奇標数体上で生成される幾何系列の自己相関

小寺　雄太[1]　日下　卓也[1]　野上　保之[1]

概要：暗号理論的擬似乱数 (CSPRNG: Cryptographically Secure Pseudorandom Number Generator) は暗号プリミティブとして現代の情報セキュリティ技術へ不可欠な役割を担っている．NTU 系列と呼ばれる擬似乱数生成器は，その乱数的な特性が理論的な側面から幅広く評価されるとともに証明が与えられている CSPRNG の 1 つである．しかしながら，NTU 系列におけるビット分布はマッピング関数の定義により偏りが生じており，一様化手法が必要となる．本稿では NTU 系列に対して一様化手法を適用するとともに，一様化した NTU 系列の自己相関を観測することでその手法が従来の NTU 系列の乱数特性に与える影響を調べる．その結果，本稿で用いた一様化手法は従来 NTU 系列において高い値を示していたピーク値を抑制することにも寄与することが判明した．

キーワード：暗号理論的擬似乱数生成器，一様な分布特性をもつ NTU 系列，自己相関

Autocorrelation of a Geometric Sequence Binarized over Odd Characteristic Field

Yuta Kodera[1]　Takuya Kusaka[1]　Yasuyuki Nogami[1]

Abstract: Cryptographically secure pseudorandom number generators (CSPRNGs) are an inseparable part of security applications as a cryptographic primitive. The NTU sequence is one of such CSPRNGs whose randomness properties have been evaluated from mathematical aspects with theoretic proofs. However, since the distribution of bits is not originally uniform due to the mapping function, it requires a uniformization technique to obtain a balanced sequence. Then, this paper observes the autocorrelation of the NTU sequence to know the properties of the sequence such as the period and the similarity. As the result, we find that the uniformization technique contributes to suppressing peak which shows a high level in the autocorrelation of the original NTU sequence.

Keywords: cryptographically secure pseudorandom number generator, uniformly distributed NTU sequence, autocorrelation

1. Introduction

Randomness is an inseparable part of communication technologies such as spread spectrum communications [1] and security applicatio [2], [3]. A pseudorandom number generator (PRNG) is a solution for recreating the randomness with computer technology and many types of generators have been investigated. However, not every RPNG is suitable for the security applications due to the shortage of the difficulty of predicting the next bit.

The cryptographically secure pseudorandom number generator (CSPRNG) is the generators, which is sufficiently evaluated the randomness of a sequence, for using security applications. For example, Blum-Blum-Shub (B. B. S.) [4], [5] was proposed as a CSPRNG. The generation procedure is quite simple and efficient described as follows. For a modular integer $M = pq$ and $1 \leq i$, an i-th coefficient s_i of B is yielded by $s_i = s_{i-1}^2 \pmod{M}$, where p and q are large primes, respectively. Since B. B.

[1] 岡山大学自然科学研究科
Graduate School of Natural Science and Technology, Okayama University

S. uses the circulation property of a prime field, the period depends on the order of a seed value. Therefore, it is noted that the calculation is efficiently carried out over a prime field, however, users carefully need to choose a seed value from $\mathbb{F}_M$ so that the random numbers do not circulate during a short span.

To know the characteristic of a sequence such as period and similarity, the autocorrelation is used. In this paper, we especially observe the autocorrelation of a geometric sequence generated by the trace function and the Legendre Symbol over an odd characteristic field. The sequence, which is called NTU sequence hereafter, has been proposed by Nogami, Tada, Uehara [6], and various type of properties such as the period, the autocorrelation, the cross-correlation, the linear complexity, and the distribution of bits have been theoretically shown [7], [8].

The NTU sequence is defined by combining the M-sequence [9] and the Legendre sequence [10], [11]. By taking full advantages of these sequences, NTU is enabled to generate a long periodic sequence with possessing the maximum linear complexity. On the other hand, the distribution of bits is not uniform due to the mapping function.

Therefore, we introduce a technique to overcome the drawback [12] without any additional calculation costs. Then, this paper purposes to evaluate the effect of the uniformization technique on the properties described above. Especially, we focus on the difference of the period and the similarity between the original NTU sequence and the uniformized NTU sequence. Thus, we observe the autocorrelation with small parameter sets to clarify the characteristics of a uniformized NTU sequence. It is noted that the behavior of the autocorrelation of an NTU sequence for another parameter sets are experimentally the same.

