2005 RISP International Workshop on Nonlinear
Circuit and Signal Processing (NCSP'05)
Hawaii, USA, Mar. 4-6, 2005.

Research on True Random Numbers with a Key Feature

Shuichi Aono†, Yoshifumi Nishio† and Hideharu Aruga*

† Department of Electrical and Electronic Engineering
Tokushima University
2-1 Minami-Josanjima, Tokushima, 770-8506 Japan
Phone:+81-88-656-7470, Fax:+81-88-656-7471
Email: {aoichi, nishio}@ee.tokushima-u.ac.jp

* Leisure Electronics Technology Co.
Hitotsubashi Building 4F, 2-6-3 Hitotsubashi Chiyoda-ku, Tokyo, 101-0003 Japan
Phone:+81-35-210-4759, Fax:+81-35-210-4753
Email: h_aruga@letech.co.jp

1. Introduction

The encryption technology has the function of defending information, and becomes the element of other information security technologies like the digital signature etc. Random numbers play an essential role in various encryption schemes [1][2]. However, pesudo-random numbers can be forecasted, because the characteristics of pseudo-random numbers depend on the type and the initialization of the function. On the other hand, true random numbers based on a physical phenomenon can be said as ideal random number sequences because it is unpredictable.

In this research, we embed a kind of key feature into true random numbers. We use true random numbers generated from the true random number generator invented by Leisure Electronics Technology Co. We replace one number per every N random numbers by a number of the Logistic Map, which is known as the simplest map generating chaotic sequence, and investigate various properties of the created sequence.

2. Logistic Map

In this research, we use the Logistic Map, which is known as the simplest map generating chaotic sequence. The Logistic Map is expressed by the following equation:

$$z(t+1) = \alpha z(t)(1 - z(t)). \tag{1}$$

Here, α is a control parameter changing the behavior of the generated sequence. In this research, we use the parameter $\alpha = 4.0$.

Figure 1 shows an example of chaotic sequences generated by the Logistic Map. Figure 2 shows the relation between two successive numbers in the chaotic sequence. The relation clearly shows the shape of the map.

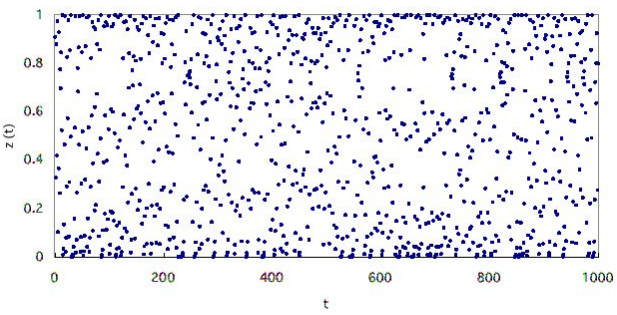


Figure 1: Chaotic sequence generated by the Logistic Map ($\alpha = 4.0$).

3. True Random Number with Key Feature

In this research, we use true random numbers generated from the true random number generator invented by Leisure Electronics Technology Co. This true random numbers generator uses pure thermal noise for the random source. The generated random numbers are experimentally confirmed to be truly random. The generation rate is 20MB per second. Moreover, this random numbers generator can automatically detect unexpected noises, accidental failures in the circuit and intentional attacks, because the statistical characteristics of the generated random numbers are always examined in real time.

In this research, we embed a kind of key feature into true

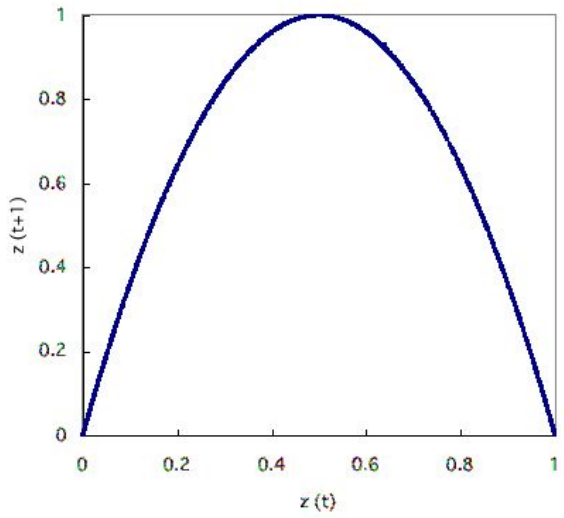


Figure 2: Relation between two successive numbers in the chaotic sequence ($\alpha = 4.0$).

random numbers generated from this true random number generator. The meaning of providing a key feature is not giving a seed to pseudo-random numbers generators, but to embed information into the random number sequence. Though true random numbers cannot be reproduced again, the random number sequence with the same information can be reproduced by giving a key feature. For example, if we can embed two different keys into the random number sequence and also can extract the key from the sequence, the true random numbers might be utilized as a carrier of some information.

We use the Logistic Map to give a key feature. Figure 3 shows the method of embedding a key feature.

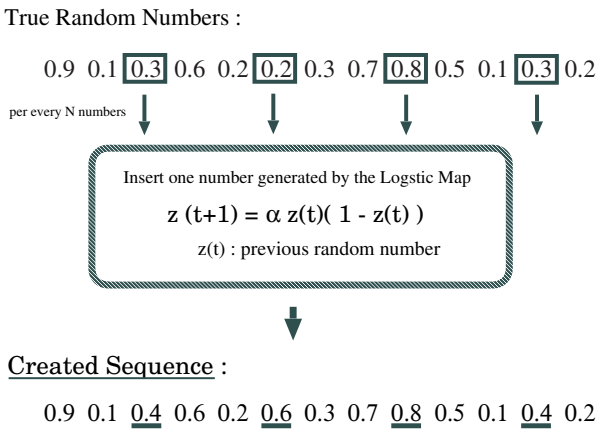


Figure 3: Making true random number with key feature.

