory, see [16].

Based on the Weil bound described in [21], we introduce the refined version (Corollary 1 in [23]) supporting the assumption $\psi_i(0) = 1$, which conforms to (4).

Proposition 1: [23] Let $f_1(x), \cdots, f_l(x)$ be l monic and irreducible polynomials in $\mathbb{F}_q[x]$ which have positive degrees $d_1, \cdots, d_l$, respectively. Let $\psi_1, \cdots, \psi_l$ be multiplicative characters of $\mathbb{F}_q$. Assume the product character $\prod_{i=1}^{l} \psi_i(f_i(x))$ is nontrivial, i.e., $\prod_{i=1}^{l} \psi_i(f_i(x)) \neq 1$ for all $x \in \mathbb{F}_q$. Let e_i be the number of distinct roots in $\mathbb{F}_q$ of $f_i(x)$, where $i = 1, \cdots, l$. If $\psi_i(0) = 1$ for each i, then for every $a_i \in \mathbb{F}_q^*$, we have

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_l f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \leq \left(\sum_{i=1}^{l} d_i - 1 \right) \sqrt{q} + \sum_{i=1}^{l} e_i. \tag{5}$$

In particular, if $\prod_{i=1}^{l} \psi_i^{d_i}(x) = 1$ for all $x \in \mathbb{F}_q^*$, then

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \leq \left(\sum_{i=1}^{l} d_i - 2 \right) \sqrt{q} + 1 + \sum_{i=1}^{l} e_i. \tag{6}$$

Proposition 1 turns out to be very useful in determining the maximum correlation magnitude of a sequence family represented by multiplicative characters, where we only need to take into account the degrees and the number of roots in $\mathbb{F}_q$ of each $f_i(x)$, a polynomial corresponding to a sequence or its cyclic shift.

III. The Structure of Sidelnikov Sequences

In this section, we study the structure of M-ary Sidelnikov sequences of period $p^{2m} - 1$, where $M \mid p^m - 1$. Throughout this section, $n = 2m$, α is a primitive element in $\mathbb{F}_{p^n}$ and $\beta = \alpha^{p^m+1}$ is a primitive element in $\mathbb{F}_{p^m}$.

A. Equivalent representation of Sidelnikov sequences

Theorem 1: An M-ary Sidelnikov sequence $\mathbf{s} = \{s(t)\}$ of period $p^{2m}-1$, if $M \mid p^m-1$, is equivalently represented by

$$s(t) \equiv \log_\beta \left(\beta^t + \mathrm{Tr}_m^n(\alpha^t) + 1\right) \mod M, \quad 0 \le t \le p^{2m}-2. \tag{7}$$

In other words, $s(t)$ is equivalently defined by

$$s(t) = \begin{cases} 0, & \text{if } \beta^t + \mathrm{Tr}_m^n(\alpha^t) = -1 \\ k, & \text{if } \beta^t + \mathrm{Tr}_m^n(\alpha^t) \in L_k \end{cases}, \quad 0 \le t \le p^{2m}-2 \tag{8}$$

where $L_k = \{\beta^{Mi+k} - 1 \mid 0 \le i < \frac{p^m-1}{M}\}$ for $0 \le k \le M-1$.

Proof: Let $w(t) = \log_\alpha(\alpha^t + 1)$ where $s(t) \equiv w(t) \pmod M$ from (3). Then,

$$\begin{aligned} (p^m+1)\cdot w(t) &\equiv (p^m+1)\cdot \log_\alpha(\alpha^t+1) \\ &\equiv \log_\alpha(\alpha^t+1)^{p^m+1} \\ &\equiv \log_\alpha(\alpha^{t(p^m+1)} + \alpha^{tp^m} + \alpha^t + 1) \\ &\equiv \log_\alpha\left(\beta^t + \mathrm{Tr}_m^n(\alpha^t) + 1\right) \mod p^{2m}-1. \end{aligned} \tag{9}$$

From (9), let $\beta^t + \mathrm{Tr}_m^n(\alpha^t) + 1 = \beta^{u(t)} \in \mathbb{F}_{p^m}$. Then,

$$\begin{aligned} &(p^m+1)\cdot w(t) \equiv \log_\alpha \beta^{u(t)} \equiv \log_\alpha \alpha^{(p^m+1)\cdot u(t)} \equiv (p^m+1)\cdot u(t) \mod p^{2m}-1 \\ \Rightarrow\ &(p^m+1)\cdot(w(t)-u(t)) \equiv 0 \mod p^{2m}-1 \\ \Rightarrow\ &w(t)-u(t) \equiv 0 \mod p^m-1. \end{aligned} \tag{10}$$

If $M \mid p^m-1$, then (10) implies

$$\begin{aligned} &w(t)-u(t) \equiv 0 \mod M \\ \Rightarrow\ &s(t) \equiv w(t) \equiv u(t) \equiv \log_\beta\left(\beta^t + \mathrm{Tr}_m^n(\alpha^t)+1\right) \mod M. \end{aligned}$$

Also, (8) is straightforward from (7), □

Theorem 1 shows the remarkable equivalence from which an M-ary Sidelnikov sequence of period $p^{2m}-1$, if $M \mid p^m-1$, can be determined by the elements of subfield $\mathbb{F}_{p^m}$, including a p^m-ary m-sequence corresponding to $\mathrm{Tr}_m^n(\alpha^t)$. The equivalent representation by the subfield elements therefore allows the efficient implementation of the M-ary Sidelnikov sequence with low complexity. Figure 1 illustrates the implementation by the subfield elements β^t+1 and a p^m-ary m-sequence generated by a 2-stage linear feedback shift register (LFSR). In the figure, note that the feedback configuration of the LFSR is determined by the primitive polynomial of degree 2 over $\mathbb{F}_{p^m}$ that defines $\mathbb{F}_{p^{2m}}$.

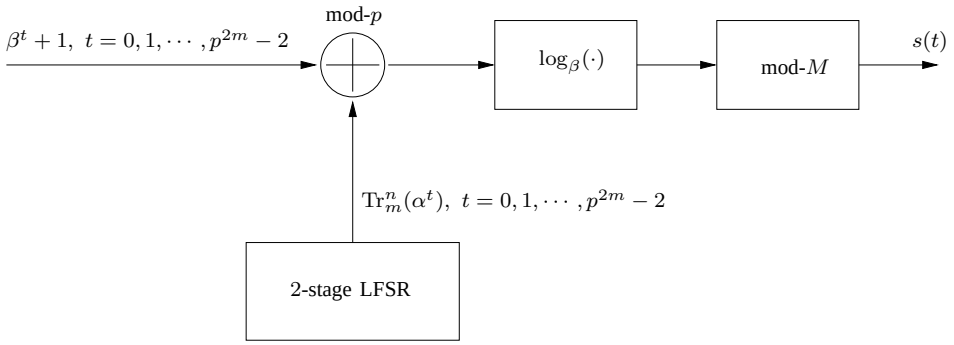

Fig. 1. The LFSR implementation of an M-ary Sidelnikov sequence of period $p^{2m}-1$, where $M \mid p^m-1$.

B. Array structure and the column sequences

In [2], Gong introduced the array (or interleaved) structure of a general sequence and presented new sequence families by exploiting the structure. Similarly, we consider the $(p^m-1)\times(p^m+1)$ array of the M-ary Sidelnikov sequence in Theorem 1.

Theorem 2: Let p be prime, m a positive integer, and $M \mid p^m-1$. Let $\mathbf{s}=\{s(t)\}$ be the M-ary Sidelnikov sequence of period $p^{2m}-1$ in Theorem 1. Let $v_l(t)$ be the l-th column sequence in the $(p^m-1)\times(p^m+1)$ array of $\mathbf{s}$, i.e,

$$v_l(t)=s\left((p^m+1)\cdot t+l\right),\quad 0\le l\le p^m,\ 0\le t\le p^m-2. \tag{11}$$

Then, $v_0(t)$ is either all zero sequence if $M=2$, or a multiple of an M-ary Sidelnikov sequence of period p^m-1 if $M>2$. For $1\le l\le\left\lfloor\frac{p^m+1}{2}\right\rfloor$, on the other hand, we have

$$v_{p^m+1-l}(t)=v_l(t-l+1). \tag{12}$$

In other words, $v_l(t),\ 1\le l\le\lfloor\frac{p^m}{2}\rfloor$ is cyclically equivalent to $v_{p^m+1-l}(t)$. In particular, if $l=\frac{p^m+1}{2}$ for odd prime p, then (12) implies that the column sequence $v_{\frac{p^m+1}{2}}(t)$ has a period of $\frac{p^m-1}{2}$.

