San Jose State University

From the SelectedWorks of Robert Henry Morelos-Zaragoza

December 1, 2016

A Multi-Value Sequence Generated by Power Residue Symbol and Trace Function over Odd Characteristic Field

Yasuyuki Nogami, *Okayama University*
Satoshi Uehara, *University of Kitakyushu*
Kazuyoshi Tsuchiya, *Koden Electronics Co. Ltd.*
Nasima Begum, *Okayama University*
Hiroto Ino, *Okayama University*, et al.

Available at: https://works.bepress.com/robert_morelos-zaragoza/47/

IEICE TRANS. FUNDAMENTALS, VOL.E99-A, NO.12 DECEMBER 2016

PAPER Special Section on Information Theory and Its Applications

A Multi-Value Sequence Generated by Power Residue Symbol and Trace Function over Odd Characteristic Field

Yasuyuki NOGAMI[†a)], Satoshi UEHARA[††b)], Kazuyoshi TSUCHIYA[†††c)], Nasima BEGUM[†], *Members*, Hiroto INO[†], *and* Robert H. MOLEROS-ZARAGOZA[††††d)], *Nonmembers*

SUMMARY This paper proposes a new multi-value sequence generated by utilizing primitive element, trace, and power residue symbol over odd characteristic finite field. In detail, let p and k be an odd prime number as the characteristic and a prime factor of $p-1$, respectively. Our proposal generates k-value sequence $\mathcal{T} = \{t_i \mid t_i = f_k(\mathrm{Tr}(\omega^i) + A)\}$, where ω is a primitive element in the extension field $\mathbb{F}_{p^m}$, $\mathrm{Tr}(\cdot)$ is the trace function that maps $\mathbb{F}_{p^m} \to \mathbb{F}_p$, A is a non-zero scalar in the prime field $\mathbb{F}_p$, and $f_k(\cdot)$ is a certain mapping function based on k-th power residue symbol. Thus, the proposed sequence has four parameters as p, m, k, and A.Then, this paper theoretically shows its period, autocorrelation, and cross-correlation. In addition, this paper discusses its linear complexity based on experimental results. Then, these features of the proposed sequence are observed with some examples.

key words: *multi-value sequence, odd characteristic, primitive polynomial, power residue symbol, trace, cross-correlation*

1. Introduction

Pseudo random sequences have been widely employed in numerous applications in cryptography [1]–[3] and spread spectrum communications [4]. The security of many cryptographic systems depend upon the generation of unpredictable random quantities. Some primitive examples include the key-stream in the one-time pad, the secret key in the AES encryption algorithm [5], unique parameters in digital signature schemes, the private key in the DSA [6], the challenges used in challenge response identification systems and the session key in network security protocols. Pseudo random sequences are also used in simulation scenario, generation of pilot signals, code division multiple access, optical and ultrawideband communication systems, in ranging systems, global positioning systems and circuit testing. In recent years, pseudo random sequences have been extensively researched. Pseudo random binary sequences such as maximum length sequence (M-sequence) [2], [7], [8] and Legendre sequence [9] are well known due to its important properties which are theoretically proven.

Manuscript received January 18, 2016.
Manuscript revised June 13, 2016.

[†]The authors are with Graduate School of Natural Science and Technology, Okayama University, Okayama-shi, 700-8530 Japan.
[††]The author is with Graduate School of Environmental Engineering, The University of Kitakyushu, Kitakyushu-shi, 808-0135 Japan.
[†††]The author is with Koden Electronics Co. Ltd., Tokyo, 146-0095 Japan.
[††††]The author is with Department of Electrical Engineering, San Jose State University, 1 Washington Square, San Jose, CA 95192-0084, USA.
a) E-mail: yasuyuki.nogami@okayama-u.ac.jp
b) E-mail: uehara@kitakyu-u.ac.jp
c) E-mail: k-tsuchiya@koden-electronics.co.jp
d) E-mail: R.Morelos-Zaragoza@IEEE.org
DOI: 10.1587/transfun.E99.A.2226

1.1 Previous Works

M-sequence [2] and Legendre sequence [9] are known as a kind of pseudo random sequences, and these sequences have been used for some applications. In our previous work [10], the authors have proposed an approach to generate a pseudo random binary sequence by combining the features of M-sequence and Legendre-sequence. In brief, the process of previous generating method is as follows: firstly, it uses primitive polynomial of degree m over odd characteristic field $\mathbb{F}_p$ to generate maximum length vector sequence as elements in $\mathbb{F}_{p^m}$, then applies trace function to map the vectors to $\mathbb{F}_p$ scalars, and finally applies Legendre symbol to map the scalars to binary values such as $\{1, -1\}$. Such a binarized sequence over finite field is often called geometric sequence and it has been well studied [11]–[14]. The pseudo random binary sequence of our previous work is characterized with two parameters m and p, where m is the degree of primitive polynomial and p is the characteristics. Our previous work [10] can successfully construct a new variety of pseudo random binary sequences which has some important properties such as period, autocorrelation, and linear complexity. These properties have been mostly proven theoretically in our previous work.

1.2 Our Motivations and Contributions

As introduced above, our previous work [10] first generates vector sequence of period $p^m - 1$ in the same of M-sequence. However, by applying Legendre symbol for the vector sequence, the newly obtained binary sequence has a shorter period $2(p^m - 1)/(p - 1)$. Accordingly, the maximum of its linear complexity is also $2(p^m - 1)/(p - 1)$. In order to not only overcome these inefficiencies but also extend the previous work, this paper adds a *non-zero* scalar in prime field as one more parameter and applies power residue symbol instead of Legendre symbol.

In this paper, we extend our previous method [10] to generate a new pseudo random multi-value sequence by adding a certain *non-zero* scalar in prime field just before applying power residue symbol. In this paper, we propose

Copyright © 2016 The Institute of Electronics, Information and Communication Engineers

a pseudo random multi-value sequence as follows: Let p be an odd characteristic and m be the degree of primitive polynomial $f(x)$ over $\mathbb{F}_p$. The polynomial $f(x)$ is possible to generate a maximum length sequence over $\mathbb{F}_{p^m}$. Let ω be its zero, that is a primitive element in $\mathbb{F}_{p^m}$, and the sequence

$$\mathcal{S} = \{s_i \mid s_i = \mathrm{Tr}\left(\omega^i\right), i = 0, 1, 2, \cdots, p^m - 2\} \tag{1}$$

is a maximum length sequence of period $p^m - 1$, where $\mathrm{Tr}(\cdot)$ is the trace function over $\mathbb{F}_p$. The process of our new proposed method is as follows: firstly, an additional *non-zero* constant $A \in \mathbb{F}_p$ is added to s_i of the trace sequence S, then the k-th power residue symbol is applied to map the sequence to the multi-value sequence $\mathcal{T}$, where $\mathcal{T}$ consists of integers between 0 to $(k-1)$ and k is a prime factor of $p-1$. The previous work [10] does not apply the addition to the sequences before applying power residue symbol. This paper shows the preliminaries about the sequence which includes primitive polynomial, power residue symbol, trace function and the features such as periodic autocorrelation, periodic cross-correlation and linear complexity. This paper explains the generating process of the extended multi-value sequence, examines the above mentioned features from the results of the experiments and also shows the mathematical proof of the correlations.

In our extended algorithm, instead of Legendre symbol, we utilize the power residue symbol. One of the motivations behind adding an additional non-zero scalar value A in the prime field $\mathbb{F}_p$ is to get an interesting cross-correlation. Then, as show in this paper, the cross-correlation is theoretically proven. In the proposed method, we have many parameters such as characteristic p, degree m, k-value, and non-zero scalar A. Hence, the proposed method can generate different varieties of random sequences with large linear complexity.

1.3 Notations

Throughout this paper, p and q denote an odd prime number and its power $q = p^m$, respectively, where m is a positive integer and mainly denotes extension degree. $\mathbb{F}_q^*$ denotes the multiplicative group of $\mathbb{F}_q$, that is $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$. Then, *multi-value* sequence in this paper means that each value in the sequence is an integer in the range of 0 to $k-1$ where k is a prime factor of $p-1$.

2. Preliminaries

This section briefly reviews some mathematical fundamentals such as primitive element, power residue symbol, trace function, and dual basis. Then, multi-value sequence and our previous works are introduced with regard to period, autocorrelation, cross-correlation, and linear complexity.

