On the design of henon and logistic map-based
random number generator

Magfirawaty1,2, Suryadi.M.T3, Kalamullah Ramli1
1 Dept Electrical of Engineering, Universitas Indonesia, Depok 16424, Indonesia
2 Sekolah Tinggi Sandi Negara, Bogor, Indonesia
3 Dept of Mathematics, Universitas Indonesia, Depok 16424, Indonesia
E-mail: magfirawaty@ui.ac.id, yadi.mt@sci.ui.ac.id, k.ramli@ee.ui.ac.id

Abstract. The key sequence is one of the main elements in the cryptosystem. True Random
Number Generators (TRNG) method is one of the approaches to generating the key sequence.
The randomness source of the TRNG divided into three main groups, i.e. electrical noise based,
jitter based and chaos based. The chaos based utilizes a non-linear dynamic system (continuous
time or discrete time) as an entropy source. In this study, a new design of TRNG based on
discrete time chaotic system is proposed, which is then simulated in LabVIEW. The principle
of the design consists of combining 2D and 1D chaotic systems. A mathematical model is
implemented for numerical simulations. We used comparator process as a harvester method to
obtain the series of random bits. Without any post processing, the proposed design generated
random bit sequence with high entropy value and passed all NIST 800.22 statistical tests.

1. Introduction
In modern cryptography, the cryptosystem is a pair of algorithms that uses a key to convert
plain text to ciphertext and vice versa. In cryptosystem, the algorithm is usually public and in
this case the security depends on the secrecy key. Good key is a series of random bit which is
generated automatically [1]. The randomness of key plays a significant role to ensures robustness
of cryptosystem.

True Random Number Generator (TRNG) is a device that generates a random number which
is unpredictable based on physical process and non-deterministic events [2]. TRNG consists of
three main components, namely, source entropy that generates randomness, harvest process
to get a randomness samplers, and post processing to minimize bias and produce random bit
sequences that pass a statistical test. Furthermore, we can classify TRNG into three main classes
according to entropy sources, (1) based on electrical noise, (2) jitter based, (3) chaos based.

The pioneer observation method of TRNG used the odd-even criterion with a Poisson
distribution acquired by calculating random pulses from an electrical noise source [3]. Currently,
the most significant concept is using ring oscillators (RO) to obtain TRNG with high throughput.
RO uses the jitter approaches to generate a random signal [4, 5]. Jitter-based TRNG perform
better than noise based, which is sensitive to external interference and easy to integrate with
digital circuits. In addition to jitter and noise based-TRNG, recent papers used chaotic systems
as a method for developing chaos based TRNG [6, 7] to increase the randomness. Chaotic is
defined in a deterministic term, which is very sensitive to the changes initial conditions. TRNGs
based on chaos use chaotic signals as an entropy source. Chaos-based TRNG can be applied
based on continuous time (CT) and discrete time (DT). DT chaotic systems are more efficient than that of CT chaotic systems. Which it can be realized using fewer of resources, thus resulting a more efficient block of cryptosystem [6,8–11].

In this study, the design of random number generator based on DT chaotic system is proposed. The design used a combination of two chaotic systems, i.e, Henon map and logistic map, to produce random bit sequence with high entropy value, simulated using LabVIEW. Randomness performance is assessed through entropy value and NIST 80.22 statistical test. This paper is structured as follows: Section II illustrates random number generator model by combining two-dimentional and one-dimentional chaotic systems. A threshold value is obtained using mathematical model, which is compared with the output of chaotic system to produces random bit. The randomness of the proposed method is analyzed and discussed in Section III. The last Section is a conclusion of the experiment conducted.

2. Random Number Generator Model
Discrete-time chaotic systems utilize a periodic iteration of a non-linear function, f, to accomplished the chaotic condition. Fig. 1 shows general concept of DT chaotic system which consists of chaos map $f(x)$ that depends on controlling parameters ($\lambda$) that guarantee chaotic regime of the system.

$$x_{n+1} = f(\lambda, x_n)$$

Figure 1: General concept of discrete time chaotic system [12]

Chaotic systems are divided into several dimensions, including one- and two-dimensions. They are different due to their complexity, probability, and density of the involved function. The basic idea of our random number generator design is presented in Fig. 2. The aim of this design is to generate high entropy random bits by combining two chaotic systems, in which its main components consist of a sampling clock, sample-hold circuit, non-linear function blocks and comparator. The sample and hold block produces and forming the chaotic dynamics and the entropy core. The function blocks implement chaotic maps to increase entropy value, which is primarily limited by the Lyapunov exponent. In this study, we use Henon map and logistic map as chaotic map functions. Then, the output of last chaotic map function is compared with the threshold value to generate a bitstream.

