ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 4, No. 2, 370-379 (2019)
www.astesj.com
Special Issue on Advancement in Engineering and Computer Science

ASTES Journal
ISSN: 2415-6698

Distribution of Bit Patterns in Binary Sequence Generated Over Sub Extension Field

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

[1]*Graduate School of Natural Science and Technology, Okayama University, 7008530, Japan*

[2]*Faculty of Environmental Engineering, The University of Kitakyushu, 8028577, Japan*

[3]*Department of Electrical Engineering, San Jose State University, CA 95192, United States*

ARTICLEINFO

Article history:
Received: 05 March, 2019
Accepted: 16 April, 2019
Online: 28 April, 2019

Keywords:
Pseudo-random sequence
Distribution of bit patterns
Primitive polynomial
Trace function
Legendre symbol

ABSTRACT

The distribution of bit patterns is an important measure to check the randomness of a sequence. The authors of this paper observed this crucial property in a binary sequence which generated by using a primitive polynomial, trace function, and Legendre symbol defined over the sub extension field. The authors create a new dimension in the sequence generation research area by considering the sub extension field, whereas all our previous works are focused in the prime field. In terms of distribution of bit patterns property, this research work has notable outcomes more specifically the binary sequence (defined over the sub extension field) holds much better (close to uniform) bit distribution than the previous binary sequence (defined over the prime field). Furthermore, the authors theoretically proved the distribution of bit property in this paper.

1 Introduction

In this IoT era, we communicate with each other through the internet. Therefore, secure communication is the major matter of concern. We use symmetric cryptosystems (Advanced Encryption Standard (AES) [1]) and asymmetric cryptosystems (Rivest Shamir Adleman (RSA) [2], and Elliptic Curve Cryptography (ECC) [3]) to establish a secure communication. A pseudo-random number is one of the crucial parts of these cryptosystems. More specifically, in case of cryptography, to generate the keys (public key, private, session key, and so on) a pseudo-random number generator is used. A prominent pseudo-random number generator is essential to generate pseudo-random number having randomness property (along with other good statistical properties). Consequently, the security of these cryptosystems deliberately depends upon the randomness property regarding a sequence. Thus, it is mandatory to evaluate the randomness of a sequence before utilized them in any cryptosystems. Basically, two crucial properties namely the linear complexity [4] and the distribution of bit patterns regarding a sequence are nowadays well-known to check the randomness of a pseudo-random sequence. In this work, the authors restrict the discussion on the distribution of bit patterns property to evaluate the randomness of a sequence.

Most renowned pseudo-random number generators are the Mersenne Twister (MT) [5], Blum-Blum-Shub (BBS) [6], Legendre sequence [7, 8], and M-sequence [9]. 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 M-sequence and Legendre sequence are prominent geometric sequences regarding the theoretical aspect. As a result, the authors attracted in the pseudo-random sequence generation research area by observing the theoretical prospect on the M-sequence and Legendre sequences.

The Legendre sequence [7, 8] is generated by applying the Legendre symbol over the odd characteristic field. It has a long period, high linear complexity, and the distribution of bit patterns of the Legendre se-

[*]Md. Arshad Ali, Graduate School of Natural Science and Technology, Okayama University, 3-1-1, Tsushima-naka, Kita, Okayama, 7008530, Japan, +81-8042661986, arshad@s.okayama-u.ac.jp

https://dx.doi.org/10.25046/aj040246

quence is known to be close to uniform [10, 11]. On the other hand, M-sequence is generated by a linear recurrence relation over the finite field. It has a maximum period but minimum linear complexity. In addition, M-sequence [9] is well-known for its uniform distribution of bit patterns [12]. Our previous work on geometric sequence [13] combines the features of the Legendre sequence and M-sequence. As mentioned previously, linear complexity and distribution of bit patterns are the important measures to evaluate the randomness of a sequence. So, regarding the linear complexity, our previous sequence [13] always possess high value. Unlike the linear complexity, the distribution of bit patterns in [13] doesn't reaches up to the mark alike the Legendre sequence and M-sequence. Hence, its a scope to improve the distribution of bit patterns in our previous sequence.

The trace calculation is an important step during our sequence generation procedure. Lets focus on the important aspect regarding this calculation. In case of prime field $\mathbb{F}_p$, the trace function maps an element of the extension field $\mathbb{F}_{q^M}$ to an element of the prime field $\mathbb{F}_p$. Therefore, the number of possible trace outputs will be in the range of $\{0 \sim p-1\}$. In other words, if we calculate the trace over the prime field, then it will output p kinds of values. On the other hand, in case of the sub extension field $\mathbb{F}_q$, the trace function maps an element of the extension field $\mathbb{F}_{q^M}$ to an element of the sub extension field $\mathbb{F}_q$ and the number of possible trace outputs will be in the range of $\{0 \sim q-1\}$ which means the trace outputs q kinds of values. It should be noted that here $M = m/m'$, $q = p^{m'}$, and m' be one of the factors of m. From the theoretical perspective, more variation in the trace values contribute to the better appearance of bits (0 and 1) in a sequence. This is one of the important aspects to consider the sub extension during the sequence generation procedure to improve the distribution of bit patterns in our previous sequence [13]. After utilizing the sub extension field, the detailed improvement in distribution of bit patterns is introduced in the result and discussion section in this paper.

Recently, the authors started to consider the sub extension field during the sequence generation procedure, which is a new dimension of our research work on generation of pseudo-random sequence (whereas our previous works on binary sequence [13] and multi-value sequence [14, 15] are considered in the prime field). As a result, our recent works on binary sequence [16] and multi-value sequence [17] experimentally observed the linear complexity, autocorrelation properties, respectively. As mentioned previously, the distribution of bit patterns is an important measure to evaluate the randomness of a sequence. Thus, the authors of this paper consider the distribution of bit patterns in a binary sequence which generated over the sub extension field.

The Legendre sequence and M-sequence are the base of the sequence research area. Their properties are already proven, therefore many researchers attracted by those sequences. As mentioned previously, our sequence also generated by the idea of the Legendre and M-sequences. Consequently, the authors thought that its properties can be theoretically proven and fortunately its proven (which shown in the later section of this paper). This is one of the contributions of the authors in this paper. Moreover, they also make a comparison between the binary sequence defined over the sub extension field with their previous work on binary sequence in terms of distribution of bit patterns property. According to the comparison result, binary sequence (defined over sub extension field) holds much better (close to uniform) distribution of bit patterns than the previous binary sequence [13]. Finding this improvement by considering the sub extension field is the major contribution of this paper.