2.1 Primitive Element and Primitive Polynomial

It is known that every finite field $\mathbb{F}_q$ has a multiplicative primitive element, that is a generator of *non-zero* elements in $\mathbb{F}_q$. In other words, let g be a generator, every non-zero element is represented by its power g^i for $i = 0, 1, 2, \cdots, q-2$. The minimal polynomial of a generator is correspondingly called a primitive polynomial.

The following property between $\mathbb{F}_q$ and $\mathbb{F}_p$ holds (*see also Theorem 1.15* [15]).

Property 1: Let g be a generator of $\mathbb{F}_q^*$, $g^{(q-1)/(p-1)}$ is a non-zero element in prime field $\mathbb{F}_p$ and is also a generator of $\mathbb{F}_p^*$. □

(Proof) Since g is a generator of $\mathbb{F}_q^*$, its order is $q-1$. Let i be a non-negative integer, the order of g^i is given by

$$\frac{q-1}{\gcd(q-1, i)}. \tag{2}$$

Therefore, the order of $g^{(q-1)/(p-1)}$ is $p-1$. It means that $g^{(q-1)/(p-1)}$ is a generator of $\mathbb{F}_p^*$. □

2.2 Power Residue Symbol

As an extension of Legendre symbol, this paper considers *power residue symbol* $\left(a/p\right)_k$ for an arbitrary element a in $\mathbb{F}_p$ and a prime factor k of $p-1$ as follows [16], [17]:

$$\left(\frac{a}{p}\right)_k = a^{(p-1)/k} \bmod p = \begin{cases} 0 & \text{when } a = 0, \\ \epsilon_k^i & \text{otherwise,} \end{cases} \tag{3}$$

where $0 \le i < k$ and ϵ_k is a primitive k-th root of unity that exists in $\mathbb{F}_p$. It is Legendre symbol when $k = 2$ [18]. Note that, for a *non-zero* element a and a fixed ϵ_k, the exponent i in Eq. (3) is uniquely determined in the range from 0 to $k-1$. Moreover, since $\epsilon_k^k = \epsilon_k^0 = 1$ and k is a prime number in this paper, the exponents are able to be dealt with as elements in $\mathbb{F}_k$. In order to represent the exponent i in Eq. (3), this paper for example uses the following notations.

$$i = \log_{\epsilon_k}\left(\left(a/p\right)_k\right) = \log_{\epsilon_k}\left(a^{(p-1)/k} \bmod p\right). \tag{4}$$

As described above, this paper utilizes the power residue symbol to map an element in $\mathbb{F}_p$ to an element in $\mathbb{F}_k$.

With regard to power residue symbol $\left(a/p\right)_k$, the following property holds.

Property 2: For each i from 0 to $k-1$, the number of non-zero elements in $\mathbb{F}_p$ such that

$$\left(\frac{a}{p}\right)_k = \epsilon_k^i \tag{5}$$

is given by $(p-1)/k$. □

(Proof) Non-zero elements in $\mathbb{F}_p$ are the roots of $x^{p-1}-1$ over $\mathbb{F}_p$ without any duplicates. Since it is factorized as

$$x^{p-1}-1=\prod_{i=0}^{k-1}\left(x^{(p-1)/k}-\epsilon_k^i\right), \tag{6}$$

it is thus found that the number is given by $(p-1)/k$. □

2.3 Trace Function and Its Properties

This paper uses the trace function to map an extension field element $X \in \mathbb{F}_{p^m}$ to a prime field element $x \in \mathbb{F}_p$ as

$$x=\mathrm{Tr}(X)=\sum_{i=0}^{m-1}X^{p^i}. \tag{7}$$

The above trace function has a linearity over prime field $\mathbb{F}_p$ as follows:

$$\mathrm{Tr}(aX+bY)=a\mathrm{Tr}(X)+b\mathrm{Tr}(Y), \tag{8}$$

where $a, b \in \mathbb{F}_p$ and $Y \in \mathbb{F}_q$.

In this paper, the following property is important. (*see also Theorem 2.23* [15]).

Property 3: For each $i=0,1,2,\cdots,p-1 \in \mathbb{F}_p$, the number of elements in $\mathbb{F}_q$ whose trace with respect to $\mathbb{F}_p$ is i is given by $q/p=p^{m-1}$. □

(Proof) Elements in $\mathbb{F}_q$ are the roots of x^q-x. It is factorized over $\mathbb{F}_p$ as follows:

$$\begin{aligned}x^q-x&=x^{p^m}-x\\&=\prod_{i=0}^{p-1}(\mathrm{Tr}(x)-i).\end{aligned} \tag{9}$$

Since the degree of $\mathrm{Tr}(x)$ is p^{m-1} and $\mathrm{Tr}(x)$ does not have any duplicated roots, this property is shown. □

Thus, the number of *non-zero* elements in $\mathbb{F}_q$ whose trace is zero is given by $q/p-1$.

2.4 Dual Bases

Dual basis that is used for some proofs shown in this paper is defined as follows:

Definition 1: Let $\mathcal{A}=\{\alpha_0,\alpha_1,\cdots,\alpha_{m-1}\}$ be a basis in $\mathbb{F}_{p^m}$, the basis $\mathcal{B}=\{\beta_0,\beta_1,\cdots,\beta_{m-1}\}$ such that

$$\mathrm{Tr}\left(\alpha_i\beta_j\right)=\begin{cases}1 & \text{if } i=j,\\ 0 & \text{otherwise}\end{cases} \tag{10}$$

is called the dual basis of $\mathcal{A}$. □

The dual basis of an arbitrary basis is uniquely determined [15]. In this paper, the following property is important.

Property 4: Let $\mathcal{A}$ and $\mathcal{B}$ be a basis and its dual basis in $\mathbb{F}_{p^m}$, respectively. Based on the definition of dual basis and the linearity of trace function, if α_l of a basis $\mathcal{A}$ in $\mathbb{F}_{p^m}$ is a non-zero prime field element,

$$\mathrm{Tr}\left(\alpha_l\beta_j\right)=\alpha_l\mathrm{Tr}\left(\beta_j\right)=\begin{cases}1 & \text{if } j=l,\\ 0 & \text{otherwise},\end{cases} \tag{11}$$

where $0 \le l, j \le m-1$. Thus, when $\alpha_l=1$, $\mathrm{Tr}(\beta_l)=1$. □

(Proof) Based on the definition of dual basis,

$$\mathrm{Tr}\left(\alpha_l\beta_j\right)=\begin{cases}1 & \text{if } j=l,\\ 0 & \text{otherwise.}\end{cases} \tag{12}$$

Since the trace function has a linearity for a non-zero prime field element α_l,

$$\mathrm{Tr}\left(\alpha_l\beta_j\right)=\alpha_l\mathrm{Tr}\left(\beta_j\right). \tag{13}$$

Thus, we obtain Eq. (11). Especially for $j=l$,

$$\mathrm{Tr}(\alpha_l\beta_l)=\alpha_l\mathrm{Tr}(\beta_l)=1. \tag{14}$$

Therefore, when $\alpha_l=1$, $\mathrm{Tr}(\beta_l)$ is determined by 1. □

2.5 Multi-Value Sequence and Its Properties

This paper deals with k-value sequence, where k is a prime factor of $p-1$.

2.5.1 Notation

Let a k-value sequence S be denoted as

$$S=\{s_i\},\ i=0,1,2,\cdots,n-1,\cdots, \tag{15}$$

where $s_i \in \{0,1,\cdots,k-1\}$ and n is the period of the sequence such as $s_i=s_{n+i}$.

2.5.2 Autocorrelation and Cross-Correlation

The periodic autocorrelation $\mathrm{R}_S(x)$ of sequence S shifted by x is generally defined as

$$\mathrm{R}_S(x)=\sum_{i=0}^{n-1}\tilde{\epsilon}_k^{s_{i+x}-s_i}, \tag{16}$$

where $\tilde{\epsilon}_k$ is a primitive k-th root of unity over the *complex numbers*. It follows that

$$\mathrm{R}_S(0)=\sum_{i=0}^{n-1}\tilde{\epsilon}_k^{0}=n. \tag{17}$$

Let $\hat{S}=\{\hat{s}_i\}$ be another k-value sequence of period n, *cross-correlation* at x shifted is defined as follows:

$$\mathrm{R}_{\hat{S},S}(x)=\sum_{i=0}^{n-1}\tilde{\epsilon}_k^{\hat{s}_{i+x}-s_i}. \tag{18}$$

2.5.3 Linear Complexity

Since this paper considers k-value sequences with coefficients $\{0, 1, \cdots, k-1\}$, the linear complexity $\mathrm{LC}(\mathcal{S})$ of sequence $\mathcal{S}$ of period n is defined as follows:

$$\mathrm{LC}(\mathcal{S}) = n - \deg\left(\gcd\left(x^n - 1, h_{\mathcal{S}}(x)\right)\right), \tag{19}$$

where $h_{\mathcal{S}}(x)$ of $\mathcal{S} = \{s_i\}$ is defined over $\mathbb{F}_k$ as

$$h_{\mathcal{S}}(x) = \sum_{i=0}^{n-1} s_i x^i. \tag{20}$$

It is noted that $\gcd(x^n - 1, h_{\mathcal{S}}(x))$ in Eq. (19) needs to be evaluated over $\mathbb{F}_k$, where k is a prime number such that k divides $p-1$. It is said that the linear complexity of pseudo random sequences for security applications is preferred to be large. On the other hand, as an counter example, it is known that the maximum length sequence of period $p^m - 1$ has the minimal linear complexity m.

