PAPER *Special Section on Signal Design and Its Applications in Communications*

Properties and Crosscorrelation of Decimated Sidelnikov Sequences**

Young-Tae KIM[†*a)], ***Nonmember***, **Min Kyu SONG**[††b)], ***Student Member***, **Dae San KIM**[†††c)], ***and*** **Hong-Yeop SONG**[††d)], ***Nonmembers***

SUMMARY In this paper, we show that if the d-decimation of a $(q-1)$-ary Sidelnikov sequence of period $q-1 = p^m - 1$ is the d-multiple of the same Sidelnikov sequence, then d must be a power of a prime p. Also, we calculate the crosscorrelation magnitude between some constant multiples of d- and d'-decimations of a Sidelnikov sequence of period $q-1$ to be upper bounded by $(d+d'-1)\sqrt{q}+3$.

key words: *Sidelnikov sequences, d-decimation sequences, constant-multiple sequences, correlation bound, Weil bound*

1. Introduction

For a prime power $q = p^m$ and a positive integer M such that $M|q-1$, Sidelnikov [1] introduced an M-ary sequences (called the Sidelnikov sequences) of period $q-1$, and showed that their non-trivial autocorrelation magnitudes are upper bounded by 4 regardless of M and q.

Binary and non-binary sequences with good autocorrelation properties have important applications in spread spectrum communications and radar engineering [2], [3]. Sequence family with further property on good (low) cross-correlation has also some important applications in multi-user communications such as cellular mobile communications [3], [4]. Non-binary sequence family constructions using the Sidelnikov sequences have been considered by many researchers [5], [6], [8]–[13].

Sampling or decimation is a well-known method for constructing a new sequence from the given sequence [2]–[4]. In this paper, we show that if the d-decimation of a $(q-1)$-ary Sidelnikov sequence of period $q-1 = p^m-1$ is the d-multiple of the same Sidelnikov sequence, then d must be a power of a prime p. Also, we calculate the crosscorrelation magnitude between some constant multiples of d- and d'-decimations of a Sidelnikov sequence of period $q-1$ to be upper bounded by $(d+d'-1)\sqrt{q}+3$.

Section 2 introduces some preliminary concepts for the main results: notation, definition of Sidelnikov sequences, correlation, Weil bound on character sums, and decimation. Main results are given in Sect. 3. Section 4 gives a brief concluding remark.

2. Preliminaries

2.1 Notation and Convention

We will use the following notation:

- p : a prime number
- q : a prime power p^m with positive integer m
- $GF(q)$: the finite field with q elements
- d : a decimation factor with $\gcd(q-1, d) = 1$
- M : a divisor of $q-1$ with $M \geq 2$
- $\omega_M = \exp(j\frac{2\pi}{M})$ where $j = \sqrt{-1}$
- β : a fixed primitive element of $GF(q)$
- ψ : the multiplicative character of $GF(q)$ of order M defined by

$$\psi(x) = \exp\left(j\frac{2\pi}{M}\log_\beta x\right) = \omega_M^{\log_\beta x}$$

We keep $\log(0) = 0$ and $\psi(0) = 1$ in this paper for convenience.

2.2 Sidelnikov Sequences

Definition 1 [1] *For any fixed primitive element β of $GF(q)$, let $D_k = \{\beta^{Mi+k} - 1 \mid 0 \leq i < \frac{q-1}{M}\}$. Then M-ary Sidelnikov sequence $\{s(t)\}$ of period $q-1$ is defined as*

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

We will say that $s(t)$ above is defined by the primitive element β.

Equivalently, it can also be expressed, with the new convention that $\log 0 = 0$, as

$$s(t) \equiv \log_\beta(\beta^t + 1) \bmod M$$

for $0 \leq t \leq q-2$.