One true random number per every N is replaced by the number generated by the Logistic Map. The value of the previous random number is used for an initial value of the Logistic Map.

4. Simulated Results

Simulated results are shown in Figs. 4 and 5. Figure 4 shows the created sequence for the case of $N = 5$. Figure 5 shows the relations between two successive numbers in the created sequence for the cases of $N = 5$ and $N = 15$.

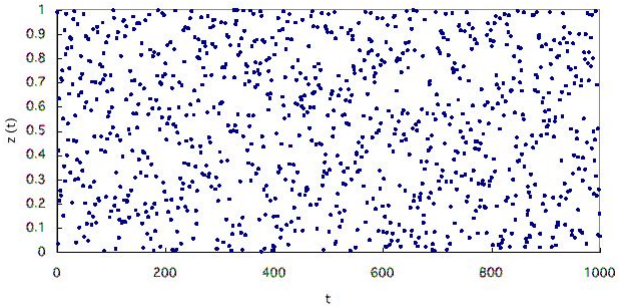


Figure 4: Created sequence.

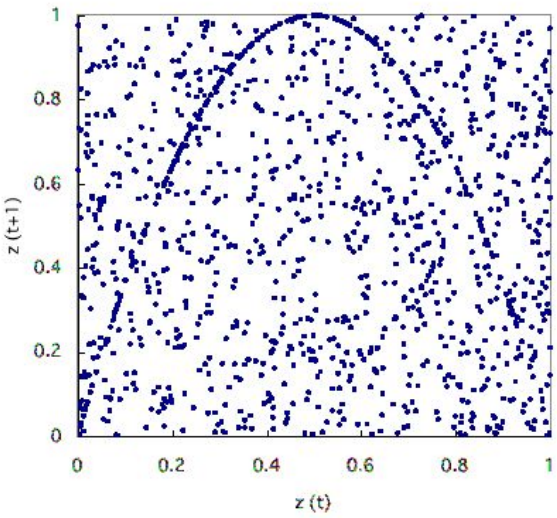
This created sequence looks similar to the true random numbers in Fig. 1. However, when we analyze the relation between two successive numbers, we can clearly observe that the shape of the Logistic Map is embedded into the sequence as a key feature.

Next, we investigate the distribution of the created sequence. Figure 6 shows the distribution of the sequence. The horizontal axis shows the value of the sequence, the vertical axis shows the number of the sequence. When the value of N is small, that is, the amount of the added chaotic value is large, the distribution of the sequence becomes non-uniform.

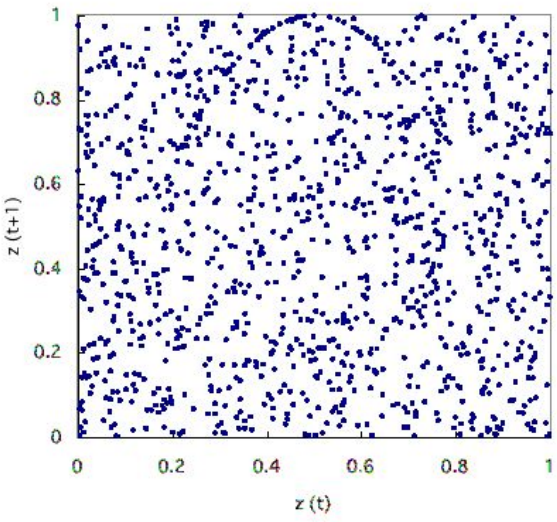
Further, we investigate the runs within the created sequence. A run is a monotonic subsequence; *Run up* is increasing subsequences and *Run down* is decreasing subsequences. The expected distribution of the number of runs for a truly random sequence is known as follows [1].

$$r_d^* = \frac{2n(d^2+3d+1)}{(d+3)!} - \frac{2(d^3+3d^2-d-4)}{(d+3)!} \qquad (2)$$

where r_d^* is the expected number of runs with the length d and n is the length of the total sequence. The expected distribution is compared against the sample distributions using the standard χ^2 formula. By executing the run test, we confirmed that the created sequence does not pass the run test for $N < 29$.



(a)



(b)

Figure 5: Relations between two successive numbers in the created sequence. (a) $N = 5$. (b) $N = 15$.

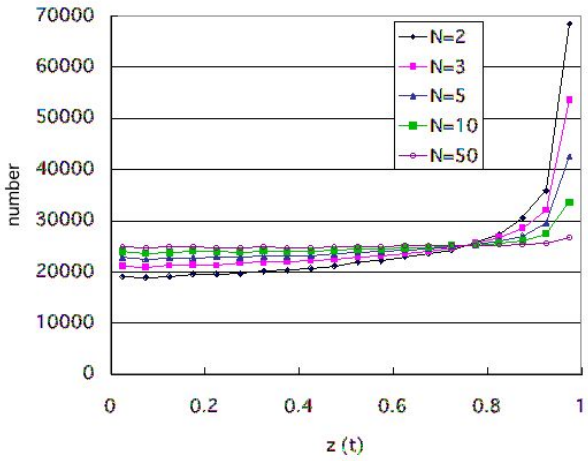


Figure 6: Distribution of the sequence.

5. Conclusion

In this research, we embedded a kind of key feature into true random numbers and investigated various properties of the created sequence.

As our future subject, we are considering to insert chaotic sequence into true random numbers in an irregular manner.

References

[1] O. Miyatake and K. Wakimoto, “Random Number and Monte Carlo Method,” Morikita Shuppan Co., 1978.

[2] D.E. Knuth, “Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd Edition,” Addison-Wesley, 1997.