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

Period and Some Distribution Properties of a Nonlinear Filter Generator with Dynamic Mapping

Yuta KODERA[†a)], ***Member***

SUMMARY This paper focuses on a pseudorandom number generator called an NTU sequence for use in cryptography. The generator is defined with an m-sequence and Legendre symbol over an odd characteristic field. Since the previous researches have shown that the generator has maximum complexity; however, its bit distribution property is not balanced. To address this drawback, the author introduces dynamic mapping for the generation process and evaluates the period and some distribution properties in this paper.

key words: *m-sequence, Legendre symbol, dynamic mapping, period, distribution property*

1. Introduction

Unpredictable behavior in a computer is an inevitable part of developments in many fields such as simulation and communication. In particular, random numbers are essential in cryptographic applications for making information unpredictable and unrecoverable without a key.

A pseudorandom number generator (PRNG) is a typical approach to mimicking the random-looking behavior of some phenomena in the real world using deterministic calculation on a computer. Cryptographic applications also utilize a type of PRNG as a ciphering system, and such an encryption scheme is known as stream cipher [1].

Most stream ciphers are classified into two families; a block cipher with counter mode, and generators that use a nonlinear filter and a linear recurrence relation over a field [2], [3]. The former case is preferred in practice owing to its efficiency and the benefits of sharing a block cipher module for random number generation and encryption. On the other hand, the properties of a PRNG, such as period, correlation, distribution, and complexity, are sometimes not ideal.

In this context, the latter approach, that is, the combination of a nonlinear filter and a linear recurrence relation, cannot be ignored as an alternative or a generator for IoT devices because of how lightweight it is. More precisely, a linear recurrence relation is well-known as a PRNG called maximum length sequence (m-sequence) [4], and a nonlinear filter is often designed as a boolean function. Such generators defined with an m-sequence and a boolean function are called nonlinear filter generators (NLFGs), and this paper focuses on a specific type of NLFG to improve its distribution property.

As a natural extension of NLFGs, NTU sequence has proposed by Nogami et al. in [5], [6]. According to the results concerning the properties of a sequence [7]–[9], it was discovered that the NTU sequence has maximum complexity; however, it cannot provide uniform distribution even if one observes a single bit in the period.

The paper investigates the drawback of the distribution property with low computational costs. One approach the author proposes is employing dynamic mapping in the filter. It has been observed that the method improves the distribution property.

However, dynamic mapping induces a symmetricity in the sequence that, while is useful for evaluating the sequence, may also be a vulnerability as a cryptographic application. Considering this, the author plans to modify the definition with an additive operation and evaluate the generator in future.

The remainder of this paper is organized as follows. Section 2 introduces some basics about finite fields and NLFGs, and Sect. 3 defines a generator. The period and some distribution properties of the generator are theoretically discussed in Sect. 4, and Sect. 5 concludes this work.

2. Preliminaries

This section briefly reviews the fundamentals of fields and some functions defined over a field [10]. Additionally, the basic concept of an NLFG is introduced.

2.1 Polynomials over Finite Fields

Let $\mathbb{F}_p$ be a finite field of characteristic p, where p is a prime number. Let $\mathbb{F}_p[x]$ denote the set of all polynomials over $\mathbb{F}_p$. A polynomial $f \in \mathbb{F}_p[x]$ of degree n is represented by a linear combination of coefficients $f_i \in \mathbb{F}_p$ for $0 \le i \le n$ and a variable x over $\mathbb{F}_p$ as follows:

$$f(x) = \sum_{i=0}^{n} f_i x^i = f_0 + f_1 x + \ldots + f_n x^n. \quad (1)$$

The polynomial $f(x) \in \mathbb{F}_p[x]$ is called a monic if the leading coefficient is 1. Since $\mathbb{F}_p$ is a field, there always exists the inverse of f_n and every polynomial can be represented as a monic polynomial over $\mathbb{F}_p$. For convenience, the author implicitly writes a polynomial as monic in what follows. Thus, Eq. (1) is rewritten as $\mathbb{F}_p[x] \ni f(x) = x^n + \sum_{i=0}^{n-1} f_i x^i$.

