I. J. Computer Network and Information Security, **2017, 9, 54-63**
Published Online September 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.09.07

Pseudo Random Ternary Sequence and Its Autocorrelation Property Over Finite Field

Md. Arshad Ali
Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama 700-8530, Japan
E-mail: arshad@s.okayama-u.ac.jp

Emran Ali, Md. Ahsan Habib, Md. Nadim
Department of Computer Science and Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur-5200, Bangladesh
E-mail: {emran.cse, ahsan.habib, mnadims}@hstu.ac.bd

Takuya Kusaka and Yasuyuki Nogami
Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama 700-8530, Japan
E-mail: {kusaka-t, yasuyuki.nogami}@okayama-u.ac.jp

Received: 14 June 2017; Accepted: 09 August 2017; Published: 08 September 2017

***Abstract*—**In this paper, the authors have proposed an innovative approach for generating a pseudo random ternary sequence by using a primitive polynomial, trace function, and Legendre symbol over odd characteristics field. Let p be an odd prime number, F_p be an odd characteristic prime field, and m be the degree of the primitive polynomial $f(x)$. Let ω be its zero and a primitive element in F_{p^m}. In the beginning, a primitive polynomial $f(x)$ generates maximum length vector sequence, then the trace function $\mathrm{Tr}(\cdot)$ is used to map an element of the extension field F_{p^m} to an element of the prime field F_p, then non-zero scalar $A \in \mathrm{F}_p$ is added to the trace value, and finally the Legendre symbol (a/p) is utilized to map the scalars into ternary sequence having the values, $\{0,1,\text{and}-1\}$. By applying the new parameter A, the period of the sequence is extended to its maximum value that is $n = p^m - 1$. Hence, our proposed sequence has some parameters such as p, m, and A. This paper mathematically explains the properties of the proposed ternary sequence such as period and autocorrelation. Additionally, these properties are also justified based on some experimental results.

***Index Terms*—**Ternary sequence, finite field, autocorrelation, primitive polynomial, trace function, Legendre symbol.

I. Introduction

Pseudo random sequences have been widely employed in numerous applications in information security, cryptography [1], [2] and spread spectrum communications [3]. The main strength of a pseudo random sequence depends on unpredictable random quantities during the sequence generation procedure [5], [6]. Binary sequence intently related to the finite field theory [4]. There is some other type of sequences whose typical properties such as period and autocorrelation have been already theoretically proven. Among them, maximum length sequence (M-sequence) [7], [8] and Legendre sequence (L-sequence) [9], [10] are well-known. By applying the ideas of these sequences, the authors have been trying to construct a sequence whose properties can also be proven.

A. Previous Work

In the previous works [11], [12], the authors have proposed an approach to generate the pseudo random binary sequence. In brief, the previous generating method was as follows:

In the beginning, it used a primitive polynomial of degree m over odd characteristics field F_p. Being a primitive polynomial, it could generate all the vector sequences as elements in F_{p^m}. Then, transformed all the vectors to multi-valued scalars by using the trace function. Next, multi-valued scalars were translated into $\{0,1,\text{and}-1\}$ valued sequence after applying the Legendre symbol. Finally, utilized a mapping function to generate $\{0 \text{ and } 1\}$ valued pseudo random binary sequence.

The previous sequence had some suitable properties such as long period and very good linear complexity. It had a major drawback such as, previous sequence held a

Copyright © 2017 MECS

shorter period of $2\left(p^m-1\right)/\left(p-1\right)$ and inconsistent appearance of 0 and 1 values in each period. Our previous work on pseudo random binary sequence was represented with the parameters p and m, where p represents the odd characteristics field and m represents the degree of the primitive polynomial.

B. Related Works

In a related work [17], the authors considered a multi-valued sequence and observed its period, autocorrelation, and cross-correlation as important properties. In another related work [18], the authors proposed an approach for generating a multi-value sequence and evaluated its linear complexity property. The authors discussed binary sequence generation procedure along with its linear complexity like crucial property [19]. All of these works [17]-[19] utilized some nonlinear mathematical function (such as trace function, Legendre symbol, and so on) during the sequence generation procedure as like the authors' proposed work in this paper.

C. Our Contributions

In this paper a ternary sequence is proposed by the authors having values $\{0,1,\text{and}-1\}$. In this work, a new parameter A is added by the authors, which is a *non-zero* prime field element that is, $A\in \mathrm{F}_p$. This new parameter A extends the shorter period of our previous sequence to its maximum value of p^m-1. Each unique value of A is responsible for generating completely different sequence but it does not have any impact in the calculation of autocorrelation. To evaluate the autocorrelation properties of our proposed sequence, the evaluation procedure is also modified. This new approach can overcome the inefficiency of our previous work [11], [12].

The authors in this paper have proposed an innovative approach for generating the ternary sequence, which extends our previous works [11], [12]. In this approach, a *non-zero* scalar $A\in \mathrm{F}_p$ is added just before applying the Legendre symbol. In brief, the procedure for generating the ternary sequence is as follows:

Let, p be an odd characteristic prime and m be the degree of the primitive polynomial $f(x)$ over F_p. It is well-known that, using the polynomial $f(x)$, it is possible to generate maximum-length vector sequence over F_{p^m}. Let ω be its *zero*, that is a primitive element in F_{p^m}. Then, the sequence-

$$\mathrm{T}=\{t_i\},\ t_i=\left(\mathrm{Tr}\left(\omega^i\right)+A\Big/p\right)\text{for},i=0,1,2,\ldots,\ p^{\mathrm{m}}-2, \quad (1)$$

becomes a maximum-length sequence having a period of p^m-1, where $\mathrm{Tr}(\cdot)$ is the trace function over F_p. After the trace calculation, an additional *non-zero* value $A\in \mathrm{F}_p$ is added to the trace value. Then, the Legendre symbol is applied to map the scalars to $\{0,1,\text{and}-1\}$ valued ternary sequence. The previous works [11], [12] did not apply the addition of *non-zero* scalar A before the Legendre calculation. The period n of the sequence becomes maximum by setting the parameter values p, m, and A.

