IEICE TRANSACTIONS

on Communications

VOL. E97-B NO. 1
NOVEMBER 2014

A PUBLICATION OF THE COMMUNICATIONS SOCIETY

The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

New Families of p-Ary Sequences of Period $\frac{p^n-1}{2}$ with Low Maximum Correlation Magnitude

Wijik LEE[†a)], **Ji-Youp KIM**[†b)], *Nonmembers*, *and* **Jong-Seon NO**[†c)], *Member*

SUMMARY Let p be an odd prime such that $p \equiv 3 \bmod 4$ and n be an odd positive integer. In this paper, two new families of p-ary sequences of period $N = \frac{p^n-1}{2}$ are constructed by two decimated p-ary m-sequences $m(2t)$ and $m(dt)$, where $d = 4$ and $d = (p^n+1)/2 = N+1$. The upper bound on the magnitude of correlation values of two sequences in the family is derived by using Weil bound. Their upper bound is derived as $\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$ and the family size is $4N$, which is four times the period of the sequence.

key words: *character, correlation, m-sequences, p-ary sequences, weil bound*

1. Introduction

Pseudorandom sequences with low correlation are widely used in wireless communications, that is, code division multiple access, spread spectrum, cryptography, and error correcting codes. Many papers on sequence families with good correlation properties have been published. Kasami [4], [5] proposed a binary sequence family with the optimal correlation property with respect to Welch's lower bound. Further, there are lots of research results for the nonbinary sequence families. Liu and Komo [10] generalized the Kasami sequence family to the p-ary case and Kumar and Moreno [8] constructed a p-ary sequence family with correlation magnitude upper bounded by $1+\sqrt{p^n}$ using bent function. Jang, Kim, No and Helleseth [3] also proposed a p-ary sequence family with the optimal correlation property. Muller [11] also proposed two p-ary sequence families, whose correlation magnitude is upper bounded by $1+2\sqrt{p^n}$ and $1+\sqrt{p^n}$, respectively. Seo, Kim, No, and Shin [12] derived the cross-correlation distribution of p-ary sequences which have good correlation property. Choi, Lim, No, and Jung [1] also proposed a p-ary sequence family with correlation magnitude upper bound $\frac{p+1}{2}\sqrt{p^n}$ and family size $\sqrt{p^n}$.

Recently, p-ary sequence families with half period, that is, $N = \frac{p^n-1}{2}$ have been proposed. Generally, half period sequences can have larger family size. Kim, Choi, and No [7] constructed the first p-ary sequence family of half period using Kloosterman sum. This sequence family has large family size of $4N$ and their correlation magnitude is upper bounded by $2\sqrt{N+\frac{1}{2}}$ for an odd prime $p \equiv 3 \pmod 4$ and an odd integer n. This result is further generalized by Kim, Chae, and Song [6], that is, they generalized this sequence family to all odd prime p. Xia and Chen [15] constructed new sequence families having family size $4N$ and the correlation magnitude upper bounded by $\frac{p}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$. In this paper, we propose new p-ary sequence families of half period, whose correlation property is almost the same as that by Kim, Choi, and No [7]. For comparison of those well known p-ary sequence families with good correlation properties, their parameters are listed in the Table 1.

Weil bound for exponential sums is often used to prove the upper bound on the magnitude of correlation values [14]. There are three types of Weil bounds. The first one is the sum of multiplicative character. The second one is sum of additive character, and the last one is the sum of multiplication of additive and multiplicative characters (hybrid type). Han and Yang [2] used multiplicative characters of Weil bound to derive the upper bound on the magnitude of correlation values. Wang and Gong [13] constructed polyphase sequence families whose correlation magnitude is derived from the Weil bound of exponential sums. They applied all three types of Weil bounds to the proof of the upper bounds.

In this paper, new p-ary sequence families with low correlation are constructed. For an odd prime $p \equiv 3 \pmod 4$ and an odd integer n, two new p-ary sequence families of period $N = \frac{p^n-1}{2}$ having the correlation magnitude upper bounded by $\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$ are constructed. These sequence families can be obtained from shift and addition of two decimated p-ary m-sequences by 2 and d. One sequence family is obtained for $d = 4$ and the other sequence family is constructed for $d = N+1$. The hybrid sum of Weil bound is used for the proof of the upper bound of correlation magnitude.