Manuscript received January 11, 2023.
Manuscript revised May 22, 2023.
Manuscript publicized August 8, 2023.

[†]The author is with Graduate School of Natural Science and Technology, Okayama University, Okayama-shi, 700-8530 Japan.
a) E-mail: yuta_kodera@okayama-u.ac.jp

DOI: 10.1587/transfun.2023SDL0001

A polynomial $f(x)$ is called an irreducible polynomial if there do not exist any smaller polynomials that divide $f(x)$, except for constant polynomials. Let $g(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. If $g(x)$ satisfies $g(x) | (x^t - 1)$ and $t = p^n - 1$, then the polynomial $g(x)$ is specially called a primitive polynomial. A root of $g(x)$ can be an element in the extension field of degree n over $\mathbb{F}_p$, which is denoted by $\mathbb{F}_{p^n}$, and such an element can generate every non-zero element in $\mathbb{F}_{p^n}$ as its power.

2.2 Field Trace and Dual Bases

Let $\mathbb{F}_{p^n}$ be an extension field of degree n over $\mathbb{F}_p$. The trace function $\mathrm{Tr}_p^{p^n} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is an $\mathbb{F}_p$-linear map defined by the sum of conjugates over $\mathbb{F}_{p^n}$, as shown in Eq. (2). It is well-known that the conjugates of an element $\boldsymbol{a} \in \mathbb{F}_{p^n}$ can be endowed by the Frobenius endomorphism $\phi_i : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, defined by $\phi_i(\boldsymbol{a}) = \boldsymbol{a}^{p^i}$.

$$\mathrm{Tr}_p^{p^n}(\boldsymbol{a}) = \sum_{i=0}^{n-1} \phi_i(\boldsymbol{a}) = \sum_{i=0}^{n-1} \boldsymbol{a}^{p^i}. \tag{2}$$

Since it is an $\mathbb{F}_p$-linear map, the trace function holds the following property:

$$\mathrm{Tr}_p^{p^n}(a_1\boldsymbol{b}_1 + a_2\boldsymbol{b}_2) = a_1\mathrm{Tr}_p^{p^n}(\boldsymbol{b}_1) + a_2\mathrm{Tr}_p^{p^n}(\boldsymbol{b}_2), \tag{3}$$

where $a_1, a_2 \in \mathbb{F}_p$ and $\boldsymbol{b}_1, \boldsymbol{b}_2 \in \mathbb{F}_{p^n}$.

Let $\mathbb{F}_p$ be a field and $\mathbb{F}_{p^n}$ be an extension field of degree n over $\mathbb{F}_p$. Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ and $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ be bases of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. These bases are said to be dual bases if the following equality holds for $0 \le i, j < n$.

$$\mathrm{Tr}_p^{p^n}(\alpha_i\beta_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases} \tag{4}$$

2.3 Legendre Symbol

A. M. Legendre introduced a multiplicative function with the values 0 and ±1 to evaluate the quadratic residuosity of an element in $\mathbb{F}_p$, where $\mathbb{F}_p$ is a field of characteristic $p(\ge 3)$. The symbol $\left(\frac{a}{p}\right)$ for $a \in \mathbb{F}_p$ is called the Legendre symbol, named after A. M. Legendre, and a is called a quadratic residue (QR) if there exists an element $b \in \mathbb{F}_p$ such that $a = b^2 \pmod p$. On the other hand, if there does not exist a square root of a, then a is called a quadratic non-residue (QNR).

