Journal of Information Security, 2019, 10, 130-154
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Multi-Value Sequence Generated over Sub Extension Field and Its Properties

Md. Arshad Ali[1]*, Yuta Kodera[1], Takuya Kusaka[1], Satoshi Uehara[2], Yasuyuki Nogami[1], Robert H. Morelos-Zaragoza[3]

[1]Graduate School of Natural Science and Technology, Okayama University, Okayama, Japan
[2]Faculty of Environmental Engineering, University of Kitakyushu, Fukuoka, Japan
[3]Department of Electrical Engineering, San Jose State University, San Jose, CA, USA
Email: *arshad@s.okayama-u.ac.jp

How to cite this paper: Ali, Md.A., Kodera, Y., Kusaka, T., Uehara, S., Nogami, Y. and Morelos-Zaragoza, R.H. (2019) Multi-Value Sequence Generated over Sub Extension Field and Its Properties. *Journal of Information Security*, **10**, 130-154.
https://doi.org/10.4236/jis.2019.103008

Received: March 28, 2019
Accepted: June 29, 2019
Published: July 2, 2019

Abstract

Pseudo-random sequences with long period, low correlation, high linear complexity, and uniform distribution of bit patterns are widely used in the field of information security and cryptography. This paper proposes an approach for generating a pseudo-random multi-value sequence (including a binary sequence) by utilizing a primitive polynomial, trace function, and *k*-th power residue symbol over the sub extension field. All our previous sequences are defined over the prime field, whereas, proposed sequence in this paper is defined over the sub extension field. Thus, it's a new and innovative perception to consider the sub extension field during the sequence generation procedure. By considering the sub extension field, two notable outcomes are: proposed sequence holds higher linear complexity and more uniform distribution of bit patterns compared to our previous work which defined over the prime field. Additionally, other important properties of the proposed multi-value sequence such as period, autocorrelation, and cross-correlation are theoretically shown along with some experimental results.

Keywords

Pseudo-Random Sequence, Trace Function, Power Residue Symbol, Sub Extension Field, Autocorrelation, Cross-Correlation, Linear Complexity, Distribution of Bit Patterns

1. Introduction

Sequences of numbers generated by using an algorithm are referred to as a pseudo-random sequence. Pseudo-random sequences are inseparable parts in information technology as well as in modern electronics. They are used in both communication (such as cellular telephones and GPS signals) and cryptographic applications (such as key stream for stream cipher, sampling data for simulations, timing measurements in radar systems, error correcting codes in satellite communications, and so on). In most cases, it is important to have the reproduce ability of the pseudo-random sequence [1]. As well as it should have many desirable characteristics such as a long period, low correlation, uniformly distributed bit patterns, high linear complexity, and statistical randomness [2] to become a prominent candidate for information security and cryptographic related applications [3] [4]. The randomness regarding a sequence is considered as the key strength of the cryptographic systems [5]. Considering this crucial point, it's better to use some non-linear mathematical calculation during sequence generation. Additionally, the sequence must have randomness property. The major substance for randomness is independency of values (or lack of correlation), unpredictability (or lack of predictability), and uniform distribution (or lack of bias) [6]. Along with these, there are some statistical tests available to judge the randomness of a sequence such as NIST, Diehard, ENT test [7]. It is mandatory to evaluate the randomness of a sequence before utilizing them in any cryptosystems.

Other geometric sequences having prominent pseudo-random properties are the Mersenne Twister (MT) [8], Blum-Blum-Shub (BBS) [9], Legendre sequence [10], maximum length sequence (M-sequence) [11], and Sidelnikov sequence [12]. Among those, the former two pseudo-random number generators (MT and BBS) are well known considering their applications in cryptography rather than the theoretical aspect. On the other hand, the latter sequences (Legendre sequence, M-sequence, and Sidelnikov sequence) are prominent geometric sequences regarding the theoretical aspect. Generally, the typical features of a pseudo-random sequence such as its period, correlation, linear complexity, and distribution of bit patterns cannot be theoretically proven. However, if a sequence is defined over the finite field, then those features are often proven. All these above-mentioned sequences generated based on some mathematics more specifically they are defined over the finite field. Therefore, most of their important properties are already theoretically proven. The authors are basically more interested in the theoretical aspects of a pseudo-random sequence rather than their applications in the cryptographic area. Therefore, the authors motivated in this research work by observing the theoretical features of the well-known Legendre sequence, M-sequence, and Sidelnikov sequence. Moreover, many researchers are also attracted by these theoretic aspects of these sequences. Our proposed sequence generated by the idea of the Legendre sequence and M-sequences, thus the authors thought that its properties can be theoretically proven and fortunately it proven.

Our previous work on binary sequence [13] uses a primitive polynomial, trace function, and Legendre symbol to generate a new variety of pseudo-random binary sequence. In brief, the previous sequence generation procedure is as follows: firstly, it utilizes a primitive polynomial over an odd characteristic field $\mathbb{F}_p$ to generate a maximum length vector sequence as elements in $\mathbb{F}_{p^m}$, then applies the trace function to map the vectors to prime field $\mathbb{F}_p$ elements, and finally uses the Legendre symbol to binarize the scalars to binary sequence. Our previous binary sequence [13] generated by combining the features of M-sequence and L-sequence. Some important properties such as period, autocorrelation, and linear complexity have been theoretically proven in our previous work. Our previous works on multi-value sequence [14] [15] utilizes a primitive polynomial, trace function, and power residue symbol over odd characteristic field. Some important features of the sequence such as period, autocorrelation, and cross-correlation are theoretically proven in our previous work. The authors previous works on the binary sequence [13], signed binary sequence [16], and multi-value sequence [15]are considered in the prime field $\mathbb{F}_p$ more specifically, the trace function $\mathrm{Tr}(\cdot)$ maps an element of the extension field $\mathbb{F}_{p^m}$ to an element of the prime field $\mathbb{F}_p$. Our previous work on multi-value sequence [17] considered on the sub extension field $\mathbb{F}_q$ characterized by four parameters however it has a shorter sequence period of

$$n = \frac{k\left(p^m - 1\right)}{q - 1}.$$

The period and autocorrelation properties of the proposed sequence explained based on some experimental results only.

The authors in this paper proposed a multi-value sequence (including a binary sequence) by applying a primitive polynomial, trace function, and k-th power residue symbol over the sub extension field $\mathbb{F}_q$. The k-th power residue symbol is an extended version of the Legendre symbol. In details, the proposed multi-value sequence generation procedure is as follows: let p be an odd characteristic prime and m be the extension degree of a primitive polynomial $f(x)$ over the extension field $\mathbb{F}_{p^m}$. It is well known that using the primitive polynomial makes it possible to generate a maximum length vector sequence over $\mathbb{F}_{p^m}$. Let ω be a zero of the primitive polynomial $f(x)$ and it's a primitive element in $\mathbb{F}^*_{p^m}$. Then the sequence

$$\mathcal{T} = \left\{t_i \mid t_i = \mathrm{Tr}_{p^m|q}\left(\omega^i\right), i = 0,1,2,\cdots,p^m - 2\right\}$$

becomes a maximum length sequence of having a period of $p^m - 1$, where, $\mathrm{Tr}_{p^m|q}(\cdot)$ is the trace function over the sub extension field $\mathbb{F}_q$. It maps an element of the extension field $\mathbb{F}_{p^m}$ to an element of the sub extension field $\mathbb{F}_q$. After the trace calculation, a *non-zero* constant element A is added to the trace values. This non-zero A can be any arbitrary element within the sub extension field $\mathbb{F}_q$ such as $A \in \{1,2,\cdots,q-1\}$. Then, the k-th power residue symbol is utilized for mapping the trace sequence $\mathcal{T}$ to a k-value sequence more specifically a multi-value sequence.

The authors recently started to consider the sub extension field $\mathbb{F}_q$ during the sequence generation procedure, whereas, almost all our previous works on pseudo-random sequence [13] [14] [15] are considered in the prime field $\mathbb{F}_p$. The trace calculation is an important step during our proposed sequence generation procedure. It should be noted that in case of prime field $\mathbb{F}_p$, the trace maps extension field $\mathbb{F}_{p^m}$ elements to prime field elements and the possible range of trace outputs are $\{0 \sim p-1\}$. On the other hand, in case of sub extension field $\mathbb{F}_q$, the trace maps extension field $\mathbb{F}_{p^m}$ elements to sub extension field $\mathbb{F}_q$ elements and possible range of trace outputs are $\{0 \sim q-1\}$. Therefore, the sub extension field allows more variations in the trace values and from the theoretical perspective, this flexibility contributes to the betterment of a sequence properties. Thus, from this point of view it's a new dimension in this research area. Some of the notable contributions of the authors in this paper are: this work is an extension of our previous works [13] [14] [15]; if the parameter *k* satisfies the condition $k \mid (p-1)$, then it also includes our previous work [15]; this work overcomes the shorter period shortcoming of our previous work [17] by adding one more additional parameter *A*; the period, autocorrelation, and cross-correlation properties regarding the proposed sequence are explained both theoretically and experimentally; this work also makes a comparison in terms of autocorrelation, linear complexity, and distribution of bit patterns, according to the comparison results, it was found that the proposed sequence holds low correlation, high linear complexity, and much better distribution of bit patterns compared to our previous work [14]. There are a lot of symbols used in this paper, thus a brief introduction about those symbols are introduced in **Table 1**.

2. Preliminaries

This section explains some fundamental concepts of the finite field theory such as a primitive polynomial, trace function, *k*-th power residue symbol, and dual basis. Then, multi-value sequence is introduced along with its properties such as period, autocorrelation, cross-correlation, linear complexity, and distribution of bit patterns.

