Evaluating the Maximum Order Complexity of a Uniformly distributed Sequence over Odd Characteristic

Yuta KODERA†, Takuya KUSAKA†, Takeru MIYAZAKI††, Yasuyuki NOGAMI†,
Satoshi UEHARA†† and Robert H. MORELOS-ZARAGOZA‡‡
†Graduate School of Natural Science and Technology Okayama University, Japan
†† The University of Kitakyushu, Japan
‡‡ San Jose State University, U.S.A
†Email: yuta.kodera@s.okayama-u.ac.jp

***Abstract*—This paper focuses on the Maximum Order Complexity of a pseudorandom sequence for security applications called NTU sequence. It shows the maximum feature on the non-linear property and several properties have been theoretically proven. However, the NTU sequence requires a uniformization technique to overcome the drawback on its bits distribution. The technique has already proposed but the non-liear feature still has not investigated. Therefore, this paper evaluates the affects on the non-linear feature of the original NTU sequence by using Maximum Order Complexity.**

I. Introduction

The randomness property is widely used for realizing the real communication systems. Especially for the security applications such as cryptosystems and authentication systems, it is an inseparable part of the security. A pseudorandom sequence is one of the techniques to realize the behavior of the random numbers, however, not every sequence is suitable for the security use. A random sequence needs to be evaluated from some specific properties such as the period, the bits distribution and the non-linear features.

The authors target a pseudorandom sequence for security applications called NTU sequence with a uniformization technique. The several properties of the original NTU sequence have been evaluated and been theoretically proven. On the other hand, the non-linear features of the uniformized NTU sequence still have not investigated. Therefore, to know the affects of the uniformization for the non-linearity of the original NTU sequence, this paper compares the Maximum Order Complexity (MOC) of the uniformized NTU sequence and the original one.

The experimental result claims that the MOC of the uniformized NTU sequence is almost equivalent to the original one. However, it is experimentally found that if an odd prime p is quite small, then the difference of the MOC of two NTU sequences become large in proportion to the size of an extension degree m. Thus, a suitable parameter selection will be requited and theoretic proofs will be considered in future works.

II. Preliminaries

This section briefly introduces a pseudorandom sequence which is expected to use for security applications such as initialization vector, stream cipher, key generation, and so on. In what follows a prime field and its extension field are denoted by $\mathbb{F}_p$ and $\mathbb{F}_{p^m}$, respectively, where p is an odd prime and m is a positive integer.

A. Mathematical fundamentals

1) Primitive elemenet and trace function: Every finite field has a primitive element which can represent every non-zero finite field element as its powers. Let ω be a primitive element in $\mathbb{F}_{p^m}$, then $\omega^i (i = 0, 1, 2, \ldots, p^m - 2)$ yields a distinct non-zero element in $\mathbb{F}_{p^m}$. For an $\mathbb{F}_{p^m}$-element, trace function is used to map it into $\mathbb{F}_p$ and is defined as $\mathrm{Tr}\left(\omega^i\right) = \sum_{j=0}^{m-1} (\omega^i)^{p^j}$.

B. Legendre symbol and mapping function

The Legendre symbol is used to check whether an $\mathbb{F}_p$-element has a square root in $\mathbb{F}_p$ or not. It is derived by calculating $\left(a/p\right) = a^{\frac{p-1}{2}} \pmod p$, where $a \in \mathbb{F}_p$. The output always corresponds to $0, 1$ or -1 and the mapping function denoted by $M_2(\cdot)$ maps 0 and 1 into 0 and -1 into 1.

C. NTU sequence and its theoretic properties

Nogami, Tada, Uehara have proposed NTU sequence in their work [1]. It is defined over an odd characteristic field with trace function and Legendre symbol denoted by $\mathrm{Tr}\left(\omega^i\right)$ and $\left(a/p\right)$, respectively, where ω denotes a primitive element in $\mathbb{F}_{p^m}$ and $a \in \mathbb{F}_p$. The i-th coefficient of an NTU sequence is generated as follows:

$$s_i = M_2\left(\left(\mathrm{Tr}\left(\omega^i\right) \Big/ p\right)\right), \tag{1}$$

where $i = 0, 1, 2, \ldots$.