The authors of this paper observed the distribution of bit patterns in a binary sequence which generated by a primitive polynomial, trace function, and Legendre symbol over the sub extension field. In brief, the sequence generation procedure is as follows: at first, it uses a primitive polynomial over the odd characteristic field $\mathbb{F}_p$ to generate maximum length vector sequence as elements in $\mathbb{F}_{q^M}$, then the trace function maps the extension field $\mathbb{F}_{q^M}$ elements to the sub extension field $\mathbb{F}_q$ elements, and finally the Legendre symbol binarizes the sub extension field $\mathbb{F}_q$ elements to a binary sequence. The authors already observed the period, autocorrelation, cross-correlation, and linear complexity properties of the binary sequence (which generated over the sub extension field) in their previous works [16, 17]. Thus, this paper focused on the distribution of bit patterns property. In brief, the authors count the number of appearances for each n-bit patterns (where $1 \leq n \leq (m/m')$). After observing many experimental results, the authors found that the number of appearances of each bit pattern is related to the number of zeros contained in each bit pattern. Furthermore, the authors theoretically proven the distribution of bit patterns equation. Moreover, they also make a comparison with their previous work [13].

Throughout this paper, p and q denote an odd prime number and its power $q = p^{m'}$, respectively, where m be a positive integer which mainly denotes extension degree and m' be one of the factors of m. In addition, $M = m/m'$ and $\mathbb{F}_q^*$ denotes the multiplicative group of $\mathbb{F}_q$, that is $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$.

2 Preliminaries

This section briefly explains some fundamental concepts of the finite field theory such as group, field, primitive polynomial, trace function, Legendre symbol, and dual bases. Then, binary sequence is introduced along with its period and distribution of bit patterns properties.

2.1 Group

A group is a non-empty set $\mathbb{G}$ with a binary operation $\circ$ on its elements denoted as $< \mathbb{G}, \circ >$, which satisfies

the following axioms.

- **Closure** For $\forall_{a,b} \in \mathbb{G}$, the result of $a \circ b$ also exists in $\mathbb{G}$ and it is uniquely given.
- **Associativity** Elements in group $\mathbb{G}$ should follow associativity. i.e. $(a \circ b) \circ c = a \circ (b \circ c)$, where $a, b, c \in \mathbb{G}$.
- **Identity element** There exists an element $e \in \mathbb{G}$ such that $\forall_a \in \mathbb{G}$, $a \circ e = e \circ a = a$.
- **Inverse element** For $\forall_a \in \mathbb{G}$, there exists an element $b \in \mathbb{G}$ such that $a \circ b = e = b \circ a$, where b is called inverse element of a.

Commutative group A group $\mathbb{G}$ will be commutative if $a \circ b = b \circ a$ for all $a, b \in \mathbb{G}$.

Group generator For a given group $\mathbb{G}$ if there is an element $g \in \mathbb{G}$ such that for any $a \in \mathbb{G}$ there exists an unique integer i with $a = g^i$ then g will be called as a generator of $\mathbb{G}$.

Order of a group The order of a group $\mathbb{G}$ often denoted as $\#\mathbb{G}$ is the number of elements in the group $\mathbb{G}$.

Cyclic group A group $\mathbb{G}$ will be cyclic if there exists at least one generator $g \in \mathbb{G}$ and it is denoted as $\mathbb{G} =< g >$. From the definition of cyclic group, it can be visualized that each element in a cyclic group can be generated with iterative operations of generator g which shown in the following Figure 1.

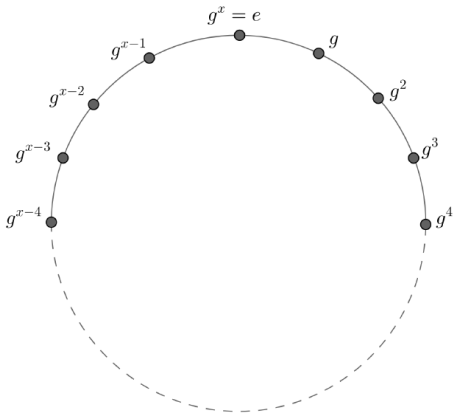

Figure 1: cyclic group.

Multiplicative group A cyclic group is called multiplicative if we tend to write its group operation in the same same way we do multiplication, that is

$$f = g \cdot x \text{ or } f = g^x.$$

2.2 Field

A field $< \mathbb{F}, +, \cdot >$ is a set that obeys two binary operations denoted by + and $\cdot$, such that

- $\mathbb{F}$ is a commutative group with respect to addition (+) having identity element 0.
- Let $\mathbb{F}^*$ is a subset of $\mathbb{F}$ having non-zero elements of $\mathbb{F}$ i.e. $\mathbb{F}^* = \mathbb{F} - \{0\}$. Then $\mathbb{F}^*$ will be called a commutative group with respect to multiplication $(\cdot)$, where every element should have multiplicative inverse in $\mathbb{F}^*$.
- For all $a, b, c \in \mathbb{F}$ the distributive law will be followed, i.e. $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

Sub field Let $\mathbb{F}_1$ is a sub field of a field $\mathbb{F}$. Then $\mathbb{F}_1$ will be called a sub field if $\mathbb{F}_1$ obeys the laws of field with respect to the field operation inherited from $\mathbb{F}$. In addition, if $\mathbb{F}_1 \neq \mathbb{F}$, then $\mathbb{F}_1$ is a proper sub field of $\mathbb{F}$.

Prime field Let p be a prime. The ring of integers modulo p is a finite field of characteristic p having field order p denoted as $\mathbb{F}_p$ is called a prime field.

Extension field A subset $\mathbb{F}_0$ of a field $\mathbb{F}$ that is itself a field under the operations of $\mathbb{F}$ will be called a sub field of $\mathbb{F}$. In this case, $\mathbb{F}$ is called an extension field of $\mathbb{F}_0$. An extension field of a prime field $\mathbb{F}_p$ can be represented as m-dimensional vector space that has m elements in $\mathbb{F}_p$. Let the vector space be the m-th extension field be denoted as $\mathbb{F}_{q^M}$. The order of a extension field $\mathbb{F}_{q^M}$ is given as p^m (here $q = p^{m'}$ and $M = m/m'$).

In very brief, it can be said that a prime field ($\mathbb{F}_p$) is a subset of sub extension field ($\mathbb{F}_q$) and sub extension field $\mathbb{F}_q$ is also a sub set of extension field $\mathbb{F}_{q^M}$ which shown in Figure 2.