Manuscript received February 27, 2014.
Manuscript revised June 11, 2014.
[†]The author is with LG Electronics, Seoul, Korea.
[††]The authors are with Yonsei University, Seoul, Korea.
[†††]The author is with Sogang University, Seoul, Korea.
[*]He had contributed to this work while he had been with Yonsei University, Seoul, Korea.
[**]This work was supported by the IT R&D program of MSIP/KEIT of Korea [10047212, Development of homomorphic encryption supporting arithmetics on ciphertexts of size less than 1kB and its applications]. Part of this paper has been presented in IWSDA 2013 held in Tokyo, Japan, from Oct. 27 to Nov. 1, 2013.
a) E-mail: youngtae88.kim@lge.com
b) E-mail: mk.song@yonsei.ac.kr
c) E-mail: dskim@sogang.ac.kr
d) E-mail: hysong@yonsei.ac.kr
DOI: 10.1587/transfun.E97.A.2562

2.3 Correlation

A correlation is a measure of distance between two sequences or sequence families. If two sequences are the same, the correlation is called auto-correlation. Otherwise, we call it cross-correlation. The following definition has been well-known [4].

Definition 2 *Let $\{a(t)\}$ and $\{b(t)\}$ be M-ary sequences of period L, where $0 \le t \le L-1$. A periodic correlation between $\{a(t)\}$ and $\{b(t)\}$ is defined by*

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

for $0 \le \tau \le L-1$, where $\omega_M = \exp(j\frac{2\pi}{M})$ and $t+\tau$ is computed modulo L.

For $\tau \equiv 0$ mod L when $\{a(t)\}$ and $\{b(t)\}$ are the same sequence, the value above becomes L, which is regarded as trivial. The values at all other cases (for all τ when $\{a(t)\}$ and $\{b(t)\}$ are two different sequences or for $\tau \not\equiv 0$ mod L when $\{a(t)\}$ and $\{b(t)\}$ are the same sequence) are called non-trivial.

For a sequence set $\mathcal{S}$, $C_{max}(\mathcal{S})$ is the maximum magnitude of all the non-trivial correlations of the pairs of sequences in $\mathcal{S}$.

2.4 Weil Bound

The Weil bound gives an upper bound on the multiplicative character sums, and has been used to calculate upper bound on the crosscorrelation of various sequences [4]. Yu and Gong [9], [13] introduced a refined version from some of the previously well-known ones, with an additional assumption that $\psi(0) = 1$. We will use a further refined version by Kim [10].

Theorem 1 [10] *Let $f_1(x), \ldots, f_m(x)$ be distinct monic irreducible polynomials over $GF(q)$ with degrees $d_1, \ldots, d_m$, with e_j the number of distinct roots in $GF(q)$ of $f_j(x)$ ($j = 1, \ldots, m$). Let $\psi_1, \ldots, \psi_m$ be nontrivial multiplicative characters of $GF(q)$, with $\psi_j(0) = 1$ ($j = 1, \ldots, m$). Then, for $a_1, \ldots, a_m \in GF(q)^\times$, we have the estimate*

$$\left| \sum_{x \in GF(q)} \psi_1(a_1 f_1(x)) \cdots \psi_m(a_m f_m(x)) \right| \le \left(\sum_{j=1}^{m} d_j - 1 \right) \sqrt{q} + \sum_{j=1}^{m} e_j.$$

2.5 Decimation and Constant Multiple

Taking decimation and/or constant multiple is a well-known method for constructing a new sequence from the given sequence [5], [7].

Definition 3 *Let $a(t)$ be an M-ary sequence of period L. Then* (1) *the d-decimation sequence $b(t)$ of $a(t)$ is $b(t) = a(dt)$ for $t = 0, 1, \ldots$;* (2) *the d-multiple sequence $c(t)$ of $a(t)$ is $c(t) = d \cdot a(t)$ for $t = 0, 1, \ldots$.*

When we apply the d-decimation to the periodic sequence of period L, we see easily that the period of decimated sequence becomes $\frac{L}{k}$ where $k = \gcd(d, L)$. Therefore, we have to choose d such that $\gcd(d, L) = 1$ in order to maintain the original period.

When we apply the d-multiple to the M-ary sequence, we see easily that the number of distinct values of the sequence becomes $\frac{M}{k}$ where $k = \gcd(d, M)$. Therefore, we have to choose d such that $\gcd(d, M) = 1$ in order to keep the resultant sequence to have truly M distinct values, i.e., to be an M-ary sequence.