2.6 Previous Work

Binary geometric sequences have been well studied [11]–[14]. The authors [10] have also proposed a binary sequence that uses primitive element in extension field, trace function for mapping vectors to scalars, and Legendre symbol for binarizing the trace values. This section briefly introduces the binary geometric sequence of the previous work [10] using its original notations. Then, note that the binary sequence in this section is given with $\{1, -1\}$ and some definitions are slightly different such as Eq. (22) and Eq. (25).

2.6.1 Definition

The binary geometric sequence $\mathcal{S}$ is given as follows:

$$\mathcal{S}_2 = \left\{s_i \mid s_i = f_2\left(\mathrm{Tr}\left(\omega^i\right)\right)\right\}, \tag{21}$$

where p is an odd prime number as the characteristic of $\mathbb{F}_p$, ω is a primitive element in $\mathbb{F}_{p^m}$, and

$$f_2(x) = \begin{cases} 1 & \text{if } x = 0 \bmod p \\ \left(\frac{x}{p}\right)_2 & \text{otherwise} \end{cases} \tag{22}$$

binarizes scalars given by the trace function $\mathrm{Tr}(\cdot)$. $\left(\frac{x}{p}\right)_2$ is just the Legendre symbol, Then, it is theoretically proven that its period is $2(p^m - 1)/(p-1)$.

2.6.2 Autocorrelation

The autocorrelation of $\mathcal{S}_2$ is theoretically given. Since the previous work [10] basically considers the binary sequence with $\{1, -1\}$, note that the calculation of the autocorrelation is slightly different from Eq. (16).

$$\begin{aligned} \mathrm{R}_{\mathcal{S}_2}(x) &= \sum_{i=0}^{n-1} s_i s_{i+x} \\ &= \begin{cases} \dfrac{2(p^m-1)}{p-1} & \text{if } x = 0, \\ -2p^{m-1} + \dfrac{2(p^{m-1}-1)}{p-1} & \text{else if } x = n/2, \\ \dfrac{2(p^{m-2}-1)}{p-1} & \text{otherwise.} \end{cases} \end{aligned} \tag{23}$$

2.6.3 Linear Complexity

Replacing $\{1, -1\}$ by $\{0, 1\}$ respectively, the linear complexity of the binary sequence $\mathcal{S}_2$ is evaluated by Eq. (19) with $k = 2$, where the polynomials in Eq. (19) need to be defined over $\mathbb{F}_2$. Then, it is experimentally observed that the linear complexity of $\mathcal{S}_2$ is the maximum, that is the period $2(p^m - 1)/(p-1)$ itself. Especially for $m = 2$, it is theoretically proven.

3. Proposal of a New Multi-Value Sequence

This paper proposes k-value sequence $\mathcal{T}$. This section at first shows its definition and then introduces some important features such as cross-correlation, autocorrelation, period, and linear complexity.

3.1 Definition

This paper proposes k-value sequence as follows:

$$\mathcal{T} = \left\{t_i \mid t_i = f_k\left(\mathrm{Tr}\left(\omega^i\right) + A\right)\right\}, \tag{24}$$

where p is an odd prime number as the characteristic of $\mathbb{F}_p$, k is a prime factor of $p-1$, ω is a primitive element in $\mathbb{F}_{p^m}$, A is a *non-zero* constant in $\mathbb{F}_p$, and

$$f_k(x) = \begin{cases} 0 & \text{if } x = 0 \bmod p \\ \log_{\epsilon_k}\left(\left(\frac{x}{p}\right)_k\right) & \text{otherwise} \end{cases} \tag{25}$$

is a mapping function from $\mathbb{F}_p$ to $\mathbb{F}_k$. As introduced in Sect. 2.2, $f_k(x)$ with a *fixed* ϵ_k maps an arbitrary element $x \in \mathbb{F}_p$ to an element in $\mathbb{F}_k$. Note here that $f_k(x)$ supports the case of $x = 0 \in \mathbb{F}_p$. This mapping function $f_k(\cdot)$ has the following property.

Property 5: Consider $x, y \in \mathbb{F}_p$. If $x \neq 0$ and $y \neq 0$,

$$f_k(x) \pm f_k(y) = f_k(xy^{\pm 1}). \tag{26}$$

□

It is found from Sect. 2.2 and Property 2 that the mapping function satisfies the following equation, where C is a non-zero element in $\mathbb{F}_p$.

$$\sum_{v=0}^{k-1} \tilde{\epsilon}_k^v = 0. \tag{27a}$$

$$\sum_{u=1}^{p-1} \tilde{\epsilon}_k^{f_k(u)} = \sum_{u=1}^{p-1} \tilde{\epsilon}_k^{f_k(u^{-1})} = \left(\frac{p-1}{k}\right) \sum_{v=0}^{k-1} \tilde{\epsilon}_k^v = 0. \tag{27b}$$

$$\sum_{u=1}^{p-1} \tilde{\epsilon}_k^{f_k(Cu)} = \sum_{u=1}^{p-1} \tilde{\epsilon}_k^{f_k(Cu^{-1})} = 0. \tag{27c}$$

3.2 Cross-Correlation

Suppose that there are two different sequences $\mathcal{T} = \{t_i\}$ and $\hat{\mathcal{T}} = \{\hat{t}_i\}$ respectively defined as

$$\mathcal{T} = \left\{ t_i \mid t_i = f_k\left(\mathrm{Tr}\left(\omega^i\right) + A\right) \right\}, \tag{28a}$$

$$\hat{\mathcal{T}} = \left\{ \hat{t}_i \mid \hat{t}_i = f_k\left(\mathrm{Tr}\left(\omega^i\right) + \hat{A}\right) \right\}. \tag{28b}$$

The relation between A and $\hat{A}$, where they are non-zero elements in $\mathbb{F}_p$, will be represented with a generator $g \in \mathbb{F}_p$ and a certain index $0 \le h \le p-2$ as

$$\hat{A} = g^h A. \tag{29}$$

Let g be $\omega^{(p^m-1)/(p-1)}$ for the following proofs[†]. Their cross-correlation is given by

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{\hat{t}_{i+x}-t_i}, \tag{30}$$

where n is the period. It is found from the following sections that the period n is given by $p^m - 1$. When $h = 0$, $\hat{A}$ is equal to A and thus the correlation is the autocorrelation of $\mathcal{T}$.

Then, Theorem 1 gives the cross-correlation $\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x)$.

Theorem 1: The cross-correlation between $\hat{\mathcal{T}}$ and $\mathcal{T}$ given by Eq. (28) is given as follows:

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = \begin{cases} p^{m-1} + \left(p^m - 1 - p^{m-1}\right)\tilde{\epsilon}_k^{f_k(g^h)} & \text{if } x = h\bar{n}, \\ p^{m-1}\left(\tilde{\epsilon}_k^{f_k(A(g^h-g^j))} + \tilde{\epsilon}_k^{-f_k(A(1-g^{h-j}))} - \tilde{\epsilon}_k^{f_k(g^j)}\right) - \tilde{\epsilon}_k^{f_k(g^h)} & \\ & \text{else if } x = j\bar{n}, \\ p^{m-2} - \tilde{\epsilon}_k^{f_k(g^h)} & \text{otherwise}, \end{cases} \tag{31}$$

where $\bar{n} = n/(p-1) = (p^m-1)/(p-1)$, h satisfies Eq. (29), and $0 \le j \ne h \le p-2$. □

The proof for each case of Eq. (31) is shown below. In what follows, it should be noted that i mainly appeared at summations means $0 \le i < n = (p^m - 1)$.