Proof: By (7) and (11), $v_l(t)$ is given by

$$\begin{aligned} v_l(t) &\equiv \log_\beta\left(\beta^{(p^m+1)t+l}+\mathrm{Tr}_m^n\left(\alpha^{(p^m+1)t+l}\right)+1\right)\\ &\equiv \log_\beta\left(\beta^{2t+l}+\beta^t\cdot\mathrm{Tr}_m^n(\alpha^l)+1\right)\mod M,\quad 0\le t\le p^m-2. \end{aligned} \tag{13}$$

where $\beta^{p^m+1}=\beta^2$. If $l=0$, the column sequence $v_0(t)$ becomes

$$v_0(t)\equiv\log_\beta(\beta^t+1)^2\equiv 2\cdot\log_\beta(\beta^t+1)\mod M.$$

Thus, $v_0(t)$ is either all zero sequence ($M = 2$) or a twice of an M-ary Sidelnikov sequence of period $p^m - 1$ ($M > 2$). On the other hand, if $1 \le l \le \left\lfloor \frac{p^m+1}{2} \right\rfloor$, then from (13),

$$\begin{aligned} v_{p^m+1-l}(t) &\equiv \log_\beta \left(\beta^{2t+p^m+1-l} + \beta^t \cdot \mathrm{Tr}_m^n(\alpha^{p^m+1-l}) + 1 \right) \\ &\equiv \log_\beta \left(\beta^{2(t+1)-l} + \beta^t \cdot \mathrm{Tr}_m^n(\alpha^{p^{2m}+p^m-lp^m}) + 1 \right) \\ &\equiv \log_\beta \left(\beta^{2(t+1)-l} + \beta^{t+1} \cdot \mathrm{Tr}_m^n(\alpha^{-lp^m-l+l}) + 1 \right) \\ &\equiv \log_\beta \left(\beta^{2(t-l+1)+l} + \beta^{t-l+1} \cdot \mathrm{Tr}_m^n(\alpha^l) + 1 \right) \mod M \\ &= v_l(t-l+1) \end{aligned}$$

Therefore, $v_l(t),\ 1 \le l \le \left\lfloor \frac{p^m}{2} \right\rfloor$ turns out to be cyclically equivalent to $v_{p^m+1-l}(t)$. In particular, if $l = \frac{p^m+1}{2}$ for odd prime p, then

$$v_{\frac{p^m+1}{2}}(t) = v_{\frac{p^m+1}{2}} \left(t - \frac{p^m-1}{2} \right)$$

which implies that the column sequence $v_{\frac{p^m+1}{2}}(t)$ has a period of $\frac{p^m-1}{2}$. □

Example 1: Let $p = 7,\ m = 1$, and $M = 6$. Consider a finite field $\mathbb{F}_{7^2}$ defined by a primitive polynomial $p(x) = x^2 + x + 3$. Then, a 6-ary Sidelnikov sequence $s(t)$ of period $7^2 - 1 = 48$ is represented by a 6×8 array as follows.

$$s(t) = [v_0(t),\ v_1(t),\ \cdots,\ v_7(t)] = \begin{bmatrix} 4 & 1 & 5 & 0 & 5 & 1 & 5 & 1 \\ 2 & 4 & 4 & 2 & 2 & 2 & 5 & 4 \\ 2 & 4 & 3 & 3 & 1 & 0 & 4 & 4 \\ 0 & 5 & 0 & 3 & 5 & 2 & 3 & 5 \\ 4 & 1 & 3 & 1 & 2 & 3 & 0 & 1 \\ 0 & 0 & 5 & 2 & 1 & 3 & 3 & 0 \end{bmatrix}.$$

In the array, $v_0(t) \equiv 2s'(t) \pmod 6$, where $s'(t) = \{2, 4, 1, 0, 5, 3\}$ is a 6-ary Sidelnikov sequence of period 6. We also see that $v_7(t) = v_1(t),\ v_6(t) = v_2(t-1)$, and $v_5(t) = v_3(t-2)$, respectively, and $v_4(t)$ has a short period of 3, as described in Theorem 2.

C. Correlations of the column sequences

In Theorem 2, it is $v_l(t),\ 1 \le l \le \left\lfloor \frac{p^m}{2} \right\rfloor$ that attracts our attention as a set of new M-ary sequences. In the following, we establish a formal definition of the sequences.

Definition 3: Let p be prime, m a positive integer, and $M \mid p^m-1$. Let $V_k=\{\beta^{Mi+k}-1 \mid 0 \le i < \frac{p^m-1}{M}\}$ for $0 \le k \le M-1$. For $1 \le l \le \left\lfloor \frac{p^m}{2} \right\rfloor$, an M-ary sequence $v_l(t)$ of period p^m-1 is defined by

$$v_l(t)=\begin{cases} 0, & \text{if } \beta^{2t+l}+\beta^t \cdot \mathrm{Tr}_m^n(\alpha^l)=-1 \\ k, & \text{if } \beta^{2t+l}+\beta^t \cdot \mathrm{Tr}_m^n(\alpha^l) \in V_k \end{cases}, \quad 0 \le t \le p^m-2.$$

By the log operation, $v_l(t)$ is equivalently defined by

$$v_l(t) \equiv \log_\beta \left(\beta^{2t+l}+\beta^t \cdot \mathrm{Tr}_m^n(\alpha^l)+1\right) \mod M, \quad 0 \le t \le p^m-2.$$

The polynomial representation of $v_l(t)$ is given by

$$V_l(x)=\beta^l x^2+\mathrm{Tr}_m^n(\alpha^l)\cdot x+1, \quad x \in \mathbb{F}_{p^m}^* \tag{14}$$

where

$$v_l(t) \equiv \log_\beta V_l(\beta^t) \mod M, \quad \omega_M^{v_l(t)}=\psi\left(V_l(\beta^t)\right), \quad 0 \le t \le p^m-2.$$

A set of $v_l(t)$ and its constant multiples is denoted as

$$\mathcal{S}_{\mathbf{v}}=\left\{c_0 v_l(t) \mid 1 \le c_0 \le M-1,\ 1 \le l \le \left\lfloor \frac{p^m}{2} \right\rfloor\right\}.$$

We now show that a pair of sequences in $\mathcal{S}_{\mathbf{v}}$ is cyclically distinct.

Theorem 3: In Definition 3, each pair of sequences in $\mathcal{S}_{\mathbf{v}}$ is cyclically distinct.

Before proving Theorem 3, we consider the following lemma.

Lemma 1: Let $1 \le l_1, l_2 \le \left\lfloor \frac{p^m}{2} \right\rfloor$. For $0 \le \tau \le p^m-2$, let $V_{l_1}(x)$ and $V_{l_2}(\beta^\tau x)$ be the polynomial representations for $v_{l_1}(t)$ and $v_{l_2}(t+\tau)$, respectively. Then, each of $V_{l_1}(x)=0$ and $V_{l_2}(\beta^\tau x)=0$ has two distinct roots in $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ for any τ, which implies that each polynomial has no roots in $\mathbb{F}_{p^m}$.

Proof: From (14), the polynomial representations are given by

$$\begin{aligned} V_{l_1}(x)&=\beta^{l_1}x^2+\mathrm{Tr}_m^n(\alpha^{l_1})\cdot x+1=(\alpha^{l_1}x+1)\cdot(\alpha^{l_1 p^m}x+1) \\ V_{l_2}(\beta^\tau x)&=\beta^{l_2+2\tau}x^2+\mathrm{Tr}_m^n(\alpha^{l_2})\cdot \beta^\tau x+1=(\alpha^{l_2}\beta^\tau x+1)\cdot(\alpha^{l_2 p^m}\beta^\tau x+1) \end{aligned} \tag{15}$$

where $\alpha \in \mathbb{F}_{p^{2m}}$ and $\beta=\alpha^{p^m+1} \in \mathbb{F}_{p^m}$. Clearly, the roots of $V_{l_1}(x)=0$ are $x_1=-\alpha^{-l_1}$ and $x_2=-\alpha^{-l_1 p^m}$, respectively. In the exponents, $-l_1 \not\equiv 0 \pmod{p^m+1}$ and $-l_1 p^m \equiv l_1 \not\equiv 0 \pmod{p^m+1}$ for $1 \le l_1 \le \left\lfloor \frac{p^m}{2} \right\rfloor$, which implies $\alpha^{-l_1},\ \alpha^{-l_1 p^m} \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$. As -1 (or 1 if $p=2$) is an element in $\mathbb{F}_{p^m}$, it is straightforward that $x_1, x_2 \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$. Hence, $V_{l_1}(x)=0$ has no roots in $\mathbb{F}_{p^m}$. Note that $x_1 \neq x_2$ since $l_1 \not\equiv l_1 p^m \pmod{p^{2m}-1}$ for $1 \le l_1 \le \left\lfloor \frac{p^m}{2} \right\rfloor$.

