Distribution of Bit Patterns on Multi-value Sequence over Odd Characteristics Field

Yuta KODERA†, Takeru MIYAZAKI††, Md. Al-Amin Khandaker†, Ali Md. ARSHAD†,
Yasuyuki NOGAMI† and Satoshi UEHARA††
†Graduate School of Natural Science and Technology Okayama University, Japan
†† The University of Kitakyushu, Japan
†Email: yuta.kodera@s.okayama-u.ac.jp

***Abstract*—The Internet of Things (IoT) provides much convenient life for us, at the same time it has brought threats for our privacy. In this context, secure and efficient cryptosystem is required to which pseudorandom sequence plays an important role. Especially, the distribution of bit patterns in the pseudorandom sequence is one of important security aspects. This paper especially focuses on the bit patterns and the distribution in an NTU sequence. As a result of a lot of observation, an important assumption about the distribution of bit patterns in an NTU sequence is introduced. It will help to obtain the balanced NTU sequence in order to enhance the security of cryptosystem on IoT communications.**

I. Introduction

The Internet of Things (IoT) is encroaching on every aspects of our lives, at the same time, it has brought threats for our privacy. The information security of IoT devices for secure and efficient cryptosystem has become an inseparable part of our daily life. In this context, various types of pseudorandom sequences are used for almost all cryptosystem and it plays important roles such as key generation and one-time pad. For such security purposes, an evaluation for the randomness of a pseudorandom sequence is required and it is evaluated by the distribution and the linear complexity[1]. They are closely related to the difficulty of calculating or predicting the next bit. Especially, this paper focuses on the bit patterns in an NTU sequence[2], [3] which linear complexity of length λ theoretically becomes λ[3]. As a result of a lot of observation, an important assumption about the distribution of bit patterns in an NTU sequence is introduced.

II. Preliminaries

This section introduces NTU sequence, and primitive polynomial, trace function, power residue, mapping function and period.

A. Primitive polynomial

Let $f(x)$ be an irreducible polynomial of degree m over prime field $\mathbb{F}_p$. Let $t \in \mathbb{Z}$ be the smallest positive integer, such that $f(x) \mid (x^t - 1)$. If $t = p^m - 1$, then $f(x)$ is called a primitive polynomial over $\mathbb{F}_p$. In what follows, $f(x)$ indicates a primitive polynomial of degree m over $\mathbb{F}_p$. Let ω be a root of $f(x)$ and $\omega \in \mathbb{F}_{p^m}$, where $\mathbb{F}_{p^m}$ is the extension field of degree m. Every non-zero element in $\mathbb{F}_{p^m}$ is represented as $\omega^i, i = 0, 1, 2, \cdots, p^m - 2$.

B. Trace function

The trace function $\mathrm{Tr}(\cdot)$ is defined as the sum of conjugates as follows:

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

For example, let us consider $\mathbb{F}_{7^2}$ with a modular polynomial $f(x) = x^2 + 1$. Let ω be a zero of $f(x)$ and $\{1, \omega\}$ forms a basis in $\mathbb{F}_{7^2}$. An arbitrary vector in $\mathbb{F}_{7^2}$ is represented with the basis such as $\mathbf{v} = 5 + 3\omega = (5, 3)$ and the p-th power of $\mathbf{v}$ is obtained as follows:

$$\begin{aligned}(5+3\omega)^p &= (5+3\omega)^7 = 5 + 3\omega^7 = 5 + 3(-1)^3\omega \\ &= 5 + 4\omega.\end{aligned}$$

Then, the trace of $\mathbf{v}$ is given as:

$$\mathrm{Tr}(5 + 3\omega) = (5 + 3\omega) + (5 + 4\omega) = 3.$$

As an important fact that the trace value always becomes element in $\mathbb{F}_p$ and the trace function is linear over $\mathbb{F}_p$.

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

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

C. Power residue and power non residue

For an arbitrary element $a \in \mathbb{F}_p$ and a positive integer $k > 1$ such that $k \mid (p-1)$, if a has k-th root in $\mathbb{F}_p$, then a is called k-th power residue (k-th PR). Otherwise, a is called k-th power non residue (k-th PNR). Through this paper, k-th PR and k-th PNR are represented as a symbol $\left(a/p\right)_k$ and it is calculated as follows:

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

where ϵ_k denotes a non-zero primitive k-th root of unity. Since $k \mid (p-1)$, ϵ_k belongs to $\mathbb{F}_p$.

978-1-5090-4017-9/17/$31.00 ©2017 IEEE

D. Mapping function

The power residue check by Eq.(3) outputs a certain power of ϵ_k or 0. In order to map the result into some value from 0 to $k-1$, this paper uses the following mapping function.

$$M_k(x) = \begin{cases} 0 & \text{if } x = 0, \\ l & \text{otherwise } x = \epsilon_k^l \neq 0. \end{cases} \quad (4)$$

III. NTU SEQUENCE

This paper introduces the NTU sequence that generates k-value pseudorandom sequence.