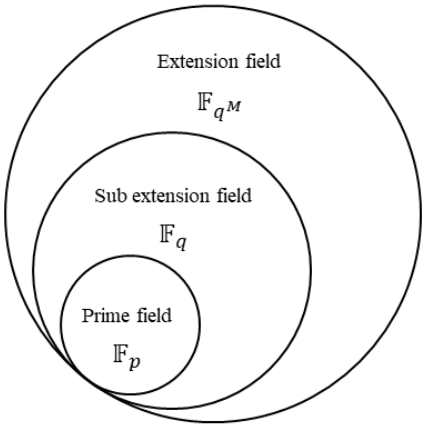

Figure 2: $\mathbb{F}_p \subset \mathbb{F}_q \subset \mathbb{F}_{q^M}$.

2.3 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 $q^M - 1$. Then $f(x)$ is especially called a primitive polynomial, when e is equal to $q^M - 1$. Its zero ω belongs to the extension field $\mathbb{F}_{q^M}$ and it becomes a primitive element in $\mathbb{F}_{q^M}$ that generates every non-zero element in $\mathbb{F}_{q^M}$ as its power ω^i (for $i = 0, 1, 2, \ldots, q^{M-2}$).

2.4 Trace Function

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

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

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,

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

where $a, b \in \mathbb{F}_q$ and $X, Y \in \mathbb{F}_{q^M}$.

2.5 Legendre Symbol

The Legendre symbol $\left(a/q\right)_2$ is used to check the quadratic residue for any arbitrary element a in $\mathbb{F}_q$. It is defined as,

$$\begin{aligned}\left(a/q\right)_2 &= a^{(q-1)/2} \\ &= \begin{cases} 0, & \text{if } a = 0, \\ 1, & \text{else if } a \text{ is a QR in } \mathbb{F}_q^*, \\ p-1, & \text{otherwise } a \text{ is a QNR in } \mathbb{F}_q^*. \end{cases}\end{aligned} \tag{3}$$

Here, QR and QNR stand for Quadratic Residue (QR) and Quadratic Non-Residue (QNR), respectively. Additionally, the non-zero element a is called the QR if it has a square root in $\mathbb{F}_q$, otherwise a is called the QNR. In this paper, the Legendre symbol is used for translating a vector sequence generated by the trace function over $\mathbb{F}_q$ to a binary sequence. Above mentioned QR and QNR in $\mathbb{F}_q$ holds the following important property.

Non-zero elements are the roots of $x^{q-1} - 1$ in $\mathbb{F}_q^*$ over $\mathbb{F}_q$ without any duplicates. Since it is factorized as follows:

$$x^{q-1} - 1 = \left(x^{(q-1)/2} - 1\right) - \left(x^{(q-1)/2} - 1\right). \tag{4}$$

It is thus found that the number of QR's and QNR's in $\mathbb{F}_q^*$ are the same and it is given by $(q-1)/2$. In addition, these numbers are important part in proving the theorem in the later section of this paper.

2.6 Dual Bases

The dual bases plays an important role in proving the theorem shown in this paper. It is defined as follows:

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

$$\mathrm{Tr}_{q^M|q}\left(\alpha_i \beta_j\right) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise}, \end{cases} \tag{5}$$

where $1 \le i, j \le m-1$.

2.7 Binary Sequence and Its Properties

This paper introduces a binary sequence along with its period and distribution of bit patterns properties as follows.

2.7.1 Generation Procedure and Period

Let ω be a primitive element in the extension field $\mathbb{F}_{q^M}$, where $M = m/m'$, m be a composite number which denotes the extension degree of the primitive polynomial, and m' be one of the factors of m. Then, by utilizing the trace function and Legendre symbol a binary sequence $\mathcal{S}$ is generated as follows:

$$\mathcal{S} = \{s_i\}, s_i = f_2\left(\left(\mathrm{Tr}_{q^M|q}\left(\omega^i\right)\Big/p\right)\right), \tag{6}$$

where $i = (0, 1, 2, \ldots, \lambda - 1, \ldots)$, $s_i \in 0, 1$ and $f_2(\cdot)$ be a mapping function, which translates the 0, 1, and $p-1$ values sequence generated by the Legendre symbol to a pseudo-random binary sequence. This mapping function is defined as follows:

$$f_2(s) = \begin{cases} 0, & \text{if } x = 0, 1 \bmod q, \\ 1, & \text{otherwise.} \end{cases} \tag{7}$$

After observing many experimental results, the authors derive the equation for the period λ of the binary sequence as,

$$\lambda = \frac{2(q^M - 1)}{q - 1}. \tag{8}$$

2.7.2 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 the 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 a uniform distribution of 1 and 0. In other words, 1 and 0 appear same in number. However, when we check 2-bit patterns on $\mathcal{S}_{12}$, we find that it only has two types of patterns (10 and 01). In this case, we can easily predict the next bit patterns after observing the previous patterns. For example, let us make a sub-sequence of $\mathcal{S}_{12}$ as $\{1, 0, 1, 0, x_5, x_6\}$, we can easily guess x_5 and x_6 as $x_5 = 1$ and $x_6 = 0$. Therefore, it is also essential to evaluate the distribution of bit patterns of the sequence to confirm its randomness. In other words, the uniformity of the distribution contributes to the randomness from the viewpoint of unpredictability.

3 Distribution of Bit Patterns in Binary Sequence

In this section, we will introduce the bit distribution of binary sequence which generated over the sub extension field. In addition, bit distribution of M-sequence and Legendre sequence is also introduced here. Throughout this section $b^{(n)}$, $Z(b^{(n)})$ and $D_{\mathcal{S}_\lambda}(b^{(n)})$ denotes a bit pattern of length n, number of 0's in $b^{(n)}$, and number of appearance of $b^{(n)}$ in $\mathcal{S}_\lambda$, respectively. For example, in a binary sequence of period 15, a 3-bit pattern $b = 101$ appears 4 times. Then, these notations become $b^{(3)} = 101$, $Z(b^{(3)}) = 1$, and $D_{\mathcal{S}_{15}}(b^{(3)}) = 4$.