According to the experimental results, it is found that the period of the uniformized NTU sequence is same as the original NTU sequence. We find that peak values of autocorrelation distributes symmetrically. In addition, the technique contributes to suppressing the peak values appeared in the autocorrelation of the original NTU sequence without any additional calculation costs.

2. Preliminaries

This section briefly reviews the definition of NTU sequence and a uniformization technique for the NTU sequence.

2.1 Mathematical fundamentals

Mathematical fundamentals of NTU sequence are introduced.

2.1.1 Primitive polynomial and its zero

Let $f(x)$ be a polynomial of degree m over prime field $\mathbb{F}_p$, where p and m are an odd prime number and a positive integer, respectively. If $f(x)$ is not factorized by any smaller degree polynomial, then it is called irreducible polynomial. Let $f(x)$ be an irreducible polynomial of degree m over $\mathbb{F}_p$. For the smallest positive integer $t \in \mathbb{Z}$ such that $f(x)|x^t-1$, if $t = p^m-1$, then $f(x)$ is especially called a primitive polynomial. In what follows, let $f(x)$ be a primitive polynomial of degree m.

Let ω denote a zero of $f(x)$, where ω is an element in $\mathbb{F}_{p^m}$. Then, this ω works as a generator of $\mathbb{F}_{p^m}$ and every extension field element is represented by a power of ω.

2.1.2 Trace function

Let ω be a zero of $f(x)$. Trace function denoted by $\mathrm{Tr}(\cdot)$ is defined as the sum of conjugates[*1] of $\omega^i, 0 \le i \le p^m-2$ as follows:

$$\mathrm{Tr}\left(\omega^i\right) = \sum_{j=0}^{m-1} \left(\omega^i\right)^{p^j}. \tag{1}$$

For example, let us consider the trace value of $2+\beta \in \mathbb{F}_{p^m}$, where β is a zero of an irreducible polynomial $g(x) = x^2+4$. The trace calculation for $2+\beta$ is carried out as follows:

$$\begin{aligned}\mathrm{Tr}(2+\beta) &= 2+\beta+(2+\beta)^7 = 2+\beta+(2+\beta^7)\\ &= 4+\beta+3^3\beta = 4.\end{aligned}$$

Readers need to be conscious that a trace function has linear property below.

$$\mathrm{Tr}(aX+bY) = a\mathrm{Tr}(X) + b\mathrm{Tr}(Y), \tag{2}$$

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

2.1.3 Legendre symbol

Let a be an element in $\mathbb{F}_p$. The Legendre symbol defined blow checks whether a has a square root or not in $\mathbb{F}_p$. If a has a square root, then it is said that a is a Quadratic Residue (QR) element. Otherwise, it is called Quadratic-Non Residue (QNR) element.

$$\begin{aligned}\left(\tfrac{a}{p}\right) &= a^{\frac{p-1}{2}} \pmod p\\ &= \begin{cases} 0 & \text{if } a = 0,\\ 1 & \text{else if } a \text{ is QR element,}\\ -1 & \text{otherwise if } a \text{ is QNR element.}\end{cases}\end{aligned} \tag{3}$$

[*1] A conjugate is derived from the p-th power of an $\mathbb{F}_{p^m}$-element. This mapping is especially called Frobenius mapping.

2.1.4 Mapping function

Let $l \in -1, 0, 1$ be an output of the Legendre symbol calculation. The mapping function used in this paper is defined below.

$$M_2(l) = \begin{cases} 0 & \text{if } l = 0 \text{ or } l = 1, \\ 1 & \text{otherwise if } l = -1. \end{cases} \tag{4}$$

2.2 NTU sequence

This section shortly reviews the definition of the NTU sequence introduced by Nogami, Tada, Uehara in [6]. The NTU sequence requires two parameters p and m which determines the period of the sequence and the parameter selection affects on the efficiency of the generationThe NTU sequence requires an odd prime P and an extension degree M. They determine the period of the sequence, and the parameter selection affects on the efficiency of the generation. Especially, to make the implementation efficient, small prime such as $p = 11, 13, 17$ is used. Therefore, we consider NTU sequence with such small prime hereafter.