In this approach, we have some parameters such as odd characteristics prime p, degree of the primitive polynomial m, and *non-zero* scalar A. This paper interprets the generating procedure of the ternary sequence, explains the above-mentioned feature based on the experiment results and shows the mathematical proof.

D. Notations

Here are some notations, which are utilized 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 it denotes the extension degree. F_q^* denotes the multiplicative group of F_p, that is $\mathrm{F}_q^*=\mathrm{F}_p-\{0\}$. The ternary sequence means that each value in this sequence is in the range of $\{0,1,\text{and}-1\}$

II. Preliminaries

This section explains some fundamental concepts of finite field theory such as primitive element, Legendre symbol, trace function, ternary sequence, and periodic autocorrelation. The well-known and important properties are briefly introduced here; see the details in [12].

A. Primitive Element and Primitive Polynomial

It is well-known that every finite field F_q has a multiplicative primitive element, that is a generator of *non-zero* elements in F_q^*. In other words, let g be a generator, every *non-zero* elements are represented by its power g^i for $i=0,1,2\ldots,(q-2)$. The minimal polynomial of a generator is correspondingly called a primitive polynomial.

The following property between F_q and F_p hold (see also Theorem 1.15 [4]).

Property 1: Let g be a generator of F_q^*, $g^{(q-1)/(p-1)}$ is a *non-zero* element in the prime field F_p and is also a generator of F_p^*.

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

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

Therefore, the order of $g^{(q-1)/(p-1)}$ becomes $p-1$. It means that $g^{(q-1)/(p-1)}$ is a generator of F_p^*.

B. Legendre Symbol

The Legendre symbol (a/p) for an arbitrary element a in F_p is generally defined as follows:

$$\left(a/p\right)=\begin{cases}0 & \text{if } a=0\\ 1 & \text{else if } a \text{ is a } non-zero\ QR\\ -1 & \text{otherwise } a \text{ is a } non-zero\ QNR,\end{cases} \quad (3)$$

Legendre symbol is calculated by-

$$\left(a/p\right)=a^{(p-1)/2}\left(\mathrm{mod}\, p\right). \quad (4)$$

Basically, the Legendre symbol is used for checking whether or not a is QR in F_p as shown in the above equation, where QR and QNR stands for *Quadratic Residue* and *Quadratic Non Residue*, respectively. In this paper, the Legendre symbol is used for translating a multi-valued sequence over F_p to a ternary sequence.

Above-mentioned QR and QNR in F_p, holds the following properties (see also Section 6.7 [13]).

Property 2: The number of QRs and that of QNRs in F_p^* are the same. In details, the number is, $(\mathrm{p}-1)/2$.

(Proof) Elements in F_p^* are the roots of $x^{(p-1)/2}-1$ over F_p without any duplicates. Since it is factorized as-

$$x^{p-1}-1=\left(x^{(p-1)/2}-1\right)\left(x^{(p-1)/2}+1\right), \quad (5)$$

It is thus found that the number of QRs and QNRs in F_p^* are the same, that is $(\mathrm{p}-1)/2$.

Property 3: Let a and b be the *non-zero* elements in F_p, then the Legendre symbol holds the following relation:

$$\left(ab/p\right)=\left(a/p\right)\left(b/p\right). \quad (6)$$

(Proof) Let g be a generator in F_p^*. Then, let a and b be represented as g^{i_a} and g^{i_b}, where i_a and i_a are certain non-negative integers. According to Legendre symbol, the following relations hold:

$$\left(ab/p\right)=(-1)^{i_a+i_b \bmod 2}, \quad (7)$$

$$\left(a/p\right)=(-1)^{i_a \bmod 2}, \quad (8)$$

$$\left(b/p\right)=(-1)^{i_b \bmod 2}, \quad (9)$$

Thus, this property is shown.

Following important property is newly added in this paper.

Property 4: Let a be a *non-zero* element in F_p, then the Legendre symbol holds the following relation:

$$\left(a/p\right)=\left(a^{-1}/p\right). \quad (10)$$

(Proof) According to the property of Legendre symbol,

$$\left(1/p\right)=1$$
$$\left(a.a^{-1}/p\right)=1. \quad (11)$$

Because of multiplicative nature of the Legendre symbol,

$$\left(a/p\right)\times\left(a^{-1}/p\right)=1. \quad (12)$$

Therefore, when both of $\left(a/p\right)$ and $\left(a^{-1}/p\right)$ are 1 or -1, it satisfies the above equation. Thus, this property is shown.

C. Trace Function

In this paper, the authors have utilized the trace function to map an element of the extension field $X\in\mathrm{F}_{p^m}$ to an element of the prime field $x\in\mathrm{F}_p$ as-

$$x=\mathrm{Tr}\left(X\right)=\sum_{i=0}^{m-1}X^{p^i}. \quad (13)$$

One crucial point is that, the trace becomes a scalar value and the trace function has a linearity property over the prime field F_p as follows:

$$\mathrm{Tr}\left(aX+bY\right)=a\mathrm{Tr}\left(X\right)+b\mathrm{Tr}\left(Y\right), \quad (14)$$

where $a, b\in\mathrm{F}_p$ and $X, Y\in\mathrm{F}_{p^m}$.

The following property is important in this paper. (see also Theorem 2.23 [4]).

Property 5: For each $i=0, 1, 2,\ldots, p-1\in\mathrm{F}_p$, the number of elements in F_q whose trace with respect to F_p is i. It is given by $q/p=p^m-1$.

(Proof) Elements in F_q are the roots of the x^q-x. It is factorized over F_p as follows:

$$x^q-x=x^{p^m}-x$$
$$=\prod_{i=0}^{p-1}\left(\mathrm{Tr}\left(x\right)-i\right) \quad (15)$$

Copyright © 2017 MECS

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

Thus, the number of elements in F_q^* whose trace becomes *zero* is given by $q/p-1$.