Similarly, the roots of $V_{l_2}(\beta^\tau x)=0$ are $x_1'=-\alpha^{-l_2-(p^m+1)\tau}$ and $x_2'=-\alpha^{-l_2p^m-(p^m+1)\tau}$, respectively, where $-l_2-(p^m+1)\tau\equiv -l_2\not\equiv 0 \pmod{p^m+1}$ and $-l_2p^m-(p^m+1)\tau\equiv l_2\not\equiv 0 \pmod{p^m+1}$ for $1\le l_2\le \lfloor\frac{p^m}{2}\rfloor$. Thus, $x_1', x_2'\in\mathbb{F}_{p^{2m}}\setminus\mathbb{F}_{p^m}$, and $V_{l_2}(\beta^\tau x)=0$ has no roots in $\mathbb{F}_{p^m}$ for any τ. Also, $x_1'\neq x_2'$ since $l_2\not\equiv l_2p^m \pmod{p^{2m}-1}$ for $1\le l_2\le\lfloor\frac{p^m}{2}\rfloor$. □

Proof of Theorem 3: Let $\mathbf{a}=\{c_1v_{l_1}(t)\}$ and $\mathbf{b}=\{c_2v_{l_2}(t)\}$ where $1\le l_1,l_2\le\lfloor\frac{p^m}{2}\rfloor$ and $1\le c_1,c_2\le M-1$. In the sequence pair, we define $E_{\mathbf{a},\mathbf{b}}(\tau)$ by

$$\begin{aligned} E_{\mathbf{a},\mathbf{b}}(\tau) &= \omega_M^{c_1v_{l_1}(t)-c_2v_{l_2}(t+\tau)}, \quad 0\le\tau\le p^m-2 \\ &= \psi\left(V_{l_1}(x)^{c_1}\right)\cdot\psi\left(V_{l_2}(\beta^\tau x)^{M-c_2}\right), \quad x\in\mathbb{F}_{p^m}^* \end{aligned} \tag{16}$$

where $V_{l_1}(x)$ and $V_{l_2}(\beta^\tau x)$ are given in (15). From Lemma 1, $V_{l_1}(x)^{c_1}=0$ and $V_{l_2}(\beta^\tau x)^{M-c_2}=0$ have no roots in $\mathbb{F}_{p^m}^*$, respectively. Then, (16) is represented as

$$E_{\mathbf{a},\mathbf{b}}(\tau)=\psi\left(V_{l_1}(x)^{c_1}\cdot V_{l_2}(\beta^\tau x)^{M-c_2}\right)=\psi\left(g(x)\right). \tag{17}$$

In (17), the sequence pair $\mathbf{a}$ and $\mathbf{b}$ are cyclically equivalent if and only if $g(x)=h(x)^M$ so that $\psi(g(x))$ may be a trivial character, where $h(x)\in\mathbb{F}_{p^m}[x]$. Therefore, we need to show $g(x)\neq h(x)^M$ for the cyclic distinctness of the pair $\mathbf{a}$ and $\mathbf{b}$. In $g(x)$, note that neither $V_{l_1}(x)^{c_1}$ nor $V_{l_2}(\beta^\tau x)^{M-c_2}$ is of the form $h'(x)^M$ for $h'(x)\in\mathbb{F}_{p^m}[x]$, because each one has distinct roots and $1\le c_1,c_2\le M-1$. Thus, if $V_{l_1}(x)\neq V_{l_2}(\beta^\tau x)$, then each factor causes $g(x)\neq h(x)^M$ for any c_1 and c_2.

Case 1. $\tau=0$: Comparing each coefficient of $V_{l_1}(x)$ and $V_{l_2}(x)$, it is clear that $g(x)=h(x)^M$ if and only if $l_1=l_2$ and $c_1=c_2$, where $\mathbf{a}=\mathbf{b}$, a trivial case.

Case 2. $0<\tau\le p^m-2$: Since $1\le l_1,l_2\le\lfloor\frac{p^m}{2}\rfloor$, $\alpha^{l_1}\neq\alpha^{l_2+(p^m+1)\tau}=\alpha^{l_2}\beta^\tau$ for any $\tau\neq 0$. Also, $l_1-l_2p^m\equiv l_1+l_2\not\equiv 0 \pmod{p^m+1}$, which implies $\alpha^{l_1}\neq\alpha^{l_2p^m+(p^m+1)\tau}=\alpha^{l_2p^m}\beta^\tau$ for any $\tau\neq 0$. Thus, $(\alpha^{l_1}x+1)$ in $V_{l_1}(x)$ cannot be identical to either $(\alpha^{l_2}\beta^\tau x+1)$ or $(\alpha^{l_2p^m}\beta^\tau x+1)$ in $V_{l_2}(\beta^\tau x)$. Therefore, $V_{l_1}(x)\neq V_{l_2}(\beta^\tau x)$ for any $\tau\neq 0$, and thus $g(x)\neq h(x)^M$.

From Cases 1 and 2, $E_{\mathbf{a},\mathbf{b}}(\tau)\neq 1$ for all x's. Finally, each pair of the column sequences $v_l(t),\ 0\le l\le\lfloor\frac{p^m}{2}\rfloor$ is cyclically distinct. □

Next, we study the correlation of a pair of sequences in $\mathcal{S}_{\mathbf{v}}$.

Theorem 4: Let $\mathbf{a}=\{c_1v_{l_1}(t)\}$ and $\mathbf{b}=\{c_2v_{l_2}(t)\}$ be a pair of sequences from $\mathcal{S}_{\mathbf{v}}$ in Definition 3, where $1\le c_1,c_2\le M-1$ and $1\le l_1,l_2\le\lfloor\frac{p^m}{2}\rfloor$. The correlation magnitude of $\mathbf{a}$ and $\mathbf{b}$ is bounded by

$$|C_{\mathbf{a},\mathbf{b}}(\tau)|\le 3\sqrt{p^m}+1. \tag{18}$$

In particular, if $c_1 = c_2$ or $c_1 - c_2 \equiv \frac{M}{2} \pmod M$, then

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \le 2\sqrt{p^m} + 2 \tag{19}$$

where $c_1 - c_2 \equiv \frac{M}{2} \pmod M$ is valid for even M and odd prime p. In (18) and (19), $0 \le \tau \le p^m - 2$, and $\tau \neq 0$ if $l_1 = l_2$ and $c_1 = c_2$.

Proof: With $V_{l_1}(x)$ and $V_{l_2}(\beta^\tau x)$ given in (15), $C_{\mathbf{a},\mathbf{b}}(\tau)$ is determined by

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p^m-1} \omega_M^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t+\tau)}, \quad 0 \le \tau \le p^m - 2 \\ &= \sum_{x \in \mathbb{F}_{p^m}^*} \psi^{c_1}\left(V_{l_1}(x)\right) \cdot \psi^{-c_2}\left(V_{l_2}(\beta^\tau x)\right) \\ &= \sum_{x \in \mathbb{F}_{p^m}} \psi_1\left(\beta^{l_1} f_1(x)\right) \cdot \psi_2\left(\beta^{l_2+2\tau} f_2(x)\right) - 1 \end{aligned}$$

where $\psi_1 = \psi^{c_1}$, $\psi_2 = \psi^{-c_2} = \psi^{M-c_2}$, and $f_1(x) = \beta^{-l_1} V_{l_1}(x)$, $f_2(x) = \beta^{-l_2-2\tau} V_{l_2}(\beta^\tau x)$. As each monic quadratic polynomial $f_i(x),\ i = 1, 2$ is irreducible in $\mathbb{F}_{p^m}$ and has distinct roots in $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ from Lemma 1, it is obvious that $d_1 = d_2 = 2$ and $e_1 = e_2 = 0$ in Proposition 1. Note that $\tau \neq 0$ if $\mathbf{a} = \mathbf{b}$. Then, the product character $\psi_1(\beta^{l_1} f_1(x)) \cdot \psi_2(\beta^{l_2+2\tau} f_2(x))$ is nontrivial from the cyclic distinctness of $\mathbf{a}$ and $\mathbf{b}$. With these parameters, we are now able to apply the bound of (5) in Proposition 1 to obtain

$$\begin{aligned} |C_{\mathbf{a},\mathbf{b}}(\tau)| &\le \left| \sum_{x \in \mathbb{F}_{p^m}} \psi_1\left(\beta^{l_1} f_1(x)\right) \cdot \psi_2\left(\beta^{l_2+2\tau} f_2(x)\right) \right| + 1 \\ &\le (d_1 + d_2 - 1)\sqrt{p^m} + e_1 + e_2 + 1 = 3\sqrt{p^m} + 1. \end{aligned}$$