According to the Fermat's little theorem, since every non-zero element $a \in \mathbb{F}_p$ satisfies $a^{p-1} = 1 \pmod p$, the Legendre symbol can be defined as follows:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a \text{ is QR in } \mathbb{F}_p, \\ -1 & \text{otherwise.} \end{cases}$$

Since it is multiplicative concerning the top argument, the following equality holds:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right), \tag{5}$$

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

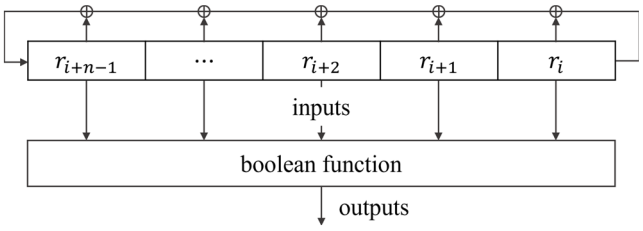

Fig. 1 A model of an NLFG.

2.4 Nonlinear Filter Generators

An NLFG is an instantiation of keystream generators for an efficient symmetric-key ciphering system, and it is commonly composed of a shift register sequence [4], also known as an m-sequence, and a boolean function as illustrated in Fig. 1, where $r_i \in \mathbb{F}_2$ in the figure.

An m-sequence is a typical PRNG generated by a linear recurrence relation over $\mathbb{F}_2$, and it is well-known that its bit distribution property is ideally uniform. More formally, let $g(x)$ be a primitive polynomial of degree n over $\mathbb{F}_2$ and let ω be a root of $g(x)$. Then, an m-sequence $S = \{s_i\}$ is generated by $s_i = \mathrm{Tr}_2^{2^n}(\omega^i)$. The above definition tells us that the generation process of an m-sequence can be naturally generalized to an arbitrary field $\mathbb{F}_q$ with a primitive polynomial over $\mathbb{F}_q$, where q is a prime power. Such an m-sequence is called a q-ary m-sequence. For convenience, the author simply refers to these m-sequences as m-sequence hereinafter.

The boolean function, also referred to as a boolean filter, of an NLFG is usually a multi-bit input and a single-bit output function, as shown in Fig. 1. Since an m-sequence is linear and vulnerable against the linear attack (e.g. Berlekamp-Massey algorithm [11]), the security of an NLFG relies on the toughness of the boolean function. In this context, many cryptographic boolean functions have been proposed [2], [3], and extended the concepts of an NLFG towards a more generic model.

As a branch of those extensions, Sidelńinkov and Lempel et al. independently introduced a generator known as a Sidelńikov sequence [12] or Lempel-Cohn-Eastman sequence [13] with a primitive element over a field $\mathbb{F}_q$ and a quadratic character of $\mathbb{F}_q$, where q is a prime power. Another direction of those extensions is the cascaded-GMW sequence (including GMW sequence) [14], [15] which is a natural extension of an m-sequence. In addition, the NTU sequence [5], [6] is said to be the combination of the above sequences in the sense that it is defined with a trace function and a Legendre symbol.

According to the previous research concerning NTU

sequences, it has been theoretically proven that an NTU sequence has the maximum complexity [7]; however, it is also known that the bit distribution property is unbalanced [8] due to the mapping function. To address this drawback, the author, in this paper, introduces dynamic mapping for an NTU sequence to improve its distribution property with less degradation of its complexity.

3. Definition and Examples of the Sequence

This section briefly reviews the structure of an NTU sequence and proposes a nonlinear filter with dynamic mapping.

3.1 Structure of an NTU Sequence

The concept of NTU sequence is primarily the same as the traditional NLFGs; however, it differs from them in that its linear generator is an m-sequence over $\mathbb{F}_p$, and its mapping function is defined with the Legendre symbol over $\mathbb{F}_p$, where p is an odd prime. More precisely, let $\eta_{\mathrm{NTU}}(x)$ be the mapping function that is defined as follows:

$$\eta_{\mathrm{NTU}}(x) = \begin{cases} 1 & \text{if } x \text{ is a QR element in } \mathbb{F}_p, \\ 0 & \text{otherwise,} \end{cases}$$

where $x \in \mathbb{F}_p$.