D. Dual Basis

In this paper, the dual basis is used for some proofs. It is generally defined as follows:

Definition 1: Let $\mathrm{A}=\{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{m-1}\}$ be a basis in F_{p^m}, the basis $\mathrm{B}=\{\beta_0, \beta_1, \beta_2, \ldots, \beta_{m-1}\}$ is called the dual basis of A such that-

$$\mathrm{Tr}(\alpha_i \beta_j)=\begin{cases}1 & \text{if } i=j\\ 0 & \text{otherwise,}\end{cases} \tag{16}$$

The dual basis of an arbitrary basis is uniquely determined in [4]. In this paper, the following property is also important.

Property 6: Let A and B be a basis and its dual basis in F_{p^m} respectively. Based on the definition of dual basis and the linearity property of trace function, if α_l is a basis of A in F_{p^m} is a *non-zero* prime field element then,

$$\mathrm{Tr}(\alpha_l \beta_j)=\alpha_l \mathrm{Tr}(\beta_j)=\begin{cases}1 & \text{if } j=l\\ 0 & \text{otherwise,}\end{cases} \tag{17}$$

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

E. Ternary Sequence

In this paper, the ternary sequence T is denoted as,

$$\mathrm{T}=\{t_i\} \text{ for } i=0, 1, 2, \ldots, n-1, \ldots, \tag{18}$$

where $t_i \in \{0, 1, -1\}$ and n is the period of the proposed ternary sequence such as $n=p^m-1$.

F. Autocorrelation

The autocorrelation $\mathrm{R}_{\mathrm{T}}(x)$ of the ternary sequence T is generally defined as follows:

$$\mathrm{R}_{\mathrm{T}}(x)=\sum_{i=0}^{n-1} t_{i+x} \cdot t_i, \tag{19}$$

where, x represents the shift value.

III. Proposed Ternary Sequence

This paper proposes a ternary sequence T. This section introduces its definition and then mathematically shows the autocorrelation property of this proposed sequence.

A. Definition

This paper proposes a ternary sequence as follows:

$$\mathrm{T}=\left\{t_i \mid t_i=\left(\mathrm{Tr}(\omega^i)+A \middle/ p\right)\right\}, \tag{20}$$

where p is an odd prime number as the characteristic of F_p, ω is a primitive element in F_{p^m}, A is a *non-zero* element in F_p. Then the period n of this sequence T is given by-

$$n=p^m-1. \tag{21}$$

It is theoretically proven along with the following autocorrelation property.

B. Autocorrelation

According to (15) the autocorrelation equation can be modified, which can be written as-

$$\mathrm{R}_{\mathrm{T}}(x)=\sum_{i=0}^{n-1}\left(\mathrm{Tr}(\omega^{i+x})+A \middle/ p\right)\left(\mathrm{Tr}(\omega^i)+A \middle/ p\right). \tag{22}$$

Theorem 1: The autocorrelation of the ternary sequence T is defined as follows:

$$\mathrm{R}_{\mathrm{T}}(x)=\begin{cases}p^m-p^{m-1}-1 & \text{if } x=0\\ (-1)^{j+1}.p^{m-1}-1 & \text{else if } x=\hat{n}j.\\ -1 & \text{otherwise}\end{cases} \tag{23}$$

The proof for each case of (23) is explained below. It should be noted that, here $\hat{n}=\left(p^m-1\right)/(p-1)$, $j=0,1,2,3,\ldots,$ and i is mainly appeared at summations and holds the relation $0 \le i < n=\left(p^m-1\right)$.

B.1. The case of $x=0$

In this case, the autocorrelation of the ternary sequence T is calculated as follows:

$$\mathrm{R}_{\mathrm{T}}(x)=\sum_{i=0}^{n-1}\left(\mathrm{Tr}(\omega^i)+A \middle/ p\right)\left(\mathrm{Tr}(\omega^i)+A \middle/ p\right). \tag{24}$$

The case that $\mathrm{Tr}(\omega^i)=0$ appears p^m-1 times. When the shift value is equal to 0, $\mathrm{Tr}(\omega^{i+x})$ and $\mathrm{Tr}(\omega^i)$ are the same. The Legendre symbol returns only $\{0, 1, \text{and } -1\}$ values. Based on this condition, all the possible values become $(0\times 0)=0, (1\times 1)=1,$ and

$(-1\times-1)=1$. Depending on whether or not $\mathrm{Tr}(\omega^i)+A=0$, (24) becomes as follows:

$$\begin{aligned}\mathrm{R_T}(x) &= \sum_{\mathrm{Tr}(\omega^i)+A=0} 0 + \sum_{\mathrm{Tr}(\omega^i)+A\neq 0} 1 \\ &= p^{m-1}\cdot 0 + (p^m - 1 - p^{m-1})\cdot 1, \end{aligned} \quad (25)$$

where, $i=0\sim p^m-2$. Thus, the following relation is obtained for the case of $x=0$,

$$\mathrm{R_T}(x) = p^m - 1 - p^{m-1}. \quad (26)$$

B.2. The case of $x=\hat{n}j$

Let g be a generator of $\mathrm{F}_{p^m}^*$. Then $g^{(p^m-1)/(p-1)}$ is a *non-zero* element in the prime field F_p and is also a generator of F_p^*. Therefore, from here on $g^{(p^m-1)/(p-1)}$ will be denoted as $\hat{g}$. Based on the linearity of the trace function, the autocorrelation is calculated as follows:

$$\mathrm{R_T}(x) = \sum_{i=0}^{n-1}\left(\hat{g}^j\mathrm{Tr}(\omega^i)+A/p\right)\left(\mathrm{Tr}(\omega^i)+A/p\right). \quad (27)$$

According to the Property 1 and (13), the above equation can be rewritten as-

$$\begin{aligned}\mathrm{R_T}(x) &= \sum_{\hat{g}^j\mathrm{Tr}(\omega^i)+A=0} 0 + \sum_{\mathrm{Tr}(\omega^i)+A=0} 0 + \\ &\sum_{\substack{\hat{g}^j\mathrm{Tr}(\omega^i)+A\neq 0 \\ \mathrm{Tr}(\omega^i)+A\neq 0}}\left(\hat{g}^j\mathrm{Tr}(\omega^i)+A/p\right)\left(\mathrm{Tr}(\omega^i)+A/p\right). \end{aligned} \quad (28)$$