2.2.1 Generating procedure of NTU sequence

Let ω be a zero of $f(x)$ and let us represent an $\mathbb{F}_{p^m}$ element by ω^i. Then i-th coefficient of an NTU sequence denoted by s_i is derived by the following calculation.

$$s_i = M_2\left(\left(\mathrm{Tr}\left(\omega^i\right)\!\Big/_{p}\right)\right), i = 0, 1, 2, \ldots. \tag{5}$$

For the efficiency, we recommend using a small odd prime number such as $p = 11, 13, 17$. This is because it enables to carry out a Legendre symbol calculation by a LUT.

2.2.2 Properties of NTU sequence

In general, various properties for a pseudorandom sequence such as the period, the autocorrelation, the cross-correlation, the linear complexity, and the distribution of bits have been focused on as an evaluation measure. Especially, every property described above for NTU sequence has been theoretically proven [7], [8].

For example, the period λ and the autocorrelation of NTU sequence $R_S(x)$ have been theoretically given by (6) and (7), respectively.

$$\lambda = \frac{2(p^m - 1)}{p - 1}. \tag{6}$$

$$\begin{aligned} R(x) &= \sum_{i=0}^{\lambda-1} (-1)^{s_{i+x} - s_i} \\ &= \begin{cases} \frac{2(p^m-1)}{p-1} & \text{if } x = 0, \\ -2p^{m-1} + \frac{2(p^{m-1}-1)}{p-1} & \text{else if } x = \frac{n}{2}, \\ \frac{2(p^{m-2}-1)}{p-1} & \text{otherwise.} \end{cases} \end{aligned} \tag{7}$$

表 1 The number of appearances of 0's, ORs, and QNRs in one period of NTU sequence generation.

Type of an output from Tr $(\cdot)$	The number of appearances
0's	$p^{m-1} - 1$
QRs	$\frac{p-1}{2} \cdot p^{m-1}$
QNRs	$\frac{p-1}{2} \cdot p^{m-1}$

In addition, it has been revealed that the distribution of bits in NTU sequence is not balanced and the distribution depends on the number of zeros contained in the bits. Thus, we additionally explain a uniformzation technique for NTU sequence in the next section.

2.3 Uniformization technique for NTU sequence

A CSPRNG should be unpredictable but NTU sequence may involve a vulnerability because of the distribution of bits. In short, by focusing on the appearance probabilities of each bit pattern, the next bit can be predictable. In order to overcome the drawback, this section introduces a technique to NTU sequence which realizes a balanced distribution.

The distribution of bits in one period of NTU sequence is not uniform because of its mapping function. In fact, the number of 0's in one period is larger than that of 1's. This is because NTU sequence uses the trace function (1) which yields the certain number of 0's, QR and QNR elements during the length $p^m - 1$ as shown in **Table** 1 but the mapping maps 0's and QRs into 0's and QNRs into 1's.

In addition, it was found that the number of appearances of each bit pattern is determined by the number of zeros contained in the pattern [8]. Thus, we focused on the output of a trace value, especially for the case that the output is 0, and have been proposed a technique [12]. The detail is as follows.

Let t_i be an output of Tr $\left(\omega^i\right)$, where ω^i denotes an element in $\mathbb{F}_{p^m}$ and $0 \le i \le p^m - 2$. According to the original definition (5), $s_i = 0$ when $t_i = 0$ or t_i is a QR element. On the other hand, $s_i = 1$ when t_i is a QNR element. Considering the number of appearances of each element as shown in **Table** 1, it is found that if the trace zero is replaced by a non-zero value obtained from $\mathbb{F}_p$ uniformly, then the number of 0's and 1's in one period becomes the same.

To realize the above requirements based on the theoretical background, a coefficient of $omega^i$ is focused on.