3. Main Result

The Sidelnikov sequence is constructed using a primitive element of a finite field. It is well-known that if β is a primitive element of $GF(q)$, then β^d is also a primitive element of $GF(q)$ whenever $\gcd(d, q-1) = 1$. It is interesting to note that the d-decimation of a Sidelnikov sequence defined by a primitive element β is a d-multiple of another Sidelnikov sequence defined by the primitive element β^d. Following has been essentially proved as Lemma 2 in [7]:

Theorem 2 (Lemma 2 in [7]) *Let $q = p^m$ and $\{s(t)\}$ be an M-ary Sidelnikov sequence of period $q-1$. Let d be relatively prime to $q-1$. Then $s(dt) \equiv d \cdot s'(t) \mod M$ where $\{s'(t)\}$ given by $s'(t) \equiv \log_\gamma(\gamma^t + 1) \mod M$ is an another M-ary Sidelnikov sequence of period $q-1$ defined by the primitive element $\gamma = \beta^d$.*

Example 1 *Table 1 shows some decimation sequences of a 10-ary Sidelnikov sequence of period $q-1 = 10$. $GF(11)$ has 4 primitive elements: $2, 6 \equiv 2^9, 7 \equiv 2^7, 8 \equiv 2^3$. We can show that $9 \cdot s_1(t) \equiv s(9t)$ where $6 \equiv 2^9$. Similarly, $7 \cdot s_2(t) \equiv s(7t)$ and $3 \cdot s_3(t) \equiv s(3t)$.*

Corollary 1 *Let $q = p^m$ and $\{s(t)\}$ be an M-ary Sidelnikov sequence of period $q-1$. If $d = p^l k$ with $\gcd(p, k) = 1$ and a nonnegative integer l, then $s(p^l kt) = p^l s(kt)$ for all t. In particular, when $k = 1$, this implies $s(p^l t) = p^l s(t)$ for all t.*

The above corollary is quite straightforward since β

Table 1 Decimation sequences of a Sidelnikov sequence in Example 1.

	t	0	1	2	3	4	5	6	7	8	9
$\beta = 2$	$s(t)$	1	8	4	6	9	0	5	3	2	7
$\gamma = 6 \equiv 2^9$	$s_1(t)$	9	3	8	7	5	0	1	4	6	2
$\gamma = 7 \equiv 2^7$	$s_2(t)$	3	9	7	4	6	0	2	1	5	8
$\gamma = 8 \equiv 2^3$	$s_3(t)$	7	2	5	9	8	0	4	6	3	1

and β^{p^l} generate the same Sidelnikov sequence, but its converse is not at all trivial. We prove the converse for the case of $M = q-1$ and $k = 1$. We guess that it is also true for any divisor M of $q-1$ and $k = 1$, but leave this as an open problem.

Theorem 3 *Let $q = p^m$, and $\{s(t)\}$ be a $(q-1)$-ary Sidelnikov sequence of period $q-1$. If there exists a d such that $s(dt) = d \cdot s(t)$ for all t, then $d = p^l$ for some nonnegative integer l.*

proof: Since the period of the sequence is $q-1$, we may assume that $d \le q-2$. We assume that $s(dt) = d \cdot s(t)$ for all t, and write, on the contrary, $d = p^l r$, where l is a nonnegative integer, $\gcd(r, p) = 1$ and $r > 1$. Then we will consider the binomial coefficient $\binom{d}{p^l}$ and see if it is divisible by p or not. It will turn out that it is divisible by p in one way, and is not in other way, giving a desired contradiction to $r > 1$.

First, we have $\log_\beta(\beta^t + 1)^d = \log_\beta(\beta^{dt} + 1)$, and hence $(\beta^t + 1)^d = \beta^{dt} + 1$ for all $0 \le t \le q-2$. Therefore, $(a+1)^d = a^d + 1$ for all $a \in GF(q)$. This implies that $p | \binom{d}{i}$ for all $1 \le i \le d-1$. In particular, this implies that $\binom{d}{p^l}$ is divisible by p.