2.1. Primitive Polynomial

Consider a polynomial $f(x)$ of degree *m* over prime field $\mathbb{F}_p$. If it is not factorized into smaller degree polynomials over the prime field $\mathbb{F}_p$, it is called an irreducible polynomial. Consider the smallest number *e* such that $x^e - 1$ is divisible by $f(x)$ over $\mathbb{F}_p$, it is known that *e* becomes a factor of $p^m - 1$. Then $f(x)$ is especially called a primitive polynomial, when *e* is equal to $p^m - 1$. Its zero ω belongs to the extension field $\mathbb{F}_{p^m}$ and it becomes a primitive element in $\mathbb{F}_{p^m}$ that generates every non-zero element in $\mathbb{F}_{p^m}$ as its power ω^i (for $i = 0, 1, 2, \cdots, p^{m-2}$). According to Fermat's little theorem, the following property between $\mathbb{F}_{p^m}$ and its base field $\mathbb{F}_p$ holds [18].

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

2.2. Trace Function

This work utilizes the trace function to map an element of the extension field $X \in \mathbb{F}_{p^m}$ to an element of the sub extension field $x \in \mathbb{F}_q$ as,

Table 1. List of symbols used in this paper.

List of symbols	
p	odd prime number
m	positive integer, mainly denotes the extension degree
m'	one of the factors of m
q	power of the odd prime $q = p^{m'}$
k	prime factor of $q-1$ such as $k \mid (q-1)$
$\mathbb{F}_p$	odd characteristic prime field
$\mathbb{F}_{p^m}$	an extension field (base p and extension degree m)
$\mathbb{F}_q$	sub extension field
$\mathbb{F}_q^*$	multiplicative group of $\mathbb{F}_q$, excluding the 0 such as $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$
$f(x)$	a primitive polynomial
ω	root of an irreducible polynomial
g	generator of a group
A	an arbitrary element in $\mathbb{F}_q^*$
$\mathrm{Tr}_{p^m \mid q}(\cdot)$	trace function maps $\mathbb{F}_{p^m}$ element to $\mathbb{F}_q$ element
ϵ_k	primitive k-th root of unity
$f_k(\cdot)$	mapping function maps $\mathbb{F}_q$ element to $\mathbb{F}_k$ element
$\mathcal{S}$	proposed sequence in this paper
n	period of a sequence
$\mathrm{R}_{\mathcal{S}}(\cdot)$	autocorrelation of a sequence $\mathcal{S}$
$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(\cdot)$	cross-correlation between the sequences $\mathcal{S}$ and $\hat{\mathcal{S}}$

$$x = \mathrm{Tr}_{p^m \mid q}(X) = \sum_{i=0}^{\frac{m}{m'}-1} X^{p^{im'}}. \tag{1}$$

A crucial point, the above trace becomes an arbitrary element in $\mathbb{F}_q$ and the trace function has a linearity property over the sub extension field $\mathbb{F}_q$ as follows,

$$\mathrm{Tr}_{p^m \mid q}(aX + bY) = a\mathrm{Tr}_{p^m \mid q}(X) + b\mathrm{Tr}_{p^m \mid q}(Y), \tag{2}$$

where $a, b \in \mathbb{F}_q$ and $X, Y \in \mathbb{F}_{p^m}$. In this paper, the following property is important [18].

Property 2. For each arbitrary element $\alpha \in \mathbb{F}_q$, the number of elements in $\mathbb{F}_{p^m}$ whose trace with respect to $\mathbb{F}_q$ becomes α is given by $p^m / q = p^{m-m'}$ and the number of non-zero elements in $\mathbb{F}_{p^m}$ whose trace is zero is given by $(p^m / q) - 1 = p^{m-m'} - 1$. □

2.3. *k*-th Power Residue Symbol

As an extension of the Legendre symbol, this paper considers the *k*-th power residue symbol $(a/q)_k$ for an arbitrary element *a* in $\mathbb{F}_q$ and a prime factor *k* of

$q-1$ as follows:

$$\left(a/q\right)_k = a^{(q-1)/k} = \begin{cases} 0, & \text{if } a=0, \\ 1=\epsilon_k^0, & \text{else if } a \text{ is a } k\text{-th PR in } \mathbb{F}_q^*, \\ \epsilon_k^i, & \text{otherwise } a \text{ is a } k\text{-th PNR in } \mathbb{F}_q^*, \end{cases} \tag{3}$$

where PR and PNR stand for Power Residue and Power Non-Residue respectively. The ϵ_k is a primitive *k*-th root of unity that exists in $\mathbb{F}_q$ and $0 \le i < k$. It becomes a Legendre symbol when $k=2$ [19] and if $k \mid (p-1)$, it becomes our previous work [15]. Note that, for a *non-zero* element *a* and a fixed ϵ_k, the exponent *i* in Equation (3) is uniquely determined in the range of $0 \sim k-1$. Moreover, since $\epsilon_k^k = \epsilon_k^0 = 1$ and *k* is a prime number in this paper, the exponents can be dealt with as elements in $\mathbb{F}_k$. This symbol is basically used for checking whether or not *a* is a *k*-th PR over $\mathbb{F}_q$ as shown above. The output of the *k*-th power residue symbol can be represented as an exponent of ϵ_k, where ϵ_k is a *k*-th primitive root. This paper uses *k*-th power residue symbol to translate a trace sequence over $\mathbb{F}_q$ to a *k* values multi-value sequence such as $\left\{0, \epsilon_k^i\right\}$, where $i \in \{0, \cdots, k-1\}$.

To represent the exponent *i* in Equation (3), this paper uses the following notations and it should be noted that the following notation excludes the case of $a=0$.

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

This paper utilizes the power residue symbol to map an element in $\mathbb{F}_q$ to an element in $\mathbb{F}_k$. Regarding the power residue symbol $\left(a/q\right)_k$, the following property holds.

Property 3. For each *i* from 0 to $k-1$, the number of non-zero elements in $\mathbb{F}_q$ such that

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

is given by $(q-1)/k$. □

2.4. Dual Bases

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

Definition 1. Let $\mathbb{F}_{p^m}$ be a finite field and $\mathbb{F}_q$ be a finite extension of $\mathbb{F}_{p^m}$. Then the two bases $\mathcal{A} = \{\alpha_0, \alpha_1, \cdots, \alpha_{m-1}\}$ and $\mathcal{B} = \{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$ of $\mathbb{F}_q$ over $\mathbb{F}_{p^m}$ are said to be the dual (or complementary) bases if

$$\mathrm{Tr}_{p^m|q}\left(\alpha_i \beta_j\right) = \begin{cases} 1, & \text{if } i=j, \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

where $1 \le i, j \le m-1$. □

The dual basis of an arbitrary basis is uniquely determined in [18]. In this paper, the following property is important.

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

$$\mathrm{Tr}_{p^m|q}\left(\alpha_l \beta_j\right) = \alpha_l \mathrm{Tr}_{p^m|q}\left(\beta_j\right) = \begin{cases} 1, & \text{if } j = l, \\ 0, & \text{otherwise,} \end{cases} \tag{7}$$

where $0 \le l, j \le m-1$. Thus, when $\alpha_l = 1$, $\mathrm{Tr}_{p^m|q}\left(\beta_l\right) = 1$. □

2.5. Multi-Value Sequence and Its Properties

This paper introduces a *k*-value sequence, more specifically a multi-value sequence as follows.

2.5.1. Notation and Period

Let multi-value sequence $\mathcal{S}$ is denoted as

$$\mathcal{S} = \left\{s_i\right\}, i = 0, 1, 2, \cdots, n-1, \cdots \tag{8}$$

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

2.5.2. Autocorrelation and Cross-Correlation

The autocorrelation of a sequence is a scope for measuring how much the original sequence varies from its each shift value. After observing this property some special characteristic about the sequence can be found such as its period, some pattern of it, and so on [20]. The autocorrelation $\mathrm{R}_{\mathcal{S}}(x)$ of sequence $\mathcal{S}$ shifted by *x* is generally defined as follows:

$$\mathrm{R}_{\mathcal{S}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{s_{i+x} - s_i}, \tag{9}$$

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

$$\mathrm{R}_{\mathcal{S}}(0) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{0} = n. \tag{10}$$

The cross-correlation is as important as the autocorrelation property. It is calculated between two different sequences of having the same period and it explains the sharing of some partial information between two sequences. In addition, if multiple sequences are used in any application (such as in security application), in that case, it is important to analyze the similarities between those sequences. To do so, the cross-correlation property needs to be evaluated. Considering the security aspects, the value of the cross-correlation preferred to be low because the higher value of cross-correlation, the more similar the sequences to each other [21]. Let $\hat{\mathcal{S}} = \left\{\hat{s}_i\right\}$ be a different sequence of having a period of *n*. Then, the cross-correlation at *x* shifted is generally defined by the following equation as,

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{\hat{s}_{i+x} - s_i}, \tag{11}$$

where $\tilde{\epsilon}_k$ is a primitive *k*-th root of unity over the complex number $\mathbb{C}$ [22].

2.5.3. Linear Complexity

The linear complexity (LC) of a sequence is closely related to how difficult it is to guess the next bit after observing the previous bits of a sequence. Since this paper considers k-value sequence with coefficients $\{0,1,\cdots,k-1\}$, the linear complexity of sequence $\mathcal{S}$ having a period of n is defined as follows.

$$\mathrm{LC}(\mathcal{S}) = n - \deg\left(\gcd\left(x^n - 1, h_{\mathcal{S}}(x)\right)\right), \tag{12}$$

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

$$h_{\mathcal{S}}(x) = \sum_{i=0}^{n-1} s_i x^i. \tag{13}$$

It should be noted that $\gcd\left(x^n - 1, h_{\mathcal{S}}(s)\right)$ in Equation (12) needs to be calculated over $\mathbb{F}_k$, where k is a prime number and $k \mid (q-1)$. It is said that linear complexity of pseudo-random sequence for security applications is preferred to be high.