In particular, if $c_1 = c_2$ or $c_1 - c_2 \equiv \frac{M}{2} \pmod M$ for even M, then

$$\prod_{i=1}^{2} \psi_i^{d_i}(x) = \psi^{2c_1 - 2c_2}(x) = 1$$

for all x in $\mathbb{F}_{p^m}^*$. Then, we can apply the improved bound (6) for the correlation, i.e.,

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \le (d_1 + d_2 - 2)\sqrt{p^m} + 1 + e_1 + e_2 + 1 = 2\sqrt{p^m} + 2.$$

□

IV. New M-ary Sequence Families

This section introduces new M-ary sequence families of period $p^m - 1$ with low correlation by employing the column sequence set $\mathcal{S}_{\mathbf{v}}$ described in Section III. Recall α is a primitive element in $\mathbb{F}_{p^{2m}}$ and $\beta = \alpha^{p^m+1}$ is a primitive element in $\mathbb{F}_{p^m}$.

A. Column sequence families

Construction 1: Let p be prime, m a positive integer, and $M \mid p^m-1$. Let $\mathbf{s} = \{s(t) \mid 0 \le t \le p^m-2\}$ be an M-ary Sidelnikov sequence of period p^m-1. Let $\mathcal{S}_{\mathbf{v}}$ be a set of the M-ary sequences of period p^m-1 in Definition 3. A new M-ary sequence family of period p^m-1 is defined by

$$\mathcal{V} = \mathcal{I}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}} = \{cs(t) \mid 1 \le c \le M-1\} \cup \left\{ c_0 v_l(t) \mid 1 \le c_0 \le M-1,\ 1 \le l \le \left\lfloor \frac{p^m}{2} \right\rfloor \right\}.$$

In particular, if M is even for odd prime p, then we define another new M-ary sequence family by

$$\begin{aligned}\mathcal{V}^{(c_1)} = \mathcal{I}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}}^{(c_1)} \cup \mathcal{S}_{\mathbf{v}}^{\left(c_1+\frac{M}{2}\right)} &= \{cs(t) \mid 1 \le c \le M-1\} \\ &\cup \left\{ c_1 v_{l_1}(t) \mid c_1 \text{ is fixed},\ 1 \le l_1 \le \frac{p^m-1}{2} \right\} \\ &\cup \left\{ \left(c_1+\frac{M}{2}\right) v_{l_2}(t) \mid 1 \le l_2 \le \frac{p^m-1}{2} \right\}\end{aligned}$$

where if $M > 2$, then $1 \le c_1 \le \frac{M}{2}-1$, and if $M = 2$, then $c_1 = 1$ and $\mathcal{S}_{\mathbf{v}}^{\left(c_1+\frac{M}{2}\right)} = \phi$.

Given the notations in Construction 1, the cyclic distinctness, the maximum correlation magnitudes, and the family sizes of $\mathcal{V}$ and $\mathcal{V}^{(c_1)}$ are shown in Theorems 5, 6, and 7, respectively.

Theorem 5: Each pair of sequences in $\mathcal{V}$ is cyclically distinct. As its subset, each pair in $\mathcal{V}^{(c_1)}$ is also cyclically distinct for any possible c_1.

Proof: In $\mathcal{V} = \mathcal{I}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}}$, it is obvious from [9] that all sequences in $\mathcal{I}_{\mathbf{s}}$ are cyclically distinct. Also, Theorem 3 has already proven the cyclic distinctness of sequences in $\mathcal{S}_{\mathbf{v}}$. Therefore, we only need to prove that a sequence pair from $\mathcal{I}_{\mathbf{s}}$ and $\mathcal{S}_{\mathbf{v}}$ is cyclically distinct.

Let $\mathbf{a} \in \mathcal{I}_{\mathbf{s}}$ and $\mathbf{b} \in \mathcal{S}_{\mathbf{v}}$. (or vice versa.) Then, $\mathbf{a} = \{cs(t)\}$ and $\mathbf{b} = \{c_0 v_l(t)\}$. Let $S(x) = x+1$ and $V_l(\beta^\tau x)$ in (14) be the polynomials for $s(t)$ and $v_l(t+\tau)$, respectively. In the sequence pair, $E_{\mathbf{a},\mathbf{b}}(\tau)$ is defined by

$$E_{\mathbf{a},\mathbf{b}}(\tau) = \omega_M^{cs(t)-c_0 v_l(t+\tau)} = \psi\left(S(x)^c\right) \cdot \psi\left(V_l(\beta^\tau x)^{M-c_0}\right), \quad 0 \le \tau \le p^m-2 \tag{20}$$

where $S(x)^c = 0$ at $x = -1$, whereas $V_l(\beta^\tau x)^{M-c_0} \ne 0$ for any x's in $\mathbb{F}_{p^m}^*$. For $x \ne -1$, (20) is represented as

$$E_{\mathbf{a},\mathbf{b}}(\tau) = \psi\left(S(x)^c V_l(\beta^\tau x)^{M-c_0}\right) = \psi\left(g(x)\right), \quad x \in \mathbb{F}_{p^m}^* \setminus \{-1\}. \tag{21}$$

For the cyclic distinctness of $\mathbf{a}$ and $\mathbf{b}$, it is sufficient to show $g(x) \ne h(x)^M$ for $h(x) \in \mathbb{F}_{p^m}[x]$, similar to the proof of Theorem 3. In (21), $S(x) \ne V_l(\beta^\tau x)$, and for $1 \le c, c_0 \le M-1$, neither

$S(x)^c$ nor $V_l(\beta^\tau x)^{M-c_0}$ is of the form $h'(x)^M$ for $h'(x) \in \mathbb{F}_{p^m}[x]$. Thus, it is clear that $g(x) \neq h(x)^M$. Consequently, $E_{\mathbf{a},\mathbf{b}}(\tau) \neq 1$ for all x's, and each sequence pair from $\mathcal{I}_\mathbf{s}$ and $\mathcal{S}_\mathbf{v}$ is cyclically distinct. Finally, each sequence pair in $\mathcal{V}$ is cyclically distinct, and so is each pair in $\mathcal{V}^{(c_1)}$, a subset of $\mathcal{V}$. □

Theorem 6: The maximum correlation magnitudes of $\mathcal{V}$ and $\mathcal{V}^{(c_1)}$ are determined by

$$C_{\max}(\mathcal{V}) = 3\sqrt{p^m} + 1, \qquad C_{\max}\left(\mathcal{V}^{(c_1)}\right) = 2\sqrt{p^m} + 2.$$

Proof: Let $\mathbf{a}$ and $\mathbf{b}$ be a pair of sequences in $\mathcal{V}$ (or $\mathcal{V}^{(c_1)}$). The maximum correlation magnitude of the pair is computed for the following cases, where we employ the notations in Proposition 1. In each case, we exclude a trivial in-phase autocorrelation of $\tau = 0$ at $\mathbf{a} = \mathbf{b}$, which drives each product character in $C_{\mathbf{a},\mathbf{b}}(\tau)$ to be nontrivial.