Depending on the Property 3 and Property 4,

$$\mathrm{R_T}(x) = \sum_{\substack{\hat{g}^j\mathrm{Tr}(\omega^i)+A\neq 0 \\ \mathrm{Tr}(\omega^i)+A\neq 0}}\left(\left(\hat{g}^j\mathrm{Tr}(\omega^i)+A\right)\left(\mathrm{Tr}(\omega^i)+A\right)^{-1}/p\right). \quad (29)$$

Let, $X=\mathrm{Tr}(\omega^i)+A$, then $X\neq 0$, the above equation is rewritten as,

$$\mathrm{R_T}(x) = \sum_{\substack{\hat{g}^j\mathrm{Tr}(\omega^i)+A\neq 0 \\ \mathrm{Tr}(\omega^i)+A\neq 0}}\left(\left(\hat{g}^j + A\left(1-\hat{g}^j\right)X_i^{-1}\right)/p\right). \quad (30)$$

Now, let $(\hat{g}^j + A\left(1-\hat{g}^j\right)X_i^{-1}$ be denoted by Y_i. Then following conditions and facts should be noted:

- $X_i \neq (-\left(\hat{g}^j\right)^{-1}\times A\left(1-\hat{g}^j\right)$, because of $\hat{g}^j\mathrm{Tr}(\omega^i)+A\neq 0$, thus Y_i cannot be 0.
- $A\left(1-\hat{g}^j\right)X_i^{-1}$ does not become 0, thus $Y_i\neq\hat{g}^j$.
- $X_i=A$, where $\mathrm{Tr}(\omega^i)=0$ appears $\left(p^{m-1}-1\right)$ times. Therefore, the case that $Y_i=1$ appears $\left(p^{m-1}-1\right)$ times.
- The other cases, where Y_i is the element of $\mathrm{F}_p-\left\{0,1,g^j\right\}$ appears p^{m-1} times.

From the above conditions, following formula is obtained:

$$\mathrm{R_T}(x) = \sum_{Y_i=0}^{p-1}\left(Y_i/p\right) - p^{m-1}\left(\hat{g}^j/p\right) - \left(1/p\right). \quad (31)$$

According to the property of the Legendre symbol, following relation is obtained for the case of $x=\hat{n}j$,

$$\begin{aligned}\mathrm{R_T}(x) &= -p^{m-1}\left(\hat{g}^j/p\right) - 1 \\ &= (-1)^{j+1}p^{m-1} - 1. \end{aligned} \quad (32)$$

B.3. The default case (otherwise)

In this case, the autocorrelation is calculated by-

$$\mathrm{R_T}(x) = \sum_{i=0}^{n-1}\left(\mathrm{Tr}(\omega^{i+x})+A/p\right)\left(\mathrm{Tr}(\omega^i)+A/p\right). \quad (33)$$

Here x is not divisible by $\hat{n}$ and ω^x does not belong to F_p.

By using ω^x, consider the following basis W in F_{p^m}:

$$\mathrm{W} = \left\{\omega^x, 1, \alpha_2, \alpha_3, \ldots, \alpha_{m-1}\right\}. \quad (34)$$

Again let B be the dual basis of W .

$$\mathrm{B} = \left\{\beta_0, \beta_1, \beta_2, \ldots, \beta_{m-1}\right\}. \quad (35)$$

Assume that ω^i can be represented like this-

$$\omega^i = \sum_{l=0}^{m-1} c_{i,l}\beta_l. \quad (36)$$

Then, ω^{i+x} is expressed by-

$$\omega^{i+x} = \sum_{l=0}^{m-1} c_{i,l}\beta_l \omega^x. \tag{37}$$

Based on the Property 6, the initial value of $\mathrm{Tr}(\omega^i)$ is given by, $\mathrm{Tr}(\omega^i) = c_{i,1}$. Hence W and B are the dual basis to each other, then the value of $\mathrm{Tr}(\omega^{i+x})$ is given by $\mathrm{Tr}(\omega^{i+x}) = c_{i,0}$. Substituting the values of $\mathrm{Tr}(\omega^i)$ and $\mathrm{Tr}(\omega^{i+x})$ in (33), the following equation is obtained:

$$\mathrm{R}_{\mathrm{T}}(x) = \sum_{i=0}^{n-1}\left(c_{i,0} + A/p\right)\left(c_{i,1} + A/p\right). \tag{38}$$

By considering all the cases inside the Legendre symbol, the above equation can be rewritten as-

$$\mathrm{R}_{\mathrm{T}}(x) = \sum_{\substack{c_{i,0}+A\neq 0\\ c_{i,1}+A\neq 0}}\left(c_{i,0} + A/p\right)\left(c_{i,1} + A/p\right) + \sum_{\substack{c_{i,0}+A=0\\ c_{i,1}+A\neq 0}} 0 + \sum_{\substack{c_{i,0}+A\neq 0\\ c_{i,1}+A=0}} 0 + \sum_{\substack{c_{i,0}+A=0\\ c_{i,1}+A=0}} 0. \tag{39}$$

Since ω^i cannot represent the *zero* vector, the number of vectors such that $c_{i,0} = 0$ and $c_{i,1} = 0$ is one less than that of the other combinations like $c_{i,0} = 0$ and $c_{i,1} = 1$. Thus, the last subtraction is required in (40).

$$\sum_{\substack{c_{i,0}+A\neq 0\\ c_{i,1}+A\neq 0}}\left(\left(c_{i,0} + A/p\right)\left(c_{i,1} + A/p\right)\right) = p^{m-2}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\left(ab/p\right) - \left(A^2/p\right)\right). \tag{40}$$

According to the Property 2, the first part of above (40) will become 0. Thus, the following relation is obtained,

$$\sum_{\substack{c_{i,0}+A\neq 0\\ c_{i,1}+A\neq 0}}\left(\left(c_{i,0} + A/p\right)\left(c_{i,1} + A/p\right)\right) = -1. \tag{41}$$

Finally, the autocorrelation of the ternary sequence T in (23) is proven.

IV. Result and Discussion

This section experimentally shows the autocorrelation property of the proposed ternary sequence with some examples. The notation T_2, denotes the proposed sequence with the parameter $A = 2$. Throughout this section, $\{-1\}$ is represented by $\{\bar{1}\}$.