2.5.4. Distribution of Bit Patterns

From the viewpoint of security, the distribution of bit patterns is as important as the linear complexity. If a sequence holds uniform distribution of bit patterns, then it becomes difficult to guess the next bit after observing the previous bit patterns. For example, let's assume a binary sequence having a period of 12 as $\mathcal{S}_{12} = \{1,0,1,0,1,0,1,0,1,0,1,0\}$. If we observe the 1-bit pattern in this sequence, then we can find that it has uniform distribution of 1 and 0. In other words, 1 and 0 appears same in number. However, when we check 2-bit patterns on $\mathcal{S}_{12}$, we find that it only has two type of patterns (10 and 01). In this case, we can easily predict the next bit patterns after observing the previous patterns. Therefore, it is also essential to evaluate the distribution of bit patterns of a sequence to confirm its randomness.

3. Proposed Multi-Value Sequence

Let ω be a primitive element in the extension field $\mathbb{F}_{p^m}$, n be the period of the proposed multi-value sequence, m be a composite number which denotes the extension degree of the primitive polynomial, and m' be one of the factors of m. This paper proposes the following sequence $\mathcal{S}$ by utilizing the trace function and k-th power residue symbol as follows:

$$\mathcal{S} = \{s_i\}, s_i = f_k\left(\mathrm{Tr}_{p^m|q}\left(\omega^i\right) + A/p\right)_k. \tag{14}$$

Here k is a prime number as well as a factor of $q-1$ such as $k \mid (q-1)$. To make the above equation more simpler, from here on $\mathrm{Tr}_{p^m|q}(\cdot)$ will be represented as $\mathrm{Tr}(\cdot)$. Therefore, the above equation becomes,

$$\mathcal{S} = \{s_i\}, s_i = f_k\left(\mathrm{Tr}\left(\omega^i\right) + A/p\right)_k. \tag{15}$$

Finally, a mapping function $f_k(\cdot)$ is used to translate the vector sequence generated by the k-th power residue symbol to a multi-value sequence. The mapping function $f_k(\cdot)$ is defined as follows:

$$f_k(x)=\begin{cases}0, & \text{if } x=0,\\ \log_{\epsilon_k}\left((x/p)_k\right), & \text{otherwise.}\end{cases} \tag{16}$$

As mentioned in Section 2.3, $f_k(x)$ with a fixed ϵ_k maps an arbitrary element $x\in\mathbb{F}_q$ to an element in $\mathbb{F}_k$. For example, by utilizing the parameter $p=5$ and $k=3$, the sequence values will be in the range of $\{0,1,2\}$, all of these values are the elements of $\mathbb{F}_3$. In addition, let us fixed [1 4 3] be as a 3-rd primitive root of unity in $\mathbb{F}_q$. Then, all of the sequence values can be represented as a exponent of this primitive root ϵ_3. More details of this example are shown in Table 2. This mapping function $f_k(\cdot)$ holds the following property.

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

$$f_k(x)\pm f_k(y)=f_k\left(xy^{\pm 1}\right). \tag{17}$$

Based on Section 2.3 and Property 3, the mapping function also satisfies the following equation, it should be noted that, here C is a non-zero element in $\mathbb{F}_q$.

$$\sum_{v=0}^{k-1}\tilde{\epsilon}_k^{\,v}=0. \tag{18a}$$

$$\sum_{u=1}^{p-1}\tilde{\epsilon}_k^{\,f_k(u)}=\sum_{u=1}^{p-1}\tilde{\epsilon}_k^{\,f_k\left(u^{-1}\right)}=\left(\frac{p-1}{k}\right)\sum_{v=0}^{k-1}\tilde{\epsilon}_k^{\,v}=0. \tag{18b}$$

$$\sum_{u=1}^{p-1}\tilde{\epsilon}_k^{\,f_k(Cu)}=\sum_{u=1}^{p-1}\tilde{\epsilon}_k^{\,f_k\left(Cu^{-1}\right)}=0. \tag{18c}$$

This section, firstly mathematically prove the cross-correlation property of the proposed multi-value sequence, then it explains the autocorrelation property, and finally the period is introduced. Additionally, these properties are also observed based on some experimental results.

3.1. Cross-Correlation

The cross-correlation is calculated between two different sequences of having the same period. These two different sequences $\hat{\mathcal{S}}$ and $\mathcal{S}$ can be defined as,

$$\hat{\mathcal{S}}=\left\{\hat{s}_i \mid \hat{s}_i=f_k\left(\mathrm{Tr}\left(\omega^i\right)+B/p\right)_k\right\}, \tag{19a}$$

$$\mathcal{S}=\left\{s_i \mid s_i=f_k\left(\mathrm{Tr}\left(\omega^i\right)+A/p\right)_k\right\}. \tag{19b}$$

Here, A and B are non-zero elements in $\mathbb{F}_q$. They can be represented with a generator g that exists in the sub extension field $\mathbb{F}_q$ and they hold the following relation.

$$B=g^hA, \tag{20}$$

where the index term h satisfies $0\leq h\leq q-2$ relation. In addition, here g needs

Table 2. Mapping procedure of $f_k(\cdot)$ for 24 different trace $\mathrm{Tr}(\cdot)$ values[1].

	Output of $\mathrm{Tr}(\cdot)$	Output of $(a/p)_k$	$\epsilon_3 = [1\ 4\ 3]$	Output of $f_k(\cdot)$
1	[0]	[3 1 2]	$[1\,4\,3]^2$	2
2	[1]	[1 4 3]	$[1\,4\,3]^1$	1
3	[2]	[3 1 2]	$[1\,4\,3]^2$	2
4	[4]	[1 4 3]	$[1\,4\,3]^1$	1
5	[0 1 2]	[1]	$[1\,4\,3]^0$	0
6	[0 2 4]	[1]	$[1\,4\,3]^0$	0
7	[0 3 1]	[1 4 3]	$[1\,4\,3]^1$	1
8	[0 4 3]	[3 1 2]	$[1\,4\,3]^2$	2
9	[1 1 2]	[1]	$[1\,4\,3]^0$	0
10	[1 2 4]	[3 1 2]	$[1\,4\,3]^2$	2
11	[1 3 1]	[1]	$[1\,4\,3]^0$	0
12	[1 4 3]	[3 1 2]	$[1\,4\,3]^2$	2
13	[2 1 2]	[1]	$[1\,4\,3]^0$	0
14	[2 2 4]	[1 4 3]	$[1\,4\,3]^1$	1
15	[2 3 1]	[3 1 2]	$[1\,4\,3]^2$	2
16	[2 4 3]	[1]	$[1\,4\,3]^0$	0
17	[3 1 2]	[1]	$[1\,4\,3]^0$	0
18	[3 2 4]	[3 1 2]	$[1\,4\,3]^2$	2
19	[3 3 1]	[3 1 2]	$[1\,4\,3]^2$	2
20	[3 4 3]	[1 4 3]	$[1\,4\,3]^1$	1
21	[4 1 2]	[0]	0	0
22	[4 2 4]	[1 4 3]	$[1\,4\,3]^1$	1
23	[4 3 1]	[1 4 3]	$[1\,4\,3]^1$	1
24	[4 4 3]	[1 4 3]	$[1\,4\,3]^1$	1

to be given by $\omega^{(p^m-1)/(q-1)}$, which used in the following proofs[2]. The cross-correlation of these two sequences $\hat{\mathcal{S}}$ and $\mathcal{S}$ is calculated as,

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{\,f_k\left(\mathrm{Tr}\left(\omega^{i+x}\right)+g^h A\right)-f_k\left(\mathrm{Tr}\left(\omega^{i}\right)+A\right)}, \tag{21}$$

where n is the period of these two sequences and according to the following section, it is given by $p^m - 1$. Furthermore, when $h = 0$, then the value of A and B becomes exactly equal to each other, therefore, the cross-correlation becomes the autocorrelation of $\mathcal{S}$.

Theorem 1. The cross-correlation between the sequence $\hat{\mathcal{S}}$ and $\mathcal{S}$ given by Equation (21) is as follows.

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = \begin{cases} p^{m-m'} + \left(p^m - 1 - p^{m-m'}\right)\tilde{\epsilon}_k^{\,f_k\left(g^h\right)}, & \text{if } x = h\overline{n}, \\ p^{m-m'}\left(\tilde{\epsilon}_k^{\,f_k\left(A\left(g^h - g^j\right)\right)} + \tilde{\epsilon}_k^{\,-f_k\left(A\left(1-g^{h-j}\right)\right)} - \tilde{\epsilon}_k^{\,f_k\left(g^j\right)}\right) - \tilde{\epsilon}_k^{\,f_k\left(g^h\right)}, & \text{else if } x = j\overline{n}, \\ p^{m-2m'} - \tilde{\epsilon}_k^{\,f_k\left(g^h\right)}, & \text{otherwise}, \end{cases} \tag{22}$$

[1] In this example, we fixed [1 4 3] as a 3rd primitive root of unity that exists in $\mathbb{F}_q$. Therefore, every element can be represented as a power of this 3rd primitive root ϵ_3.

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

where $\overline{n} = n/(q-1) = \left(p^m - 1\right)/(q-1)$ and h satisfies the relation in Equation (20) as well as $0 \le j \ne h \le q-2$. □

The proof for each case of Equation (22) is explained below. It should be noted that *i* holds the relation $0 \le i < n = \left(p^m - 1\right)$ and it is mainly appeared at summations. Furthermore, in the following section m/m' is denoted as *r*.