Let ω be a primitive element in an extension field of extension degree n over $\mathbb{F}_p$. An NTU sequence $S_{\mathrm{NTU}} = \{s_i\}$ is generated by

$$s_i = \eta_{\mathrm{NTU}}\left(\mathrm{Tr}_p^{p^n}\left(\omega^i\right)\right).$$

Since p is an odd prime, the output of the trace function is in the range $\{0, 1, \ldots, p-1\}$ and the mapping function η_{NTU} cannot classify those elements into 0 or 1 evenly. In addition, as the trace function provides each non-zero element p^{n-1} times and the 0's $\left(p^{n-1}-1\right)$ times, the output of η_{NTU} can be balanced if 0's are classified into two sets (0 or 1) uniformly and less intentionally.

3.2 Definition of the Filter and the Sequence

Let $\mathbb{F}_p$ and $\mathbb{F}_{p^n}$ be a finite field of characteristic p and the extension field of degree n over $\mathbb{F}_p$, respectively. Since the mapping function in the NTU sequence has an unbalanced property, the author proposes to introduce dynamic mapping with a lower computational cost. Let ω be a primitive element in $\mathbb{F}_{p^n}$ and η denotes a mapping function defined with an element $g \in \mathbb{F}_p$ obtained by Eq. (7) as follows:

$$\eta(x) = \begin{cases} 0 & \text{if } x = 0 \text{ and } g^{u+v} \text{ is QR over } \mathbb{F}_p, \\ 0 & \text{if } x \neq 0 \text{ and } x \text{ is QR over } \mathbb{F}_p, \\ 1 & \text{if } x = 0 \text{ and } g^{u+v} \text{ is QNR over } \mathbb{F}_p, \\ 1 & \text{if } x \neq 0 \text{ and } x \text{ is QNR over } \mathbb{F}_p, \end{cases} \tag{6}$$

$$g = \frac{\mathrm{Tr}_p^{p^n}\left(\omega^{\kappa+\lambda}\right)}{\mathrm{Tr}_p^{p^n}\left(\omega^{\kappa}\right)}, \tag{7}$$

where κ is a positive integer such that $\mathrm{Tr}_p^{p^n}(\omega^\kappa) \neq 0$ and $\lambda = \frac{p^n-1}{p-1}$. In addition, it is noted that $u = \lfloor i/\lambda \rfloor$ and $v = i \pmod{\lambda}$ for λ and $i = 0, 1, \ldots, 2\lambda - 1$. As the evaluation of g^{u+v} whether QR or QNR can be conducted by $u + v \pmod 2$, implementation cost would not be expensive.

For the mapping function η, a sequence $S = \{s_i\}$ is generated by

$$s_i = \eta\left(\mathrm{Tr}_p^{p^n}\left(\omega^i\right)\right).$$

As seen from the definition of the proposed generator, it can take over the implementation tactics of NLFGs such as a shift register and a lookup table.

4. Some Properties of the Sequence

In this section, the author shows some theoretic properties of the proposed sequence.

4.1 Period of the Sequence

The period of the proposed sequence is the same as that of the NTU sequence. Let $S = \{s_i\}$ be a proposed sequence for $i = 0, 1, 2, \ldots, 2\lambda - 1$ and let $\overline{s_i}$ denote the bit reverse of s_i. Since the sequence holds the symmetricity shown below, the period of the proposed sequence is given by 2λ.

Lemma 4.1. The proposed sequence satisfies $s_{i+\lambda} = \overline{s_i}$.