3.2.1 The Case of $x = h\bar{n}$

In this case, the cross-correlation is calculated by

$$\begin{aligned} \mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) &= \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k(g^h\mathrm{Tr}(\omega^i)+g^hA)-f_k(\mathrm{Tr}(\omega^i)+A)} \\ &= \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k(g^h(\mathrm{Tr}(\omega^i)+A))-f_k(\mathrm{Tr}(\omega^i)+A)}. \end{aligned} \tag{32}$$

Applying Property 5 and corresponding to whether or not $\mathrm{Tr}\left(\omega^i\right) + A = 0$, it is developed as

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = \sum_{\mathrm{Tr}(\omega^i)+A=0} \tilde{\epsilon}_k^0 + \sum_{\mathrm{Tr}(\omega^i)+A\ne 0} \tilde{\epsilon}_k^{f_k(g^h)}, \tag{33}$$

where it should be also noted that $g^h \ne 0$. Thus, based on Property 3, the following relation is obtained.

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = p^{m-1} + \left(p^m - 1 - p^{m-1}\right)\tilde{\epsilon}_k^{f_k(g^h)}. \tag{34}$$

3.2.2 The Case of $x = j\bar{n}$, $j \ne h$

In this case, the cross-correlation is calculated by

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k(g^j\mathrm{Tr}(\omega^i)+g^hA)-f_k(\mathrm{Tr}(\omega^i)+A)}. \tag{35}$$

Using Property 5 and depending on the values of $\mathrm{Tr}(\omega^i) + A$ and $g^j\mathrm{Tr}(\omega^i) + g^hA$, it is developed as follows:

$$\begin{aligned} \mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = &\sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA\ne 0 \\ \mathrm{Tr}(\omega^i)+A=0}} \tilde{\epsilon}_k^{f_k(A(g^h-g^j))} \\ &+ \sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA=0 \\ \mathrm{Tr}(\omega^i)+A\ne 0}} \tilde{\epsilon}_k^{-f_k(A(1-g^{h-j}))} \\ &+ \sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA\ne 0 \\ \mathrm{Tr}(\omega^i)+A\ne 0}} \tilde{\epsilon}_k^{f_k\left((g^j\mathrm{Tr}(\omega^i)+g^hA)(\mathrm{Tr}(\omega^i)+A)^{-1}\right)}. \end{aligned} \tag{36}$$

For example, when $\mathrm{Tr}\left(\omega^i\right) + A = 0$, since $j \ne h$,

$$g^j\mathrm{Tr}\left(\omega^i\right) + g^hA = A(g^h - g^j) \ne 0. \tag{37}$$

Based on Property 3, the first and second summations are respectively calculated by

$$\sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA\ne 0 \\ \mathrm{Tr}(\omega^i)+A=0}} \tilde{\epsilon}_k^{f_k(A(g^h-g^j))} = p^{m-1}\tilde{\epsilon}_k^{f_k(A(g^h-g^j))}, \tag{38}$$

$$\sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA=0 \\ \mathrm{Tr}(\omega^i)+A\ne 0}} \tilde{\epsilon}_k^{-f_k(A(1-g^{h-j}))} = p^{m-1}\tilde{\epsilon}_k^{-f_k(A(1-g^{h-j}))}, \tag{39}$$

where the following condition and facts should be noted.

- As introduced, A is a *non-zero* constant in $\mathbb{F}_p$.

[†]Since ω is a generator of $\mathbb{F}_{p^m}^*$, $g = \omega^{(p^m-1)/(p-1)}$ is a generator of $\mathbb{F}_p^*$.

- When $\mathrm{Tr}\left(\omega^i\right) + A = 0$, $g^j\mathrm{Tr}\left(\omega^i\right) + g^hA \neq 0$.
- When $g^j\mathrm{Tr}\left(\omega^i\right) + g^hA = 0$, $\mathrm{Tr}\left(\omega^i\right) + A \neq 0$.

Consider the third term of R.H.S of Eq. (36). Let $X_i = \mathrm{Tr}\left(\omega^i\right) + A \neq 0$.

$$\sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA\neq 0\\ \mathrm{Tr}(\omega^i)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left((g^j\mathrm{Tr}(\omega^i)+g^hA)(\mathrm{Tr}(\omega^i)+A)^{-1}\right)} = \sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA\neq 0\\ \mathrm{Tr}(\omega^i)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(g^j+A(g^h-g^j)X_i^{-1}\right)}. \tag{40}$$

In order to evaluate Eq. (40), consider the possible value of $X_i \in \mathbb{F}_p$. As shown in Property 3 and noting the exceptions for the first and second terms of R.H.S. in Eq. (36),

$$\#\{X_i|X_i = 0\} = p^{m-1}, \tag{41a}$$
$$\#\{X_i|X_i = A(1-g^{h-j})\} = p^{m-1}, \tag{41b}$$
$$\#\{X_i|X_i = A\} = p^{m-1} - 1, \tag{41c}$$
$$\#\{X_i|X_i = u\} = p^{m-1}, \tag{41d}$$

where $0 \leq i < n$ and for each $u \in \mathbb{F}_p - \{0, A, A(1-g^{h-j})\}$. The first and second summations in Eq. (36) correspond to the cases of Eq. (41a) and Eq. (41b), respectively.

On the other hand, let $Y_i = g^j + A(g^h - g^j)X_i^{-1}$ that is the input of $f_k(\cdot)$ at Eq. (40). Y_i for Eq. (40) does not become 0 because it corresponds to the case of $X_i = A(1-g^{h-j})$ and the case is excluded by the second summation in Eq. (36). In addition, Y_i for Eq. (40) does not become g^j because $h \neq j$. Therefore, Eq. (40) is developed as Eq. (42). (B) in Eq. (42) is added for adjusting the case of $Y_i = g^j$. (C) is for adjusting the number of cases of $X_i = A$ because of Eq. (41c). Then, Eq. (27b) holds at (A).

Then, the cross-correlation is given by

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = p^{m-1}\tilde{\epsilon}_k^{f_k\left(A(g^h-g^j)\right)} + p^{m-1}\tilde{\epsilon}_k^{-f_k\left(A(1-g^{h-j})\right)} - p^{m-1}\tilde{\epsilon}_k^{f_k(g^j)} - \tilde{\epsilon}_k^{f_k(g^h)}. \tag{43}$$

3.2.3 Otherwise

In this case, the cross-correlation is given as follows:

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k\left(\mathrm{Tr}(\omega^{i+x})+g^hA\right)-f_k\left(\mathrm{Tr}(\omega^i)+A\right)}. \tag{44}$$

Since x is not divisible by $\bar{n}$, ω^x does not belong to $\mathbb{F}_p$. By using ω^x, consider the following basis in $\mathbb{F}_{p^m}$:

$$\mathcal{W} = \{\omega^x, 1, \alpha_2, \alpha_3, \cdots, \alpha_{m-1}\} \tag{45}$$

and let $\mathcal{B}$ be the dual basis of $\mathcal{W}$.

$$\mathcal{B} = \{\beta_0, \beta_1, \beta_2, \beta_3, \cdots, \beta_{m-1}\}. \tag{46}$$

Suppose that ω^i is represented as

$$\omega^i = \sum_{l=0}^{m-1} c_{i,l}\beta_l. \tag{47}$$

Then, ω^{i+x} is given by

$$\omega^{i+x} = \sum_{l=0}^{m-1} c_{i,l}\beta_l\omega^x. \tag{48}$$

Based on Property 4, $\mathrm{Tr}\left(\omega^i\right)$ is at first given by

$$\mathrm{Tr}\left(\omega^i\right) = c_{i,1}. \tag{49}$$

Then, since $\mathcal{W}$ and $\mathcal{B}$ are dual bases to each other, it is found that $\mathrm{Tr}\left(\omega^{i+x}\right)$ is given as follows:

$$\mathrm{Tr}\left(\omega^{i+x}\right) = c_{i,0}. \tag{50}$$

Substituting these traces, Eq. (44) is written as

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k(c_{i,0}+g^hA)-f_k(c_{i,1}+A)}. \tag{51}$$

Based on Eq. (27), it is developed as follows:

$$\begin{aligned}\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = &\sum_{\substack{c_{i,0}+g^hA\neq 0\\ c_{i,1}+A\neq 0}} \tilde{\epsilon}_k^{f_k\left((c_{i,0}+g^hA)(c_{i,1}+A)^{-1}\right)}\\ &+ \sum_{\substack{c_{i,0}+g^hA\neq 0\\ c_{i,1}+A=0}} \tilde{\epsilon}_k^{f_k(c_{i,0}+g^hA)}\\ &+ \sum_{\substack{c_{i,0}+g^hA=0\\ c_{i,1}+A\neq 0}} \tilde{\epsilon}_k^{-f_k(c_{i,1}+A)}\\ &+ \sum_{\substack{c_{i,0}+g^hA=0\\ c_{i,1}+A=0}} \tilde{\epsilon}_k^{0}.\end{aligned} \tag{52}$$