3.1 Bit Distribution of M-sequence

The M-sequence [9] is generated by a linear recurrence relation over the finite field. M-sequence has a maximum period and uniform distribution of bit pattern except for the case of $Z(b^{(n)}) = n$ but it has minimum linear complexity. Let, $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$, then using the linear recurrence relation a M-sequence of period 15 becomes as follows.

$$\mathcal{S}_{15} = \{1,0,0,0,1,1,1,1,0,1,0,1,1,0,0\}. \quad (9)$$

The distribution of n-bit pattern in (9) is shown in Table 1, here $1 \le n \le m$. In the case of M-sequence, except the all-zero pattern, every pattern appears same in number. For example, when $n = 3$ all patterns appear 2 times (except 000 pattern). In other words, they are uniformly distributed. Every M-sequence has such good distribution of bit pattern feature.

Table 1: Bit distribution of the M-sequence $\mathcal{S}_{15}$.

n	$b^{(n)}$	$Z(b^{(n)})$	$D_{S_{15}}(b^{(n)})$
1	0	1	7
	1	0	8
2	00	2	3
	01	1	4
	10	1	4
	11	0	4
3	000	3	1
	001	2	2
	010	2	2
	100	2	2
	011	1	2
	101	1	2
	110	1	2
	111	0	2

3.2 Bit Distribution of LegendreSequence

Legendre sequence [7, 8] is generated by applying the Legendre symbol over the odd characteristic field. Legendre sequence has a long period, high linear complexity, and the distribution of bit pattern is close to uniform. Let, $p = 23$, then the Legendre sequence of period 23 becomes as follows.

$$\mathcal{S}_{23} = \{0,0,0,0,0,1,0,1,0,0,1,1,0,0,1,1,0,0,1,0,1,0,1,1,1\}. \quad (10)$$

The distribution of n-bit pattern in (10) is shown in Table 2. In case of Legendre symbol, bit patterns appearance is close to uniform.

Table 2: Bit distribution of the Legendre sequence $\mathcal{S}_{23}$.

n	$b^{(n)}$	$Z(b^{(n)})$	$D_{S_{23}}(b^{(n)})$
1	0	1	12
	1	0	11
2	00	2	6
	01	1	6
	10	1	5
	11	0	5
3	000	3	3
	001	2	3
	010	2	3
	100	2	3
	011	1	2
	101	1	3
	110	1	2
	111	0	2

3.3 Bit Distribution of the Proposed Binary Sequence

Let $\mathcal{S}_\lambda$ be a binary sequence of having a period of λ. Again, let $b^{(n)}$, $Z(b^{(n)})$, and $D_{\mathcal{S}_\lambda}(b^{(n)})$ denotes a bit pattern of length n, number of 0's in $b^{(n)}$, and number of appearance of $b^{(n)}$ in $\mathcal{S}_\lambda$, respectively. Then, the distribution of bit patterns in the binary sequence which defined over the sub extension field can be given by the following theorem.

$$D_{S_\lambda}\left(b^{(n)}\right) = \begin{cases} q^{M-(n\cdot m')} \cdot \left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)-1} \cdot \left(\frac{q+1}{2}\right)^{Z\left(b^{(n)}\right)} & \text{(11a)} \\ \qquad \text{when } 0 \le Z\left(b^{(n)}\right) < n, & \\ \lambda - \sum_{u=0}^{Z\left(b^{(n)}\right)} {}_nC_u \cdot D_{S_\lambda}\left(b^{(n)}\right) & \text{(11b)} \\ \qquad \text{when } Z\left(b^{(n)}\right) = n. & \end{cases}$$

Let ω be a primitive element in the extension field $\mathbb{F}_{q^M}$, where $M = m/m'$, m be a composite number which denotes the extension degree of the primitive polynomial, and m' be one of the factors of m. Then, utilizing the trace function and Legendre symbol one period of a binary sequence is generated as follows.

$$\mathcal{S}_\lambda = \{s_i\}, s_i = f_2\left(\left(\mathrm{Tr}_{q^M|q}\left(\omega^i\right)\Big/\!\!\Big/ p\right)\right), i = 0,1,2,\ldots,\lambda-1,\ldots, \quad (12)$$

Here λ be the period of the sequence and it is given by the following equation as,

$$\lambda = \frac{2(q^M - 1)}{q - 1}. \quad (13)$$

At first, a primitive polynomial is used, then the trace value is calculated, then the Legendre symbol outputs zero, QR or QNR in $\mathbb{F}_q$, and finally the sequence coefficients s_i is given by the mapping function $f_2(\cdot)$.

The authors of this paper observe the distribution of n-bit patterns in a binary sequence. It should be noted that here n satisfies $1 \leq n \leq (m/m')$ relation. The distribution of n-bit patterns evaluated by observing the consecutive sequence coefficients $(s_i, s_{i+1}, \ldots, s_{i+(n-1)})$. Particularly,

$$\begin{aligned} s_{i+0} &= f_2\left(\left(\mathrm{Tr}\left(\omega^i \cdot \omega^0\right)\right\rVert_p\right), \\ s_{i+1} &= f_2\left(\left(\mathrm{Tr}\left(\omega^i \cdot \omega^1\right)\right\rVert_p\right), \\ &\vdots \\ s_{i+(n-1)} &= f_2\left(\left(\mathrm{Tr}\left(\omega^i \cdot \omega^{n-1}\right)\right\rVert_p\right), \end{aligned}$$

where $0 \leq i \leq (q^M - 2)$. By observing the above sequence coefficients, the distribution of bit patterns $D_{\mathcal{S}_\lambda}$ is determined by the following trace values.

$$\mathrm{Tr}\left(\omega^i \cdot \omega^0\right), \mathrm{Tr}\left(\omega^i \cdot \omega^1\right), \ldots, \mathrm{Tr}\left(\omega^i \cdot \omega^{n-1}\right). \quad (14)$$

Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ be a basis, ω be a primitive element and with this basis ω^i is represented as,

$$\omega^i = \sum_{j=0}^{m-1} a_{i,j}\alpha_j, \text{where } a_{i,j} \in \mathbb{F}_q \text{ and } 0 \leq i \leq q^M - 2. \quad (15)$$

Again let $\mathcal{B} = \{\omega^0, \omega^1, \ldots, \omega^{n-1}, \beta_n, \ldots, \beta_{m-1}\}$ be a dual basis of $\mathcal{A}$ in $\mathbb{F}_q$ over $\mathbb{F}_{q^M}$. Then we also have

$$\omega^t = \omega^t + \sum_{j=0}^{\frac{m}{m'}-1} 0 \cdot \beta_j, \text{where } 0 \leq t < n. \quad (16)$$

Since $\mathcal{A}$ and $\mathcal{B}$ are dual bases to each other, then $\mathrm{Tr}\left(\omega^i \cdot \omega^t\right)$ be calculated as follows.