3.1.1. The Case of $x = h\overline{n}$

In this case, the cross-correlation between the sequences $\hat{\mathcal{S}}$ and $\mathcal{S}$ becomes as follows:

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k\left(\mathrm{Tr}\left(\omega^{i+h\overline{n}}\right)+g^h A\right)-f_k\left(\mathrm{Tr}\left(\omega^i\right)+A\right)} = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k\left(g^h\left(\mathrm{Tr}\left(\omega^i\right)+A\right)\right)-f_k\left(\mathrm{Tr}\left(\omega^i\right)+A\right)}. \tag{23}$$

According to Property 5 and depending on the condition of whether or not $\mathrm{Tr}\left(\omega^i\right) + A = 0$, the above equation can be rewritten as follows:

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = \sum_{\mathrm{Tr}\left(\omega^i\right)+A=0} \tilde{\epsilon}_k^{f_k\left(g^h \cdot 0\right)-f_k(0)} + \sum_{\mathrm{Tr}\left(\omega^i\right)+A\ne 0} \tilde{\epsilon}_k^{\left(g^h\left(\mathrm{Tr}\left(\omega^i\right)+A\right)\right)-f_k\left(\mathrm{Tr}\left(\omega^i\right)+A\right)}. \tag{24}$$

Thus, the above equation becomes as,

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = \sum_{\mathrm{Tr}\left(\omega^i\right)+A=0} \tilde{\epsilon}_k^{0} + \sum_{\mathrm{Tr}\left(\omega^i\right)+A\ne 0} \tilde{\epsilon}_k^{f_k\left(g^h\right)}. \tag{25}$$

It should be noted that $g^h \ne 0$. Therefore, according to Property 2, the cross-correlation between the sequence $\hat{\mathcal{S}}$ and $\mathcal{S}$ for the case of $x = h\overline{n}$ holds the following relation.

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = p^{m-m'} + \left(p^m - 1 - p^{m-m'}\right)\tilde{\epsilon}_k^{f_k\left(g^h\right)}. \tag{26}$$

3.1.2. The Case of $x = j\overline{n}$, $j \ne h$

In this case, the cross-correlation between the sequences $\hat{\mathcal{S}}$ and $\mathcal{S}$ becomes as follows:

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k\left(\mathrm{Tr}\left(\omega^{i+j\overline{n}}\right)+g^h A\right)-f_k\left(\mathrm{Tr}\left(\omega^i\right)+A\right)} = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{f_k\left(g^j\mathrm{Tr}\left(\omega^i\right)+g^h A\right)-f_k\left(\mathrm{Tr}\left(\omega^i\right)+A\right)}. \tag{27}$$

According to Property 5, depending on the condition whether or not $\mathrm{Tr}\left(\omega^i\right) + A = 0$ and $g^j\mathrm{Tr}\left(\omega^i\right) + g^h A = 0$ following relation is obtained.

$$\begin{aligned} \mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x) = & \sum_{\substack{g^j\mathrm{Tr}\left(\omega^i\right)+g^h A\ne 0 \\ \mathrm{Tr}\left(\omega^i\right)+A=0}} \tilde{\epsilon}_k^{f_k\left(A\left(g^h-g^j\right)\right)} + \sum_{\substack{g^j\mathrm{Tr}\left(\omega^i\right)+g^h A=0 \\ \mathrm{Tr}\left(\omega^i\right)+A\ne 0}} \tilde{\epsilon}_k^{-f_k\left(A\left(1-g^{h-j}\right)\right)} \\ & + \sum_{\substack{g^j\mathrm{Tr}\left(\omega^i\right)+g^h A\ne 0 \\ \mathrm{Tr}\left(\omega^i\right)+A\ne 0}} \tilde{\epsilon}_k^{f_k\left(\left(g^j\mathrm{Tr}\left(\omega^i\right)+g^h A\right)\left(\mathrm{Tr}\left(\omega^i\right)+A\right)^{-1}\right)}. \end{aligned} \tag{28}$$

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

$$g^j\mathrm{Tr}\left(\omega^i\right) + g^h A = A\left(g^h - g^j\right) \ne 0. \tag{29}$$

Depending on Property 2, first and second summations in Equation (28) respectively becomes as follows:

$$\sum_{\substack{g^j \mathrm{Tr}\left(\omega^i\right)+g^h A\neq 0 \\ \mathrm{Tr}\left(\omega^i\right)+A=0}} \tilde{\epsilon}_k^{f_k\left(A\left(g^h-g^j\right)\right)} = p^{m-m'} \tilde{\epsilon}_k^{f_k\left(A\left(g^h-g^j\right)\right)}, \tag{30}$$

$$\sum_{\substack{g^j \mathrm{Tr}\left(\omega^i\right)+g^h A=0 \\ \mathrm{Tr}\left(\omega^i\right)+A\neq 0}} \tilde{\epsilon}_k^{-f_k\left(A\left(1-g^{h-j}\right)\right)} = p^{m-m'} \tilde{\epsilon}_k^{-f_k\left(A\left(1-g^{h-j}\right)\right)}, \tag{31}$$

where the following facts and conditions should be noted for the above two summations:

- In this paper, the parameter A is not 0 and $A \in \mathbb{F}_q$.
- The case of $\mathrm{Tr}\left(\omega^i\right)+A=0$, $g^j \mathrm{Tr}\left(\omega^i\right)+g^h A \neq 0$.
- While $g^j \mathrm{Tr}\left(\omega^i\right)+g^h A=0$, $\mathrm{Tr}\left(\omega^i\right)+A \neq 0$.

Assume, $X_i = \mathrm{Tr}\left(\omega^i\right)+A \neq 0$. Then the third summation in Equation (28) becomes as follows:

$$\sum_{\substack{g^j \mathrm{Tr}\left(\omega^i\right)+g^h A\neq 0 \\ \mathrm{Tr}\left(\omega^i\right)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(\left(g^j \mathrm{Tr}\left(\omega^i\right)+g^h A\right)\left(\mathrm{Tr}\left(\omega^i\right)+A\right)^{-1}\right)} = \sum_{\substack{g^j \mathrm{Tr}\left(\omega^i\right)+g^h A\neq 0 \\ \mathrm{Tr}\left(\omega^i\right)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(g^j + A\left(g^h-g^j\right)X_i^{-1}\right)}. \tag{32}$$

Now all of the possible values of $X_i \in \mathbb{F}_q$ needs to be consider to resolve Equation (32). According to Property 2 and considering the exceptions for the first and second summations in Equation (28), following relations are obtained,

$$\#\left\{i \mid X_i = 0\right\} = p^{m-m'}, \tag{33a}$$

$$\#\left\{i \mid X_i = A\left(1-g^{-j}\right)\right\} = p^{m-m'}, \tag{33b}$$

$$\#\left\{i \mid X_i = A\right\} = p^{m-m'} - 1, \tag{33c}$$

$$\#\left\{i \mid X_i = u\right\} = p^{m-m'}, \tag{33d}$$

here $0 \leq i < n$ and for each $u \in q - \left\{0, A, A\left(1-g^{h-j}\right)\right\}$. The cases of Equation (33a) and Equation (33b) respectively comply the first and second summations in Equation (28).

Furthermore, assume $Y_i = g^j + A\left(g^h - g^j\right)X_i^{-1}$ this is the input of mapping function $f_k\left(\cdot\right)$ as defined in Equation (32). Hence, considering the cases of $X_i = A\left(1-g^{h-j}\right)$ and $X_i = 0$, the value of Y_i in Equation (32) cannot be 0 and g^j, respectively. These two cases already separated in Equation (28) as the first and second summations. As a consequence, Equation (32) can be rewritten as in Equation (34). In order to conform, the case of $Y_i = g^j$ part (B) is added in Equation (34). Furthermore, part (C) in Equation (34) is for adjusting the number of cases of $X_i = A$, which mentioned in Equation (33c). Therefore, (18b) holds at part A in Equation (34).

Hence, the cross-correlation of the sequence $\hat{\mathcal{S}}$ and $\mathcal{S}$ becomes as follows for the case of $x = j\overline{n}, j \neq h$,

$$
\begin{aligned}
&\sum_{\substack{g^j \mathrm{Tr}\left(\omega^i\right)+g^h A\neq 0\\ \mathrm{Tr}\left(\omega^i\right)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(g^j+A\left(g^h-g^j\right)X_i^{-1}\right)}\\
&=\left(\tilde{\epsilon}_k^{f_k\left(g^h\right)}-\tilde{\epsilon}_k^{f_k\left(g^h\right)}\right)+\left(p^{m-m'}\tilde{\epsilon}_k^{f_k\left(g^j\right)}-p^{m-m'}\tilde{\epsilon}_k^{f_k\left(g^j\right)}\right)+\sum_{\substack{g^j \mathrm{Tr}\left(\omega^i\right)+g^h A\neq 0\\ \mathrm{Tr}\left(\omega^i\right)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(g^j+A\left(g^h-g^j\right)X_i^{-1}\right)}\\
&=\underline{\left[\sum_{\substack{g^j \mathrm{Tr}\left(\omega^i\right)+g^h A\neq 0\\ \mathrm{Tr}\left(\omega^i\right)+A\neq 0}} \tilde{\epsilon}_k^{f_k\left(g^j+A\left(g^h-g^j\right)X_i^{-1}\right)}+\underline{p^{m-m'}\tilde{\epsilon}_k^{f_k\left(g^j\right)}}_{(\mathrm{B})}+\underline{\tilde{\epsilon}_k^{f_k\left(g^h\right)}}_{(\mathrm{C})}\right]}_{(\mathrm{A})}\\
&\quad-p^{m-m'}\tilde{\epsilon}_k^{f_k\left(g^j\right)}-\tilde{\epsilon}_k^{f_k\left(g^h\right)}\\
&=\underline{0}_{(\mathrm{A})}-p^{m-m'}\left(\tilde{\epsilon}_k^{f_k\left(g^j\right)}\right)-\tilde{\epsilon}_k^{f_k\left(g^h\right)}=-p^{m-m'}\left(\tilde{\epsilon}_k^{f_k\left(g^j\right)}\right)-\tilde{\epsilon}_k^{f_k\left(g^h\right)}.
\end{aligned}
\tag{34}
$$

$$
\begin{aligned}
\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x)&=p^{m-m'}\tilde{\epsilon}_k^{f_k\left(A\left(g^h-g^j\right)\right)}+p^{m-m'}\tilde{\epsilon}_k^{-f_k\left(A\left(1-g^{h-j}\right)\right)}-p^{m-m'}\tilde{\epsilon}_k^{f_k\left(g^j\right)}-\tilde{\epsilon}_k^{f_k\left(g^h\right)}\\
&=p^{m-m'}\left(\tilde{\epsilon}_k^{f_k\left(A\left(g^h-g^j\right)\right)}+\tilde{\epsilon}_k^{-f_k\left(A\left(1-g^{h-j}\right)\right)}-\tilde{\epsilon}_k^{f_k\left(g^j\right)}\right)-\tilde{\epsilon}_k^{f_k\left(g^h\right)}.
\end{aligned}
\tag{35}
$$