Since $\omega^i, 0 \leq i < n$ represent every non-zero element in $\mathbb{F}_{p^m}$, we obtain Eq. (53a) and Eq. (53b) by using Eq. (27b).

$$\sum_{\substack{c_{i,0}+g^hA\neq 0\\ c_{i,1}+A=0}} \tilde{\epsilon}_k^{f_k(c_{i,0}+g^hA)} = 0. \tag{53a}$$

$$\sum_{\substack{c_{i,0}+g^hA=0\\ c_{i,1}+A\neq 0}} \tilde{\epsilon}_k^{-f_k(c_{i,1}+A)} = 0. \tag{53b}$$

In addition, we have

$$\sum_{\substack{c_{i,0}+g^hA=0\\ c_{i,1}+A=0}} \tilde{\epsilon}_k^{0} = p^{m-2}. \tag{53c}$$

On the other hand, in the same of the calculation procedure of Eq. (42), the first term of R.H.S. in Eq. (52) is developed as

$$\sum_{\substack{c_{i,0}+g^hA\neq 0\\ c_{i,1}+A\neq 0}} \tilde{\epsilon}_k^{f_k\left((c_{i,0}+g^hA)(c_{i,1}+A)^{-1}\right)} = p^{m-2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\tilde{\epsilon}_k^{f_k(ab^{-1})} - \tilde{\epsilon}_k^{f_k(g^h)}. \tag{54}$$

Since ω^i cannot represent the zero vector, the number of

$$\sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA\neq 0\\ \mathrm{Tr}(\omega^i)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(g^j+A(g^h-g^j)X_i^{-1}\right)} = \left(\tilde{\epsilon}_k^{f_k(g^h)} - \tilde{\epsilon}_k^{f_k(g^h)}\right) + \left(p^{m-1}\tilde{\epsilon}_k^{f_k(g^j)} - p^{m-1}\tilde{\epsilon}_k^{f_k(g^j)}\right) + \sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA\neq 0\\ \mathrm{Tr}(\omega^i)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(g^j+A(g^h-g^j)X_i^{-1}\right)}$$

$$= \underbrace{\left[\sum_{\substack{g^j\mathrm{Tr}(\omega^i)+g^hA\neq 0\\ \mathrm{Tr}(\omega^i)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(g^j+A(g^h-g^j)X_i^{-1}\right)} + \underbrace{p^{m-1}\tilde{\epsilon}_k^{f_k(g^j)}}_{\text{(B)}} + \underbrace{\tilde{\epsilon}_k^{f_k(g^h)}}_{\text{(C)}}\right]}_{\text{(A)}} - p^{m-1}\tilde{\epsilon}_k^{f_k(g^j)} - \tilde{\epsilon}_k^{f_k(g^h)}$$

$$= \underbrace{0}_{\text{(A)}} - p^{m-1}\tilde{\epsilon}_k^{f_k(g^j)} - \tilde{\epsilon}_k^{f_k(g^h)}. \tag{42}$$

vectors such that $c_{i,0} = 0$ and $c_{i,1} = 0$ is one less than that of the other combinations such as $c_{i,0} = 0$ and $c_{i,1} = 1$. Therefore, the last subtraction $-\tilde{\epsilon}_k^{f_k(g^h)}$ in Eq. (54) is required. The first summation of R.H.S. in Eq. (54) becomes 0 from Eq. (27b). Thus, the following relation holds.

$$\sum_{\substack{c_{i,0}+g^hA\neq 0\\ c_{i,1}+A\neq 0}} \tilde{\epsilon}_k^{f_k\left((c_{i,0}+g^hA)(c_{i,1}+A)^{-1}\right)} = -\tilde{\epsilon}_k^{f_k(g^h)}. \tag{55}$$

Thus, the cross-correlation $\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x)$ is given by

$$\mathrm{R}_{\hat{\mathcal{T}},\mathcal{T}}(x) = p^{m-2} - \tilde{\epsilon}_k^{f_k(g^h)}. \tag{56}$$

Finally, the cross-correlation of the sequences $\hat{\mathcal{T}}$ and $\mathcal{T}$, that is Eq. (31), is proven.

3.3 Autocorrelation and Period

The autocorrelation of the sequence $\mathcal{T}$ is evaluated by just substituting $h = 0$ to the cross-correlation of Eq. (31).

$$\mathrm{R}_{\mathcal{T}}(x) = \begin{cases} p^m - 1 & \text{if } x = h\bar{n}, \\ p^{m-1}\left(\tilde{\epsilon}_k^{f_k(A(1-g^j))} + \tilde{\epsilon}_k^{-f_k(A(1-g^{-j}))} - \tilde{\epsilon}_k^{f_k(g^j)}\right) - 1 & \\ & \text{else if } x = j\bar{n}, \\ p^{m-2} - 1 & \text{otherwise.} \end{cases} \tag{57}$$

Based on the above autocorrelation, it is found that the period of the sequence is explicitly given by $p^m - 1$.

3.4 Linear Complexity

Though this paper could not theoretically show, by testing a lot of cases of parameters p, m, k, and A, it was experimentally observed that the linear complexity of the proposed sequence mostly satisfied the following relation.

$$\mathrm{LC}(\mathcal{T}) = \frac{C(p^m - 1)}{p - 1}, \tag{58}$$

where C is a positive constant less than or equal to $p - 1$. When $C = p - 1$, the linear complexity is $p^m - 1$ that is the maximum because the period of the proposed sequence is $p^m - 1$. It is found from the following examples that the proposed sequence often has the maximum linear complexity. Chan and Games [11] have theoretically shown a similar property for q-ary M-sequences where q is a power of odd prime number.

4. Examples and Discussion

This section experimentally shows the properties of the proposed sequence such as autocorrelation, cross-correlation, and linear complexity with some examples. In this section, the notation $\mathcal{T}_2$, for example, denotes the proposed sequence with the parameter $A = 2$. In the observation, $|x|$ gives the absolute value of a complex number x and the floor function $\lfloor y \rfloor$ gives the greatest integer smaller than y.

4.1 $p = 7, m = 2, k = 3$, and $A = 2, 3$

Consider the primitive polynomial $f(x) = x^2 + 5x + 3$ over $\mathbb{F}_7$. In this case, the period of sequence is $p^m - 1 = 48$. Then, $\mathcal{T}_2$ is given as follows:

$$\begin{aligned} \mathcal{T}_2 = \{&1,1,0,0,2,1,0,1,0,0,1,0,2,0,0,0,\\ &0,0,2,1,2,0,1,0,0,0,1,2,2,0,2,0,\\ &1,1,0,1,2,1,1,1,2,2,0,0,2,2,0,2\}. \end{aligned} \tag{59}$$

The autocorrelation of $\mathcal{T}_2$ is given as follows:

$$|R_{\mathcal{T}_2}(x)| = \begin{cases} 48 & \text{if } x = 0 \\ 6 & \text{else if } x = 8, 16, 32, 40 \\ 15 & \text{else if } x = 24 \\ 0 & \text{otherwise} \end{cases}, \tag{60}$$

and Fig. 1 is drawn. Then, the linear complexity is

$$\mathrm{LC}(\mathcal{T}_2) = 32. \tag{61}$$

On the other hand, $\mathcal{T}_3$ is given as follows:

$$\begin{aligned} \mathcal{T}_3 = \{&2,2,0,0,1,2,0,2,2,2,1,0,1,2,0,2,\\ &0,0,0,1,1,0,1,0,0,0,2,0,1,0,0,0,\\ &1,1,2,2,1,1,2,1,0,0,0,2,1,0,2,0\}. \end{aligned} \tag{62}$$

It should be noted that $\mathcal{T}_3$ is different from $\mathcal{T}_2$. Then, the

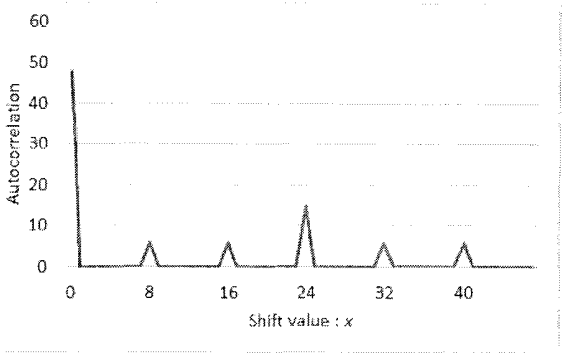


Fig. 1 $|R_{\mathcal{T}_2}(x)|$ with $p = 7, m = 2, k = 3$.