Now we use Kummer's criterion [14]: the power of p dividing $\binom{n}{k}$ is the number of carries when we add k to $n-k$ in base p. We may divide r by p and write $r = pa + j$ for some $1 \le j \le p-1$. By Kummer's criterion, the power of p dividing $\binom{d}{p^l}$ is the number of carries when adding p^l to $d - p^l = p^l(r-1)$ in base p. Observe that the right-most nonzero digit (in base p) of $p^l(r-1)$ is $(j-1)$ when $a = 0$ and those of p^l is 1, and hence, there are no carries in the sum that is just j. Therefore, $\binom{d}{p^l}$ is not divisible by p. Similarly, it is obvious that $\binom{d}{p^l}$ is not divisible by p when $a > 0$. This is a desired contradiction to $r > 1$. ■

Let $s(t)$ be an M-ary Sidelnikov sequence of period $q-1$. We will now derive the maximum correlation bound between $c_1 \cdot s(dt)$ and $c_2 \cdot s(d't)$ where c_1, c_2, d and d' are some constants. If p divides d, i.e. $d = p^l k$, where $l > 0$, then $s(dt) = p^l \cdot s(kt)$ by Corollary 1. Especially, if $d = p^l$ and $d' = p^{l'}$, then the correlation between $c_1 \cdot s(dt)$ and $c_2 \cdot s(d't)$ becomes just a correlation between two different constant multiples of a Sidelnikov sequence, and it was computed earlier by Kim and Song [5] and also by Yu and Gong [13]. Consequently, we need to consider only the case where p divides neither d nor d'.

Lemma 1 *Let d, d' be positive integers with $(d, q-1) = (d', q-1) = 1$, and let $0 \le \tau \le q-2$. Then we have the following:*

(a) *The only root in $GF(q)$ of $x^d + 1 = 0$ is -1. The only root in $GF(q)$ of $x^{d'} + \beta^{-d'\tau} = 0$ is $-\beta^{-\tau}$.*
(b) *If p does not divide d, then $x^d + 1$ has no multiple roots. If p does not divide d', then $x^{d'} + \beta^{-d'\tau}$ has no multiple roots.*
(c) *$x^d + 1$ and $x^{d'} + \beta^{-d'\tau}$ have a common root if and only if $\tau = 0$.*

proof: (a) If γ and δ are roots of $x^d + 1$, then $\left(\frac{\gamma}{\delta}\right)^d = 1$. But the only root of $x^d = 1$ in $GF(q)$ is 1, as $\beta^{id} = 1 \Rightarrow q-1 | id \Rightarrow q-1 | i$, since $(d, q-1) = 1$. So $\beta^i = 1$, and hence $\gamma = \delta$. If d is odd, then the root of $x^d + 1 = 0$ is -1. And if d is even, then q is even since $(d, q-1) = 1$, and hence the characteristic is 2. Hence, $-1 = +1$ is the only root of $x^d + 1$ over $GF(q)$, q even. The other case is similar.

(b) If p does not divide d, the $x^d + 1$ and its derivative dx^{d-1} are relatively prime. The other case is similar.

(c) If $\tau = 0$, then -1 is the common root. Conversely, let $\gamma^d + 1 = 0$ and $\gamma^{d'} + \beta^{-d'\tau} = 0$. Then $\gamma = -\zeta = -\beta^{-\tau}\eta$, with $\zeta^d = 1$ and $\eta^{d'} = 1$. So $\beta^\tau = \eta\zeta^{-1}$. Raising dd'-th power of both sides, we have $\beta^{\tau dd'} = 1$, which implies $\tau = 0$, since $(d, q-1) = (d', q-1) = 1$. ■

Theorem 4 *Assume that $(d, q-1) = (d', q-1) = 1$ and that p divides neither d nor d'. Let $a(t) = c_1 \cdot s(dt)$ and $b(t) = c_2 \cdot s(d't)$ are cyclically inequivalent for some M-ary Sidelnikov sequence $s(t)$ of period $q-1$ and constants $1 \le c_1, c_2 \le M-1$. Then we have*

$$\left| \max_\tau \{C_{a,b}(\tau)\} \right| \le (d + d' - 1)\sqrt{q} + 3$$

where τ runs over the integers $0 \le \tau \le q-2$.

