A Construction Method of a Binary Sequence Using a Logistic Map over F_p for IoT Device

Takato NAGANO[†], Takeru MITAZAKI[†], Satoshi UEHARA[†],
and Yasuyuki NOGAMI[‡]
[†]The University of Kitakyushu, Fukuoka, Japan.
[‡]Okayama University, Japan.

***Abstract*—With the spread of IoT, it is necessary to implement of encryption and decryption in order to secure information handled by each device. We focus on generating a sequence having random number property for a microcomputer with a short available bit length. We propose binary sequences combined from two random number sequences of 16 bits or less, one is an interleaving operation and the other is a combination by using a Gray code. In this paper, we discussed about how to generate a sequence and random number properties.**

I. Introduction

Information security is an indispensable basic technology in the operation of a safety electronic information society.

Logistic maps are generally known as chaotic maps. It can generate many pseudorandom numbers from simple mathematical expressions and behave like a chaos. In this research, we studied on an implementation for small devices with low specifications of hardware used for IoT/IoE. In addition, we know that a long period sequence can be generated by using a doubly safe prime (DSP) on the Logistic maps even if the performance of the small devices is low [1]. So we used this characteristic.

Currently, we succeeded in making a long sequence by combining two sequences with 7 bits removed from upper 16 bits. We used this logistic map over prime field and generated a random number that can be loaded in a small device with less waste without taking out upper bits by using a Gray code.

II. Preparations

A. Logistic Maps

The logistic map over the real domain is given by

$$\mathrm{LM}_R(r) = \mu r(1-r), \tag{1}$$

where r is a real number in [0,1], and μ is a control parameter. Let r_i be an input, where i acts as the discrete time. The iterative mapping for Eq. (1) can be represented by

$$r_{i+1} = \mu r_i(1-r_i). \tag{2}$$

B. Logistic Maps over Prime Field

We define a logistic map over prime field $\mathrm{LM}_{Z_p}(X)$ as follows.

Definition 1. Let p be an odd prime and Z_p a prime field modulo p. Let X be an element in Z_p. Then we define the logistic map $\mathrm{LM}_{Z_p}(X)$ over prime filed as

$$\mathrm{LM}_{Z_p}(X) = \frac{\mu_p X(p-1-X)}{p-1} \mod p, \tag{3}$$

where μ_p is a control parameter with $\mu_p \in [1, p-1]$. Moreover, Eq. (3) can calculate simply like as

$$\mathrm{LM}_{Z_p}(X) = \mu_p X(X+1) \mod p. \tag{4}$$

□

C. Gray Code

Gray code is one of numerical encoding methods, and it has a rule of which each Hamming distance of two successive numbers is definitely 1. In case of Z_4, the code is mapped as

$$0 \to (0,0),\ \ 1 \to (0,1),\ \ 2 \to (1,1),\ \ 3 \to (1,0).$$

In this research, we treat two bits as the argument of the Gray code.

Definition 2. Let $A = \{A_i\}_{i\geq 0}$ and $B = \{B_i\}_{i\geq 0}$ be two binary sequences with period N_a and N_b, respectively. Here we define a conversion C_G denoted as

$$C_G(A_i, B_i) = \begin{cases} 00 & \text{if } (A_i, B_i) = (0,0), \\ 01 & \text{if } (A_i, B_i) = (0,1), \\ 11 & \text{if } (A_i, B_i) = (1,0), \\ 10 & \text{if } (A_i, B_i) = (1,1). \end{cases} \tag{5}$$

□

III. Proposed Method

We propose two constructing methods of binary sequences by using two distinct sequence derived from logistic maps over prime field.

Let A and B be two sequences generated by two different initial values and two different DSP's of q bits. Here, we denote two initial values as A_0 and B_0, and two primes as p_a and p_b. However, it is no problem if A_0 and B_0 are same values. There are formulas for generating A and B as follows,

$$\begin{cases} A_{i+1} = \mu A_i(A_i+1) & \mod p_a, \\ B_{i+1} = \mu B_i(B_i+1) & \mod p_b, \end{cases} \tag{6}$$

where we use the control parameter $\mu = 2$ for the condition of the maximum period. Moreover, we express each element of A and B as the q-bit pattern, i.e., $A_i = (a_{i,0}, a_{i,1}, \cdots, a_{i,q-1})$, $B_i = (b_{i,0}, b_{i,1}, \cdots, b_{i,q-1})$. Namely, we can represent them as $A_i = a_{i,0} + 2a_{i,1} + \cdots + 2^{q-1}a_{i,q-1}$ and $B_i = b_{i,0} + 2b_{i,1} + \cdots + 2^{q-1}b_{i,q-1}$. Then, we have two types sequences $C =$

$\{C_i\}_{i\geq 0}$ and $D = \{D_i\}_{i\geq 0}$ from the following combining operations,

$$\begin{cases} C_i = (\{a_{i,j} \oplus b_{i,(j+r) \bmod q}\}_{j=0,\cdots,q-1}), \\ D_i = (\{a_{i,(j+r) \bmod q} \oplus b_{i,j}\}_{j=0,\cdots,q-1}), \end{cases} \quad (7)$$

where r is a cyclic shift number and $\oplus$ is a binary additive operator. There are two constructing methods by using C and D under the parameters $\{p_a, p_b, A_0.B_0, q, r\}$.