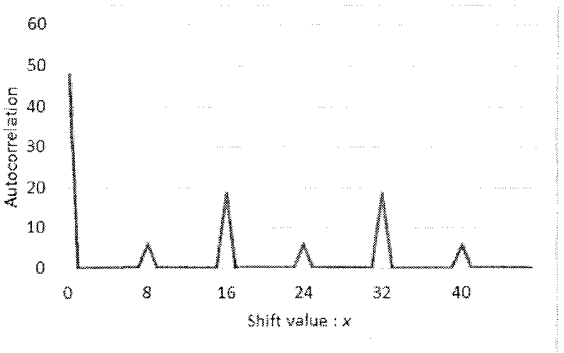


Fig. 2 $|R_{\mathcal{T}_3}(x)|$ with $p = 7, m = 2, k = 3$.

autocorrelation of $\mathcal{T}_3$ becomes as follows:

$$\lfloor |R_{\mathcal{T}_3}(x)| \rfloor = \begin{cases} 48 & \text{if } x = 0 \\ 6 & \text{else if } x = 8, 24, 40 \\ 18 & \text{else if } x = 16, 32 \\ 0 & \text{otherwise} \end{cases}, \tag{63}$$

and Fig. 2 is drawn. In this case, the linear complexity is the maximum.

$$\mathrm{LC}(\mathcal{T}_3) = 48. \tag{64}$$

The cross-correlation of $\mathcal{T}_2$ and $\mathcal{T}_3$ becomes as follows:

$$\lfloor |R_{\mathcal{T}_2,\mathcal{T}_3}(x)| \rfloor = \begin{cases} 7 & \text{if } x = 0, 8, 16 \\ 13 & \text{else if } x = 24 \\ 17 & \text{else if } x = 32. \\ 37 & \text{else if } x = 40 \\ 1 & \text{otherwise} \end{cases} \tag{65}$$

Figure 3 shows the graph of cross-correlation $|R_{\mathcal{T}_2,\mathcal{T}_3}(x)|$. As previously described, it has one large peek.

4.2 $p = 11, m = 2, k = 5$, and $A = 4, 5$

Consider the primitive polynomial $f(x) = x^2 + 3x + 6$ over

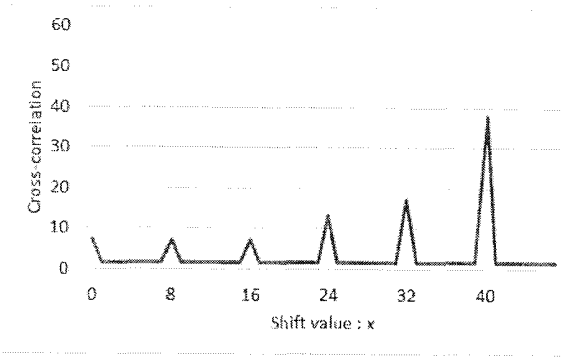


Fig. 3 $|R_{\mathcal{T}_2,\mathcal{T}_3}(x)|$ with $p = 7, m = 2, k = 3$.

$\mathbb{F}_{11}$. In this case, the period of sequence is $p^m - 1 = 120$. Then, $\mathcal{T}_4$ and $\mathcal{T}_5$ are given as Eq. (66). Figure 4 and Fig. 5 show their autocorrelation graphs.

Their linear complexities are both the maximum.

$$\mathrm{LC}(\mathcal{T}_4) = 120, \tag{67a}$$
$$\mathrm{LC}(\mathcal{T}_5) = 120. \tag{67b}$$

Their cross-correlation becomes as shown in Fig. 6. It is found that the cross-correlation has one large peek that corresponds to the case of $x = h\bar{n}$ in Eq. (31).

4.3 $p = 13, m = 3, k = 3$, and $A = 5, 6$

Consider the primitive polynomial $f(x) = x^3 + 7x^2 + 3x + 6$ over $\mathbb{F}_{13}$. In this case, the period of sequence is given by $p^m - 1 = 2196$. As examples, Fig. 7 and Fig. 8 show the autocorrelations of $\mathcal{T}_5$ and $\mathcal{T}_6$, respectively.

Their linear complexities are

$$\mathrm{LC}(\mathcal{T}_5) = 1647, \tag{68a}$$
$$\mathrm{LC}(\mathcal{T}_6) = 2196. \tag{68b}$$

Their cross-correlation is shown in Fig. 9.

4.4 Observation and Practicality of the Proposed Sequence

It was shown that the proposed random sequence could have a long period and high linear complexity by appropriately setting the parameters p, m, k, and A. These properties are important for security applications such as stream cipher. Particularly, since the autocorrelation of the proposed sequence has been theoretically shown as Eq. (57), it theoretically guarantees a long period. In addition, since the autocorrelation has a few peaks only such as Fig. 8 and it has a high linear complexity that is experimentally observed. The proposed sequence efficiently realizes the difficulty of the bit estimation by the eavesdropper. On the other hand, the cross-correlation given by Eq. (31) also has a few peaks even with another parameter A. Particularly, one of the peaks become a large value as shown in Fig. 9. It means that these

$$\mathcal{T}_4 = \{1,0,0,4,3,4,3,3,1,4,4,0,1,2,2,0,0,0,3,0,1,2,0,2,0,1,1,2,4,2,3,4,0,4,2,1,3,1,1,1,2,1,3,2,3,0,1,1,0,0,0,1,4,1,3,4,0,2,1,0,$$
$$4,3,3,0,0,0,3,0,4,1,0,3,2,0,0,3,2,3,3,2,2,1,3,0,4,4,4,0,1,0,3,1,4,0,0,4,0,2,2,4,1,4,3,1,0,3,4,2,2,4,4,2,0,2,3,0,2,0,2,4\}, \quad (66a)$$

$$\mathcal{T}_5 = \{3,4,4,0,2,0,1,2,3,2,0,4,1,4,4,4,0,4,1,0,1,3,4,4,0,3,3,4,2,4,1,2,0,0,4,3,2,1,1,3,3,3,1,3,2,4,3,1,0,0,0,1,0,1,1,0,0,4,1,0,$$
$$2,2,2,0,4,0,1,4,2,3,0,2,3,0,0,2,4,2,1,4,3,1,2,0,0,2,2,0,3,0,1,3,0,0,0,2,4,3,3,2,1,2,1,1,4,2,2,3,4,0,0,3,0,3,1,0,4,0,3,0\}. \quad (66b)$$

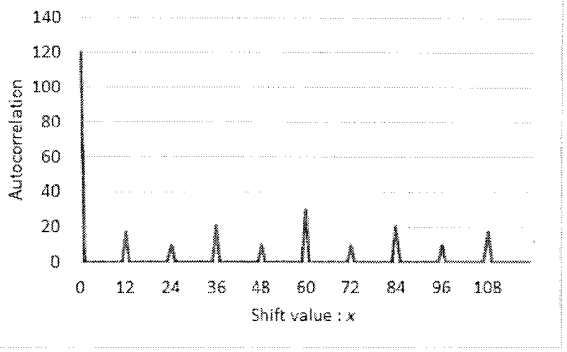


Fig. 4 $|R_{\mathcal{T}_4}(x)|$ with $p = 11, m = 2, k = 5$.

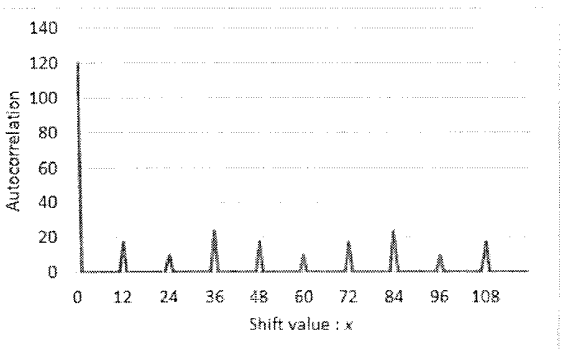


Fig. 5 $|R_{\mathcal{T}_5}(x)|$ with $p = 11, m = 2, k = 5$.