proof: By the definition of Sidelnikov sequences and its decimation, we see that $a(t) = c_1 \log_\beta(\beta^{dt} + 1)$ and $b(t) = c_2 \log_\beta(\beta^{d't} + 1)$. Then, their correlation becomes as follows:

$$\begin{aligned} &C_{a,b}(\tau) \\ &\quad = \sum_{t=0}^{q-2} \omega_M^{a(t)-b(t+\tau)} \\ &\quad = \sum_{t=0}^{q-2} \omega_M^{c_1 \log_\beta(\beta^{dt}+1) - c_2 \log_\beta(\beta^{d'(t+\tau)}+1)} \\ &\quad = \sum_{x \in GF(q)} \psi^{c_1}(x^d + 1) \cdot \psi^{M-c_2}(\beta^{d'\tau} x^{d'} + 1) - 1 \\ &\quad = \sum_{x \in GF(q)} \psi^{c_1}(x^d + 1) \cdot \psi^{M-c_2}(\beta^{d'\tau}(x^{d'} + \beta^{-d'\tau})) - 1 \end{aligned}$$

Case 1. $\tau \neq 0$.
Lemma 1 says that, for any τ with $1 \le \tau \le q-2$, $f_1(x) = x^d + 1$ and $f_2(x) = x^{d'} + \beta^{-d'\tau}$ are relatively prime (cf. Lemma 1(c)) with the respective number e, e' of distinct roots in $GF(q)$ equal to $e = e' = 1$. (cf. Lemma 1(a)). Since M does not divide c_1 and $M - c_2$, $\psi_1 = \psi^{c_1}$ and $\psi_2 = \psi^{M-c_2}$ are not trivial. Therefore we have

$$\begin{aligned} &\psi_1(x^d + 1) \cdot \psi_2(\beta^{d'\tau}(x^{d'} + \beta^{-d'\tau})) \\ &\quad = \psi_1(x+1) \cdot \psi_1(h_1(x)) \cdot \psi_2(\beta^{d'\tau}(x+\beta^{-\tau})) \cdot \psi_2(h_2(x)) \end{aligned}$$

where $x^d + 1 = (x+1)h_1(x)$ and $x^{d'} + \beta^{-d'\tau} = (x+\beta^{-\tau})h_2(x)$ for some polynomials $h_1(x)$ and $h_2(x)$. By Lemma 1, $h_1(x)$ and

Table 2 Comparison between true max and bound in Cor. 2 for $c = 1$, $d' = 1$, $\gcd(d, q-1) = 1$ and p not dividing d.

p	q	d	M	True Max	Bound = $d\sqrt{q}+3$
2	$64 = 2^6$	5	7	17.62	43.00
3	$243 = 3^5$	5	11	41.78	80.94
2	$256 = 2^8$	7	15	49.79	115.00
17	$289 = 17^2$	5	8	45.96	88.00
		7	8	38.88	122.00
7	$343 = 7^3$	5	9	47.78	95.60
2	$512 = 2^9$	5	7	56.58	68.88

$h_2(x)$ are products of some distinct monic irreducible polynomials over $GF(q)$ of degrees greater than 1 (cf. Lemma 1(b)). Therefore, we can apply Weil bound in Theorem 1, and hence

$$|C_{a,b}(\tau)| \leq (d + d' - 1)\sqrt{q} + 3.$$

Case 2. $\tau = 0$.
In this case, we have

$$C_{a,b}(\tau = 0) = \sum \psi^{c_1}(x^d + 1) \cdot \psi^{M-c_2}(x^{d'} + 1) - 1. \quad (1)$$

Assume that $d = d'$. Then (1) becomes $\sum \psi^{c_1-c_2}(x^d + 1) - 1$. If $c_1 = c_2$, then two sequences are the same. Otherwise,

$$|C_{a,b}(\tau = 0)| \leq (d - 1)\sqrt{q} + 2$$

by Weil bound and Lemma 1.