$$\begin{aligned} \mathrm{Tr}\left(\omega^i \cdot \omega^t\right) &= \mathrm{Tr}\left(\sum_{j=0}^{m-1} a_{i,j}\alpha_j \cdot \left(\omega^t + \sum_{j=0}^{\frac{m}{m'}-1} 0 \cdot \beta_j\right)\right) \\ &= a_{i,t}. \end{aligned}$$

Therefore, by using the dual basis, the distribution of bit patterns $D_{\mathcal{S}_\lambda}\left(b^{(n)}\right)$ determined by the trace values becomes as follows.

$$\begin{aligned} &\mathrm{Tr}\left(\omega^i \cdot \omega^0\right), \mathrm{Tr}\left(\omega^i \cdot \omega^1\right), \ldots, \mathrm{Tr}\left(\omega^i \cdot \omega^{n-1}\right) \\ &= (a_{i,0}, a_{i,1}, \ldots, a_{i,n-1}). \end{aligned}$$

Thus, instead of using sequence coefficients $(s_i, s_{i+1}, \ldots, s_{i+(n-1)})$, we can consider the dual basis representation of these coefficients as $\left(a_{i,0}, a_{i,1}, \ldots, a_{i,(n-1)}\right)$. Additionally, all the above trace values belong to the sub extension field $\mathbb{F}_q$.

Furthermore, $\omega^i\left(0 \leq i \leq q^M - 2\right)$ in (15) represents every non-zero vectors in the extension field $\mathbb{F}_{q^M}$ as,

$$\left\{\mathrm{Tr}\left(\omega^0\right), \mathrm{Tr}\left(\omega^1\right), \mathrm{Tr}\left(\omega^2\right), \mathrm{Tr}\left(\omega^3\right), \ldots, \mathrm{Tr}\left(\omega^{q^M-2}\right)\right\}. \quad (17)$$

According to the trace property, non-zero $\mathbb{F}_q$ elements appear $q^{M-m'}$ times and zero appears one less than the other elements i.e. $q^{M-m'} - 1$ times in the above equation.

3.3.1 Relation Between the Sequence Coefficients With the Trace Values and Legendre Symbol Calculation

Depending on the three different types of trace values (0, QR, and QNR), the Legendre symbol outputs three different values (0, 1, and $p-1$), and finally the mapping function outputs 0 and 1 as sequence coefficients s_i. This dependency between the trace and Legendre symbol is explained as follows.

Table 3: Relation between the sequence coefficients with trace and Legendre symbol calculation -I.

s_i	$\mathrm{Tr}\left(\omega^i\right)$
0	0 or QR in $\mathbb{F}_q^*$
1	QNR in $\mathbb{F}_q^*$

According to the above table, the sequence coefficient 0 comes from the two cases: one is for the $\mathrm{Tr}(0)$ case and another one is for the QR in $\mathbb{F}_q^*$ case. To deal with this two cases uniquely, let us denote **0** and 0 for the first and second cases, respectively. In addition, 1 comes for QNR in $\mathbb{F}_q^*$ case. Thus the above table can be further modified as follows.

Table 4: Relation between the sequence coefficients with trace and Legendre symbol calculation -II.

s_i	$\mathrm{Tr}\left(\omega^i\right)$
0	0
0	QR in $\mathbb{F}_q^*$
1	QNR in $\mathbb{F}_q^*$

To distinguish the appearance of 0, this paper uses the notation **0**, when zero comes from $\mathrm{Tr}(0)$ and 0 when zero comes from QR. Let the number of **0** be denoted by u and $T_{u,n}$ denotes the number of bit patterns including u times **0** and $Z(b^{(n)}) - u$ times 0. Thus, T_n can be considered as,

$$\sum_{u=0}^{Z\left(b^{(n)}\right)} T_{u,n}. \quad (18)$$

In the following section, the distribution of bit patterns in the binary sequence defined over the sub extension field theoretically proven.

3.3.2 Proof of (11a)

The period of the binary sequence is given by the following equation as,

$$\lambda = \frac{2(q^M-1)}{q-1}. \tag{19}$$

After rewriting the above equation we obtain,

$$q^M - 1 = \lambda \cdot \left(\frac{q-1}{2}\right). \tag{20}$$

To observe the distribution of bit patterns, the above relation becomes as follows.

$$D_{\mathcal{S}_{q^M-1}}\left(b^{(n)}\right) = D_{\mathcal{S}_\lambda}\left(b^{(n)}\right) \cdot \left(\frac{q-1}{2}\right). \tag{21}$$

Thus, we must consider two cases of the sequence length such as $\mathcal{S}_{q^M-1}$ and $\mathcal{S}_\lambda$. Hence, we will observe the distribution of bit patterns in $\mathcal{S}_{q^M-1}$ as $D_{\mathcal{S}_{q^M-1}}\left(b^{(n)}\right)$ and $\mathcal{S}_\lambda$ as $D_{\mathcal{S}_\lambda}\left(b^{(n)}\right)$.

In the previous section, we explained that n-bit patterns can be considered as $b^{(n)} = (a_{i,0}, a_{i,1}, \ldots, a_{i,n-1})$. On the other hand, the remaining $(m-(n\cdot m'))$-bit patterns are composed of $(a_{i,nm'}, a_{i,nm'+1}, \ldots, a_{i,m-1})$ coefficients of ω^i, which is given by the (16). In addition, the number of combinations of $(a_{i,nm'}, a_{i,nm'+1}, \ldots, a_{i,m-1})$ becomes $q^{M-nm'}$. It should be noted that here ω^i represents all of the non-zero coefficients in the extension field $\mathbb{F}_{q^M}$.