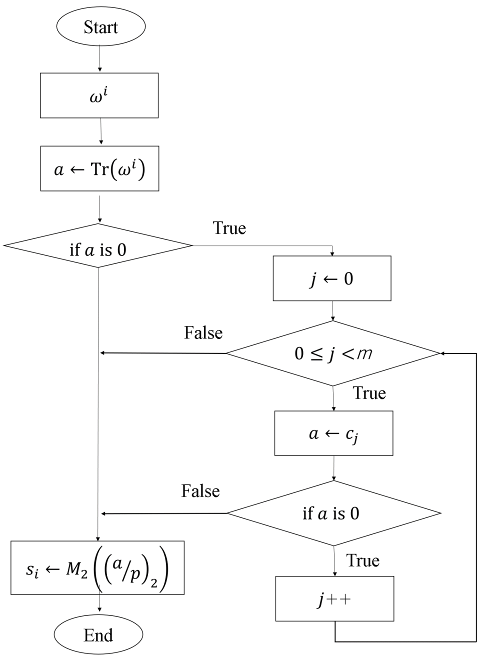

図 1　The generating procedure of the proposed NTU sequence

In short, the uniformization technique is simply replacing trace zeros by a coefficient of ω^i as shown in **Figure** 1. Therefore, this uniformization technique does not require any additional calculations, moreover, it greatly contributes to improving unbalanced distribution.

The purpose of this work is to observe the effects of this uniformization technique for the autocorrelation property. We guess that this technique suppresses the level of each peak values without losing the high non-linear feature. In fact, it is found that the MOC, which is used for evaluating the non-linearity of a sequence [13], of the uniformized NTU sequence is almost the same as the original one [14].

3. Autocorrelation of NTU sequence with uniformization technique

In this section, we observe the autocorrelation of the uniformized NTU sequence. Let us recall that the definition of autocorrelation for a sequence S of length n. It is given as follows:

$$R_S(x) = \sum_{i=0}^{n-1} (-1)^{s_{i+x}-s_i}. \tag{8}$$

3.1 Example of the autocorrelation of a uniformized NTU sequence

Here, we shortly show some observations for the autocorrelation of a uniformized NTU sequence with several parameter sets. However, the features to be seen from the figures have also confirmed for another parameter sets.

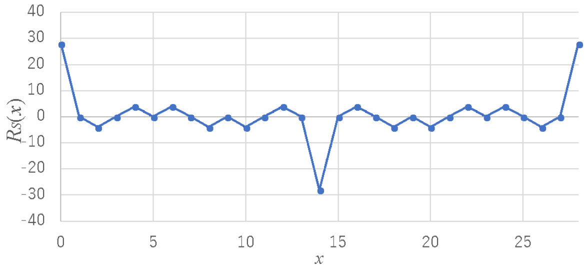

図 2　The autocorrelation of an NTU sequence when $p = 13$ and $m = 2$.

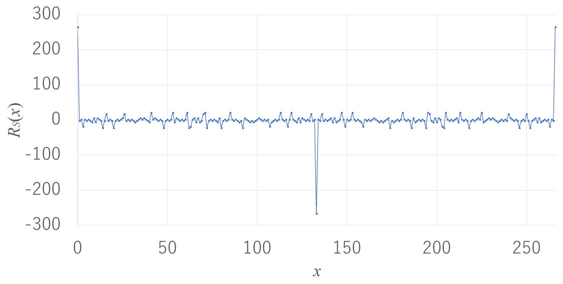

図 3　The autocorrelation of an NTU sequence when $p = 11$ and $m = 3$.

3.1.1 $p = 13$ and $m = 2$

A uniformized NTU sequence of length 28 with $f(x) = x^2 + 7x + 2$ is as follows:

$$S = \{1111100110010100000110011010\}.$$

The autocorrelation of this sequence is shown in **Figure** 2.

3.1.2 $p = 11$ and $m = 3$

A uniformized NTU sequence of length 266 with $f(x) = x^3 + 6x^2 + 7x + 4$ is as follows:

$$\begin{aligned} S = \{&0001000111101011011110010110111001101000011\\ &1000101010101100111001000101111000111101011\\ &0011001010111111100100110111111001000011110101\\ &1111111011100001010010000110100100011001011\\ &1100011101010101001100011011101000011100001\\ &0100110011010100000011011001000001101111000\\ &10100000\}.\end{aligned}$$

The autocorrelation of this sequence is shown in **Figure** 3.