3.1.3. Otherwise

In this case, the cross-correlation between the sequences $\hat{\mathcal{S}}$ and $\mathcal{S}$ becomes as follows:

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}(x)=\sum_{i=0}^{n-1}\tilde{\epsilon}_k^{f_k\left(\mathrm{Tr}\left(\omega^{i+x}\right)+g^h A\right)-f_k\left(\mathrm{Tr}\left(\omega^i\right)+A\right)}. \tag{36}$$

Here, x is not divisible by $\bar{n}$ and ω^x does not belongs to $\mathbb{F}_q$. We assume the following basis $\mathcal{G}$ in $\mathbb{F}_{p^m}$, by using this ω^x as,

$$\mathcal{G}=\left\{\omega^x,1,\gamma_2,\gamma_3,\cdots,\gamma_{r-1}\right\}. \tag{37}$$

Again let $\mathcal{T}$ be the dual basis of $\mathcal{G}$.

$$\mathcal{T}=\left\{\theta_0,\theta_1,\theta_2,\theta_3,\cdots,\theta_{r-1}\right\}. \tag{38}$$

Assume that ω^i can be represented with θ as follows:

$$\omega^i=\sum_{l=0}^{r-1}v_{i,l}\theta_l. \tag{39}$$

Then, ω^{i+x} is given by

$$\omega^{i+x}=\sum_{l=0}^{r-1}v_{i,l}\theta_l\omega^x. \tag{40}$$

Based on Property 4, initial value of ω^i is as,

$$\mathrm{Tr}\left(\omega^i\right)=v_{i,1}. \tag{41}$$

As previously mentioned that, $\mathcal{W}$ and $\mathcal{B}$ are the dual bases to each other, therefore $\mathrm{Tr}\left(\omega^{i+x}\right)$ can be expressed as follows:

$$\mathrm{Tr}\left(\omega^{i+x}\right)=v_{i,0}. \tag{42}$$

After substituting these trace values, Equation (36) becomes as follows.

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}\left(x\right)=\sum_{i=0}^{n-1}\tilde{\epsilon}_k^{f_k\left(v_{i,0}+g^hA\right)-f_k\left(v_{i,1}+A\right)}. \tag{43}$$

Based on Equation (18), the above equation is rewritten as,

$$\begin{aligned}\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}\left(x\right)=&\sum_{\substack{v_{i,0}+g^hA=0\\ v_{i,1}+A=0}}\tilde{\epsilon}_k^{0}+\sum_{\substack{v_{i,0}+g^hA=0\\ v_{i,1}+A\neq0}}\tilde{\epsilon}_k^{-f_k\left(v_{i,1}+A\right)}+\sum_{\substack{v_{i,0}+g^hA\neq0\\ v_{i,1}+A=0}}\tilde{\epsilon}_k^{f_k\left(v_{i,0}+g^hA\right)}\\ &+\sum_{\substack{v_{i,0}+g^hA\neq0\\ v_{i,1}+A\neq0}}\tilde{\epsilon}_k^{f_k\left(\left(v_{i,0}+g^hA\right)\left(v_{i,1}+A\right)^{-1}\right)}.\end{aligned} \tag{44}$$

According to Equation (18b) and ω^i holds the relation $0\leq i<n$, which actually represents every non-zero element in $\mathbb{F}_{p^m}$, therefore, the second and third summations holds the following relations.

$$\sum_{\substack{v_{i,0}+g^hA=0\\ v_{i,1}+A\neq0}}\tilde{\epsilon}_k^{-f_k\left(v_{i,1}+A\right)}=0. \tag{45a}$$

$$\sum_{\substack{v_{i,0}+g^hA\neq0\\ v_{i,1}+A=0}}\tilde{\epsilon}_k^{f_k\left(v_{i,0}+g^hA\right)}=0. \tag{45b}$$

In addition, by considering the sub extension field $\mathbb{F}_q$ and fixing the values of $v_{i,0}$ and $v_{i,1}$ the first summation holds the following relation as,

$$\sum_{\substack{v_{i,0}+g^hA=0\\ v_{i,1}+A=0}}\tilde{\epsilon}_k^{0}=p^{m-2m'}. \tag{45c}$$

Considering the same calculation procedure of Equation (34), the fourth summation in Equation (44) becomes as follows:

$$\sum_{\substack{v_{i,0}+g^hA\neq0\\ v_{i,1}+A\neq0}}\tilde{\epsilon}_k^{f_k\left(\left(v_{i,0}+g^hA\right)\left(v_{i,1}+A\right)^{-1}\right)}=p^{m-2m'}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\tilde{\epsilon}_k^{f_k\left(ab^{-1}\right)}-\tilde{\epsilon}_k^{f_k\left(0+g^hA\right)-f_k\left(0+A\right)}. \tag{46}$$

Since ω^i cannot represent the zero vector, the number of vectors such that $v_{i,0}=0$ and $v_{i,1}=0$ is one less than that of the other combinations like $v_{i,0}=0$ and $v_{i,1}=1$. That is why, the last subtraction $\tilde{\epsilon}_k^{f_k\left(0+g^hA\right)-f_k\left(0+A\right)}$ is required in Equation (46). According to the condition from Equation (18b), the first summation in Equation (46) becomes 0. Therefore, the following relation is obtained,

$$\sum_{\substack{v_{i,0}+g^hA\neq0\\ v_{i,1}+A\neq0}}\tilde{\epsilon}_k^{f_k\left(\left(v_{i,0}+g^hA\right)\left(v_{i,1}+A\right)^{-1}\right)}=-\tilde{\epsilon}_k^{f_k\left(g^h\right)}. \tag{47}$$

Therefore, the cross-correlation of the sequences $\hat{\mathcal{S}}$ and $\mathcal{S}$ becomes as follows for this case,

$$\mathrm{R}_{\hat{\mathcal{S}},\mathcal{S}}\left(x\right)=p^{m-2m'}-\tilde{\epsilon}_k^{f_k\left(g^h\right)}. \tag{48}$$

Finally, the cross-correlation of the sequences $\hat{\mathcal{S}}$ and $\mathcal{S}$, that is in Equation (22), is proven.

3.2. Autocorrelation and Period

If the value of $h=0$, then $\hat{\mathcal{S}}$ and $\mathcal{S}$ becomes the same sequence. In this case, the cross-correlation in Equation (22) becomes the autocorrelation after replacing the value $h=0$.

$$\mathrm{R}_{\mathcal{S}}(x)=\begin{cases} p^m-1, & \text{if } x=h\bar{n}, \\ p^{m-m'}\left(\tilde{\epsilon}_k^{f_k\left(A\left(1-g^j\right)\right)}+\tilde{\epsilon}_k^{-f_k\left(A\left(1-g^{-j}\right)\right)}-\tilde{\epsilon}_k^{f_k\left(g^j\right)}\right)-1, & \text{else if } x=j\bar{n}, \\ p^{m-2m'}-1, & \text{otherwise.}\end{cases} \quad (49)$$

Corresponding to the above autocorrelation equation, the period of the proposed multi-value sequence explicitly given by p^m-1.

4. Examples and Discussions

This section experimentally observes the properties of the proposed sequence such as period, autocorrelation, and cross-correlation along with some examples. Throughout this section, $|x|$ provides the absolute value of a complex number *x*. In addition, the notation $\mathcal{S}_3$ denotes the proposed sequence with the parameter $A=3$.

4.1. $p=5, m=4, m'=2, k=2$ and $A=3,4$

Let $f(x)=x^4+2x^3+2x^2+2x+2$ be a primitive polynomial over $\mathbb{F}_5$. In this case, the period of this sequence becomes $p^m-1=624$. Then the sequence $\mathcal{S}_3$ is shown in Equation (50) and its autocorrelation becomes as follows and Figure 1 shows its autocorrelation graph.

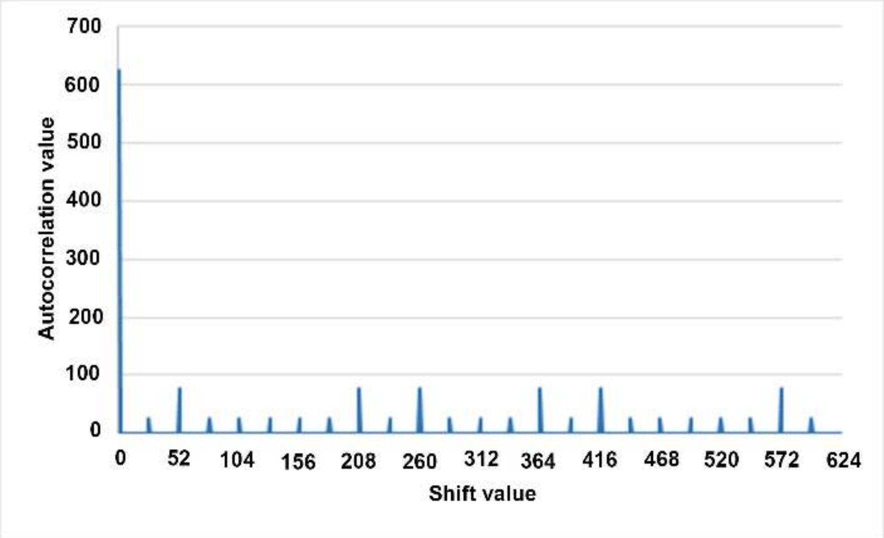

Figure 1. $\left|\mathrm{R}_{\mathcal{S}_3}(x)\right|$ with $p=5, m=4, m'=2, k=2$, and $A=3$.