Case 1. $\mathbf{a}, \mathbf{b} \in \mathcal{I}_\mathbf{s}$: In this case, $\mathbf{a} = \{cs(t)\}$ and $\mathbf{b} = \{c's(t)\}$ each of which is a constant multiple of an M-ary Sidelnikov sequence of period $p^m - 1$. From [9], the correlation of the pair is given by

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq \begin{cases} 4, & \text{if } c = c' \\ \sqrt{p^m} + 3, & \text{if } c \neq c'. \end{cases}$$

Case 2. $\mathbf{a} \in \mathcal{I}_\mathbf{s}$ and $\mathbf{b} \in \mathcal{S}_\mathbf{v}$ (or $\mathbf{b} \in \mathcal{S}_\mathbf{v}^{\left(c_1 + i\frac{M}{2}\right)},\ i = 0, 1.$): If $\mathbf{a} \in \mathcal{I}_\mathbf{s}$ and $\mathbf{b} \in \mathcal{S}_\mathbf{v}$ (or vice versa), then $\mathbf{a} = \{cs(t)\}$ and $\mathbf{b} = \{c_0 v_l(t)\}$. With the polynomials $S(x) = x + 1$ and $V_l(x)$ in (14), the correlation of $\mathbf{a}$ and $\mathbf{b}$ is given by

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{x \in \mathbb{F}_{p^m}^*} \psi^c\left(S(x)\right) \cdot \psi^{-c_0}\left(V_l(\beta^\tau x)\right) \\ &= \sum_{x \in \mathbb{F}_{p^m}} \psi_1\left(f_1(x)\right) \cdot \psi_2\left(\beta^{l+2\tau} f_2(x)\right) - 1 \end{aligned}$$

where $\psi_1 = \psi^c$ and $\psi_2 = \psi^{-c_0} = \psi^{M-c_0}$. The monic polynomial $f_1(x) = S(x)$ has a single root in $\mathbb{F}_{p^m}$. On the other hand, $f_2(x) = \beta^{-l-2\tau} V_l(\beta^\tau x)$ is a monic quadratic polynomial in $\mathbb{F}_{p^m}[x]$, where its roots are distinct in $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ from Lemma 1. Obviously, each polynomial is irreducible in $\mathbb{F}_{p^m}$. With the notations of Proposition 1, it is therefore clear that $d_1 = 1$, $d_2 = 2$ and $e_1 = 1$, $e_2 = 0$. The cyclic distinctness of $\mathbf{a}$ and $\mathbf{b}$ guarantees that the product character $\psi_1\left(f_1(x)\right) \cdot \psi_2\left(\beta^{l+2\tau} f_2(x)\right)$ is nontrivial. With the parameters, we obtain from (5)

$$\begin{aligned} |C_{\mathbf{a},\mathbf{b}}(\tau)| &\leq \left| \sum_{x \in \mathbb{F}_{p^m}} \psi_1\left(f_1(x)\right) \cdot \psi_2\left(\beta^{l+2\tau} f_2(x)\right) \right| + 1 \\ &\leq (d_1 + d_2 - 1)\sqrt{p^m} + e_1 + e_2 + 1 = 2\sqrt{p^m} + 2. \end{aligned} \tag{22}$$

Meanwhile, if $\mathbf{a} \in \mathcal{I}_{\mathbf{s}}$ and $\mathbf{b} \in \mathcal{S}_{\mathbf{v}}^{\left(c_1+i\frac{M}{2}\right)}$ (or vice versa), (22) is also true since $\mathcal{S}_{\mathbf{v}}^{\left(c_1+i\frac{M}{2}\right)} \subset \mathcal{S}_{\mathbf{v}}$, where $i = 0, 1$.

Case 3. $\mathbf{a}, \mathbf{b} \in \mathcal{S}_{\mathbf{v}}$ (or $\mathbf{a}, \mathbf{b} \in \mathcal{S}_{\mathbf{v}}^{\left(c_1+i\frac{M}{2}\right)}$, $i = 0, 1$.): If $\mathbf{a}$, $\mathbf{b} \in \mathcal{S}_{\mathbf{v}}$, then $|C_{\mathbf{a},\mathbf{b}}(\tau)|$ is bounded by (18) from Theorem 4. In particular, if $\mathbf{a}, \mathbf{b} \in \mathcal{S}_{\mathbf{v}}^{\left(c_1+i\frac{M}{2}\right)}$, $i = 0, 1$, it is immediate that the correlation magnitude is bounded by (19).

From Cases $1 - 3$, the proof is completed. □

Theorem 7: The family size of $\mathcal{V}$ and $\mathcal{V}^{(c_1)}$ are determined by

$$|\mathcal{V}| = \left(\left\lfloor \frac{p^m}{2} \right\rfloor + 1\right) \cdot (M-1)$$

$$\left|\mathcal{V}^{(c_1)}\right| = \begin{cases} p^m + M - 2, & \text{if } M > 2 \\ \frac{p^m+1}{2}, & \text{if } M = 2. \end{cases}$$

Proof: The family size of $\mathcal{V}$ is straightforward from a simple counting of $1 \le l \le \left\lfloor \frac{p^m}{2} \right\rfloor$ and $1 \le c, c_0 \le M-1$. Similarly, the family size of $\mathcal{V}^{(c_1)}$ is immediate from $1 \le l_1, l_2 \le \frac{p^m-1}{2}$ and $1 \le c \le M-1$ for a fixed integer c_1. □

Remark 1: In Construction 1, if $c_1 = \frac{M}{2}$, then we may define $\mathcal{V}^{\left(\frac{M}{2}\right)} = \mathcal{I}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}}^{\left(\frac{M}{2}\right)}$, where the correlation magnitude is bounded by $2\sqrt{p^m} + 2$ in the same way as the proof of Theorem 6. Although the family size is smaller than the other cases ($c_1 \neq \frac{M}{2}$), it can be utilized in the combination of sequence families, which will be discussed in next subsection.

B. Combination of sequence families

We construct new M-ary sequence families by combining the column sequence families introduced in previous subsection, and known Sidelnikov-based ones presented in [5] and [10].

Construction 2: Let p be prime, m a positive integer, and $M \mid p^m - 1$. Let $\mathbf{s} = \{s(t) \mid 0 \le t \le p^m - 2\}$ be an M-ary Sidelnikov sequence of period $p^m - 1$. Let $\mathcal{S}_{\mathbf{v}}$ be a set of the M-ary sequences of period $p^m - 1$ in Definition 3. A new M-ary sequence family of period $p^m - 1$ is defined by

$$\begin{aligned} \mathcal{U} =& \mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}} \\ =& \{cs(t) \mid 1 \le c \le M-1\} \\ & \cup \left\{ c_0 s(t) + c_1 s(t+l_1) \mod M \mid 1 \le c_0, c_1 \le M-1,\ 1 \le l_1 \le \left\lfloor \frac{p^m-1}{2} \right\rfloor \right\} \\ & \cup \left\{ c_2 v_{l_2}(t) \mid 1 \le c_2 \le M-1,\ 1 \le l_2 \le \left\lfloor \frac{p^m}{2} \right\rfloor \right\} \end{aligned}$$

where $c_0 < c_1$ if $l_1 = \frac{p^m-1}{2}$ for odd prime p.

In particular, if M is even for odd prime p, another new M-ary sequence family is defined by

$$\begin{aligned}\widetilde{\mathcal{U}} =& \mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}}^{(0)} \cup \mathcal{S}_{\mathbf{v}}^{(\frac{M}{2})} \\ =& \{cs(t) \mid 1 \le c \le M-1\} \\ & \cup \left\{ c_0 s(t) + c_1 s(t+l_1) \mod M \mid c_0 + c_1 \equiv 0 \mod M,\ 1 \le l_1 \le \frac{p^m-1}{2} \right\} \\ & \cup \left\{ \frac{M}{2} v_{l_2}(t) \mid 1 \le l_2 \le \frac{p^m-1}{2} \right\}\end{aligned}$$

where $1 \le c_0, c_1 \le M-1$, and $c_0 < c_1$ if $l_1 = \frac{p^m-1}{2}$.

Note that $\mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}} = \mathcal{L}$ is the M-ary sequence family presented in [10], while $\mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}}^{(0)} = \tilde{\mathcal{F}}_{\mathbf{s}}$ is the M-ary sequence family presented in [5]. Given the notations in Construction 2, the cyclic distinctness, the maximum correlation magnitudes, and the family sizes of $\mathcal{U}$ and $\widetilde{\mathcal{U}}$ are shown in Theorems 8, 9, and 10, respectively.

Theorem 8: Each pair of sequences in $\mathcal{U}$ is cyclically distinct. As its subset, each pair in $\widetilde{\mathcal{U}}$ is also cyclically distinct.

Proof: Note that $\mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}} = \mathcal{L}$ in [10] and $\mathcal{I}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}} = \mathcal{V}$ in Construction 1, which implies the cyclic distinctness of sequences in the subsets of $\mathcal{U}$. For the cyclic distinctness of all sequences in $\mathcal{U}$, it is therefore sufficient to prove that each sequence pair from $\mathcal{A}_{\mathbf{s}}$ and $\mathcal{S}_{\mathbf{v}}$ is cyclically distinct.