2. Preliminaries

This section introduces some basic definitions and concepts that are used in this paper.

A. Notations and Definitions

1) Let p be an odd prime such that $p \equiv 3 \bmod 4$ and n be an odd positive integer, where $q = p^n$.

2) Let $\mathbb{F}_q$ be the finite field with q elements and α be a primitive element of $\mathbb{F}_q$.

3) The trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ is defined as

Manuscript received April 17, 2014.
Manuscript revised July 25, 2014.

[†]The authors are with the Department of ECE, INMC, Seoul National University, Seoul 151-744, Korea.
a) E-mail: leewj422@ccl.snu.ac.kr
b) E-mail: lakroforce@ccl.snu.ac.kr
c) E-mail: jsno@snu.ac.kr

DOI: 10.1587/transcom.E97.B.2311

Table 1 Comparison with some well-known sequence families.

Family	Alphabet	n	Period N	Family size	$C_{\max}$
Liu and Komo [10]	odd p	even	p^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
Jang et al. [3]	odd p	even or odd	p^n-1	$N+1$	$\sqrt{N+1}+1$
Kumar and Moreno [8]	odd p	even or odd	p^n-1	$N+1$	$\sqrt{N+1}+1$
Seo et al. [12]	odd p	even	p^n-1	$\sqrt{N+1}$	$2\sqrt{N+1}+1$
Choi et al. [1]	odd p	even	p^n-1	$\sqrt{N+1}$	$\frac{p+1}{2}\sqrt{N+1}+1$
Kim et al. [7]	$p \equiv 3 \pmod 4$	odd	$\frac{p^n-1}{2}$	$4N$	$2\sqrt{N+\frac{1}{2}}$
Kim et al. [6]	all p	even or odd	$\frac{p^n-1}{e}$	e^2N	$2\sqrt{eN+1}$
Xia and Chen [15]	$p \equiv 1 \pmod 4$	even or odd	$\frac{p^n-1}{2}$	$4N$	$\frac{p}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$
	$p \equiv 3 \pmod 4$	even	$\frac{p^n-1}{2}$	$4N$	$\frac{p}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$
Proposed family S	$p \equiv 3 \pmod 4$	odd	$\frac{p^n-1}{2}$	$4N$	$\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$

$$\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{p^i}.$$

4) $\omega = e^{\frac{2\pi i}{p}}$ is a primitive complex pth root of unity, where $i = \sqrt{-1}$.

5) For some $\beta \in \mathbb{F}_q^*$, a p-ary m-sequence of period $q-1$ is defined as

$$m(t) = \mathrm{Tr}_1^n(\beta\alpha^t).$$

6) Let $a(t)$ and $b(t)$ be p-ary sequences of period N. A cross-correlation between $a(t)$ and $b(t)$ is defined as

$$C_{a,b}(\tau) = \sum_{t=0}^{N-1} \omega^{a(t)-b(t+\tau)}.$$

If $a = b$, then the cross-correlation function becomes the autocorrelation function, denoted by $C_a(\tau)$. Let S be a family of sequences of period N. Then the maximum magnitude of correlation values of the sequences in S is defined as

$$C_{\max} = \max\left\{\left|C_{a,b}(\tau)\right| : a,b \in S, 0 \le \tau \le N-1, \tau \ne 0 \text{ if } a = b\right\}.$$

B. Characters and Weil Bound

There are two types of characters, that is, additive characters and multiplicative characters as follows [9].

Definition 1: (Additive Character): For $\beta \in \mathbb{F}_q$, an additive character of $\mathbb{F}_q$ is defined as

$$\psi(x) = e^{\frac{2\pi i \mathrm{Tr}_1^n(\beta x)}{p}}, x \in \mathbb{F}_q$$

and ψ_0, $\psi(x)$ with $\beta = 0$, denotes the trivial additive character such that $\psi_0(x) = 1$ for all $x \in \mathbb{F}_q$.