A. Analysis for $p = 3, m = 4$ and $A = 2$

Let $f(x)$ be $x^4 + x^3 + x^2 + 2x + 2$, which a primitive polynomial over F_3. Here, the period of the sequence T_2 becomes $p^m - 1 = 80$ and the sequence becomes as follows:

$$\begin{aligned}\mathrm{T}_2 = \{&01111\bar{1}11010\bar{1}100\bar{1}1\bar{1}1\bar{1}\\ &\bar{1}1\bar{1}00\bar{1}\bar{1}111001\bar{1}\bar{1}\bar{1}10\bar{1}0\\ &10000\bar{1}00101\bar{1}011\bar{1}0\bar{1}0\bar{1}\\ &\bar{1}0\bar{1}111\bar{1}\bar{1}000110\bar{1}\bar{1}101\bar{1}1\}.\end{aligned} \tag{42}$$

The autocorrelation of T_2 is given as follows:

$$\mathrm{R}_{\mathrm{T}_2}(\mathrm{x}) = \begin{cases} 53 & \text{if } x = 0\\ 26 & \text{else if } x = 40\\ -1 & \text{otherwise,}\end{cases} \tag{43}$$

and Fig. 1 shows its autocorrelation graph.

B. Analysis for $p = 7, m = 3$ and $A = 6$

Let $f(x)$ be $x^3 + 6x^2 + 6x + 2$, which a primitive polynomial over F_7. Here, the period of the sequence T_6 becomes $p^m - 1 = 342$ and the sequence becomes as flows:

$$\begin{aligned}\mathrm{T}_6 = \{&1011\bar{1}100\bar{1}1110\bar{1}1\bar{1}\bar{1}\bar{1}\bar{1}1\bar{1}\bar{1}1011\bar{1}\bar{1}\bar{1}\bar{1}01\\ &\bar{1}11\bar{1}\bar{1}001001\bar{1}\bar{1}0\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1}10\bar{1}010\bar{1}1\bar{1}111\bar{1}1\\ &1110\bar{1}\bar{1}1\bar{1}\bar{1}1\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}1\bar{1}0111\bar{1}10\bar{1}\bar{1}0\bar{1}\bar{1}111111\bar{1}\\ &\bar{1}\bar{1}1\bar{1}11\bar{1}\bar{1}10111\bar{1}1\bar{1}1\bar{1}\bar{1}\bar{1}1\bar{1}00\bar{1}111\bar{1}\bar{1}11\bar{1}1\\ &11\bar{1}\bar{1}\bar{1}1111\bar{1}\bar{1}111\bar{1}1\bar{1}\bar{1}\bar{1}10\bar{1}\bar{1}\bar{1}1\bar{1}\bar{1}\bar{1}1\bar{1}1111\bar{1}\\ &\bar{1}11\bar{1}\bar{1}\bar{1}\bar{1}11\bar{1}\bar{1}111\bar{1}\bar{1}\bar{1}10\bar{1}10\bar{1}\bar{1}0\bar{1}1\bar{1}11111111\\ &1\bar{1}\bar{1}110\bar{1}1100111\bar{1}111\bar{1}1\bar{1}01\bar{1}\bar{1}\bar{1}11\bar{1}11110\bar{1}\\ &\bar{1}\bar{1}11\bar{1}11\bar{1}01\bar{1}1111110\bar{1}011\bar{1}0\bar{1}\bar{1}1\bar{1}\bar{1}0\bar{1}1\bar{1}\bar{1}\\ &0110101\bar{1}\bar{1}\bar{1}\bar{1}111101\bar{1}\bar{1}11\bar{1}1101\bar{1}1\bar{1}1\bar{1}\bar{1}1\bar{1}11\bar{1}\}.\end{aligned} \tag{44}$$

The autocorrelation of T_6 is given as follows:

$$\mathrm{R}_{\mathrm{T}_6}(\mathrm{x}) = \begin{cases} 293 & \text{if } x = 0\\ 48 & \text{else if } x = 57, 171, 285\\ -50 & \text{else if } x = 144, 228\\ -1 & \text{otherwise,}\end{cases} \tag{45}$$

and Fig. 2 shows its autocorrelation graph.

C. Analysis for $p = 11, m = 2$ and $A = 5$

Let $f(x)$ be $x^2 + 5x + 2$, which a primitive polynomial over F_{11}. Here, the period of the sequence T_5 becomes $p^m - 1 = 120$ and the sequence becomes as follows:

$$\begin{aligned}\mathrm{T}_5=\{&\bar{1}0111\bar{1}1\bar{1}0\bar{1}\bar{1}01\bar{1}1\bar{1}\bar{1}11\bar{1}\bar{1}\bar{1}1\bar{1}\bar{1}\bar{1}1\bar{1}\bar{1}1\\&11\bar{1}11\bar{1}\bar{1}1\bar{1}1111\bar{1}1\bar{1}111\bar{1}011\bar{1}1\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}\\&1\bar{1}\bar{1}11011\bar{1}10\bar{1}11\bar{1}\bar{1}\bar{1}\bar{1}1111\bar{1}1\bar{1}1100\bar{1}\\&1111\bar{1}101\bar{1}\bar{1}\bar{1}11\bar{1}1\bar{1}11\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}10\bar{1}0\bar{1}\bar{1}\}.\end{aligned}\tag{46}$$

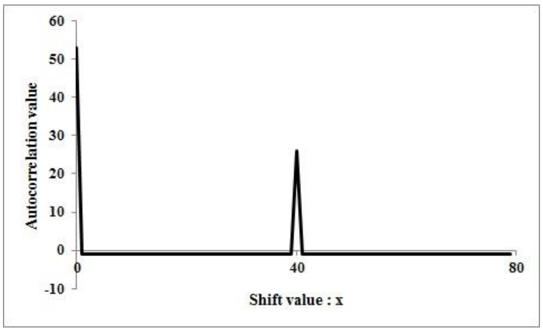


Fig.1. $\mathrm{R}_{\mathrm{T}_2}(x)$ with $p=3, m=4$ and $A=2$.