Otherwise, assume that $d \neq d'$. Then (1) becomes $\sum \psi^{c_1-c_2}(x+1) \cdot \psi^{c_1}(x^{d-1} - x^{d-2} + \cdots - x + 1) \cdot \psi^{M-c_2}(x^{d'-1} - x^{d'-2} + \cdots - x + 1) - 1$. Second and third polynomials of degree $d-1$ and $d'-1$ inside the character are products of distinct monic irreducible polynomials over $GF(q)$ by Lemma 1. Therefore, we can apply Weil bound, and hence

$$|C_{a,b}(\tau = 0)| \leq (d + d' - 2)\sqrt{q} + 2.$$

∎

Corollary 2 *Assume that* $\gcd(d, q-1) = 1$, *and that p does not divide d. Let s(t) be an M-ary Sidelnikov sequence of period* $q-1$. *Let* $a(t) = c \cdot s(t)$ *and* $b(t) = s(dt)$. *Then we have*

$$\left|\max_{\tau}\{C_{a,b}(\tau)\}\right| \leq d\sqrt{q} + 3.$$

Example 2 *Table 2 shows the difference between the exact maximal correlation magnitude and our correlation bound given in the above corollary for some q, d,* $c = 1$ *and M.*

Example 3 *Figure 1 shows the correlation function of the* 11*-ary Sidelnikov sequence of period* $3^5 - 1 = 242$ *and its* 5*-decimation. The horizontal dotted line in the figure indicates the correlation bound in the main result, also shown in Table 2, which is about* 81. *The true max turns out to be about* 42, *showing some gap between the two numbers. Figure 2 shows the correlation function of the* 9*-ary Sidelnikov sequence of period* $7^3 - 1 = 342$ *and its* 5*-decimation. In this case, the true max turns out to be about* 48.

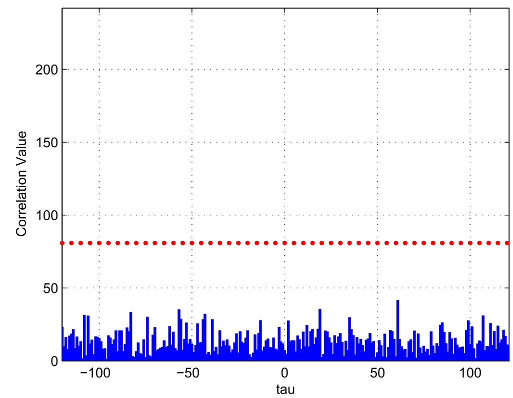

Fig. 1 Correlation between a 5-ary Sidelnikov sequence of period 242 and its 5-decimation.

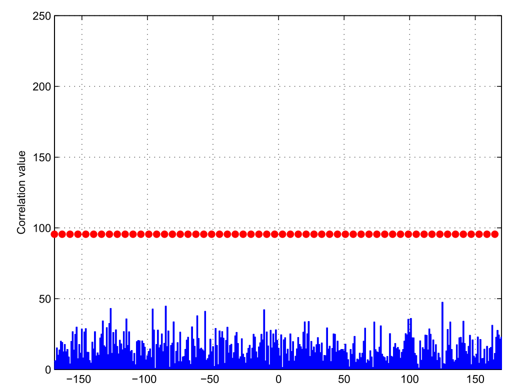

Fig. 2 Correlation between a 9-ary Sidelnikov sequence of period 342 and its 5-decimation.

4. Concluding Remark

Both figures in the above example show that there is a gap between the true max and the bound calculated using the Weil bound. This gap will increase when the constant multiple c is not relatively prime to M. For example, when $q = 343$ and $M = 9$ (cf. Example for Fig. 2), the true max between $3 \cdot s(t)$ and $s(5t)$ is around 20 while the bound in Cor. 2 is also 95.6. We guess that these gaps can be reduced by some direct calculation of the correlation between $c \cdot s(t)$ and $s(dt)$ for $1 \leq c \leq M-1$ and $\gcd(d, q-1) = 1$. It would be interesting in the future to see and compare these gaps between those from the direct calculation and from the Weil bound.

References

[1] V.M. Sidelnikov, "Some k-valued pseudo-random sequences and

nearly equidistant codes," Probl. Inf. Transm., vol.5, no.1, pp.12–16, 1969.

[2] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications Handbook, Computer Science Press, Rockville, MD, 1985; revised edition, McGraw-Hill, 1994.