Definition 2: (Multiplicative Character): Let g be a fixed primitive element of $\mathbb{F}_q$. For each $j = 1, 2, \cdots, q-2$, a multiplicative character of $\mathbb{F}_q$ is defined as

$$\chi(g^k) = e^{\frac{2\pi i jk}{q-1}}$$

where $\chi(0) = 0$ and $\chi_0, \chi(g^k)$ with $j = 0$, denotes the trivial multiplicative character such that $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q^*$.

We consider the quadratic character η in this paper, which is defined as

$$\eta(y) = \begin{cases} 1, & \text{if } y \text{ is nonzero square in } \mathbb{F}_q \\ -1, & \text{if } y \text{ is nonzero nonsquare in } \mathbb{F}_q \\ 0, & \text{if } y = 0. \end{cases}$$

Lemma 3: (Gaussian sum [9]): Let ψ be an additive character of $\mathbb{F}_q$ and χ be a multiplicative character of $\mathbb{F}_q$. Then the Gaussian sum $G(\psi,\chi)$ is defined as

$$G(\psi,\chi) = \sum_{x \in \mathbb{F}_q} \psi(x)\chi(x),$$

which satisfies

$$G(\psi,\chi) = \begin{cases} p^n - 1 & \text{for } \psi = \psi_0 \text{ and } \chi = \chi_0 \\ 0 & \text{for } \psi = \psi_0 \text{ and } \chi \ne \chi_0 \\ -1 & \text{for } \psi \ne \psi_0 \text{ and } \chi = \chi_0 \end{cases}$$

and for $\psi \ne \psi_0$ and $\chi \ne \chi_0$,

$$|G(\psi,\chi)| = q^{1/2}.$$

The following Weil bounds are often used to prove the correlation property of the sequence.

Theorem 4: (Weil bound [14]): Let ψ be a nontrivial additive character of $\mathbb{F}_q$ and χ be a nontrivial multiplicative character of $\mathbb{F}_q$ with order M and $\chi(0) = 0$. Let $f(x) \in \mathbb{F}_q[x]$

with degree e and $g(x) \in \mathbb{F}_q$ with s distinct roots in $\overline{\mathbb{F}}_q$, where $g(x) \neq c \cdot h^M(x)$ for some $c \in \mathbb{F}_q$ and $h(x) \in \mathbb{F}_q[x]$, and $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$. Then

$$\left|\sum_{x\in\mathbb{F}_q} \chi(g(x))\psi(f(x))\right| \leq (e+s-1)\sqrt{q}.$$

Theorem 5: (Additive type of Weil bound [9]): Let $f \in \mathbb{F}_q[x]$ be of degree $n \geq 1$ with $\gcd(n,q)=1$ and let ψ be a nontrivial additive character of $\mathbb{F}_q$. Then

$$\left|\sum_{x\in\mathbb{F}_q} \psi(f(x))\right| \leq (n-1)\sqrt{q}.$$

3. New Sequence Families and Their Correlation Bound

In this section, we will propose two new p-ary sequence families of period $N = \frac{p^n-1}{2}$ and family size $4N$ and derive their correlation bound. Let $m(t)$ be a p-ary m-sequence of period $q-1$. We consider the sequence $m(2t)$ and $m(dt)$, where $d = 4$ and $N+1$. Since $q-1$ is even, the decimated sequence $m(2t)$ has the period N. Since $\gcd(q-1,d)=2$ for both cases, the period of $m(dt)$ is also N. Then we define the new p-ary sequence family of period N and family size $4N$ as

$$S = \{m(2t+i)+m(d(t+l)+j) | 0 \leq i,j \leq 1, 0 \leq l \leq N-1\}.$$

We will show that the magnitude of cross-correlation and nontrivial autocorrelation values of the sequences in the family S is upper bounded by $\frac{\sqrt{3}}{2}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$. For the proof of the upper bound, we use Theorems 4 and 5.