As mentioned previously, when the trace value is equal to 0 or QR, then the sequence coefficients becomes **0** and 0, respectively. In addition, if the trace value is equal to QNR, then the sequence coefficients becomes 1. Additionally, u denotes the number of **0** in $b^{(n)}$ $\left(\text{where } 0 \le u \le Z\left(b^{(n)}\right)\right)$ from $\mathrm{Tr}(0)$, then the other 0's comes from $Z\left(b^{(n)}\right) - u$ QR's, and finally 1's comes from $n - Z\left(b^{(n)}\right)$ QNR's. Therefore, by separating 0, $T_{u,n}$, and T_n the combination of n-bit patterns can be given as follows.

$$\begin{aligned} T_{u,n} = {}& {}_nC_u \cdot {}_{n-u}C_{Z\left(b^{(n)}\right)-u} \cdot \left(\frac{q-1}{2}\right)^{Z\left(b^{(n)}\right)} \\ & \times {}_{n-Z\left(b^{(n)}\right)}C_{n-Z\left(b^{(n)}\right)} \cdot \left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)} \end{aligned} \tag{22}$$

Furthermore, T_n can be derived as,

$$\begin{aligned} T_n &= \sum_{u=0}^{Z\left(b^{(n)}\right)} T_{u,n} \\ &= \sum_{u=0}^{Z\left(b^{(n)}\right)} {}_nC_u \cdot {}_{n-u}C_{Z\left(b^{(n)}\right)-u} \cdot \left(\frac{q-1}{2}\right)^{Z\left(b^{(n)}\right)} \\ &\quad \times \left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)} \end{aligned} \tag{23}$$

According to the above equation, T_n can be calculated by $Z\left(b^{(n)}\right)$. In addition, there are ${}_nC_{Z\left(b^{(n)}\right)}$ possible bit patterns that have the same $Z\left(b^{(n)}\right)$. To calculate the $D_{\mathcal{S}_{q^M-1}}\left(b^{(n)}\right)$ for each $b^{(n)}$, T_n needs to be divided by ${}_nC_{Z\left(b^{(n)}\right)}$.

$$\begin{aligned} D_{\mathcal{S}_{q^M-1}}\left(b^{(n)}\right) &= q^{M-(n\cdot m')} \cdot \frac{T_n}{{}_nC_{Z\left(b^{(n)}\right)}} \\ &= q^{M-(n\cdot m')} \sum_{u=0}^{Z\left(b^{(n)}\right)} \frac{{}_nC_u \cdot {}_{n-u}C_{Z\left(b^{(n)}\right)-u}}{{}_nC_{Z\left(b^{(n)}\right)}} \\ &\quad \times \left(\frac{q-1}{2}\right)^{Z\left(b^{(n)}\right)-u} \cdot \left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)} \end{aligned} \tag{24}$$

The above equation can be further modified as follows.

$$\begin{aligned} & \sum_{u=0}^{Z\left(b^{(n)}\right)} {}_nC_u \cdot {}_{n-u}C_{Z\left(b^{(n)}\right)-u} \\ &= \frac{n!}{\left(n-Z\left(b^{(n)}\right)\right)!} \cdot \sum_{u=0}^{Z\left(b^{(n)}\right)} \cdot \frac{1}{u!\left(Z\left(b^{(n)}\right)-u\right)!} \\ &= \frac{n!}{\left(n-Z\left(b^{(n)}\right)\right)!} \cdot \sum_{u=0}^{Z\left(b^{(n)}\right)} \cdot \frac{1}{u!\left(Z\left(b^{(n)}\right)-u\right)!} \\ &\qquad \times \frac{\left(Z\left(b^{(n)}\right)\right)!\left(n-Z\left(b^{(n)}\right)\right)!}{n!} \\ &= \sum_{u=0}^{Z\left(b^{(n)}\right)} \frac{(Z(b^{(n)}))!}{u!(Z(b^{(n)}))!} = {}_{Z\left(b^{(n)}\right)}C_{Z\left(b^{(n)}\right)-u}. \end{aligned} \tag{25}$$

Thus, (24) becomes as follows:

$$\begin{aligned} D_{\mathcal{S}_{q^M-1}}\left(b^{(n)}\right) &= q^{M-(n\cdot m')} \sum_{u=0}^{Z\left(b^{(n)}\right)} {}_{Z\left(b^{(n)}\right)}C_{Z\left(b^{(n)}\right)-u} \\ &\quad \times \left(\frac{q-1}{2}\right)^{Z\left(b^{(n)}\right)-u} \cdot \left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)} \end{aligned} \tag{26}$$

By using the bilinear theorem, the above equation can be rewritten as,

$$\begin{aligned} D_{\mathcal{S}_{q^M-1}}\left(b^{(n)}\right) &= q^{M-(n\cdot m')} \cdot \left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)} \\ &\quad \times \left(\frac{q-1}{2}+1\right)^{Z\left(b^{(n)}\right)} \\ &= q^{M-(n\cdot m')} \cdot \left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)} \cdot \left(\frac{q+1}{2}\right)^{Z\left(b^{(n)}\right)}. \end{aligned} \tag{27}$$

From the (21), $D_{\mathcal{S}_\lambda}\left(b^{(n)}\right)$ holds the following relation as follows,

$$D_{\mathcal{S}_\lambda}\left(b^{(n)}\right) = D_{\mathcal{S}_{q^M-1}}\left(b^{(n)}\right) \cdot \left(\frac{q-1}{2}\right)^{-1}. \tag{28}$$

Therefore, using the (27), $D_{\mathcal{S}_\lambda}\left(b^{(n)}\right)$ can be given by the following relation as,

$$\begin{aligned} D_{\mathcal{S}_\lambda}\left(b^{(n)}\right) &= q^{M-(n\cdot m')}\cdot\left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)} \\ &\quad\times\left(\frac{q+1}{2}\right)^{Z\left(b^{(n)}\right)}\cdot\left(\frac{q-1}{2}\right)^{-1} \\ &= q^{M-(n\cdot m')}\cdot\left(\frac{q-1}{2}\right)^{n-Z\left(b^{(n)}\right)-1}\cdot\left(\frac{q+1}{2}\right)^{Z\left(b^{(n)}\right)}. \end{aligned} \tag{29}$$

Thus, the first part of the (11a) is proven.

3.3.3 Proof of (11b)

Let us consider the case that $Z\left(b^{(n)}\right)=n$. Therefore, the combination of n-bit patterns except the all-zero patterns is given as follows:

$${}_nC_{Z\left(b^{(n)}\right)}. \tag{30}$$

Thus, the distribution of all-zero patterns becomes

$$D_{\mathcal{S}_\lambda}\left(b^{(n)}\right)=\lambda-\sum_{u=0}^{n-1}{}_nC_u\cdot D_{\mathcal{S}_\lambda}\left(b^{(n)}\right). \tag{31}$$

Thus, the second part of the (11b) is proven. In addition, the theorem in (11) is also proven.

4 Result and Discussion

This section explains the distribution of bit patterns in the binary sequence which generated over the sub extension field based on some experimental results. Then, a comparison between the binary sequence defined over the sub extension field and our previous geometric sequence [13] also introduces in terms of the distribution of bit patterns property. Here, H_{wt} denotes the hamming weight.