3.2 Consideration

It is found that the period of the uniformized NTU sequence corresponds to the original NTU sequence. That is $\lambda = \frac{2(p^m-1)}{p-1}$. As we expected peak values observed in the original NTU sequence have been suppressed. Every peak values appeared in the autocorrelation of the original NTU sequence is higher than the square root of the maximum peak value. However, the most of peak values become less than the square root of the maximum. We think that the above aspect is one of the positive improvements that the technique brigs to NTU sequence.

In addition, NTU sequence using the uniformization technique seems to hold the relationship $s_i = \overline{s_{i+\frac{\lambda}{2}}}$, where $\overline{s_i}$ denotes the bit invert of s_i. We guess that the relationship is caused by the cyclic property of a primitive element utilized for the uniformization.

4. Conclusion

We observed the autocorrelation for a geometric pseudorandom sequence called NTU sequence with a uniformization technique. It was found that the period of the uniformized NTU sequence corresponds to the original NTU sequence. In addition, a sequence coefficient seems to invert after the half period.

Originally, the autocorrelation of NTU sequence has $p-1$ peak values and each value is not acceptably low level. However, the technique introduced in this paper enables to suppress peak values appeared in the autocorrelation of the original NTU sequence.

Considering the almost less effect on the non-linearity feature on the sequence, we conclude that the technique using in this paper is useful in order to enhance not only the security aspects but the autocorrelation feature. We will formulate the autocorrelation of the uniformized NTU sequence with theoretic proof as a future work.

Acknowledgment

This work was partly supported by a JSPS KAKENHI Grant-in-Aid for Scientific Research (A) 16H01723.

参考文献

[1] M. K. Simon, J. K. Omura, R. A. Scholtz and B. K. Levitt, “Spread Spectrum Communications Handbook,” McGraw-Hill, 1994, Revised.

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

[3] A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, “Handbook of Applied Cryptography,” CRC Press, 1996.

[4] L. Blum, M. Blum and M. Shub, ”A simple unpredictable pseudorandom number generator,” SIAM J. Comput. vol. 15, 1986.

[5] A. Sidorenko and B. Schoenmakers, “Concrete Security of the Blum-Blum-Shub Pseudorandom Generator,” Cryptography and Coding, pp. 355–375, Springer Berlin Heidelberg, 2015.

[6] Y. Nogami, K. Tada and S. Uehara, “A Geometric Sequence Binarized with Legendre Symbol over Odd Characteristic Field and Its Properties,” IEICE Trans., vol. E97-A, no. 1, pp. 2336-2342, 2014.

[7] 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., vol. E99-A, no. 12, pp. 2226-2237, 2016.

[8] Y. Kodera, T. Miyazaki, Md. A. Khandaker, Md. A. Ali, T. Kusaka, Y. Nogami and S. Uehara, “Distribution of Digit Patterns in Multi-value Sequence over the Odd Characteristic Field,” IEICE Trans. Special Section on Discrete Mathematics and Its Applications, vol.E101-A, No.9, 2018 (in press).

[9] S. W. Golomb, “Shift Register Sequences,” Holden-Day, San Francisco, 1967.

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

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

[12] Y. Kodera, T. Miyazaki, T. Kusaka, Md. A. Ali, Y. Nogami and S. Uehara, “Uniform Binary Sequence Generated over Odd Characteristic Field,” IJIEE, pp. 5-9, 2018, also accepted by 2017 ICIT, Singapore, 2017.

[13] C. J. A. Jansen, “The Maximum Order Complexity of Sequence Ensembles,” Davies D.W. (eds) Advances in Cryptology — EUROCRYPT ’ 91. EUROCRYPT 1991. *LNCS*, vol 547. Springer, Berlin, Heidelberg, 1991.

[14] Y. Kodera, T. Kusaka, T. Miyazaki, Y. Nogami, S. Uehara and R. H. Morelos-Zaragoza,“Evaluating the Maximum Order Complexity of a Uniformly distributed Sequence over Odd Characteristic,” 2018 ICCE-TW, Taiwan, 2018.