The correlation function between two sequences in S, $m(2t+i_1)+m(d(t+l_1)+j_1)$ and $m(2t+i_2)+m(d(t+l_2)+j_2)$, except for the trivial autocorrelation ($\tau = 0, i_1 = i_2, j_1 = j_2, l_1 = l_2$), is given as

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{N-1} \omega^{\mathrm{Tr}_1^n(\alpha^{2t+i_1})+\mathrm{Tr}_1^n(\alpha^{d(t+l_1)+j_1})-\mathrm{Tr}_1^n(\alpha^{2(t+\tau)+i_2})-\mathrm{Tr}_1^n(\alpha^{d(t+\tau+l_2)+j_2})} \\ &= \sum_{t=0}^{N-1} \omega^{\mathrm{Tr}_1^n(\alpha^{2t}(\alpha^{i_1}-\alpha^{2\tau+i_2})+\alpha^{dt}(\alpha^{dl_1+j_1}-\alpha^{d\tau+dl_2+j_2}))}. \end{aligned}$$

Let $a = \alpha^{i_1} - \alpha^{2\tau+i_2}$ and $b = \alpha^{dl_1+j_1} - \alpha^{d\tau+dl_2+j_2}$. Then

$$C(\tau) = \sum_{t=0}^{N-1} \omega^{\mathrm{Tr}_1^n(a\alpha^{2t}+b\alpha^{dt})}.$$

We will derive the upper bound of $C_{\max}$ for $d = 4$ and $N+1$ in the following two theorems.

Theorem 6: For $d = 4$, we have

$$C(\tau) = \sum_{t=0}^{N-1} \omega^{\mathrm{Tr}_1^n(a\alpha^{2t}+b\alpha^{4t})}.$$

Then, the maximum magnitude of $C(\tau)$ is given as

$$C_{\max} \leq \frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}.$$

Proof: Let $x = \alpha^{2t}$ and QR be the set of quadratic residues of $\mathbb{F}_q$. Then we have

$$\begin{aligned} C(\tau) &= \sum_{x\in \mathrm{QR}} \omega^{\mathrm{Tr}_1^n(ax+bx^2)} \\ &= \frac{1}{2}\left(\sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}_1^n(ax+bx^2)} + \sum_{x\in\mathbb{F}_q^*} \eta(x)\omega^{\mathrm{Tr}_1^n(ax+bx^2)}\right). \quad (1) \end{aligned}$$

Since the trivial autocorrelation case is excluded, it is easy to check that $a = b = 0$ should not be considered because $i_1, i_2, j_1, j_2 \in \{0,1\}$.

(i) $b = 0$ and $a \neq 0$:
In this case, (1) can be rewritten as

$$\frac{1}{2}\left(\sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}_1^n(ax)} + \sum_{x\in\mathbb{F}_q^*} \eta(x)\omega^{\mathrm{Tr}_1^n(ax)}\right). \quad (2)$$

The first term in (2) is given as

$$\sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}_1^n(ax)} = -1. \quad (3)$$

Let $\chi = \eta, g(x) = x$, and $f(x) = ax$ in Theorem 4. Then the second term in (2) is computed as

$$\left|\sum_{x\in\mathbb{F}_q^*} \eta(x)\omega^{\mathrm{Tr}_1^n(ax)}\right| \leq \sqrt{q}. \quad (4)$$

From (3) and (4), (2) can be computed as

$$\begin{aligned} |C(\tau)| = \frac{1}{2}\left|\left(\sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}_1^n(ax)} + \sum_{x\in\mathbb{F}_q^*} \eta(x)\omega^{\mathrm{Tr}_1^n(ax)}\right)\right| &\leq \frac{\sqrt{q}+1}{2} \\ &= \frac{\sqrt{2N+1}}{2}+\frac{1}{2} \\ &= \frac{1}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}. \quad (5) \end{aligned}$$

(ii) $b \neq 0$:
From Theorem 5 with $f(x) = ax + bx^2$, the first term in (1) can be derived as

$$\left|\sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}_1^n(ax+bx^2)}\right| \leq \sqrt{q}+1. \quad (6)$$

Let $\chi = \eta, g(x) = x$, and $f(x) = ax + bx^2$ in Theorem 4. Then, the second term in (1) is computed as

$$\left|\sum_{x\in\mathbb{F}_q^*} \eta(x)\omega^{\mathrm{Tr}_1^n(ax+bx^2)}\right| \leq 2\sqrt{q}. \quad (7)$$