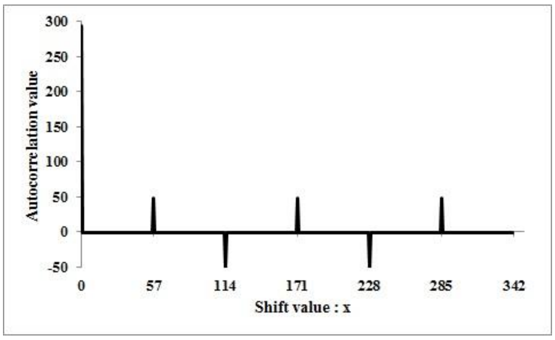


Fig.2. $\mathrm{R}_{\mathrm{T}_6}(x)$ with $p=7, m=3$ and $A=6$.

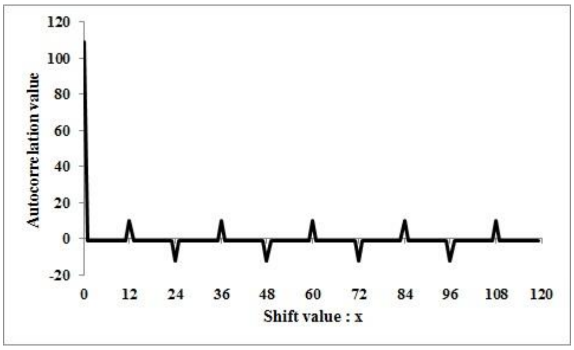


Fig.3. $\mathrm{R}_{\mathrm{T}_5}(x)$ with $p=11, m=2$ and $A=5$.

In this sequence $0, 1, \text{and} -1$ appears $11, 54, \text{and } 55$ times, respectively. This also ensures the identical appearance of 1 and -1 in the whole sequence. The autocorrelation of T_5 is given as follows:

$$\mathrm{R}_{\mathrm{T}_5}(\mathrm{x})=\begin{cases}109 & \text{if } x=0\\ 10 & \text{else if } x=12,36,60,84,108\\ -12 & \text{else if } x=24,48,72,96\\ -1 & \text{otherwise,}\end{cases}\tag{47}$$

and Fig. 3 shows its autocorrelation graph.

D. Analysis for $p=13, m=2$ *and* $A=10$

Let $f(x)$ be $x^2+4x+11$, which a primitive polynomial over F_{13}. Here, the period of the sequence T_{10} becomes $p^m-1=168$ and the sequence becomes as follows:

$$\begin{aligned}\mathrm{T}_{10}=\{&1\bar{1}101\bar{1}11\bar{1}\bar{1}010\bar{1}\bar{1}\bar{1}11\bar{1}1111\bar{1}1\bar{1}1\bar{1}\\&\bar{1}\bar{1}11\bar{1}\bar{1}\bar{1}1\bar{1}1101\bar{1}\bar{1}1\bar{1}1\bar{1}0\bar{1}10\bar{1}1111\\&1\bar{1}\bar{1}\bar{1}11\bar{1}11\bar{1}\bar{1}1\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}11111\bar{1}1\bar{1}\bar{1}\\&\bar{1}11\bar{1}\bar{1}1\bar{1}11\bar{1}\bar{1}\bar{1}\bar{1}11\bar{1}\bar{1}11\bar{1}\bar{1}1\bar{1}01\bar{1}1\bar{1}\\&\bar{1}0\bar{1}\bar{1}\bar{1}\bar{1}11\bar{1}1\bar{1}\bar{1}\bar{1}0011\bar{1}0\bar{1}\bar{1}1\bar{1}1\bar{1}1\bar{1}1\\&11\bar{1}11101111\bar{1}11110\bar{1}1\bar{1}11\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}1\}.\end{aligned}\tag{48}$$

The autocorrelation of T_{10} is given as follows:

$$\mathrm{R}_{\mathrm{T}_{10}}(\mathrm{x})=\begin{cases}155 & \text{if } x=0\\ 12 & \text{else if } x=14,42,70,98,126,154\\ -14 & \text{else if } x=28,56,84,112,140\\ -1 & \text{otherwise,}\end{cases}\tag{49}$$

and Fig. 4 shows its autocorrelation graph.

E. Analysis for $p=17, m=2$ *and* $A=8$

Let $f(x)$ be $x^2+15x+12$, which a primitive polynomial or F_{17}. Here, the period of the sequence T_8 becomes $p^m-1=288$ and the sequence becomes as follows:

$$\begin{aligned}\mathrm{T}_8=\{&\bar{1}\bar{1}\bar{1}\bar{1}1\bar{1}11\bar{1}110\bar{1}1\bar{1}0\bar{1}\bar{1}11\bar{1}\bar{1}1\bar{1}1\bar{1}\bar{1}1\bar{1}\bar{1}1\bar{1}\\&\bar{1}\bar{1}\bar{1}1\bar{1}\bar{1}1\bar{1}\bar{1}\bar{1}\bar{1}1\bar{1}1\bar{1}\bar{1}11\bar{1}\bar{1}\bar{1}\bar{1}11111\bar{1}\bar{1}1\bar{1}1\\&1\bar{1}\bar{1}01\bar{1}1100\bar{1}1111111\bar{1}\bar{1}1\bar{1}1\bar{1}10\bar{1}\bar{1}1\bar{1}11\\&\bar{1}\bar{1}11111\bar{1}\bar{1}1\bar{1}\bar{1}\bar{1}\bar{1}11\bar{1}\bar{1}1\bar{1}\bar{1}1011\bar{1}111\bar{1}\bar{1}\bar{1}\\&11\bar{1}10111\bar{1}\bar{1}\bar{1}\bar{1}1\bar{1}1\bar{1}\bar{1}\bar{1}\bar{1}111\bar{1}\bar{1}11\bar{1}1\bar{1}111\\&1\bar{1}11\bar{1}\bar{1}\bar{1}1\bar{1}111\bar{1}111\bar{1}1\bar{1}1111\bar{1}1\bar{1}\bar{1}0\bar{1}1\bar{1}1\\&\bar{1}\bar{1}\bar{1}1\bar{1}1\bar{1}\bar{1}\bar{1}10\bar{1}\bar{1}\bar{1}\bar{1}11\bar{1}111\bar{1}1\bar{1}111\bar{1}\bar{1}11\bar{1}\\&111\bar{1}01\bar{1}\bar{1}\bar{1}11101\bar{1}\bar{1}1\bar{1}\bar{1}1\bar{1}1\bar{1}1111111\bar{1}0\\&\bar{1}1\bar{1}\bar{1}111\bar{1}\bar{1}\bar{1}0\bar{1}01\bar{1}\bar{1}\bar{1}\bar{1}\bar{1}0110111\bar{1}\bar{1}\bar{1}1\bar{1}\bar{1}\}.\end{aligned}\tag{50}$$