4.1 Experimental Results

Let us consider the distribution of bit patterns in the binary sequence, introduced in this paper which generated over the sub extension field in the following examples.

Example 1 *Let $p=5, m=4$, and $m'=2$, then the sequence having a period of* 52 *becomes as follows its distribution of n-bit patterns is shown in Table 5.*

$$\begin{aligned} \mathcal{S}_{52} = \{&0100110100000010101111001 1 \\ &1011001011111001010000110 0\}. \end{aligned} \tag{32}$$

Table 5: Bit distribution of the binary sequence $\mathcal{S}_{52}$ with $p=5, m=4$, and $m'=2$.

n	$H_{wt}(b^{(n)})$	$Z(b^{(n)})$	$D_{S_{52}}(b^{(n)})$
1	0	1	27
	1	0	25
2	0	2	14
	1	1	13
	2	0	12

Example 2 *Let $p=3, m=6$, and $m'=2$, then the sequence having a period of* 182 *becomes as follows its distribution of n-bit patterns is shown in Table 6.*

Table 6: Bit distribution of the binary sequence $\mathcal{S}_{182}$ with $p=3, m=6$, and $m'=2$.

n	$H_{wt}(b^{(n)})$	$Z(b^{(n)})$	$D_{S_{182}}(b^{(n)})$
1	0	1	101
	1	0	81
2	0	2	56
	1	1	45
	2	0	36
3	0	3	31
	1	2	25
	2	1	20
	3	0	16

Example 3 *Let $p=7, m=9$, and $m'=3$, then the sequence having a period of* 235986 *becomes as follows its distribution of n-bit patterns is shown in Table 7.*

Table 7: Bit distribution of the binary sequence $\mathcal{S}_{235986}$ with $p=7, m=9$, and $m'=3$.

n	$H_{wt}(b^{(n)})$	$Z(b^{(n)})$	$D_{S_{235986}}(b^{(n)})$
1	0	1	118337
	1	0	117649
2	0	2	59341
	1	1	58996
	2	0	58653
3	0	3	29757
	1	2	29584
	2	1	29412
	3	0	29241

4.1.1 Observation

It was found that the experimental results explicitly support the (11). In addition, the number of appearance of each bit pattern is related to the number of zeros contained in each bit pattern. Moreover, $D_{\mathcal{S}_\lambda}(b^{(n)})$

increases in proportion to $Z(b^{(n)})$. To confirm this, let us check the **Example** 2 with $n = 3$.

$Z(b^{(3)}) = 0$:

$$D_{S_{182}}(b^{(3)} = 111) = 3^{6-(3\times2)} \cdot 4^{3-0-1} \cdot 5^0 = 16.$$

$Z(b^{(3)}) = 1$:

$$D_{S_{182}}(b^{(3)} = 011) = 3^{6-(3\times2)} \cdot 4^{3-1-1} \cdot 5^1 = 20,$$
$$D_{S_{182}}(b^{(3)} = 101) = 3^{6-(3\times2)} \cdot 4^{3-1-1} \cdot 5^1 = 20,$$
$$D_{S_{182}}(b^{(3)} = 111) = 3^{6-(3\times2)} \cdot 4^{3-1-1} \cdot 5^1 = 20.$$

$Z(b^{(3)}) = 2$:

$$D_{S_{182}}(b^{(3)} = 001) = 3^{6-(3\times2)} \cdot 4^{3-2-1} \cdot 5^2 = 25,$$
$$D_{S_{182}}(b^{(3)} = 010) = 3^{6-(3\times2)} \cdot 4^{3-2-1} \cdot 5^2 = 25,$$
$$D_{S_{182}}(b^{(3)} = 100) = 3^{6-(3\times2)} \cdot 4^{3-2-1} \cdot 5^2 = 25.$$

$Z(b^{(3)}) = 3$:

$$D_{S_{182}}(b^{(3)} = 000) = 182 - (1 \times 16 + 3 \times 20 + 3 \times 25) = 31.$$

4.2 Comparison With Our Previous Work

By combining the features of the M-sequence and Legendre sequence our previous work [13] proposed a geometric sequence, namely NTU (Nogami-Tada-Uehara) sequence. According to our previous research work, NTU sequence always holds long period, low correlation, high linear complexity properties which are the important considerations to use any sequence in cryptographic applications. Another crucial consideration before utilizing them in any secure applications, is to judge the randomness of a sequence. To do so, we need to evaluate the distribution of bit patterns property in a sequence. After the experimental observation, it was found that in terms of distribution of bit patterns 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), we 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 tables (Table 8 and Table 9).

It should be noted that the NTU sequence is controlled by 2 parameters (p and m), on the other hand the sequence over the sub extension field is controlled by 3 parameters (p, m, and m'). Therefore, it is not possible to make the comparison between these two sequences in terms of the same length (in other words, the same period λ). The authors kept the difference as minimum as possible.

One of the most notable outcomes of this comparison result is the NTU sequence holds higher difference in terms of the appearance between the 'all zero' and 'all one' patterns. In other words, it also confirms the ununiform distribution of bit patterns. On the other hand, sequence defined over the sub extension field minimizes this difference to make it close to uniform. This comparison graphically shown in Figure 3.

Table 8: Comparison in bit distribution between the sub field binary sequence and NTU sequence -I.

n	$H_{wt}(b^{(n)})$	$D_{S_{182}}(b^{(n)})$	%	$D_{NTU_{242}}(b^{(n)})$	%
1	0	101	55.49	161	66.52
	1	81	44.51	81	33.48
2	0	56	30.76	107	44.21
	1	45	24.72	54	22.31
	2	36	19.78	27	11.15
3	0	31	17.03	71	29.33
	1	25	13.73	36	14.87
	2	20	10.98	18	7.43
	3	16	8.79	9	3.71

Table 9: Comparison in bit distribution between the sub field binary sequence and NTU sequence -II.

n	$H_{wt}(b^{(n)})$	$D_{S_{240200}}(b^{(n)})$	%	$D_{NTU_{275514}}(b^{(n)})$	%
1	0	122551	51.02	156865	56.93
	1	117649	48.98	117649	43.07
2	0	62526	26.03	89637	32.53
	1	60025	24.98	67228	24.40
	2	57624	23.99	50421	18.30
3	0	31901	13.28	51221	18.59
	1	30625	12.74	38416	13.94
	2	29400	12.23	28812	10.45
	3	28224	11.75	21609	7.84
4	0	16276	6.77	29269	10.62
	1	15625	6.50	21952	7.96
	2	15000	6.24	16464	5.97
	3	14400	5.99	12348	4.48
	4	13824	5.75	9261	3.36

Recently, there are lots of considerations to use a long period pseudo-random sequence in cryptographic applications. The use of binary sequence in a stream cipher is one of the most common application. Before applying a sequence in such applications, the linear complexity and distribution of bit patterns are considered as the most important properties regarding a sequence to check its randomness. Among these two, the authors observed the linear complexity property in their previous work [16] and it always holds a maximum value of the linear complexity. As a continuation, the authors focused on the distribution of bit patterns in this paper. According to the comparison results, the binary sequence generated over the sub extension field holds much better (close to uniform) compared to our previous binary sequence in terms of distribution of bit patterns. Therefore, the binary sequence defined over the sub extension field can be a suitable candidate for some cryptographic applications.