Figure 2: Proposed design
In mathematical terms, Eqn. (2) shows Henon map as a two-dimensional non-linear function block. It is a discrete time dynamical system that simplifies Lorenz system and Poincare map. The Henon equations can be expressed as

\[
(x, y) \in \mathbb{R}^2 \\
x_{n+1} = 1 - \alpha x_n^2 + y_n \\
y_{n+1} = \beta x_n
\] (2)

in which \(\alpha\) and \(\beta\) are the chaos controlling parameters of non-linear function block, where \(n\) is 0, 1, 2, etc. The initial are values symbolized by \((x_0, y_0)\). The evolution samples of Henon map is shown in Fig. 3.

Choosing an arbitrary initial state (which is assumed to be determined by the real time clock of hardware) is the early stages of this work, Henon map as a first non-linear function block on each iteration generates a new value relying on the disposition of chaotic samples. The chaotic behavior of Henon map is controlled by parameter values \((\alpha, \beta)\), in which \(\alpha = 1.4\) and \(\beta = 0.3\). For example, starting from an initial value \(x_0 = 0.063752\) and \(y_0 = 0.098551\), the Henon map chaotic trajectory for 8 time iterations are \(x_{n+1} = \{0.063752, 1.092861, -0.65296, 0.730963, 0.056082, 1.214886, -1.0495, -0.17757\}\). Fig. 4 shows the outline of a two-dimensional sphere for the Henon map after 10000 iterations starting from initial point \((0.1, 0.1)\). Furthermore, the values of \(x_{n+1}\) are normalized in range \([0,1]\).

![Figure 3: Evolution 250 samples of Henon map](image)

![Figure 4: Henon map attractor after 10000 iterations](image)
The second non-linear function block uses the logistic map to increase the entropy value and randomness of the output that is generated by the system. Logistic map is expressed as

\[ X_{n+1} = \gamma X_n (1 - X_n) \]  

(3)

where \( \gamma \) is the control parameter setting. The output value of the normalized Henon map serve as an initial value for the non-linear function block second \( (X_n) \). Then, the threshold comparator system can be expressed as

\[ b_n = B(X_n) = \begin{cases} 0, & 0 \leq X_n \leq T_h \\ 1, & T_h < X_n \leq 1 \end{cases} \]  

(4)

The randomness performance of the DT chaos based TRNG model depends on two critical parameters namely chaos controlling parameter \( \gamma \) and bit generation threshold \( T_h \). We used method [7] to calculate the optimum threshold for independent bit generation. A pair of bits \( (b_n, b_{n+1}) \) generated from last function block. Their joint probability as the product of marginal probabilities, having the form of

\[ P_{ij} = P(b_n = i, b_{n+1} = j) = P(b_n = i)P(b_{n+1} = j) \text{ for } i, j \in 0, 1 \]  

(5)

The probabilities of marginal bit generation can be obtained from

\[ P_0 = P(0 \leq X_n \leq T_h) = \int_0^{T_h} f_X(X)dX = T_h \]  

(6)

\[ P_1 = P(T_h \leq X_n \leq 1) = 1 - P_0 = 1 - T_h \]  

(7)

The threshold parameter is \( T_h \leq \frac{2}{\gamma} \) and \( X_n = \frac{2}{\gamma} \), the joint probability \( P_{00} \) as

\[ P_{00} = P(b_n = 0, b_{n+1} = 0) = P(X_n \leq T_h, X_{n+1} \leq T_h) \]  

(8)

by additivity,

\[ = P(X_n \leq T_h, X_{n+1} \leq T_h, X_n \leq \frac{2}{\gamma}) \]

\[ + P(X_n \leq T_h, X_{n+1} \leq T_h, X_n > \frac{2}{\gamma}) \]

and by utilizing \( X_{n+1} \) from Eqn. 3

\[ = P(X_n \leq T_h, \gamma X_n (1 - X_n) \leq T_h, X_n \leq \frac{2}{\gamma}) \]

\[ + P(X_n \leq T_h, \gamma X_n (1 - X_n) \leq T_h, X_n > \frac{2}{\gamma}) \]

\[ = \int_0^{2T_h/\gamma} f_X(u)du = \frac{2T_h}{\gamma} \]  

(9)

By combining \( P_0 \) as marginal probability that defined by Eqn.6 and equating to zero for \( \gamma = 4 \), the optimum value of \( T_h \) is expressed as

\[ \Psi_{00} = P_{00} - P_1 P_0 = \frac{2T_h}{\gamma} - T_h^2 |_{\gamma=4} = 0 \]

\[ \Rightarrow T_h = 0.5 \]  

(10)
3. Analysis and Discussion

3.1. Entropy Analysis
Theoretically, the proposed TRNG design is capable of producing a sequence which is distributed independently and unpredictable. Therefore, it is necessary to calculate the entropy value of the generated bit. The entropy in Shannon theory is a measure of uncertainty of the value of the next generated bit. According to Shannon theory, the entropy value of number series can be obtained by

$$H = - \sum_{i=0}^{1} P_i \log_2 P_i$$  \hspace{1cm} (11)$$

where $P_i$ is the probability of generating a value of zero or one. Ideally, the probabilities $P_0$ and $P_1$ are equal to $\frac{1}{2}$ resulting in an entropy of 1, which is the maximum value of the entropy function. Simulation result of the proposed design obtained bit sequence, which the information entropy was approximately 0.9998. The obtained value was very close to a maximum value of the entropy function.