Interleaving Operation :

$$\begin{aligned} S_I &= (s_{I0}, s_{I1}, s_{I2}, s_{I3}, \cdots), \\ &= (c_{0,0}, d_{0,0}, c_{0,1}, d_{0,1}, \cdots, d_{0,q-1}, c_{1,0}, d_{1,0}, \cdots). \end{aligned}$$

Gray Code Conversion :

$$\begin{aligned} S_G &= (s_{G0}, s_{G1}, s_{G2}, s_{G3}, \cdots), \\ &= (C_G(c_{0,0}, d_{0,0}), \cdots, C_G(c_{0,q-1}, d_{0,q-1}), C_G(c_{1,0}, d_{1,0}), \cdots). \end{aligned}$$

IV. Evaluation

A. NIST Statistical Test

We evaluate the proposal sequence by using the NIST statistical test [2]. This test requires $1,000$ sequences in which a size of each one contains 10^6 bits. Hence we prepared 10^9 bit-length sequences. A number of items judged in the test is 188. Tables 1 and 2 indicate the number of errors in the items by using the interleave and the Gray code, respectively. Note that we only evaluate them by $2r < q$ to prevent the sequence duplication.

TABLE I
NUMBER OF ERROR ITEMS BY USING THE INTERLEAVE OPERATION.

		q					
		15bit	14bit	13bit	12bit	11bit	10bit
r	1	3	15	1	16	1	17
	2	1	15	0	17	0	19
	3	0	15	0	17	1	18
	4	0	15	0	16	0	18
	5	0	15	0	17	0	
	6	1	16	0			
	7	2					

TABLE II
NUMBER OF ERROR ITEMS BY USING THE GRAY CODE CONVERSION.

		q					
		15bit	14bit	13bit	12bit	11bit	10bit
r	1	0	0	0	0	1	0
	2	0	0	0	0	0	0
	3	0	0	0	0	0	0
	4	0	0	0	0	0	0
	5	0	0	0	0	0	
	6	0	0	0			
	7	0					

B. Random Excursions

Since the most of error items displayed in Table 1 are "Random excursions test", we focus on it. On this test, it evaluates a sequence $\underline{S} = (\underline{S}_0, \underline{S}_1, \cdots)$ generated by an input bit sequence x_i as the followings:

$$\underline{S}_0 = 2x_0 - 1, \ \ \underline{S}_{i+1} = \underline{S}_i + 2x_i - 1, \ \text{ for } i = 0, 1, 2, \cdots.$$

Let l be the number of times occurrences when $\underline{S}_i = 0$. In this test, l must be greater than 500. Let $\underline{S}$ be an integer. If $\underline{S}_{i+1} = \underline{S}$, there is just two cases: one is $\underline{S}_i = \underline{S} + 1$ and the other is $\underline{S}_i = \underline{S} - 1$. Hence we investigated in the occurrence rates that $\underline{S}_{i+1}$ is 1 to 4, and -4 to -1 by these two cases. Tables 3 and 4 give these rates by using the interleave method and the Gray code method, respectively, where $q = 14$ and $r = 1$.

TABLE III
OCCURRENCE RATES OF $\underline{S}_{i+1} = \underline{S}$ BY USING THE INTERLEAVE OPERATION.

	$\underline{S}$			
	1	2	3	4
$\underline{S}-1 \to \underline{S}$	6.6%	5.8%	5.9%	6.6%
$\underline{S}+1 \to \underline{S}$	5.8%	5.9%	6.6%	6.7%
total	12.4%	11.7%	12.5%	13.4%
	-1	-2	-3	-4
$\underline{S}-1 \to \underline{S}$	6.5%	5.7%	5.8%	6.7%
$\underline{S}+1 \to \underline{S}$	5.7%	5.8%	6.7%	6.9%
total	12.3%	11.5%	12.5%	13.6%

TABLE IV
OCCURRENCE RATES OF $\underline{S}_{i+1} = \underline{S}$ BY USING THE GRAY CODE CONVERSION.

	$\underline{S}$			
	1	2	3	4
$\underline{S}-1 \to \underline{S}$	6.3%	6.3%	6.2%	6.4%
$\underline{S}+1 \to \underline{S}$	6.3%	6.2%	6.4%	6.1%
total	12.6%	12.5%	12.6%	12.5%
	-1	-2	-3	-4
$\underline{S}-1 \to \underline{S}$	6.3%	6.3%	6.3%	6.2%
$\underline{S}+1 \to \underline{S}$	6.3%	6.3%	6.2%	6.2%
total	12.6%	12.5%	12.6%	12.5%

V. Conclution

In this paper, we discussed two methods of constructing a random number bit sequence from two distinct generated sequences of the logistic map over prime fields by using the interleaving and the Gray code. Since there are some errors of the statistical randomness tests in the interleaving method with extracting even numbers of bits, we recommend to extract only odd numbers when this method is used. We consider the reason of occurrence these errors as a bias of the occurrence rates we have presented in Table 3.

On the contrary, the almost all numbers of errors in the Gray code method are 0. Therefore, we also recommend to use this method for any conditions about the width of extracting bits. We have been studying the reason why the Gray code method makes good properties to the proposed sequence. We will explain it in the oral presentation.

Acknowledgement

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

References

[1] T. Miyazaki, S. Araki, and S. Uehara, "A Study of an Automorphism on the Logistic Maps over Prime Fields", ISITA2014, Melbourme, October 26-29, 2010.

[2] NIST, "A statistical test suite for random and pseudorandom number generators for cryptographic aplications," NIST Special Publication 800-22, 2001.