$$\begin{aligned}\mathcal{S}_3 = \{&0010001110100000000100000000110101001100011001001101110101011\\&010100001001001010000101001001101000110000100001110101101010\\&0100001000001101110111101001111011000000101100010000001111001\\&100100100001100001001011110111011110001110111001010001110101\\&1111001001110001100110000000011110000111110110000111110110110\\&000001101100011101000011100101010100111110001000100001110011\\&011110010110111010101000101110010000111001001101010100011111\\&010100001011101011010110111101101010001110000010010111101000\\&100101101101111010100000100001011001001001100001110000110000\\&111111110101010101100110110110111110100011010011111101100110\\&001001101100101001100110\}\end{aligned} \tag{50}$$

$$\left|\mathrm{R}_{\mathcal{S}_3}(x)\right| = \begin{cases} 624, & \text{if } x = 0 \\ 24, & \text{else if } x = 26,78,104,130,156,182,234,286,312,338,390,442,468,494,520,546,598, \\ 76, & \text{else if } x = 52,208,260,364,416,572, \\ 0, & \text{otherwise} \end{cases} \tag{51}$$

On the other hand, it should be noted that $\mathcal{S}_4$ is different from $\mathcal{S}_3$ and its autocorrelation is given as follows and **Figure 2** shows its autocorrelation graph.

$$\left|\mathrm{R}_{\mathcal{S}_4}(x)\right| = \begin{cases} 624, & \text{if } x = 0 \\ 24, & \text{else if } x = 26,78,104,130,56,182,234,286,312,338,390,442,468,494,520,546,598, \\ 76, & \text{else if } x = 52,208,260,364,416,572, \\ 0, & \text{otherwise} \end{cases} \tag{52}$$

The cross-correlation of $\mathcal{S}_3$ and $\mathcal{S}_4$ becomes as follows and **Figure 6** shows its cross-correlation graph.

$$\left|\mathrm{R}_{\mathcal{S}_3,\mathcal{S}_4}(x)\right| = \begin{cases} 24, & \text{if } x = 0,26,52,78,130,182,234,260,286,312,338,390,442,468,494,546,598, \\ 76, & \text{else if } x = 104,208,364,416,520,572, \\ 624, & \text{else if } x = 156, \\ 0, & \text{otherwise} \end{cases} \tag{53}$$

4.2. $p = 7, m = 4, m' = 2, k = 3$ and $A = 3,4$

Let $f(x) = x^4 + 4x^3 + 3x^2 + 5x + 3$ be a primitive polynomial over $\mathbb{F}_7$. In this case, the period of the sequence becomes $p^m - 1 = 2400$. **Figure 3**, **Figure 4**, and **Figure 5** show the autocorrelation graphs of $\mathcal{S}_3$, $\mathcal{S}_4$, and the cross-correlation between the $\mathcal{S}_3$ and $\mathcal{S}_4$, respectively.

By observing the experimental results, it is found that in every case, the cross-correlation graph has exactly $q-1$ number of peaks. Among those, only one has a maximum value. For example, in **Figure 6**, the maximum cross-correlation value is 624, which corresponds to the first case of $x = h\bar{n}$, the remaining $q-2$ smaller peaks conform the second case of $x = j\bar{n}$, and except

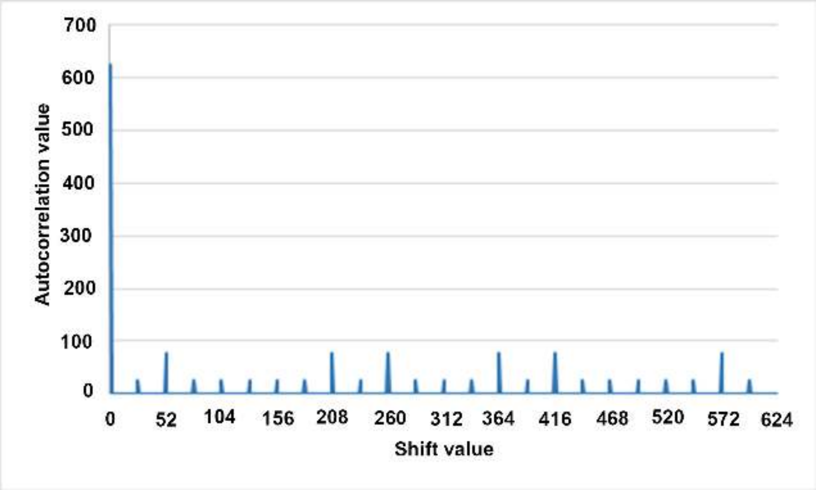

Figure 2. $\left|R_{\mathcal{S}_4}(x)\right|$ with $p=5, m=4, m'=2, k=2$, and $A=4$.

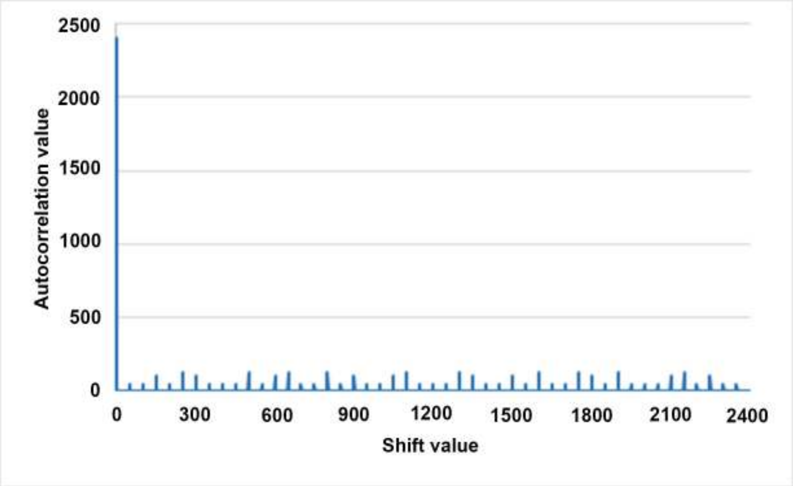

Figure 3. $\left|R_{\mathcal{S}_3}(x)\right|$ with $p=7, m=4, m'=2, k=3$, and $A=3$.

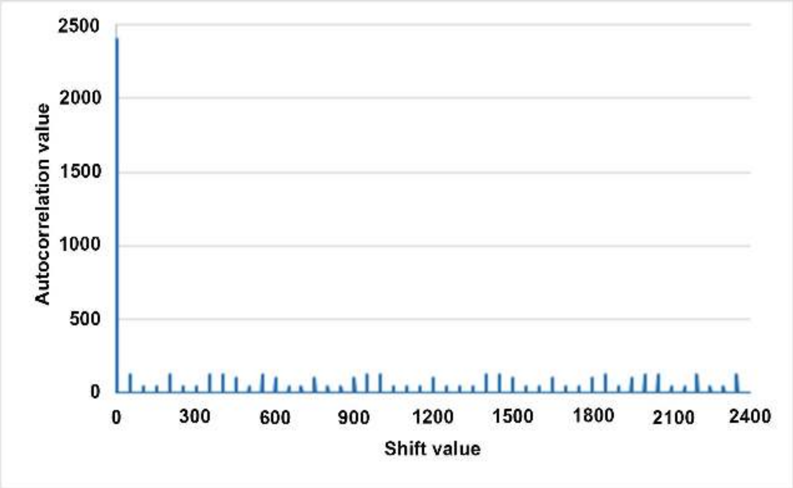

Figure 4. $\left|R_{\mathcal{S}_4}(x)\right|$ with $p=7, m=4, m'=2, k=3$, and $A=4$.

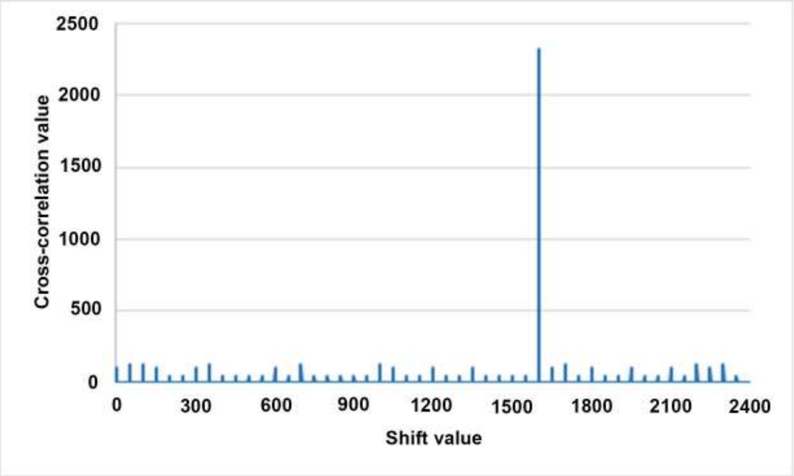

Figure 5. $\left|\mathrm{R}_{\mathcal{S}_3,\mathcal{S}_4}(x)\right|$ with $p=7, m=4, m'=2, k=3$, and $A=3,4$.

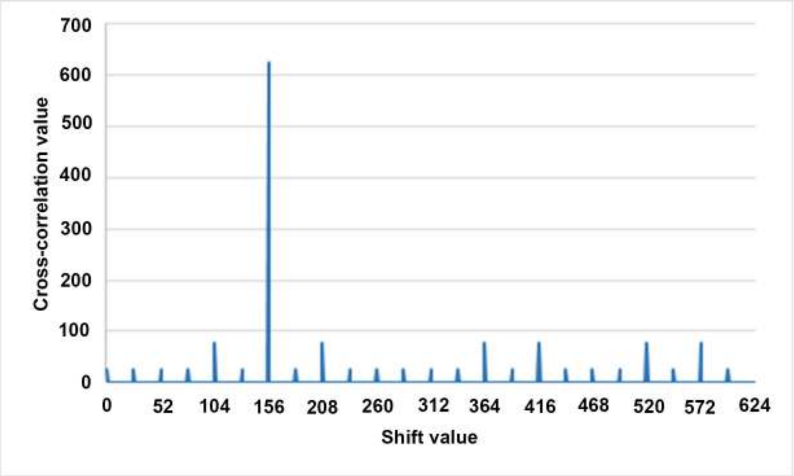

Figure 6. $\left|\mathrm{R}_{\mathcal{S}_3,\mathcal{S}_4}(x)\right|$ with $p=5, m=4, m'=2, k=2$, and $A=3,4$.

these $q-1$ peaks the remaining part in the graph always holds a constant value of 0, which corresponds the case third case in Equation (22). It means that all this cross-correlation graph can be explained by Equation (22). It is also observed that by changing all the parameter values does not have any impact in the cross-correlation evaluation. On the other hand, as like the cross-correlation, the autocorrelation graph also has $q-1$ number of peaks. Among them, only one holds the maximum value, the others have small values, the remaining part always holds a constant value of 1, and all these autocorrelation graphs can be explained by Equation (49).