The autocorrelation of T_8 is given as follows:

$$\mathrm{R}_{\mathrm{T}_8}(\mathrm{x})=\begin{cases}271 & \text{if } x=0\\ 16 & \text{else if } x=18,54,90,126,162,198,234,270\\ -18 & \text{else if } x=36,72,108,144,180,216,252\\ -1 & \text{otherwise,}\end{cases}\tag{51}$$

and Fig. 5 shows its autocorrelation graph.

F. Features of the sequence

By observing all the above autocorrelation graphs, it is found that the period n of the sequence becomes

maximum by setting the parameters $p, m,$ and *non-zero* A. The autocorrelation of the proposed sequence has been mathematically shown in (23). This equation also theoretically guarantees the maximum period.

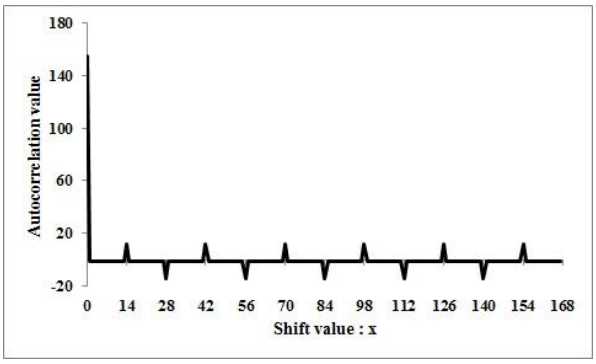


Fig.4. $R_{T_{10}}(x)$ with $p=13, m=2$ and $A=10$.

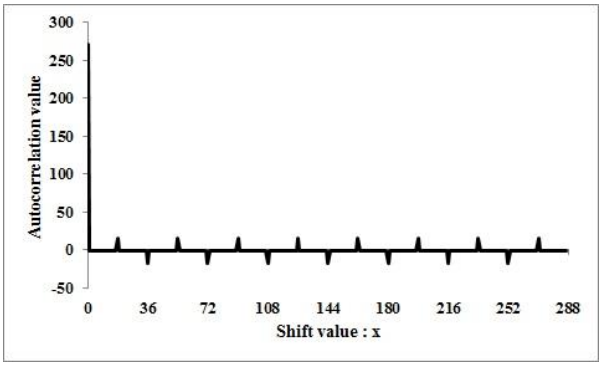


Fig.5. $R_{T_8}(x)$ with $p=17, m=2$ and $A=8$.

One crucial point about the *non-zero* prime field scalar value A is that, by adding this new parameter A does not have any impact in the autocorrelation calculation because (23) confirms that autocorrelation does not depend on the value of A. However, each individual value of A is responsible for generating completely different sequences.

In addition, for each case, the autocorrelation has $(p-1)$ peaks only such as in Fig. 1 – Fig. 5. Among all the peaks, only one of them has the maximum value. As example, in Fig. 2 the maximum peak value is 293 that corresponds to the case of $x=0$ in (23). The other $(p-2)$ smaller peaks conforms the case of $x=\hat{n}j$ in (23). Except the $(p-1)$ peaks, other parts in the autocorrelation graph always have a constant value of -1, which corresponds to the last case in (23). Therefore, the autocorrelation graph can be explained by (23).

The autocorrelation and cross-correlation properties of a sequence are important in the code division multiple access (CDMA) communication systems, where the ternary sequence of having *low* values of the autocorrelation property can be used as a signature sequence for each user. Additionally, this can improve the self-synchronization capability of the CDMA communication system [14]–[16].

V. Conclusion and Future Works

In this paper, the authors have proposed an approach to generate a ternary sequence by utilizing a primitive polynomial, trace function, Legendre symbol, and a *non-zero* scalar A over the odd characteristic prime field F_{p^m}. Choosing the parameters $p, m,$ and A, the number of peaks and the length of the sequences are appropriately controlled. In addition, the mathematical proof of typical features like the period and autocorrelation are also explained in this paper. Furthermore, these properties of the proposed sequence are also observed based on some experimental results.

As future works, the authors will evaluate the linear complexity of their proposed pseudo random ternary sequence. In addition, more efficient calculation procedure will be introduced. Furthermore, the evaluation of the cross-correlation property of the proposed sequence will be one of their important future works.

References

[1] W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, North-Holland Mathematical Library. Elsevier Science, 1998.

[2] S. W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967.

[3] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill, 1994.

[4] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopaedia of Mathematics and Its Applications*, Cambridge University Press, 1984.

[5] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[6] A. Kinga, F. Aline, E. Christain, "Generation and Testing of Random Numbers for Cryptographic Applications", *Proceedings of Romania Academy*, vol. 13, no. 4, pp. 368-377, 2012.

[7] C. Ding, T. Helleseth, and W. Shan, "On the Linear Complexity of Legendre Sequences", *IEEE Trans. on Inform. Theory*, vol. 44, pp. 1276-1278, 1998.

[8] N. Zierler, "Linear Recurring Sequences", *Journal of the Society for Industrial and Applied Mathematics (SIAM)*, vol. 7, issue 1, pp. 31-48, 1959.

[9] 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. on Inform. Theory*, vol. 42, pp. 2254-2255, 1996.

[10] N. Zierler, *Legendre Sequence*, M.I.T. Lincoln Publications, 1958.