Proof. Let ω be a primitive element in $\mathbb{F}_{p^n}$ and let g be an $\mathbb{F}_p$-element endowed by Eq. (7). Since every nonzero element $\gamma \in \mathbb{F}_{p^n}$ satisfies Euler's totient theorem, we obtain $\gamma^{p^n-1} \equiv \left(\gamma^{\frac{p^n-1}{p-1}}\right)^{p-1} \equiv 1$ and can therefore induce that $\gamma^{\frac{p^n-1}{p-1}}$ is an $\mathbb{F}_p$-element. Here, let $\lambda = \frac{p^n-1}{p-1}$ and let us consider $\omega^{\frac{p^n-1}{p-1}} = \omega^\lambda \in \mathbb{F}_p$. Since $\mathrm{Tr}_p^{p^n}\left(\gamma^\lambda\right) = \gamma^\lambda$ according to Eq. (3) and g is given by Eq. (7), we obtain the equation as follows:

$$g = \frac{\omega^\lambda \mathrm{Tr}_p^{p^n}\left(\omega^\kappa\right)}{\mathrm{Tr}_p^{p^n}\left(\omega^\kappa\right)} = \omega^\lambda.$$

Therefore, $\mathrm{Tr}_p^{p^n}\left(\omega^{i+\lambda}\right) = g\mathrm{Tr}_p^{p^n}\left(\omega^i\right)$ is held for every i $(0 \leq i < \lambda)$.

Assume $\mathrm{Tr}_p^{p^n}\left(\omega^i\right) \neq 0$. Because the mapping function η involves Legendre symbol calculation in the process, the trace values of phase shifted elements ω^i and $\omega^{i+\lambda}$ satisfy

$$\left(\frac{\mathrm{Tr}_p^{p^n}\left(\omega^i\right)}{p}\right) = -1 \times \left(\frac{g\mathrm{Tr}_p^{p^n}\left(\omega^i\right)}{p}\right) (\because \text{Eq. (5)}).$$

Assume $\mathrm{Tr}_p^{p^n}\left(\omega^i\right) = 0$. Since η replaces the element by g^{u+v}, $\left(\frac{g^{u_1+v}}{p}\right) = -1 \times \left(\frac{g^{u_2+v}}{p}\right)$ holds, where $u_1 = \lfloor i/\lambda \rfloor$ and $u_2 = \lfloor (i+\lambda)/\lambda \rfloor = \lfloor i/\lambda \rfloor + 1$. Therefore, $s_{i+\lambda} = \overline{s_i}$. □

Theorem 4.2. The period of the proposed sequence is 2λ.

Proof. Assume that the period of the proposed sequence $S = \{s_i\}$ is κ, where $0 < \kappa \leq \lambda$, and it endows the relation $s_{i+\kappa} = s_i$. If $\kappa|\lambda$, then $s_i = s_{i+\lambda}$, and this contradicts Lem. 4.1. Therefore, κ is not a divisor of λ, and $s_{i+2\lambda} = s_i$ induces $\kappa|2\lambda$ according to Lem. 4.1. This indicates that the sequence S comprises one of the 2-bit patterns (00, 01, 10, or 11). However, considering the distribution property of an m-sequence over $\mathbb{F}_p$, S must include the other 2-bit patterns. Therefore, $\kappa|2$ contradicts this fact, and the period of S can be given by 2λ. □

4.2 Distribution Property

This section shows some distribution properties of the proposed sequence S. Let $b^{(l)}$ be an l-bit pattern in S and let $N\left(b^{(l)}\right)$ be a function which returns the number of $b^{(l)}$ in S, where $1 \leq l \leq n$.

Theorem 4.3. The proposed sequence holds the following distribution properties:

$$N\left(b^{(1)} = 0\right) = N\left(b^{(1)} = 1\right) = \lambda, \tag{8}$$

$$N\left(b^{(l)}\right) = N\left(\overline{b^{(l)}}\right). \tag{9}$$

Proof. According to Lem. 4.1 and Thm. 4.2, the properties Eq. (8) and Eq. (9) are endowed. More formally, let us discuss Eq. (8) first. Let $T = t_i$ be an auxiliary sequence concerning a primitive element ω which is derived as

$$t_i = \begin{cases} \mathrm{Tr}_p^{p^n}\left(\omega^i\right) & \text{if } \mathrm{Tr}_p^{p^n}\left(\omega^i\right) \neq 0, \\ g^{u+v} & \text{if } \mathrm{Tr}_p^{p^n}\left(\omega^i\right) = 0, \end{cases}$$

where $u = \lfloor i/\lambda \rfloor, v = \lfloor i/\lambda \rfloor + 1$ and $g = \omega^\lambda$ for $\lambda = (p^n - 1)/(p - 1)$.