Let $\mathbf{a} \in \mathcal{A}_{\mathbf{s}}$ and $\mathbf{b} \in \mathcal{S}_{\mathbf{v}}$. (or vice versa.) Then, $\mathbf{a} = \{c_0 s(t) + c_1 s(t+l_1)\}$ and $\mathbf{b} = \{c_2 v_{l_2}(t)\}$. Let $S(x) = x+1$ and $V_{l_2}(\beta^\tau x)$ in (15) be the polynomials for $s(t)$ and $v_{l_2}(t+\tau)$, respectively. Then, $E_{\mathbf{a},\mathbf{b}}(\tau)$ is defined by

$$\begin{aligned}E_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p^m-1} \omega_M^{c_0 s(t) + c_1 s(t+l_1) - c_2 v_{l_2}(t+\tau)}, \quad 0 \le \tau \le p^m - 2 \\ &= \psi\left(S(x)^{c_0}\right) \cdot \psi\left(S(\beta^{l_1}x)^{c_1}\right) \cdot \psi\left(V_{l_2}(\beta^\tau x)^{M-c_2}\right)\end{aligned} \tag{23}$$

where $S(x)^{c_0} = 0$ at $x_1 = -1$ and $S(\beta^{l_1}x)^{c_1} = 0$ at $x_2 = -\beta^{-l_1}$, whereas $V_{l_2}(\beta^\tau x)^{M-c_2} \neq 0$ for any x's in $\mathbb{F}_{p^m}^*$. For $x \in \mathbb{F}_{p^m}^* \setminus \{x_1, x_2\}$, (23) is represented as

$$E_{\mathbf{a},\mathbf{b}}(\tau) = \psi\left(S(x)^{c_0} S(\beta^{l_1}x)^{c_1} V_{l_2}(\beta^\tau x)^{M-c_2}\right) = \psi\left(g(x)\right), \quad x \in \mathbb{F}_{p^m}^* \setminus \{x_1, x_2\}.$$

Similar to the proof of Theorem 3, it is easily checked that $g(x) \neq h(x)^M$ for any nontrivial l_1, l_2, c_0, c_1, c_2, and τ, where $h(x) \in \mathbb{F}_{p^m}[x]$. Hence, each sequence pair from $\mathcal{A}_{\mathbf{s}}$ and $\mathcal{S}_{\mathbf{v}}$ is cyclically distinct. Finally, each pair of sequences in $\mathcal{U}$ is cyclically distinct, and so is each pair in $\widetilde{\mathcal{U}}$, a subset of $\mathcal{U}$. □

Theorem 9: The maximum correlation magnitudes of $\mathcal{U}$ and $\widetilde{\mathcal{U}}$ are determined by

$$C_{\max}(\mathcal{U}) = 3\sqrt{p^m} + 5, \qquad C_{\max}(\widetilde{\mathcal{U}}) = 2\sqrt{p^m} + 6. \tag{24}$$

Proof: Note that $C_{\max}\left(\mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}}\right) = C_{\max}\left(\mathcal{L}\right) = 3\sqrt{p^m}+5$ from [10], and $C_{\max}\left(\mathcal{I}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}}\right) = C_{\max}\left(\mathcal{V}\right) = 3\sqrt{p^m}+1$ from Theorem 6. For $C_{\max}(\mathcal{U}) = C_{\max}(\mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}})$, therefore, it is sufficient to investigate the correlation between a sequence pair from $\mathcal{A}_{\mathbf{s}}$ and $\mathcal{S}_{\mathbf{v}}$. Similarly, $C_{\max}\left(\mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}}^{(0)}\right) = C_{\max}\left(\tilde{\mathcal{F}}_{\mathbf{s}}\right) = 2\sqrt{p^m}+6$ from [5], and $C_{\max}\left(\mathcal{I}_{\mathbf{s}} \cup \mathcal{S}_{\mathbf{v}}^{\left(\frac{M}{2}\right)}\right) = 2\sqrt{p^m}+2$ from Remark 1. Hence, we only need to examine the correlation between a sequence pair from $\mathcal{A}_{\mathbf{s}}^{(0)}$ and $\mathcal{S}_{\mathbf{v}}^{\left(\frac{M}{2}\right)}$ for $C_{\max}(\widetilde{\mathcal{U}}) = C_{\max}\left(\mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}}^{(0)} \cup \mathcal{S}_{\mathbf{v}}^{\left(\frac{M}{2}\right)}\right)$. In computing the maximum correlation magnitudes, we use the notations in Proposition 1.

First of all, let $\mathbf{a} \in \mathcal{A}_{\mathbf{s}}$ and $\mathbf{b} \in \mathcal{S}_{\mathbf{v}}$. (or vice versa.) Then $\mathbf{a} = \{c_0 s(t) + c_1 s(t+l_1)\}$ and $\mathbf{b} = \{c_2 v_{l_2}(t)\}$. Let $S(x) = x + 1$ and $V_{l_2}(\beta^\tau x)$ in (15) be the polynomials for $s(t)$ and $v_{l_2}(t+\tau)$, respectively. Then,

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{x \in \mathbb{F}_{p^m}^*} \psi^{c_0}\left(S(x)\right) \cdot \psi^{c_1}\left(S(\beta^\tau x)\right) \cdot \psi^{-c_2}\left(V_{l_2}(\beta^\tau x)\right) \\ &= \sum_{x \in \mathbb{F}_{p^m}} \psi_1\left(f_1(x)\right) \cdot \psi_2\left(\beta^\tau f_2(x)\right) \cdot \psi_3\left(\beta^{l_2+2\tau} f_3(x)\right) - 1 \end{aligned} \tag{25}$$

where $\psi_1 = \psi^{c_0}$, $\psi_2 = \psi^{c_1}$, and $\psi_3 = \psi^{-c_2} = \psi^{M-c_2}$. In (25), the monic polynomials $f_1(x) = S(x)$ and $f_2(x) = \beta^{-\tau} S(\beta^\tau x)$ have a single root in $\mathbb{F}_{p^m}$, respectively. On the other hand, the monic quadratic polynomial $f_3(x) = \beta^{-l_2-2\tau} V_{l_2}(\beta^\tau x)$ has distinct roots in $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ from Lemma 1. Obviously, each polynomial is irreducible in $\mathbb{F}_{p^m}$. Moreover, $d_1 = d_2 = 1$, $d_3 = 2$, and $e_1 = e_2 = 1$, and $e_3 = 0$ in Proposition 1. Also, the product character $\psi_1\left(f_1(x)\right) \cdot \psi_2\left(\beta^\tau f_2(x)\right) \cdot \psi_3\left(\beta^{l_2+2\tau} f_3(x)\right)$ is nontrivial from the cyclic distinctness of $\mathbf{a}$ and $\mathbf{b}$. With the parameters, we are able to apply the bound of (5) to obtain

$$\begin{aligned} |C_{\mathbf{a},\mathbf{b}}(\tau)| &\le \left| \sum_{x \in \mathbb{F}_{p^m}} \psi_1\left(f_1(x)\right) \cdot \psi_2\left(\beta^\tau f_2(x)\right) \cdot \psi_3\left(\beta^{l_2+2\tau} f_3(x)\right) \right| + 1 \\ &\le (d_1 + d_2 + d_3 - 1)\sqrt{p^m} + e_1 + e_2 + e_3 + 1 = 3\sqrt{p^m} + 3. \end{aligned} \tag{26}$$

In particular, if $\mathbf{a} \in \mathcal{A}_{\mathbf{s}}^{(0)}$ and $\mathbf{b} \in \mathcal{S}_{\mathbf{v}}^{\left(\frac{M}{2}\right)}$, then $c_0 + c_1 \equiv 0 \pmod{M}$ and $c_2 = \frac{M}{2}$. Thus,

$$\prod_{i=1}^{3} \psi_i^{d_i}(x) = \psi^{c_0+c_1-2\cdot c_2}(x) = 1$$

for all x in $\mathbb{F}_{p^m}^*$. Then, we can apply the improved bound (6) for the correlation, i.e.,

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \le (d_1 + d_2 + d_3 - 2)\sqrt{p^m} + 1 + e_1 + e_2 + e_3 + 1 = 2\sqrt{p^m} + 4. \tag{27}$$

Finally, (26) and (27) meets $C_{\max}(\mathcal{U})$ and $C_{\max}(\widetilde{\mathcal{U}})$ in (24), respectively. □

Theorem 10: The family size of $\mathcal{U}$ and $\widetilde{\mathcal{U}}$ are determined by

$$|\mathcal{U}| = \begin{cases} \frac{M(M-1)}{2} \cdot (p^m - 2) + M - 1, & \text{if } p > 2 \\ (M-1) \cdot (M \cdot 2^{m-1} - M + 2), & \text{if } p = 2. \end{cases}$$
$$\left|\widetilde{\mathcal{U}}\right| = p^m \cdot \frac{M}{2} - 1. \tag{28}$$

Proof: In [10], $|\mathcal{L}| = |\mathcal{I}_{\mathbf{s}}| + |\mathcal{A}_{\mathbf{s}}|$ is given by $\frac{(M-1)^2(p^m-3)+M(M-1)}{2}$ for $p > 2$, or $(M-1)^2(2^{m-1}-1)+M-1$ for $p = 2$. Then,

$$|\mathcal{U}| = |\mathcal{I}_{\mathbf{s}}| + |\mathcal{A}_{\mathbf{s}}| + |\mathcal{S}_{\mathbf{v}}| = |\mathcal{L}| + (M-1) \cdot \left\lfloor \frac{p^m}{2} \right\rfloor$$

which leads us to $|\mathcal{U}|$ in (28).