Several properties of this NTU sequence such as period, autocorrelation, cross-correlation, linear complexity, and bits distribution have already clarified. In addition, every property except for the bits distribution has theoretically proven and the

linear complexity becomes maximum. For example, the period of the NTU sequence is given by

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

However, it has been found that the bits distribution of an NTU sequence is leaning due to the mapping function. To overcome the drawback of the bits distribution, a uniformization technique has developed [2].

D. Uniformization technique for NTU sequence

The authors have proposed a uniformization technique [2]. That is quite simple but it improves the bits distribution without additional computation to the generating procedure. It is realized by swapping trace-zeros with a non-zero coefficient of ω^i. The flowchart of the generating procedure with this technique is shown in Figure 1.

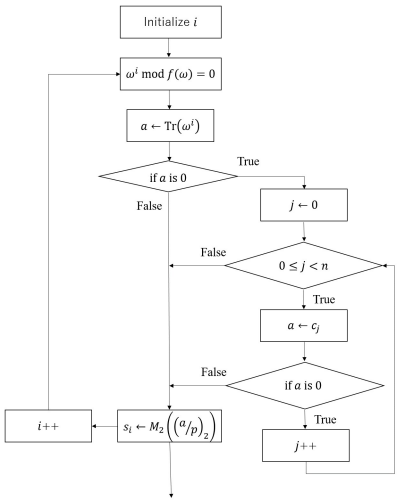

Fig. 1. The generating procedure of uniformized NTU sequence

It was experimentally found that the period of this uniformized NTU sequence corresponds to that of original NTU sequence. However, the difficulty of prediction still has not evaluated based on the non-linear propery. Therefore, this paper evaluates the affects of this uniformization technique by focusing on the Maximum Order Complexity of the uniformized NTU sequence and the original NTU sequence.

III. Evaluating the affects of the uniformization technique with Maximum Order Complexity

This section evaluates the uniformized NTU sequence by using Maximum Order Complexity (MOC) [3]. The MOC of a sequence is a natural generalization of the well-known linear complexity (LC) by allowing non-linear feedback functions for the feedback shift register (FSR) which generates a given sequence. Therefore, the MOC of a periodic sequence S_λ, denoted as MOC(S_λ), where λ be the period of S, is the length of the shortest FSR allowing nonlinear feedback functions which generate S_λ. For example, it is known that the MOC of an M-sequence corresponds to the Linear Complexity (LC), therefore, the MOC is given by m.

The MOC of the uniformized NTU sequence and the original NTU sequence are shown in **Table** I.

TABLE I
The MOC of the uniformized NTU and the original NTU

p	m	Uniformized NTU	Original NTU
5	2	4	4
	3	9	10
	4	10	11
	5	14	18
7	2	5	4
	3	8	10
	4	13	13
	5	16	18
11	3	5	5
	4	14	15
13	2	6	6
	3	11	11
	4	16	17
17	2	6	6
	3	12	12

A. Consideration

Experimentally, it was found that the Maximum Order Complexity of the uniformized NTU sequence and that of the original NTU sequence seems to be depending on the size of p. It is considered that the uniformization technique sometimes causes a small leaning on the distribution when p is small. The authors guess that the leaning is due to the fewer variations of coefficients of ω^i when p is quite small and as a result, the run length of 0's and 1's becomes longer . According to the experimental result, p is better not to be quite small, however, to generate long periodic sequence efficiently, a small prime is better to use.

IV. Conclusion and future work

This paper observed the MOC of the uniformized NTU sequence and comparing it with the MOC of the original one. As the experimental results show that the MOC of the uniformized NTU sequence seems to be depending on the size of p and m. Therefore, a suitable parameter selection will be required and be investigated in a future work. In conclusion, the uniformization technique for NTU sequence does not have critical effect on the MOC of the original NTU sequence but an odd prime p should be chosen suitably to stabilize the bits distribution and the MOC. Experimentally, it was found that the properties of the uniformized NTU sequence seem to be suitable for the security applications. Therefore, theoretic proofs for the properties will be considered in a future work.

Acknowledgement

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

References

[1] Y. Nogami, K. Tada, andS. 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.

[2] Y. Kodera, T. Miyazaki, T. Kusaka, Md. A. Ali, Y. Nogami, and S. Uehara, "Uniform Binary Sequence Generated over Odd Characteristic Field," 2017 ICIT, Singapore, 2017.

[3] 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.