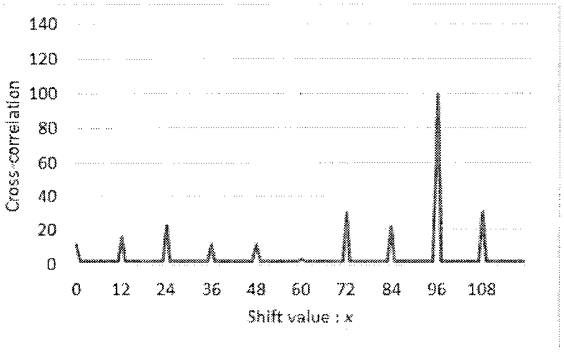


Fig. 6 $|R_{\mathcal{T}_4,\mathcal{T}_5}(x)|$ with $p = 11, m = 2, k = 5$.

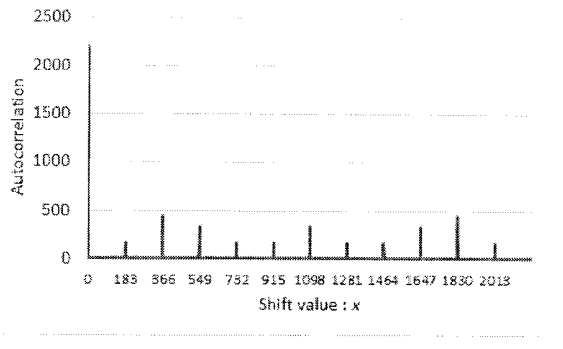


Fig. 7 $|R_{\mathcal{T}_5}(x)|$ with $p = 13, m = 3, k = 3$.

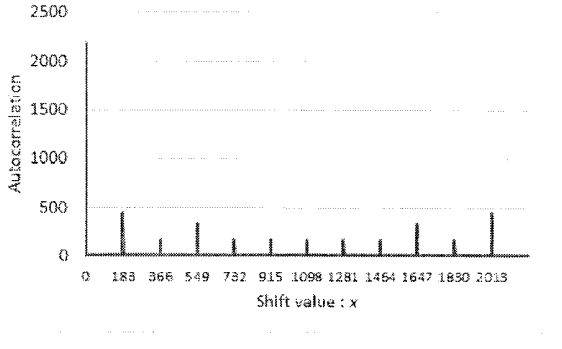


Fig. 8 $|R_{\mathcal{T}_6}(x)|$ with $p = 13, m = 3, k = 3$.

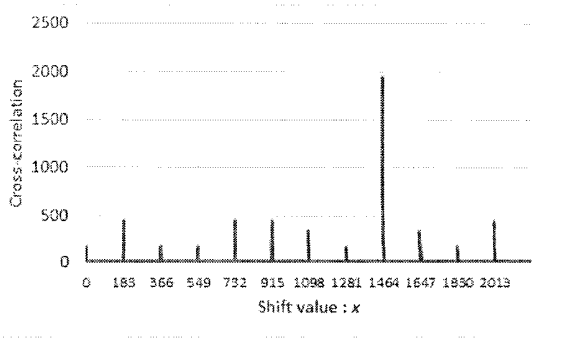


Fig. 9 $|R_{\mathcal{T}_5,\mathcal{T}_6}(x)|$ with $p = 13, m = 3, k = 3$.

sequences with different A's are able to share some partial information. When we apply another *non-conjugate* primitive element as ω of Eq. (24), a different tendency of the cross-correlation is observed as introduced in the appendix. It means that, from the security viewpoint, the use of the proposed sequences with the same primitive element and different A's must be careful.

As introduced above, the proposed method generates pseudo random multi-value sequences of long period and

high linear complexity for the use of security applications. As far as the authors know, there are lots of considerations to use multi-value (*non binary*) sequences for communications from the viewpoints of auto and cross-correlations [19], [20]; however, there are few papers about security applications with pseudo random *non binary* sequences of high linear complexity. The most typical security application of pseudo random sequence will be an XOR-based stream cipher for which a pseudo random *binary* sequence of long period and high linear complexity is used and it needs to be quickly generated. For this purpose, the proposed method is able to generate a pseudo random binary sequence with $k = 2$; however, it is not practical as it is because it needs to calculate Legendre symbol. As an approach for overcoming this inefficiency, let the characteristic p be small such as 3 or 5 and then the calculation of Legendre symbol will be implemented with a look up table. In this case, the degree m inversely needs to be large for satisfying a long period and high linear complexity. However, as reported in our previous work [10], the numbers of values in a period of the proposed sequence are not balanced because of the mapping function Eq. (25). It is not appropriate for security applications. In order to balance it, the authors are still trying several approaches [21].

5. Conclusion and Future Works

In this paper, we have proposed a multi-value sequence by utilizing primitive element, power residue symbol, and trace function. The features of the proposed sequence such as period, autocorrelation, cross-correlation, and linear complexity are determined from four parameters which are: characteristic p, extension degree m, prime factor k of $p-1$, and a non-zero scalar A in $\mathbb{F}_p$. Then, this paper observed some examples from the viewpoints of these features. We also showed the mathematical proofs of these features except for linear complexity.

As a future work, some inefficiencies in the calculation procedure should be improved. In detail, it requires trace calculation, exponentiation for power residue symbol, and index calculation for the mapping function $f_k(\cdot)$. Some ideas such as appropriately choosing parameters and then utilizing look up tables will be applied in the future works.

Acknowledgment

This work has been supported by JSPS KAKENHI Grant-in-Aid for Scientific Research (B) Number 25280047.

References

[1] T.W. Cusick, C. Ding, and A. Renvall, Stream Ciphers and Number Theory, North-Holland Mathematical Library, vol.55, Elsevier Science, 1998.
[2] S.W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, 1967.
[3] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, Discrete Mathematics and Its Applications, CRC Press, 1996.
[4] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications Handbook, Revised ed., McGraw-Hill, 1994.
[5] NIST FIPS197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[6] NIST FIPS186-4, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[7] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," IEEE Trans. Inform. Theory, vol.42, no.6, pp.2254–2255, 1996.
[8] C. Ding, T. Hesseseth, and W. Shan, "On the linear complexity of Legendre sequences," IEEE Trans. Inform. Theory, vol.44, no.3, pp.1276–1278, 1998.
[9] N. Zierler, Legendre Sequence, M.I.T. Lincoln Publications, 1958.
[10] Y. Nogami, K. Tada, and S. Uehara, "A geometric sequence binarized with legendre symbol over odd characteristic field and its properties," IEICE Trans. Fundamentals, vol.E97-A, no.12, pp.2336–2342, 2014.
[11] A.H. Chan and R.A. Games, "On the linear span of binary sequences obtained from q-ary m-sequences, q odd," IEEE Trans. Inform. Theory, vol.36, no.3, pp.548–552, 1990.
[12] W. Sun, A. Klapper, and Y.X. Yang, "On correlations of a family of generalized geometric sequences," IEEE Trans. Inform. Theory, vol.47, no.6, pp.2609–2618, 2001.
[13] A. Klapper, "Cross-correlations of geometric sequences in characteristic two," Des. Codes Crypt., vol.3, no.4, pp.347–377, 1993.
[14] A. Klapper, "Large families of sequences with near-optimal correlations and large linear span," IEEE Trans. Inform. Theory, vol.42, no.4, pp.1241–1248, 1996.
[15] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1984.
[16] S.Y. Yan, Number Theory for Computing, 2nd ed., Springer, 2002.
[17] M. Joye and B. Libert, "Efficient cryptosystems from 2^k-th power residue symbols," Advances in Cryptology, EUROCRYPT 2013, Lecture Notes in Computer Science, vol.7881, pp.76–92, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
[18] E.R. Berlekamp, Algebraic Coding Theory, Revised Edition, Aegean Park Press, 1984.
[19] Y.K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," IEEE Trans. Inform. Theory, vol.55, no.4, pp.1815–1823, 2009.
[20] N.Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," IEEE Trans. Inform. Theory, vol.56, no.12, pp.6376–6387, 2010.
[21] K. Tsuchiya, Y. Nogami, and S. Uehara, "Interleaved sequence of NTU sequences of two types," 2016 Symposium on Cryptography and Information Security (SCIS2016), 2016.

Appendix A: Cross-Correlation of the Proposed Sequences with Different and Non-Conjugate Primitive Elements

This section experimentally observes the cross-correlation of the proposed sequences with different and non-conjugate primitive elements.