[3] P. Fan and M. Darnell, Sequence Design for communications applications, John Wiley & Sons, New York, NY, 1996.

[4] S.W. Golomb and G. Gong, Sequence Design for Good Correlation, Cambridge University Press, New York, NY, 2005.

[5] Y.-J. Kim and H.-Y. Song, "Cross correlation of Sidelnikov sequences and their constant multiples," IEEE Trans. Inf. Theory, vol.53, no.3, pp.1220–1224, March 2007.

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

[7] J.-S. Chung, Y.-S. Kim, T.-H. Lim, J.-S. No, and H. Chung, "On some properties of M-ary Sidelnikov sequences," IEICE Trans. Fundamentals, vol.E92-A, no.1, pp.342–345, Jan. 2009.

[8] 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, April 2009.

[9] N.Y. Yu and G. Gong, "New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences," IEEE Trans. Inf. Theory, vol.56, no.8, pp.4061–4070, Aug. 2010.

[10] D.S. Kim, "A family of sequences with large size and good correlation property arising from M-ary Sidelnikov sequences of period $q^d - 1$," arXiv:1009.1225v1[cs.IT], 7 Sept. 2010.

[11] Y.-T. Kim, D.-S. Kim, and H.-Y. Song, "Some properties of 2-dimensional array structure of Sidelnikov sequences of period $q^d - 1$," 2013 International Workshop on Sequence Design and its Applications in Communications (IWSDA), held in Tokyo, Japan, Oct.–Nov. 2013.

[12] Y.-T. Kim, D.-S. Kim, and H.-Y. Song, "New M-ary sequence families with low correlation from the array structure of Sidelnikov sequences," pri-print, submitted to IEEE Trans. Inf. Theory, 2013.

[13] N.Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," IEEE Trans. Inf. Theory, vol.56, no.12, pp.6376–6387, Dec. 2010.

[14] D. Mihet, "Legendre's and Kummer's Theorems Again," REASONANCE, vol.15, no.12, pp.1111–1121, Dec. 2010.

Young-Tae Kim received his B.S. degree in Mathematics and M.S. degree in Electrical and Electronic Engineering both from Yonsei University, Seoul, Korea, in 2011 and 2013, respectively. He is currently working in LG Electronics, Seoul, Korea. His area of research interest includes design and analysis of PN sequences, and implementation of global navigation satellite system (GNSS) on mobile handsets.

Min Kyu Song received his B.S. degree in Electronic Engineering from Konkuk University, Seoul, Korea, and M.S. degree in Electrical and Electronic Engineering from Yonsei University, Seoul, Korea, in 2011 and 2013, respectively. He is currently a Ph.D. candidate working in Channel Coding and Crypto Lab. at Yonsei University. His area of research interest includes PN sequences, cryptography, and coding theory.

Dae San Kim received his B.S. and M.S. degrees in mathematics from Seoul National University, Seoul, Korea, in 1978 and 1980, respectively, and the Ph.D. degree in mathematics from University of Minnesota, Minneapolis, MN, in 1989. He is a professor in the Department of Mathematics at Sogang University, Seoul, Korea. He has been there since 1997, following a position at Seoul Women's University. His research interests include number theory (exponential sums, modular forms, zeta functions, p-adic analysis) and coding theory.

Hong-Yeop Song received his B.S. degree in Electronic Engineering from Yonsei University in 1984, MSEE and Ph.D. degrees from the University of Southern California, Los Angeles, CA, in 1986 and 1991, respectively, specializing in the area of communication theory and coding. He spent 2 years as a senior engineer at Qualcomm Inc., San Diego, CA, from 1994 to 1995, contributed to a team developing North American CDMA Standards for PCS and cellular air-interface systems. Finally, in the fall of 1995, he joined the Dept. of Electrical and Electronic Engineering at Yonsei University, Seoul, Korea, and is currently working as a professor. He visited Dr. G. Gong at University of Waterloo, Canada, in the year 2002. He is interested in Communication and Coding Theory, including error-correcting codes, PN sequences, and crypto algorithms. He is a senior member of IEEE, member of MAA (Mathematical Association of America), and domestic societies: IEEK, KICS, KIISC and KMS (Korean Mathematical Society).