Since the mapping function η classifies 0's into QR elements and QNR elements uniformly, the number of QR elements and QNR elements in T of length $p^n - 1$, denoted by N_{QR} and N_{QNR}, respectively, can be derived by

$$N_{\mathrm{QR}} = \frac{p^{n-1} - 1}{2} + \frac{p-1}{2} \times p^{n-1} = \frac{p^n - 1}{2},$$

$$N_{\mathrm{QNR}} = \frac{p^{n-1} - 1}{2} + \frac{p-1}{2} \times p^{n-1} = \frac{p^n - 1}{2}.$$

Because the proposed sequence S is obtained by applying Legendre symbol to T with mapping $1 \to 0$ and $-1 \to 1$, the number of QRs and QNRs in S is obtained as

$$N\left(b^{(1)} = 0\right) = \frac{2}{p-1} \times N_{\mathrm{QR}} = \frac{p^n - 1}{p-1},$$

$$N\left(b^{(1)} = 1\right) = \frac{2}{p-1} \times N_{\mathrm{QNR}} = \frac{p^n - 1}{p-1},$$

Therefore, Eq. (8) holds.

Next, let us focus on Eq. (9). Let ω be a primitive element that is used to generate the proposed sequence $S = \{s_i\}$. Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a basis of $\mathbb{F}_{p^n}$ and let $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ be a dual basis of $\mathcal{A}$, where $1 \leq l \leq n$ and $\alpha_j = \omega^j$ for $0 \leq j < l$.

Assume that $\omega^t (0 \leq t < l \leq n)$ and $\omega^i (0 \leq i < p^n - 1)$ are represented by the bases $\mathcal{A}$ and $\mathcal{B}$, respectively. It is noted that $\omega^t (0 \leq t < l \leq n)$ is defined according to the distribution property of an m-sequence, according to which can have a uniform distribution less than or equal to n. Since dual bases satisfy Eq. (4), Eq. (10) is obtained, and it tells us that trace values can be represented by the coefficients of ω^i, where $a_{i,j} \in \mathbb{F}_p$ denotes the j-th coefficient of ω^i.

$$\mathrm{Tr}_p^{p^n}\left(\omega^t \times \omega^i\right) = \mathrm{Tr}_p^{p^n}\left(\omega^t \sum_{j=0}^{n-1} a_{i,j}\alpha_j\right) = a_{i,t}. \tag{10}$$

Thus, continuous l-characters $\left(\mathrm{Tr}_p^{p^n}\left(\omega^i\right), \ldots, \mathrm{Tr}_p^{p^n}\left(\omega^{i+l-1}\right)\right)$ of an m-sequence are given by $\left(a_{i,0}, a_{i,1}, \ldots, a_{i,l-1}\right)$.

Since the auxiliary sequence T is obtained by replacing the zeros in an m-sequence by a power of g, a discussion whether $\mathrm{Tr}_p^{p^n}\left(\omega^{i+j}\right) = 0$, where $0 \leq j < l$, should be included in the tuple is required. First, assume that the tuple is composed of non-zero elements. Since ω and g hold the relation $\omega^\lambda \times \omega^i = g\omega^i$ for $0 \leq i < p^n - 1$, every element in the tuple always satisfies $g \times a_{i,j} \neq 0$ and $a_{i,j} = a_{i+\lambda,j}$ for $0 \leq j < l$, where $a_{i+\lambda,j}$ is the corresponding coefficient of $g\omega^i$.

Next, assume that some of elements in the tuple are 0 and replaced by $g^{u_j+v_j}$ with $u_j = \lfloor (i+j)/\lambda \rfloor$ and $v_j = i + j \pmod{\lambda}$. Considering the definition of v_j, $a_{(i+\lambda)+j} = 0$ is replaced by $g^{u_j+v_j+1}$. Therefore, every entries in the tuple satisfies $g \times a_{i,j} \neq 0$ and $a_{i,j} = a_{i+\lambda,j}$ for $0 \leq j < l$.