5. Comparison with Previous Work

Although nowadays multi-value sequence does not have enough application except the binary sequence (especially in security applications), therefore, in this section, the authors will emphasis on the binary case of their proposed sequence.

Even though the authors proposed sequence is a multi-value sequence. but it can be easily mapped into binary sequence by setting the parameter value $k = 2$. In this section the authors will introduce a comparison of their proposed sequence (binary case) with their previous work [14] in terms of autocorrelation, linear complexity, and distribution of bit patterns properties. In this section, the authors previous sequence proposed in [14] will be called as NTU (Nogami-Tada-Uehara) sequence.

5.1. Autocorrelation

The autocorrelation of a sequence is a measure for how much the sequence differs from its each shift value. In addition, by evaluating this property some special characteristics about the sequence such as its period, some pattern of the sequence, and so on can be also found and the value of the autocorrelation always preferred to be as low as possible [22]. The autocorrelation of the proposed sequence (defined over sub extension field) and our previous sequence (NTU) (defined over prime field) is shown in **Figure 7** and **Figure 8**, respectively. By observing their autocorrelation graph, it was found that on one hand, the number of peak values is increases in the sub field sequence, on the other hand, the difference between the maximum peak value with the smaller peak values are much smaller in the proposed sequence compared to our previous sequence. Moreover, in the proposed sequence except the peaks remaining autocorrelation value always remains at 0. It should be noted that in case of correlation evaluation, the less difference between the peak values are more crucial rather than the number of peaks [22].

5.2. Linear Complexity

The unpredictability of a sequence can be measured by the length of the shortest Linear Feedback Shift Register (LFSR) which can generate the given sequence. This approach is particularly appealing since there exists an efficient procedure

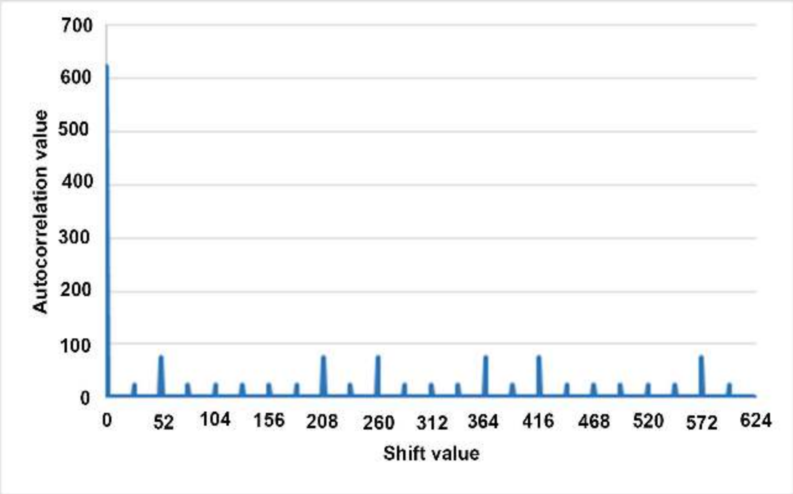

Figure 7. Autocorrelation of proposed sequence.

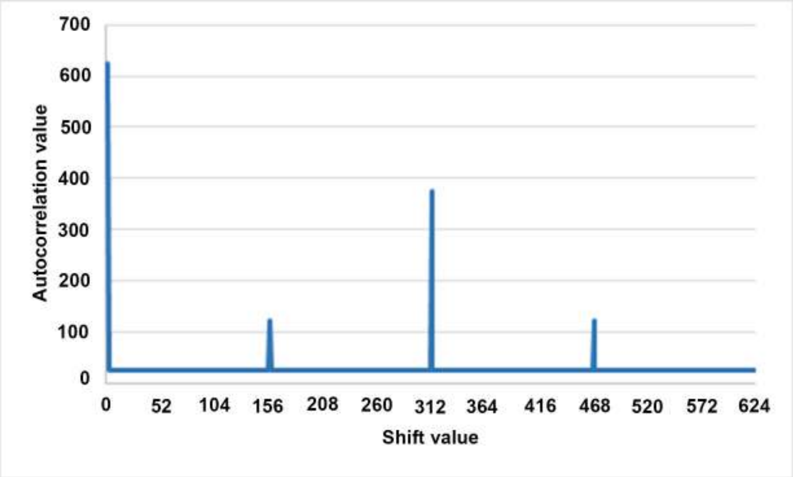

Figure 8. Autocorrelation of NTU sequence.

(it is so called the Berlekamp-Massy algorithm [23]) for finding the shortest LFSR. This length is referred as the linear complexity associated with the sequence. The linear complexity property regarding a sequence is an important parameter which tells how difficult it is to predict the next bit pattern by observing the previous bit pattern of a sequence. Thus, the linear complexity of a sequence is always preferred to be high. The linear complexity of the proposed sequence (defined over sub extension field) and our previous sequence (NTU) (defined over prime field) is shown in **Figure 9** and **Figure 10**, respectively. By observing their linear complexity graph, it was found that the proposed sequence (which defined over the sub extension field) always hold high linear complexity compared to the NTU sequence. In other words, in terms of linear complexity the sequence defined over the sub extension field hold higher linear complexity than the sequence defined over the prime field.

5.3. Distribution of Bit Patterns

The distribution of bit patterns is another important measure to check the randomness of a sequence. From the viewpoint of security, the distribution of bit patterns is as important as the linear complexity. If a sequence holds the uniform distribution of bit patterns, then it becomes difficult to guess the next bit after observing the previous bit patterns. After the experimental observation, it was found that the NTU sequence is not uniformly distributed. In other words, in case of binary NTU sequence, there is much difference in appearance between the 0 and 1. To improve this drawback, instead of prime field (which used in the NTU sequence generation procedure), the authors focused on the sub extension field during the sequence generation procedure in this research work. As a result, after utilizing the sub extension field, the distribution of bit patterns becomes close to uniform. This comparison is shown in the following **Table 3**. In the following table, $b^{(d)}$, $H_{wt}\left(b^{(d)}\right)$, and $D_{S_n}\left(b^{(d)}\right)$ denotes a bit pattern *b* of length *d*, the hamming weight of the bit pattern *b*, and the number of appearances of

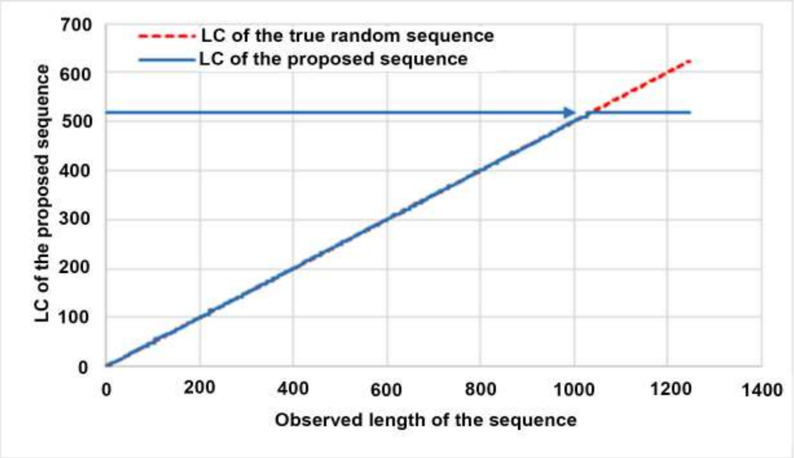

Figure 9. LC of the proposed sequence.

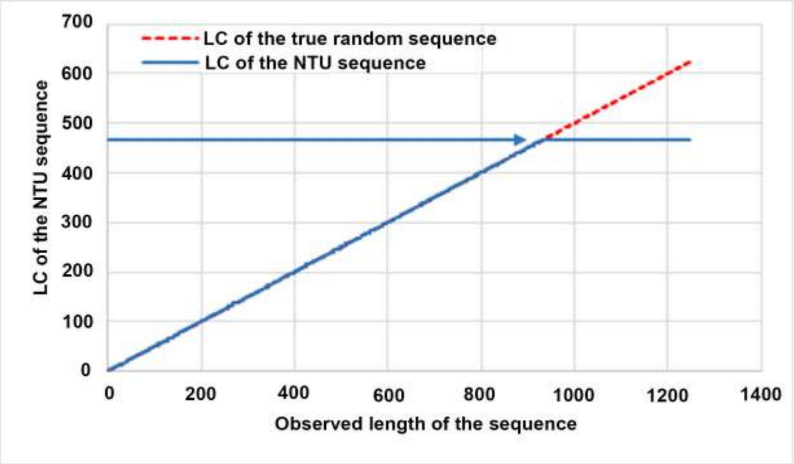

Figure 10. LC of the NTU sequence.

Table 3. Comparison in bit distribution between the sub field binary sequence and NTU sequence.

d	$H_{wt}\left(b^{(d)}\right)$	$D_{S_{15624}}\left(b^{(d)}\right)$	%	$D_{NTU_{15624}}\left(b^{(d)}\right)$	%
1	0	8124	51.99	9374	59.99
	1	7500	48.01	6250	40.01
2	0	4224	27.03	5624	35.99
	1	3900	24.96	3750	24.00
	2	3600	23.04	2500	16.00
3	0	2196	14.05	3374	21.59
	1	2028	12.98	2250	14.40
	2	1872	11.98	1500	9.60
	3	1728	11.05	1000	6.40
4	0	1140	7.29	2024	12.95
	1	1056	6.75	1350	8.60
	2	972	6.22	900	5.76
	3	900	5.76	600	3.84
	4	828	5.29	400	2.56

$b^{(n)}$, respectively. In terms of the distribution of bit patterns, the sequence defined over the sub extension field hold much better distribution (close to uniform) of 0 and 1 than the sequence defined over the prime field.