[11] A. Md. Arshad, Y. Nogami, "A Pseudo-Random Binary Sequence Generated by Using Primitive Polynomial of Degree 2 over Odd Characteristic Field F_p", *International Conference on Consumer Electronics-Taiwan*, pp.15-16, May 2016.

[12] Y. Nogami, K. Tada, and S. Uehara, "A Geometric Sequence Binarized with Legendre Symbol over Odd Characteristic Field and Its Properties", *IEICE Trans.*, vol. 97-A, no. 12, pp. 2336–2342, 2014.

[13] E. R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press, 1984.

[14] B. Fassi, A. Djebbari, and A. Taleb-Ahmed, "Ternary Zero Correlation Zone Sequence Sets for Asynchronous

DS-CDMA", *Journal Communications and Network*, vol.6, issue 4, pp. 209-217, 2014.
[15] P. Z.Fan, "Spreading Sequence Design and Theoretical Limits for quasi-synchronous CDMA Systems", *EURASIP Journal on wireless Communications and Networking*, pp. 19-31, 2004.
[16] H. Donelan, T. O'Farrell, "Large Families of Ternary Sequences with Aperiodic Zero Correlation Zones for a MC-DS-CDMA System", *Proc. Of 13 th. IEEE Intl. SPIMRC*, vol. 5, pp. 2322-2326, 2002.
[17] Y. Nogami, S. Uehara, K. Tsuchiya, N. Begum, H. Ino, and R. H. Morelos-Zaragoza, "A Multi-value Sequence Generated by Power Residue Symbol and Trace Function over Odd Characteristic Field*", IEICE Transactions on Fundamentals*, vol. E99-A, issue 12, pp. 2226-2237, 2016.
[18] B. Nasima, Y. Nogami, S. Uehara, and R. H. Morelos-Zaragoza, "Multi-valued Sequences Generated by Power Residue Symbol over Odd Characteristic Fields", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E100.A, issue 4, pp. 922-929,2017.
[19] Y. Nogami, K. Tada, and S. Uehara, "A Geometric Sequence Binarized with Legendre Symbol over Odd Characteristic Field and Its Properties", *IEICE Transactions on Fundamentals*, vol. E97-A, issue 12, pp. 2336-2342, 2014.

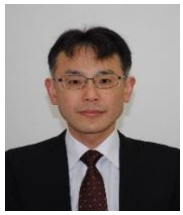
Authors' Profiles

Md. Arshad Ali received the Bachelor of Science in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh in the year of 2007. In May 2009, he joined as a Part-time Teacher in the Computer Science and Engineering Faculty, HSTU, Dinajpur-5200, Bangladesh. Then, he worked as a Lecturer in the same faculty from May 2010 to May 2013. Then, he became an Assistant Professor in May 2013. Currently he is a Master's Course Student in the Graduate School of Natural Science and Technology, Okayama University, Japan. His research interest includes Information Security, Advance Encryption Standard, Pseudo random Binary Sequence, Elliptic Curve Cryptography, and Homomorphic Encryption. Now his research field is Pseudo Random Binary Sequence. He is a member of IEEE.

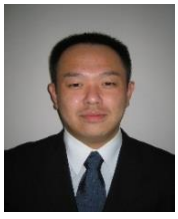
Emran Ali received the Bachelor of Science in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh in the year of 2010. From February 2012 to August 2014 he worked on Software and Application development for Smartphone in various software firms in the country. In September 2014, he joined as a Lecturer in the department of Computer Science and Engineering, HSTU, Dinajpur-5200, Bangladesh. His research interest includes Information Security and Cryptanalysis, Artificial Intelligence, Image Processing, Bio-informatics and IoT.

Md. Ahsan Habib received the Master of Engineering in Information and Communication Technologies from Asian Institute of Technology (AIT), Bangkok, Thailand in the year of 2007, and the Bachelor of Science in Computer Science and Engineering from Shahjalal University of Science and Technology (SUST), Sylhet-3114, Bangladesh in the year of 2003. In 2003, he started working as a Lecturer in Computer Science and Engineering department in Asian University of Bangladesh, Dhaka-1230, Bangladesh. Then in 2005, he went to Thailand for his postgraduate study. In 2007, after finishing Master degree, he joined iSoftel (Thailand) Co. Ltd., Bangkok-10160, Thailand, as a Senior Software Engineer and Solution Specialist. Then in 2009, he moved to Mobile-Technologies Ltd., Bangkok-10110, Thailand, as a Software Development Manager and worked there till April 2012. Then he moved to G5-Technologies Ltd, Dhaka-1207, Bangladesh as the Chief Technical Officer. In 2014, he joined as a Senior Lecturer in Computer Science and Engineering department in the University of Liberal Arts Bangladesh (ULAB), Dhaka-1209, Bangladesh. Finally, in 2015, he joined as an Assistant Professor in the Computer Science and Engineering faculty, Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh and is currently working there. His research interest includes Machine Learning, Data Mining, Computer Security, and Intrusion Detection.

Md. Nadim received the Bachelor of Science in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh in the year of 2010. In February 01, 2012, he joined as a Lecturer in the Computer Science and Engineering Faculty, HSTU, Dinajpur-5200, Bangladesh. He is upgraded as Assistant Professor in 1st February 2015. His main research interest includes Machine Learning, AI, Computer Vision, Big Data Management, Data Mining, Information Security, Random Number Generation etc.



Takuya Kusaka was born in 1970. He received the B.E. degree in Electric Engineering from Kobe University in 1994, and he received M.E. and Ph.D. degrees in Information Science from the Graduate School of Information Science, Nara Institute of Science and Technology in 1996 and 1999, respectively. In 2004, he joined Okayama University. His current research interests include coding theory and information security.



Yasuyuki Nogami graduated from Shinshu University in 1994 and received the PhD degree in 1999 from Shinshu University. He is now a 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.

How to cite this paper: Md. Arshad Ali, Emran Ali, Md. Ahsan Habib, Md. Nadim, Takuya Kusaka, Yasuyuki Nogami,"Pseudo Random Ternary Sequence and Its Autocorrelation Property Over Finite Field", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.9, pp.54-63, 2017.DOI: 10.5815/ijcnis.2017.09.07

Copyright © 2017 MECS