3.2. Statistical Analysis
The output of proposed design has been analyzed statistically. Final report file of NIST 800-22 is used to explain the randomness of bit output. Table 1 lists the NIST statistical testing results. These tests detect the non-randomness of output sequences resulted from pseudo random or random number generators. Two approaches recommended by NIST that we adopted. First, the testing of the proportion of binary output sequences that pass statistical test, check the uniformity of distribution of P-values is second approach.

The confidence interval is used to determine the acceptable proportions range. For a significance level of $\alpha = 0.01$, 100-bit sequences with $10^6$ length of each sequence, the confidence interval was equal to $0.99 \pm 0.02985$. To pass each statistical test, the proportion of sequences should be above 0.96015. Fig. 5a shows the proportion value of each statistical test is greater than 0.96015. It proves with the output bit sequence is random. NIST second approach is to ensure that uniformity of P-values distribution interval range [0,1] is divided into 10 sub-intervals. P-value determine the uniformity of bit sequence. Applying a $\chi^2$ and an additional
process, we acquire a new P-value ($P_T$). If $P_T \geq 0.01$, then the sequences can be considered as uniformly distributed. As shown in Table 1, the value of the $P_T$ for all statistical tests was greater than 0.01, and hence the proposed design is uniformly distributed. Furthermore, histogram can be used to visualize the distribution of p-value, as shown in the Fig. 5b.

### 4. Conclusion

We designed a TRNG combining two chaotic systems to generate random bit sequence with high entropy value. We used Henon map and Logistic map as chaotic systems. We utilized a discrete time chaotic system to generate bit sequence which is distributed independently and unpredictable. The proposed design was simulated in LabVIEW. The output randomness was influenced by chaos parameter and threshold value.

The proposed design is a simple and an excellent method for generating random bits, which the information entropy was very close to a maximum value of the entropy function, and pass all NIST 800-22 statistical tests. Our design has not been implemented on hardware, and our future experiment will be performed it on FPGA board.

**Acknowledgment**

This research is partly funded by PITTA Grant of Universitas Indonesia, under contract number 2129/UN.R12/HKP.05.00/2016.

**References**

[1] Schneier B 1996 *John Wiley and Sons, NY* (Oct. 1995)

[2] Schindler W and Çetin Kaya K 2009 *About Cryptographic Engineering* (New York: Springer) ISBN 9780387718163

[3] Maddocks R, Bucci M and Luzzi R 1972 *Journal of Physics E: Scientific Instruments* **5** (6) 542–544

[4] Sunar B, Martin W J and Stinson D R 2007 *IEEE Transactions on Computers* **56** 109–119
[5] Wold K and Tan C H 2009 *International Journal of Reconfigurable Computing* **2009**

[6] Cicek I, Pusane A E and Dundar G 2013 A novel dual entropy core true random number generator *8th International Conference on Electrical and Electronics Engineering (ELECO)* (IEEE) pp 332–335 ISBN 6050105049

[7] Cicek I, Pusane A E and Dundar G 2014 *the VLSI Journal Integration* **47** 38–47

[8] Cicek I and Dundar G 2013 A chaos based integrated jitter booster circuit for true random number generators *European Conference on Circuit Theory and Design (ECCTD)* (IEEE) pp 1–4

[9] Katz O, Ramon A and Wagner I 2008 *VLSI System, IEEE Transactions on* **16** 1677–1686

[10] Pareschi F, Setti G and Rovatti R 2006 A fast chaos-based true random number generator for cryptographic applications *Proceedings of the 32nd European Solid-State Circuits Conference (ESSCIRC)* (Montreux: IEEE) pp 130–133 ISBN 1424403030

[11] Stojanovski T, Phil J and Kocarev L 2001 *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **48** 382–385

[12] Aguilar Angulo J A, Kussener E, Barthelemy H and Duval B 2014 Discrete chaos-based Random Number Generator *IEEE Faible Tension Faible Consommation (FTFC)* (IEEE) pp 1–4

[13] Rukhin A, Soto J, Nechvatal J, Barker E, Leigh S, Levenson M, Banks D, Heckert A, Dray J and Vo S 2010