From (6) and (7), we have

$$\frac{1}{2}\left|\left(\sum_{x\in\mathbb{F}_q^*}\omega^{\mathrm{Tr}_1^n(ax+bx^2)}+\sum_{x\in\mathbb{F}_q^*}\eta(x)\omega^{\mathrm{Tr}_1^n(ax+bx^2)}\right)\right|\le\frac{3}{2}\sqrt{q}+\frac{1}{2}$$
$$=\frac{3}{\sqrt{2}}\sqrt{\frac{q}{2}}+\frac{1}{2}=\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}. \quad (8)$$

From (5) and (8), we prove the theorem.

Theorem 7: Let $d = N + 1$. $C(\tau)$ can be rewritten as

$$C(\tau)=\sum_{t=0}^{N-1}\omega^{\mathrm{Tr}_1^n(a\alpha^{2t}+b\alpha^{(N+1)t})}. \quad (9)$$

Then, the maximum magnitude of $C(\tau)$ can also be derived as

$$C_{\max}\le\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}.$$

Proof: Let $x = \alpha^t$. It is easy to check that -1 is a nonsquare in $\mathbb{F}_{p^n}$ for an odd integer n and an odd prime $p \equiv 3 \pmod 4$. Let $x = y^2$ for a square x and $x = -y^2$ for a nonsquare x. Since $N + 1$ is even, we have the same form of

$$\mathrm{Tr}_1^n(ax^2+bx^{N+1})=\mathrm{Tr}_1^n(ay^4+by^2)$$

for both $x = y^2$ and $-y^2$. Then (9) can be rewritten as

$$C(\tau)=\frac{1}{2}\sum_{y\in\mathbb{F}_q^*}\omega^{\mathrm{Tr}_1^n(ay^4+by^2)}$$
$$=\frac{1}{2}\left(\sum_{y\in\mathbb{F}_q^*}\omega^{\mathrm{Tr}_1^n(ay^2+by)}+\sum_{y\in\mathbb{F}_q^*}\eta(y)\omega^{\mathrm{Tr}_1^n(ay^2+by)}\right). \quad (10)$$

Since (10) is the same as (1) by swapping a and b, the proof is the same as that of Theorem 6. Thus the proof is done.

Theorem 8: The family size of S is $4N$.

Proof: If there are two cyclically equivalent sequences in S, then their cross-correlation value is equal to N. From Theorems 6 and 7, the magnitude of the cross-correlation values of arbitrary two sequences are upper bounded by $\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$ and thus the sequences in S are cyclically inequivalent.

Even though the maximum magnitude of correlation values of the proposed sequence families is upper bounded, the number of distinct correlation values increases as N becomes large. Table 2 shows the number of distinct correlation values and the normalized maximum magnitude of $C_{\max}$ by $\sqrt{N}$ for some p and n. In case of $p = 3$ and odd n, the number of distinct correlation values is less than 6 and the correlation distribution is studied in [15].

Table 2 Simulation results of $C_{\max}$ and number of correlation values for some p and n.

p	n	N	$\frac{C_{\max}}{\sqrt{N}}$	Number of distinct values
3	3	13	2.1650	5
	5	121	2.1259	6
	7	1093	2.1219	6
	9	9841	2.1214	6
7	3	171	2.0304	94
	5	8403	2.0951	852
11	3	665	2.0003	450

4. Conclusion

In this paper, for an odd positive integer n and an odd prime p such that $p \equiv 3 \pmod 4$, two new families of p-ary sequences with low maximum correlation magnitude are constructed where the period of sequences is $N = \frac{p^n-1}{2}$ and the family size $4N$. The sequences in the family are obtained using shift and additions of the decimated p-ary m-sequences $m(2t)$ and $m(dt)$, where $d = 4$ and $N + 1$. The upper bound for the magnitude of cross-correlation and nontrivial autocorrelation values of the sequences in the family S can be evaluated as $\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$ using the Weil bound and the family size is four times the period of sequences, $4N$.