A. Generation Procedure

Let ω be a zero of $f(x)$ and s_i $(0 \leq s_i \leq k-1)$ denotes i-th coefficient in an NTU sequence. Then an NTU sequence is generated by the following calculation:

$$S = \{s_i\}, s_i = M_k\left(\left(\mathrm{Tr}\left(\omega^i\right)\Big/_p\right)_k\right), i = 0, 1, 2, \cdots. \quad (5)$$

B. Period

The period λ in an NTU sequence theoretically becomes[3]

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

Let us consider the case that $p = 7, m = 2$ and $k = 3$, the period becomes 24 and an NTU sequence is given as follows:

$$1, 1, 0, 0, 0, 1, 2, 1, 2, 2, 1, 1, 0, 2, 0, 2, 0, 0, 2, 2, 0, 0, 1, 0.$$

C. Observation

This section observes the bit patterns in an NTU sequence S. At first let $b^{(n)}$ denotes a pattern b of length n. Let $Z(b^{(n)})$ and $D_{S,Z}(b^{(n)})$ symbolize the number of 0's in $b^{(n)}$ and the number of appearance of $b^{(n)}$ in one period of S, respectively. Then let us consider n $(1 \leq n \leq m)$ bit patterns for an M-sequence. For example, consider $n = 3$ with a primitive polynomial $f(x) = x^4 + x + 1$, an M sequence of period 15 is given as follows:

$$1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0.$$

In this case $D_{S,Z}(b^{(3)})$ becomes as shown in **Table** I. Except all-zero pattern, every pattern appears twice respectively. In other words they are uniformly distributed. Every M-sequence haws such a typical feature about the distribution of bit patterns.

In the same way, let us consider an NTU sequence of $p = 5, m = 3$ and $k = 2$. In this case the period becomes 62 and an NTU sequence is given as follows:

1,0,1,1,0,0,0,1,0,1,1,1,0,1,0,1,0,0,0,0,0,0,1,0,0,0,0,1,0,0,0,
0,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0,0,1,0,1,1,0,0,1,1,1,1,0,0,0,1.

With a careful observation, it was found that for bit patterns $b_1^{(n)}$ and $b_2^{(n)}$, if $Z(b_1^{(n)}) = Z(b_2^{(n)})$, then $D_{S,Z}(b_1^{(n)}) = D_{S,Z}(b_2^{(n)})$. For example, in the case of $n = 3$, $D_{S,Z}(b^{(3)})$ becomes as shown in **Table** II. Focusing on the patterns 001, 010 and 100 in the **Table** II, $D_{S,2}(b^{(3)})$ satisfies the following relations.

$$Z(110^{(3)}) = Z(010^{(3)}) = Z(100^{(3)}) = 2,$$
$$D_{S,Z}(001^{(3)}) = D_{S,2}(010^{(3)}) = D_{S,2}(100^{(3)})) = 9.$$

Moreover, observing n bit patterns with an attention for the value of $Z(b^{(n)})$ for various parameter settings, $D_{S,Z}(b^{(n)})$ seems to increase in proportion to $Z(b^{(n)})$ multiplicatively. Then, this paper assumes $D_{S,Z}(b^{(n)})$ as follows:

$$D_{S,Z}(b^{(n)}) \quad = \quad p^{m-n} \cdot l^{n-Z(b^{(n)})-1} \cdot (l+1)^{Z(b^{(n)})}, \quad (7)$$

where p, m, n are as explained above and l is defined as $l = (p-1)/k$ and $0 \leq Z(b^{(n)}) < n$. For example, let us consider the case that $p = 5, m = 3, n = 3, Z(b^{(3)}) = 1$ and $l = (5-1)/2 = 2$, the Eq.(7) is calculated as follows:

$$D_{S,Z}(b^{(3)}) \quad = \quad 5^{3-3} \cdot 2^{3-1-1} \cdot (2+1)^1 = 6.$$

TABLE I
THE NUMBER OF 3BIT PATTERNS IN AN M SEQUENCE

$b^{(3)}$	000	001	010	011	100	101	110	111
$D_{S,Z}(b^{(3)})$	1	2	2	2	2	2	2	2

TABLE II
THE NUMBER OF 3 BIT PATTERNS $D_{S,Z}(b^{(3)})$ IN AN NTU SEQUENCE WITH $p = 5, m = 2$ AND $k = 2$

$b^{(3)}$	000	001	010	011	100	101	110	111
$D_{S,Z}(b^{(3)})$	13	9	9	6	9	6	6	4

D. Comparison

Comparing to the **Table** I and **Table** II, it can be seen that $D_{S,Z}$ for NTU sequence has deviations respects to the number of zeros $Z(b^{(n)})$.

E. Consideration

It seems that the proposed equation Eq.(7) in III-C shows the number of bit patterns correctly according to our extensive research.

IV. CONCLUSION AND FUTURE WORK

An assumption about the distribution of bit patterns on NTU sequence was given in this paper and it seems to be correct. As a problem of NTU sequence, the numbers of 0 and 1 are not balanced. This paper will contribute to find out a procedure to obtain a balanced NTU sequence.

ACKNOWLEDGEMENT

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

REFERENCES

[1] 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.

[2] K. Tebe, Y. Nogami, and S. Uehara, "A Geometric Sequence Generated by Primitive Polynomial and Power Residue Property over Odd Characteristic Field," Symposium on Information Theory and its Applications 2014(SITA2014), 2014.

[3] 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.