Consider the following sequences with two different and *non-conjugate* primitive elements ω, $\bar{\omega}$:

$$\mathcal{T} = \left\{ t_i \mid t_i = f_k\left(\mathrm{Tr}\left(\omega^i\right) + A\right) \right\}, \tag{A·1a}$$

$$\bar{\mathcal{T}} = \left\{ \bar{t}_i \mid \bar{t}_i = f_k\left(\mathrm{Tr}\left(\bar{\omega}^i\right) + \bar{A}\right) \right\}. \tag{A·1b}$$

Then, their cross-correlation $\mathrm{R}_{\bar{\mathcal{T}},\mathcal{T}}(x)$ was experimentally

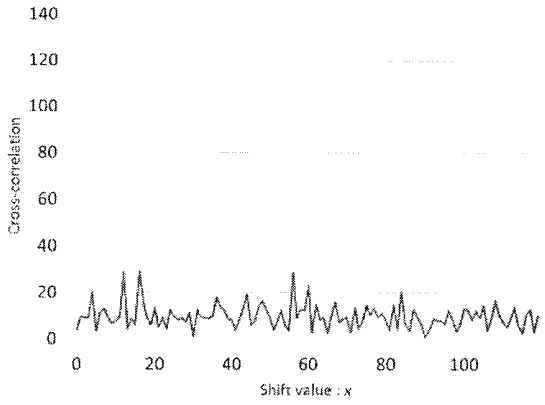


Fig. A·1 $|R_{\tilde{\mathcal{T}}_4,\mathcal{T}_4}(x)|$ with $p = 11, m = 2, k = 5, A = 4, 4$.

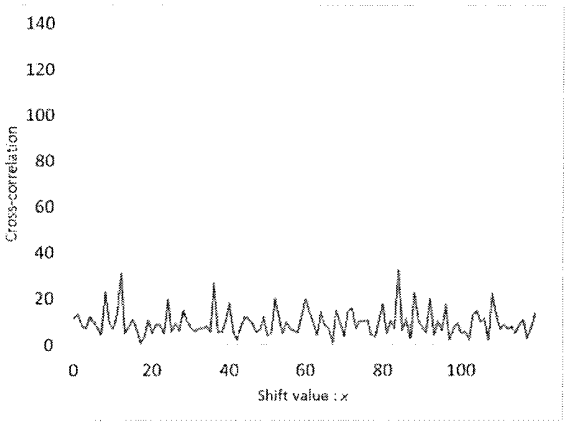


Fig. A·2 $|R_{\tilde{\mathcal{T}}_4,\mathcal{T}_5}(x)|$ with $p = 11, m = 2, k = 5, A = 4, 5$.

observed for which the authors experimented many cases by changing parameters. Figure A·1, Fig. A·2, Fig. A·3, and Fig. A·4 show examples of cross-correlations with the following parameters, respectively:

1. $p = 11, k = 2, m = 5$, and $A = 4, 4$
2. $p = 11, k = 2, m = 5$, and $A = 4, 5$
3. $p = 13, k = 3, m = 3$, and $A = 5, 5$
4. $p = 13, k = 3, m = 3$, and $A = 5, 6$

The difference from that with the same primitive element such as Fig. 9 is explicitly observed.

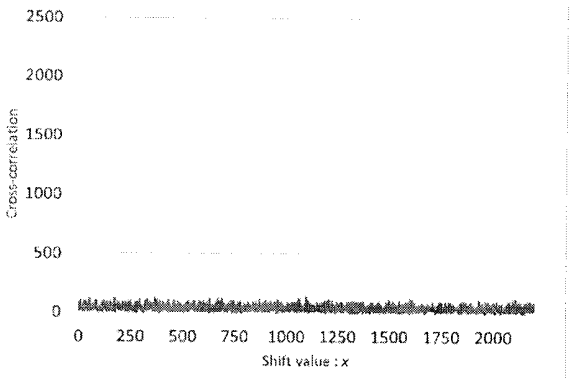


Fig. A·3 $|R_{\tilde{\mathcal{T}}_5,\mathcal{T}_5}(x)|$ with $p = 13, m = 3, k = 3, A = 5, 5$.

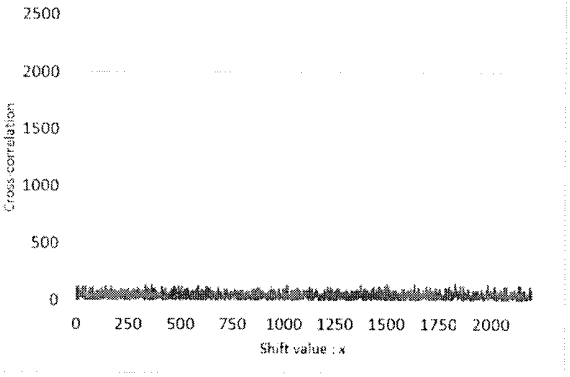
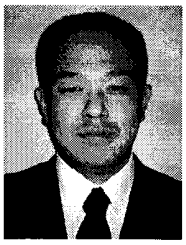
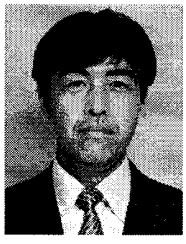


Fig. A·4 $|R_{\tilde{\mathcal{T}}_5,\mathcal{T}_6}(x)|$ with $p = 13, m = 3, k = 3, A = 5, 6$.



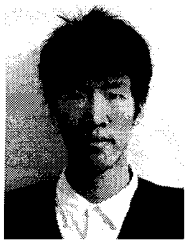
Yasuyuki Nogami graduated from Shinshu University in 1994 and received the Ph.D. degree in 1999 from Shinshu University. He is now an associate professor of Okayama University. His main fields of research are finite field theory and its applications such as recent public key cryptographies. He is now studying about elliptic curve cryptography, pairing-based cryptography, Lattice-based cryptography, pseudo random number generator, Advanced Encryption Standard, and homomorphic encryptions. Recently, he is a member of security research group in Okayama university and particularly focusing on IoT security from the viewpoints of software and hardware implementations. He is a member of IEICE and IEEE.



Satoshi Uehara received the B.E. degree from Saga University and the M.E. degree from Kyushu University, and the Dr. Eng. degree in computer science and system engineering from Kyushu Institute of *Technology, in 1987*, 1989 and 1998, respectively. From 1989 to 2000, he was a research associate at Kyushu Institute of Technology. From 2000, he was with the Department of Information and Media Engineering, The University of Kitakyushu as associate professor, and became a professor in 2009. He is engaged in research on sequence design for cryptography and spread spectrum applications.

Kazuyoshi Tsuchiya received the B.S., the M.S. and the Ph.D. degrees in mathematics from Chuo University, Tokyo, Japan in 1998, 2000 and 2004, respectively. He is a researcher at Koden Electronics Co., Ltd. His research interests include sequences and their applications.

Nasima Begum received the Ph.D. degree in Cryptography and Information Security from Graduate School of Natural Science and Technology, Okayama University, Japan in 2014. She received the B.Sc. and M.Sc. degree in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh, in 2006 and 2010 respectively. She joined as a Lecturer at the department of Computer Science and Engineering, Manarat International University, Dhaka, Bangladesh in January 2007. She became Senior Lecturer in the same department in February 2010. Currently, she is working as a Research Fellow in Secure Wireless System Lab, Graduate School of Natural Science and Technology, Okayama University, Japan. Her research interests include Applied Cryptography & Information Security, Anonymous Communication, Privacy-Preserving Techniques, Pseudo-random Number and its Complexity, Elliptic Curve Cryptography (ECC), Pairing-based Computation, Signal and Image Processing, Artificial Intelligence and Biometric Authentication. She is a member of IEICE, ACM and IEEE.



Hiroto Ino graduated from Okayama University in 2015. He is now a student of the graduate school of natural science and technology, Okayama University. He is interested in pseudo random number defined over finite field.

Robert H. Moleros-Zaragoza received the BSEE and MSEE degrees from the National Autonomous University of Mexico (UNAM) in 1985 and 1987, respectively, and the Ph.D. degree in Electrical Engineering from the University of Hawaii at Manoa in 1992. Robert has research interests in the areas of error correcting coding and digital signal processing for wireless communication and digital storage systems. He is the author of twenty peer-reviewed journal papers, over ninety international peer-reviewed conference papers and the book The Art of Error Correcting Coding (2nd edition, John Wiley and Sons, 2006). Prof. Morelos-Zaragoza holds eighteen patents in the USA, Japan and Europe, and has served as reviewer, editor and technical program committee member in numerous international IEEE conferences and journals in Information Theory and Wireless Communication Systems.