Since Legendre symbol holds Eq. (5), it can be observed that Eq. (9) holds for the sequence S. □

5. Conclusion

In this paper, the author focused on the mapping function of the NTU sequence and proposed a dynamic mapping function to improve the distribution property. The mapping function was defined with a dynamic substitution and Legendre symbol. The period and some distribution properties of the proposed sequence are discussed theoretically throughout the paper. As a result, it can be observed that the period using the proposed method is the same as the original NTU sequence, and the proposed sequence has symmetricity, which influences the distribution property. Though the goal was successfully achieved by introducing dynamic mapping, it induced a different characteristic, that is, symmetricity, which is helpful in revealing the properties of the sequence; however, this feature may lead to vulnerability as a cryptographic PRNG. Considering this, the author plans to modify the sequence furthermore by introducing an additive operation based on the structure analysis and evaluating the sequence in future works.

Acknowledgments

The author would like to thank Editage (www.editage.com) for English language editing.

References

[1] J. Hoffstein, J. Pipher, and J.H. Silverman, An Introduction to Mathematical Cryptograph, 2nd ed., Springer Publishing Company, Incorporated, 2014.
[2] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, Heidelberg, 1986.
[3] T.W. Cusick, C. Ding, and A. Renvall, Stream Cihpers and Number Theory Revised Edition, Elsevier Science, 2004.
[4] S.W. Golomb, Shift Register Sequences, Aegean Park Press, Laguna Hills, CA, USA, 1981.
[5] Y. Nogami, K. Tada, and S. Uehara, "A geometric sequence binarized with legendre symbol over odd characteristic field and its properties," IEICE Trans. Fundamentals, vol.E97-A, no.1, pp.2336–2342, Dec. 2014.
[6] 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. Fundamentals, vol.E99-A, no.12, pp.2226–2237, Dec. 2016.
[7] K. Tsuchiya, C. Ogawa, Y. Nogami, and S. Uehara, "Linear complexity of generalized NTU sequences," IWSDA'17, pp.74–78, IEEE, 2017.
[8] Y. Kodera, T. Miyazaki, M.A. Khandaker, M.A. Ali, T. Kusaka, Y. Nogami, and S. Uehara, "Distribution of digit patterns in multi-value sequence over odd characteristic field," IEICE Trans. Fundamentals, vol.E101-A, no.9, pp.1525–1536, Sept. 2018.
[9] Y. Kodera, M.A. Ali, T. Miyazaki, T. Kusaka, Y. Nogami, S. Uehara, and R.H. Morelos-Zaragoza, "Algebraic group structure of the random number generator: Theoretical analysis of NTU sequence(s)," IEICE Trans. Fundamentals, vol.E102-A, no.12, pp.1659–1667, Dec. 2019.
[10] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, New York, NY, 1986.
[11] A. Canteaut, "Berlekamp-massey algorithm," Encyclopedia of Cryptography and Security, pp.29–30, Springer, Boston, MA, 2005.
[12] V.M. Sidelnikov, "Some k-value pseudo-random sequences and nearly equidistant codes," Problems of Information Transmission, vol.5, no.1, pp.12–16, 1969.
[13] A. Lempel, M. Cohn, and W.L. Eastman, "A class of binary sequences with optimal autocorrelation properties," IEEE Trans. Inf. Theory, vol.23, no.1, pp.38–42, 1977.
[14] R. Scholtz and L. Welch, "GMW sequences (corresp.)," IEEE Trans. Inf. Theory, vol.30, no.3, pp.548–553, 1984.
[15] A. Klapper, A.H. Chan, and M. Goresky, "Cascaded GMW sequences," IEEE Trans. Inf. Theory, vol.39, no.1, pp.177–183, 1993.