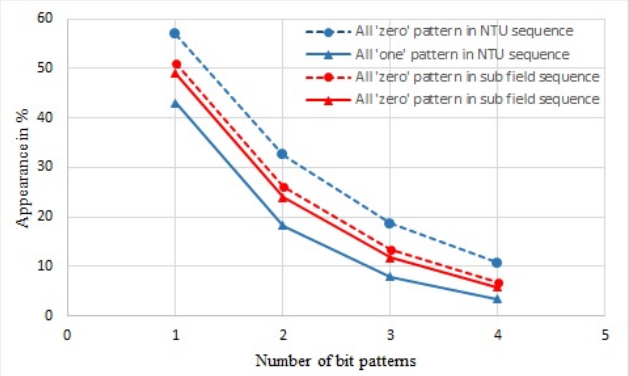

Figure 3: Appearance of 'all zero' and 'all one' bit patterns in the NTU and sub field sequence.

5 Conclusion

In this paper, the authors observed the distribution of bit patterns in a binary sequence which defined over the sub extension. The number of appearances is related to the number of zeros contained in each bit pattern. Furthermore, the authors theoretically prove the distribution of bit patterns property. In addition, they also made a comparison between the binary sequence defined over the sub extension field and our previous work on binary sequence based on distribution of bit patterns property. According to the comparison results, the binary sequence generated over the sub extension field holds much better (close to uniform) compared to our previous binary sequence. As a future work, we would like to consider an efficient implementation to enhance the usability of our proposed sequence a Cryptographically Secure Pseudo Random Number Generator (CSPRNG).

Conflict of Interest The authors declare no conflict of interest.

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

References

[1] J. Daemen and V. Rijmen, The Design of Rijndael, Springer-Verlag Berlin Heidelberg, Germany, 2002.

[2] Richard A. Mollin, RSA and Public-Key Cryptography, Chapman & Hall CRC, 2002.

[3] H. Cohen and G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Mathematics and Its Applications, Chapman & Hall CRC, 2005.

[4] V. Edemskiy, On the Linear Complexity of Interleaved Binary Sequences of Period 4p Obtained from Hall Sequences or Legendre and Hall Sequences, IEEE Electronic Letter, 50, 8, 604–605, 2014.

[5] M. Matsumoto and T. Nishimura, "Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudo-Random Number Generator", ACM Trans. on Modeling and Computer Simulation, **8**(1), 3–30, 1998. http://doi.org/10.1145/272991.272995

[6] L. Blum, M. Blum, and M. Shub, "A simple Unpredictable Pseudo-Random Number Generator", SIAM Journal on Computing, **15**(2), 364–383, 1986. http://doi.org/10.1137/0215025

[7] X. Tang and G. Gong, "New Constructions of Binary Sequences with Optimal Autocorrelation Value/Magnitude", IEEE Trans. Inf. Theory, **56**(3), 1278–1286, 2010. http://doi.org/10.1109/TIT.2009.2039159

[8] J. S. No, H. K. Lee, H. Chung, H. Y. Song, and K. Yang, "Trace Representation of Legendre Sequence of Mersenne Prime Period", IEEE Trans. on Inform. Theory, **42**(6 PART 2), 2254–2255, 1996. https://doi.org/10.1109/18.556617

[9] J. Ren, "Design of Long Period Pseudo-Random Sequence from the Addition of m-sequences over $\mathbb{F}_p$", EURASIP Journal on Wireless Communication and Networking, **1**, 12–18, 2004. http://doi.org/10.1155/S1687147204405052

[10] C. Ding, "Pattern Distributions of Legendre Sequences", IEEE Transactions on Information Theory, **44**(4), 1693–1698, 1998. http://doi.org/10.1109/18.681353

[11] B. Z. Moroz, "The distribution of power residues and non-residues", Vestnik Leningrad Univ. Math, **16**, 164–169, 1961. (In Russian with English summary)

[12] T. Helleseth, "Maximal-length sequences", Encyclopedia of Cryptography and Security, 2nd Ed. Springer, 5–14, 2011. https://doi.org/10.1007/978-1-4419-5906-5_359

[13] Y. Nogami, K. Tada, and S. Uehara, "Geometric Sequence Binarized with Legendre Symbol over Odd Characteristic Field and Its Properties", IEICE Trans. on Fund. of Electronics and Computer Sciences, **E97.A**(12), 2336–2342, 2014. https://doi.org/10.1587/transfun.E97.A.2336

[14] 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 Trans. on Fund. of Electronics, Communications and Computer Sciences, **E99.A**(12), 2226–2237, 2016. https://doi.org/10.1587/transfun.E99.A.2226

[15] A. M. Arshad, Y. Nogami, H. Ino, and S. Uehara, "Auto and Cross Correlation of Well Balanced Sequence Over Odd Characteristic Field", Fourth International Symposium on Computing and Networking (CANDAR), Hiroshima, Japan, 2016. http://doi.org/10.1109/CANDAR.2016.0109

[16] A. M. Arshad, T. Miyazaki, S. Heguri, Y. Nogami, S. Uehara, and R. H. Morelos-Zaragoza, "Linear Complexity of Pseudo Random Binary Sequence Generated by Trace Function and Legendre Symbol Over Proper Sub Extension Field", Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA), Sapporo, Japan, 2017. http://doi.org/10.1109/IWSDA.2017.8095741

[17] A. M. Arshad, T. Miyazaki, Y. Nogami, S. Uehara, and R. H. Morelos-Zaragoza, "Multi-value Sequence Generated by Trace Function and Power Residue Symbol Over Proper Sub Extension Field", IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), Taipei, Taiwan, 2017. http://10.1109/ICCE-China.2017.7991089