As mentioned previously, NTU sequence proposed in [14] is defined over the prime field and proposed sequence in this paper is defined over the sub extension field. After the comparison results it is concluded that in terms of correlation the proposed sequence holds low correlation compared to NTU sequence; about linear complexity proposed sequence possesses high linear complexity than NTU sequence; regarding the distribution of bit patterns proposed sequence hold much better distribution of bit patterns (close to uniform) than NTU sequence.

One of the most common applications of the pseudo-random binary sequence is in a stream cipher. Basically, stream cipher is divided into two classes: block cipher and stream cipher. Among these in case of block cipher, same key is used for both encryption and decryption of each block (≥64 bits) of data. On the other hand, in case of stream cipher, encryption and decryption are performed by the bit wise $\oplus$ (XOR) operation with a key stream. Here, the authors restrict the discussion of their proposed pseudo-random binary sequence in a stream cipher. An image of the stream cipher is shown in **Figure 11**. Few important considerations during the design of a stream cipher are the key (which used for both encryption and decryption) should have large period, good randomness, and unpredictability properties due to the usage of same key in both encryption and decryption. Here, the encryption is carried out by applying a bit-wise $\oplus$ (XOR) operation between the plain-text of byte stream M and encryption key K. Then, the cipher-text C transmitted through a network. On the other hand, during the decryption, after the bit-wise $\oplus$ operation between the cipher-text C and the same key K we will get the original plain-text M. In a stream cipher, a lot of sequences are assigned to several users, respectively. If these sequences have some correlation, then it will make some security vulnerabilities. Under this circumstance, it is important to observe the cross-correlation property between several sequences. Additionally, its linear complexity and distribution of bit patterns needs to be high and uniform, respectively to confirm its randomness. The authors proposed method can generate a long period pseudo-random sequence with typical auto and cross-correlation, high linear complexity, and almost uniformly distributed bit patterns features. After observing the experimental and comparison results, it can be concluded that the authors proposed sequence which defined over the sub extension field can be a prominent candidate for a stream cipher like applications.

6. Conclusions and Future Works

The authors in this paper have proposed a multi-value sequence (including a binary sequence) by utilizing a primitive polynomial, trace function, k-th power residue symbol over the sub extension field. The notable outcomes of this

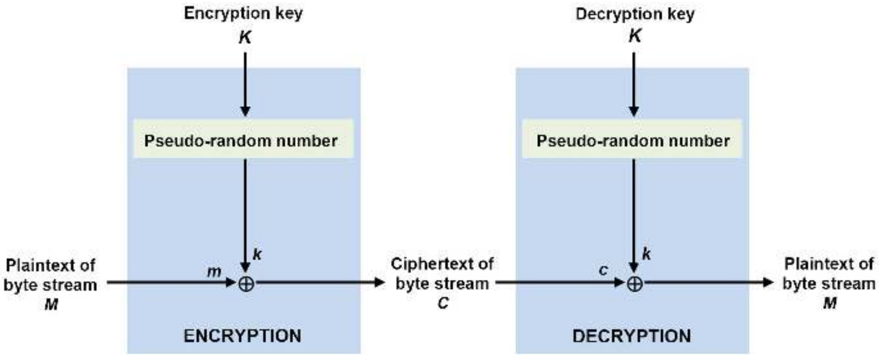

Figure 11. Application of the proposed sequence in stream cipher.

research work are as follows:

- This is an extension of our previous works [13] [14] [15].
- This work overcomes the shorter period shortcoming of our previous work [17].
- The period, autocorrelation, and cross-correlation properties regarding the proposed sequence are theoretically explained.
- The authors make a comparison in terms of autocorrelation, linear complexity and distribution of bit patterns properties with their previous work [14].
- According to the comparison results, the proposed sequence holds low correlation, high linear complexity, and much better distribution of bit patterns compared to our previous work [14].
- The proposed sequence can be a prominent candidate for stream cipher like cryptographic applications due to its exemplary properties.

As future works, the following points should be researched:

- Mathematically prove the linear complexity and distribution of bit patterns properties.
- To introduce more efficient calculation instead of the power residue calculation.

Acknowledgements

This work has been supported by JSPS KAKENHI Grant-in-Aid for Scientific Research (A) Number 16H01723.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Goresky, M. and Klapper, A. (2012) Algebraic Shift Register Sequences. Cambridge University Press, Cambridge.

[2] Hamza, R. (2017) A Novel Pseudo Random Sequence Generator for Image-Cryptographic Applications. *Journal of Information Security and Applications*, **35**, 119-127. https://doi.org/10.1016/j.jisa.2017.06.005

[3] Golomb, S.W. (1967) Shift Register Sequences. Holden-Day, San Francisco, CA.

[4] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A. (1996) Handbook of Applied Cryptography. CRC Press, Boca Raton, FL.

[5] Salhab, O., Jweihan, N., Jodeh, M.A., Taha, M.A. and Farajallah, M. (2018) Survey paper: Pseudo Random Number Generators and Security Tests. *Journal of Theoretical and Applied Information Technology*, **96**, 1951-1970.

[6] Kinga, A., Aline, F. and Christain, E. (2012) Generation and Testing of Random Numbers for Cryptographic Applications. *Proceedings of Romanian Academy*, **13**, 368-377.

[7] Parvees, M.Y.M., Samath, J.A. and Bose, B.P. (2019) Cryptographically Secure Diffusion Sequences—An Attempt to Prove Sequences Are Random. In: Peter, J., Alavi, A. and Javadi, B., Ed., *Advances in Big Data and Cloud Computing*, Springer, Singapore, 433-442. https://doi.org/10.1007/978-981-13-1882-5_37

[8] Matsumoto, M. and Nishimura, T. (1998) Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudo-Random Number Generator. *ACM Transactions on Modeling and Computer Simulation*, **8**, 3-30.
https://doi.org/10.1145/272991.272995

[9] Blum, L., Blum, M. and Shub, M. (1986) A Simple Unpredictable Pseudorandom Number Generator. *SIAM Journal on Computing*, **15**, 364-383.
https://doi.org/10.1137/0215025

[10] Zierler, N. (1958) Legendre Sequence. MIT Lincoln Publications, Lexington, MA.

[11] Zierler, N. (1959) Linear Recurring Sequences. *Journal of the Society for Industrial and Applied Mathematics*, **7**, 31-48. https://doi.org/10.1137/0107003

[12] Sidelnikov, V.M. (1971) On Mutual Correlation of Sequences. *Soviet Mathematics-Doklady*, **12**, 197-201.

[13] Nogami, Y., Tada, K. and Uehara, S. (2014) Geometric Sequence Binarized with Legendre Symbol over Odd Characteristic Field and Its Properties. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E97-A**, 2336-2342. https://doi.org/10.1587/transfun.E97.A.2336

[14] Nogami, Y., Uehara, S., Tsuchiya, K., Begum, N., Ino, H. and Morelos-Zaragoza, R.H. (2016) A Multi-Value Sequence Generated by Power Residue Symbol and Trace Function over Odd Characteristic Field. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E99-A**, 2226-2237.
https://doi.org/10.1587/transfun.E99.A.2226

[15] Arshad, A.M., Nogami, Y., Ino, H. and Uehara, S. (2016) Auto and Cross Correlation of Well Balanced Sequence Over Odd Characteristic Field. 2016 *Fourth International Conference on Computing and Networking*, Hiroshima, Japan, 22-25 November 2016, 604-609. https://doi.org/10.1109/CANDAR.2016.0109

[16] Arshad, A.M., Nogami, Y., Ogawa, C., Ino, H., Uehara, S., Morelos-Zaragoza, R. and Tsuchiya, K. (2016) A New Approach for Generating Well Balanced Pseudo-random Signed Binary Sequence Over Odd Characteristic Field. 2016 *International Symposium on Information Theory and Its Applications*, Monterey, CA, 30 October-2 November 2016, 777-780.

[17] Arshad, A.M., Miyazaki, T., Nogami, Y., Uehara, S. and Morelos-Zaragoza, R. (2017) Multi-Value Sequence Generated by Trace Function and Power Residue Symbol Over Proper Sub Extension Field. *IEEE International Conference on Consumer Electronics-Taiwan*, Taipei, Taiwan, 12-14 June 2017, 249-250.
https://doi.org/10.1109/ICCE-China.2017.7991089

[18] Lidl, R. and Niederreiter, H. (1984) Finite Fields, Encyclopedia of Mathematics and Its Applications. Cambridge University Press, Cambridge.

[19] Berlekamp, E.R. (1984) Algebraic Coding Theory. Aegean Park Press, Walnut Creek, CA.

[20] Helleseth, T. and Kumar, P.V. (1998) Sequences with low correlation. In: *Handbook of Coding Theory*, North-Holland, Amsterdam.

[21] Hertel, D. (2005) Cross-Correlation Properties of Perfect Binary Sequence. In: Helleseth, T., Sarwate, D., Song, H.Y. and Yang, K., Eds., *Sequences and Their Applications*: *SETA* 2004. *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg. https://doi.org/10.1007/11423461_14

[22] Kumar, P.J. and Moreno, O. (1991) Prime-Phase Sequences with Periodic Correlation Properties Better Than Binary Sequences. *IEEE Transactions on Information Theory*, **37**, 603-616. https://doi.org/10.1109/18.79916

[23] Alecu, A. and Salagean, A. (2007) Modified Berlekamp-Massey Algorithm for Approximating the *k*-Error Linear Complexity of Binary Sequences. In: Galbraith, S.D., Ed., *Cryptography and Coding*. *Cryptography and Coding* 2007. *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 220-232. https://doi.org/10.1007/978-3-540-77272-9_14