Similarly, $|\mathcal{F}_{\mathbf{s}}| = |\mathcal{I}_{\mathbf{s}}| + \left|\mathcal{A}_{\mathbf{s}}^{(0)}\right| = \frac{(M-1)(p^m-1)}{2} + \frac{M}{2} - 1$ in [5] for even M and odd prime p. Then,

$$\left|\widetilde{\mathcal{U}}\right| = |\mathcal{F}_{\mathbf{s}}| + \left|\mathcal{S}_{\mathbf{v}}^{\left(\frac{M}{2}\right)}\right| = |\mathcal{F}_{\mathbf{s}}| + \frac{p^m - 1}{2}$$

from which $\left|\widetilde{\mathcal{U}}\right|$ in (28) is immediate. □

Compared to [5] and [10], $\mathcal{U}$ and $\widetilde{\mathcal{U}}$ provide more cyclically distinct M-ary sequences of period $p^m - 1$ than the known Sidelnikov-based sequence families $\mathcal{L}$ and $\tilde{\mathcal{F}}_{\mathbf{s}}$, respectively, where $C_{\max}(\mathcal{U}) = C_{\max}(\mathcal{L})$ and $C_{\max}(\widetilde{\mathcal{U}}) = C_{\max}(\tilde{\mathcal{F}}_{\mathbf{s}})$. Table I compares the parameters of well known polyphase sequence families with low correlation, where the last four entries are the new sequence families found in this paper.

Remark 2: For $M = 4$, Table I shows that $\widetilde{\mathcal{U}}$ has the family size $2L+1$ with $C_{\max}(\widetilde{\mathcal{U}}) = 2\sqrt{L+1}+6$, and $\mathcal{U}$ has the family size $6L-3$ with $C_{\max}(\mathcal{U}) = 3\sqrt{L+1}+5$. In fact, it is $\mathbb{Z}_4$ sequence families [12] that provide the largest family sizes for the given maximum correlation magnitudes for $M = 4$. The advantage of $\widetilde{\mathcal{U}}$ and $\mathcal{U}$ is that they have the flexibility by providing a variety of sequence periods and alphabet sizes that cannot be covered by the $\mathbb{Z}_4$ sequence families.

Remark 3: Let $\mathcal{S} = \{\mathbf{s}^{(0)}, \mathbf{s}^{(1)}, \cdots, \mathbf{s}^{(N-1)}\}$ be a general M-ary sequence family of period $p^m - 1$ and size N, where each sequence $\mathbf{s}^{(l)} = \{s_l(t) \mid l = 0, \cdots, N-1\}$ is represented by multiplicative characters. Let $P_l(x)$ be the polynomial representation of $s_l(t)$, where $P_l(x) \in \mathbb{F}_{p^m}[x]$. In determining $C_{\max}(\mathcal{S})$, the (refined) Weil bound in Proposition 1 suggests that the degree of the largest square free divisor of $P_l(x)$ must be as small as possible for low correlation. In particular, if we want $C_{\max}(\mathcal{S}) \leq 2\sqrt{p^m} + \epsilon$ for a small positive integer ϵ, the degree must be at most 2. Therefore, constructing such a sequence family demands polynomials in $\mathbb{F}_{p^m}[x]$ that have the degrees of at most 2.

TABLE I

THE COMPARISON OF WELL KNOWN POLYPHASE SEQUENCE FAMILIES (p IS AN ODD PRIME)

	Period L	Alphabet	$C_{\max}$	Family size
Trachtenberg [20]	p^m-1, m odd	p	$\sqrt{p(L+1)}+1$	$L+2$
Helleseth [6]	p^m-1, m even $p^{m/2}\not\equiv 2 \pmod 3$	p	$2\sqrt{L+1}+1$	$L+2$
Sidelnikov [19]	p^m-1	p	$\sqrt{L+1}+1$	$L+1$
Bent [11]	p^m-1, m even	p	$\sqrt{L+1}+1$	$\sqrt{L+1}$
Kumar, Moreno [13]	p^m-1	p	$\sqrt{L+1}+1$	$L+1$
Gong [2]	$(p^m-1)^2$	p	$2\sqrt{L}+3$	$\sqrt{L}$
$\mathbb{Z}_4$ Family $S(0)$ [12]	2^m-1	4	$\sqrt{L+1}+1$	$L+2$
$\mathbb{Z}_4$ Family $S(1)$ [12]	2^m-1	4	$2\sqrt{L+1}+1$	$\geq L^2+3L+2$
$\mathbb{Z}_4$ Family $S(2)$ [12]	2^m-1	4	$4\sqrt{L+1}+1$	$\geq L^3+4L^2+5L+2$
$\tilde{\mathcal{F}}_{\mathbf{r}}$ [5]	p	M	$2\sqrt{L}+5$	$\left(\frac{L+1}{2}\right)\cdot(M-1)$
$\mathcal{F}_{\mathbf{r}}$ [5]	p	M	$3\sqrt{L}+4$	$M-1+\frac{(M-1)^2(L-1)}{2}$
$\tilde{\mathcal{F}}_{\mathbf{s}}$ [5]	p^m-1	M	$2\sqrt{L+1}+6$	$(M-1)\cdot\frac{L}{2}+\left\lfloor\frac{M-1}{2}\right\rfloor$
$\mathcal{L}$ [10]	p^m-1	M	$3\sqrt{L+1}+5$	$\frac{(M-1)^2(L-2)}{2}+\frac{M(M-1)}{2}$
$\mathcal{V}^{(c_1)}$	p^m-1	$M>2$ even	$2\sqrt{L+1}+2$	$L+M-1$
$\mathcal{V}$	p^m-1	M	$3\sqrt{L+1}+1$	$\left(\frac{L}{2}+1\right)\cdot(M-1)$
$\widetilde{\mathcal{U}}$	p^m-1	M even	$2\sqrt{L+1}+6$	$(L+1)\cdot\frac{M}{2}-1$
$\mathcal{U}$	p^m-1	M	$3\sqrt{L+1}+5$	$\frac{M(M-1)(L-1)}{2}+M-1$

In this paper, $\mathcal{V}^{(c_1)}$ and $\widetilde{\mathcal{U}}$ employ the polynomial $S(x)=x+1$ of degree 1, which corresponds to an M-ary Sidelnikov sequence. They also take the new polynomial of degree 2, $V_l(x)$ in (14), which has an element of $\mathbb{F}_{p^{2m}}$ and its conjugate as its roots. Interestingly, the new polynomial corresponds to a column sequence obtained by the array structure of Sidelnikov sequences of period $p^{2m}-1$. Moreover, $\widetilde{\mathcal{U}}$ adds another polynomial of degree 2, $S(x)S(\beta^l x)$, corresponding to the shift and addition of a Sidelnikov sequence, which is a well known technique in [5] and [10]. Note that we disregard $c,\ c_0,\ c_1$, and c_2 in the polynomial degrees, since they can be included in ψ_i in the Weil sums. By employing the polynomials, we successfully constructed the sequence families $\mathcal{V}^{(c_1)}$ and $\widetilde{\mathcal{U}}$ with low correlation and significantly large family sizes. We could find no other polynomials of degree of at most 2 in $\mathbb{F}_{p^m}$ that provide a large number of distinct sequences as well as low correlation, which is left open.