References

[1] S.T. Choi, T.H. Lim, J.S. No, and H.B. Chung, "On the cross-correlation of a p-ary m-sequence of period $p^{2m} - 1$ and its decimated sequences by $\frac{(p^m+1)^2}{2(p+1)}$," IEEE Trans. Inf. Theory, vol.58, no.3, pp.1873–1879, March 2012.

[2] 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, April 2009.

[3] J.W. Jang, Y.S. Kim, J.S. No, and T. Helleseth, "New family of p-ary sequences with optimal correlation property and large linear span," IEEE Trans. Inf. Thoery, vol.50, no.8, pp.1839–1844, Aug. 2004.

[4] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Science Laboratory, Univ. of Illinois, Urbana, Tech. Rep. R-285 (AD 632574), April 1966.

[5] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in Combinatorial Mathematics and Its Applications, Univ. of North Carolina Press, Chapel Hill, NC, 1969.

[6] D.S. Kim, H.J. Chae, and H.Y. Song, "A generalization of the family of p-ary decimated sequences with low correlation," IEEE Trans. Inf. Theory, vol.57, no.11, pp.7614–7617, Nov. 2011.

[7] J.Y. Kim, S.T. Choi, and J.S. No, "A new family of p-ary sequences of period $(p^n - 1)/2$ with low correlation," IEEE Trans. Inf. Theory, vol.57, no.6, pp.3825–3829, June 2011.

[8] P.V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," IEEE Trans. Inf. Theory, vol.37, pp.603–616, May 1991.

[9] R. Lidl and H. Niederreliter, Finite Fields, vol.20, Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Amsterdam, The Netherlands, 1983.

[10] S.C. Liu and J.F. Komo, "Nonbinary Kasami sequences over GF(p)," IEEE Trans. Inf. Theory, vol.38, no.4, pp.1409–1412, July 1992.

[11] E.N. Muller, "On the cross-correlation of sequences over GF(p) with short periods," IEEE Trans. Inf. Theory, vol.45, no.1, pp.289–295, Jan. 1999.

[12] E.Y. Seo, Y.S. Kim, J.S. No, and D.J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k} - 1$ and its decimated sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$," IEEE Trans. Inf. Theory, vol.54, no.7, pp.3140–3149, July 2008.

[13] Z. Wang, G. Gong, and N.Y. Yu, "New polyphase sequence families

with low correlation derived from the Weil bound of exponential sums," IEEE Trans. Inf. Theory, vol.59, no.6, pp.3990–3998, June 2013.
[14] A. Weil, "On some exponential sums," Proc. Natl. Acad. Sci. USA, vol.34, no.5, pp.204–207, 1948.
[15] Y. Xia and S. Chen, "A new family of p-ary sequences with low correlation constructed from decimated sequences," IEEE Trans. Inf. Theory, vol.58, no.9, pp.6037–6046, Sept. 2012.

Wijik Lee received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2012, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His area of research interests includes pseudorandom sequences, cryptography, and error-correcting codes.

Ji-Youp Kim received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2009, where he is currently pursuing the Ph.D. degree in electrical engineering and computer science. His area of research interests includes pseudorandom sequences, cryptography, and error-correcting codes, and communication theory.

Jong-Seon No received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, Korea, from September 1990 to July 1999. He joined the faculty of the Department of Electrical and Computer Engineering, Seoul National University, in August 1999, where he is currently a Professor. From 1996 to 2008, he served as a Founding Chair of Seoul Chapter, IEEE Information Theory Society. He was a General Chair for Sequence and Their Applications 2004 (SETA2004) in Seoul, Korea. He also served as a General Co-Chair for International Symposium on Information Theory and Its Applications 2006 (ISITA 2006) and International Symposium on Information Theory 2009 (ISIT 2009) in Seoul, Korea. He was a recipient of IEEE Information Theory Society Chapter of the Year Award in 2007. He is elevated to IEEE Fellow in Research Engineer/Scientist through IEEE Information Theory Society, November, 2011. He has become Co-Editor-in-Chief of Journal of Communications and Networks, January, 2012. His area of research interests includes error-correcting codes, sequences, cryptography, LDPC codes, interference alignment and wireless communication systems.