TABLE II

THE EQUALITY OF NORMALIZED SIDELNIKOV BOUND FOR $\widetilde{\mathcal{U}}$

	$N_{\max,lb}(\widetilde{\mathcal{U}})$				
m	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
2	1.2110	1.3475	1.3810	1.4009	1.4047
3	1.3526	1.4014	1.4096	1.4130	1.4135
4	1.3943	1.4117	1.4136	1.4141	1.4142
5	1.4076	1.4137	1.4141	1.4142	1.4142
6	1.4120	1.4141	1.4142	1.4142	1.4142
7	1.4135	1.4142	1.4142	1.4142	1.4142
8	1.4140	1.4142	1.4142	1.4142	1.4142
9	1.4141	1.4142	1.4142	1.4142	1.4142
10	1.4142	1.4142	1.4142	1.4142	1.4142

C. The asymptotic behavior of $\widetilde{\mathcal{U}}$

We examine the asymptotic behavior of $\widetilde{\mathcal{U}}$ when $L = M = p^m - 1$, and compare it to the Sidelnikov bound [19]. We introduce the bound on periodic correlation of nonbinary sequences, as described in [7].

Proposition 2: Let $\mathcal{S}$ be a nonbinary sequence family of period L and size N. Let k be a nonnegative integer. Then, the maximum correlation magnitude of $\mathcal{S}$ is lower bounded by

$$C_{\max}(\mathcal{S}) \geq \sqrt{\left(\frac{k+1}{2}\right) \cdot (2L-k) - \frac{2^k L^{2k+1}}{N(k!)^2 \binom{2L}{k}}}. \tag{29}$$

Normalizing (29) by $\sqrt{L+1}$, we denote the equality of the lower bound as $N_{\max,lb}(\mathcal{S})$, i.e.,

$$\frac{C_{\max}(\mathcal{S})}{\sqrt{L+1}} \geq \sqrt{\left(\frac{k+1}{2}\right) \cdot \left(\frac{2L-k}{L+1}\right) - \frac{2^k L^{2k+1}}{N(L+1)(k!)^2 \binom{2L}{k}}} = N_{\max,lb}(\mathcal{S}). \tag{30}$$

Now, we apply the lower bound for the maximum correlation magnitude of our M-ary sequence family $\widetilde{\mathcal{U}}$ of $L = M = p^m - 1$, where $N = \frac{L(L+1)}{2} - 1$ from Theorem 10. By applying the parameters to (30), we can compute $N_{\max,lb}(\widetilde{\mathcal{U}})$, the equality of the lower bound on $C_{\max}(\widetilde{\mathcal{U}})$.

Table II shows the values of $N_{\max,lb}(\widetilde{\mathcal{U}})$ computed for various p and m, where k is chosen in $0 \leq k \leq 15$ such that $N_{\max,lb}(\widetilde{\mathcal{U}})$ has the largest value for each p and m. From the table, we observe that $N_{\max,lb}(\widetilde{\mathcal{U}}) \approx \sqrt{2}$ for sufficiently large $L = p^m - 1$. Therefore, if $M = p^m - 1$, the Sidelnikov bound for $\widetilde{\mathcal{U}}$ becomes

$$C_{\max}(\widetilde{\mathcal{U}}) \geq \sqrt{2}\sqrt{L+1} \tag{31}$$

for sufficiently large L. From Theorem 9, we already found that $C_{\max}(\widetilde{\mathcal{U}}) = 2\sqrt{p^m} + 6 = 2\sqrt{L+1} + 6$. Consequently, we conclude that if $M = p^m - 1$, the actual maximum correlation magnitude of $\widetilde{\mathcal{U}}$ asymptotically achieves $\sqrt{2}$ times the equality of the Sidelnikov's lower bound in (31).

V. Conclusion

In this paper, we have showed that M-ary Sidelnikov sequences of period $p^{2m}-1$, if $M \mid p^m - 1$, can be equivalently generated by the operation of elements in $\mathbb{F}_{p^m}$, including a p^m-ary m-sequence of period $p^{2m}-1$. The equivalent generation over $\mathbb{F}_{p^m}$ costs low complexity for implementing the Sidelnikov sequences of period $p^{2m}-1$. Discussing the $(p^m-1)\times(p^m+1)$ array structure of the sequences, we then discovered that a half of the column sequences and their constant multiples have low correlation enough to construct new M-ary sequence families of period p^m-1, where the families $\mathcal{V}$ and $\mathcal{V}^{(c_1)}$ have the maximum correlation magnitude of $2\sqrt{p^m}+2$ (for even M) and $3\sqrt{p^m}+1$, respectively. Moreover, we constructed new M-ary sequence families of period p^m-1 by combining the column sequence families with known Sidelnikov-based families. The new families $\mathcal{U}$ and $\widetilde{\mathcal{U}}$ provide the largest family size of all known Sidelnikov-based sequence families with the same maximum correlation magnitudes. Finally, examining the asymptotic behavior of the new M-ary sequence family $\widetilde{\mathcal{U}}$, we showed that if $M = p^m - 1$ for odd prime p, its maximum correlation magnitude asymptotically achieves $\sqrt{2}$ times the equality of the Sidelnikov's lower bound.

References

[1] S. W. Golomb and G. Gong, *Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar*. Cambridge University Press, 2005.

[2] G. Gong, "New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2847-2867, Nov. 2002.

[3] Z. Guohua and Z. Quan, "Pseudonoise codes constructed by Legendre sequence," *Electron. Lett.*, vol. 38, pp. 376-377, Apr. 2002.

[4] Y. K. Han and K. Yang, "New M-ary power residue sequence families with low correlation," *in Proc. of IEEE Int. Symp. Information Theory (ISIT2007)*, pp. 2616-2620, Nice, France, Jun. 2007.

[5] Y. K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1815-1823, Apr. 2009.

[6] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209-232, 1976.

[7] T. Helleseth and P. V. Kumar, *Sequences with Low Correlation*. A chapter in *Handbook of Coding Theory*. Edited by V. Pless and C. Huffman. Elsevier Science Publishers, 1998.

[8] Y.-J. Kim, H.-Y. Song, G. Gong, and H. Chung, "Crosscorrelation of q-ary power residue sequences of period p," *in Proc. of IEEE Int. Symp. Information Theory (ISIT2006)*, pp. 311-315, Seattle, WA, Jul. 2006.

[9] Y.-J. Kim and H.-Y. Song, "Cross correlation of Sidel'nikov sequences and their constant multiples," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1220-1224, Mar. 2007.

[10] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "New families of M-ary sequences with low correlation constructed from Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3768-3774, Aug. 2008.

[11] P. V. Kumar, *On Bent Sequences and Generalized Bent Functions*, Ph. D. Dissertation, Univ. Southern Calif., Los Angeles, CA, 1983.

[12] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons Jr., "Large families of quaternary sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 579-592, Mar. 1996.

[13] P. V. Kumar and O. Moreno, "Prime-phase sequqences with periodic correlation properties better than binary sequences," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 603-616, May 1991.

[14] A. Lempel, M. Cohn, and W. Eastman, "A class of balanced binary sequences with optimal autocorrelation property," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 1, pp. 38-42, Jan. 1977.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, in *Encyclopedia of Mathematics and Its Applications*, vol. 20, Cambridge University Press, 1997.

[16] K. G. Paterson, "Applications of exponential sums in communication theory," *Lecture Notes in Computer Sciences (LNCS)*, vol. 1746, Springer-Verlag, pp. 1-24, 1999.

[17] J. J. Rushanan, "Weil sequences: A family of binary sequences with good correlation properties," *in Proc. of IEEE Int. Symp. Information Theory (ISIT2006)*, pp. 1648-1652, Seattle, WA, Jul. 2006.

[18] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, pp. 12-16, 1969.

[19] V. M. Sidelnikov, "On mutual correlation of sequences," *Soviet Math. Dokl.*, vol. 12, no. 1, pp. 197-201, 1971.

[20] H. M. Trachtenberg, *On the Cross-Correlation Functions of Maximal Linear Sequences*, Ph. D. Dissertation, Univ. Southern Calif., Los Angeles, CA, 1970.

[21] D. Wan, "Generators and irreducible polynomials over finite fields," *Math. Comput.*, vol. 66, no. 219, pp. 1195-1212, Jul. 1997.

[22] A. Weil, *Basic Number Theory*, 3rd. Ed., Springer-Verlag, 1974.

[23] N. Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," *IEEE Trans. Inf. Theory*, submitted. Also available at CACR 2009-25, *CACR Technical Report*, University of Waterloo, 2009.