True Random-Bit Generation Using a Continuous-Time Chaotic Oscillator

Chatchai Wannaboon

Electronic and Photonic System Engineering
Kochi University of Technology
Tosayamada, Kami-City, Kochi, 782-8502, Japan
e-mail : 198007y@gs.kochi-tech.ac.jp

Tachibana Masayoshi

Electronic and Photonic System Engineering
Kochi University of Technology
Tosayamada, Kami-City, Kochi, 782-8502, Japan
e-mail : tachibana.masayoshi@kochi-tech.ac.jp

Abstract - This paper presents a true random-bit generation through a continuous-time chaotic oscillator, which provides automatically chaotic signals and is fully implemented on 0.18 CMOS standard technology. Chaotic dynamics of the oscillator are exhibited in terms of chaotic strange attractor in phase-space domain. In order to achieve true-random property, a simple designed of post-processing method is utilized. Finally, the quality of randomness is analyzed through 1,000,000 binary sequences which are verified by statistical test methods and NIST standard tests suite. The proposed system has offered a cost-effective and a compact random-bit generator for computer security applications.

I. Introduction

Due to increasing demand of data storage on the internet, an information security has become a significant issue in both industrial and research fields. During the last decade, data encryption has been the best solution for the information security where searching for an effective key generation has still motivated many researchers. Basically, several key generations have been performed by random number generator (RNG). However, since rapidly advance in computer technology, pure RNG might not be acceptable against an advanced cryptography algorithm. For this reason, true random number generator (TNRG) is widely utilized many applications not only the encryption, but also cryptography as well as some searching algorithm. Thus, extraction of proper randomness source is still a challenging topic in the research area.

Recently, chaotic system has been extensively studied due to various fascinating properties such as extremely sensitivity on initial conditions and impossible for prediction. Several chaotic-based TNRG have been proposed using discrete-time chaotic map, for example, logistic map [1], tent map [2] and piecewise-linear chaotic map [3-4]. Such systems provide robust chaotic signals through a one-dimensional chaotic function and are proper as the random sources. On the other hand, implementation on large-scale integrated (LSI) circuits is still challenging.

A continuous-time chaotic system has attracted a great attention since a discovery of Chua's circuit [5], where the chaotic dynamic derives from a set of ordinary-differential equation (ODE). Several oscillators based on such a system have been presented such as Chen's system oscillator [6] and Van Der Pol oscillator [7]. These circuits truly provide the chaotic behavior, but inappropriate for transistor level due to large value of passive components. Recently presented by Radwan et al. [8] and Güler et al. [9] have suggested the appropriate chaotic oscillator for the LSI design, where the circuit is simply designed based on a Gm-C integrator and a push-pull inverter.

Therefore, this paper presents a true random-bit generation which a continuous-time chaotic oscillator is employed as the random signals source. The chaotic behavior of the oscillator is firstly examined through the chaotic attractor, waveform in time and frequency domain (Section 2). Section 3 describes the structural of overall TNRG system. In section 4, the statistical test methods i.e., histogram, autocorrelation and NIST standard test suite are used in order to verify the randomness of bit sequences.

II. Double-Score-Like Chaotic Oscillator

Typically, the chaotic oscillator can be synthesized based on three-dimensional ODE [10] system which is given by

$$\dddot{x} = -\lambda\left[\ddot{x} + \dot{x} + x - G(x)\right] \tag{1}$$

where $G(x)$ and λ are a nonlinear function and adjusting parameter, respectively. Various approaches have been implemented by using a signum function as a nonlinear function, thus, dual supply is required. In this paper, a nonlinear function is consequently replaced by the hyperbolic tangent in order to operate on a single supply. Fig. 1 illustrates the chaotic oscillator comprises three stage of Gm-C integrators, current mirror circuits and approximated hyperbolic tangent portion. As a result, the set of first-order ODE system can be expressed as

$$\begin{aligned} \dot{v}_x &= \frac{g}{C_3} v_y \\ \dot{v}_y &= \frac{g}{C_2} v_z \\ \dot{v}_z &= \frac{g}{C_1}\left[-v_x - v_y - v_z + (\tanh(ax-b)+c)\right] \end{aligned} \tag{2}$$

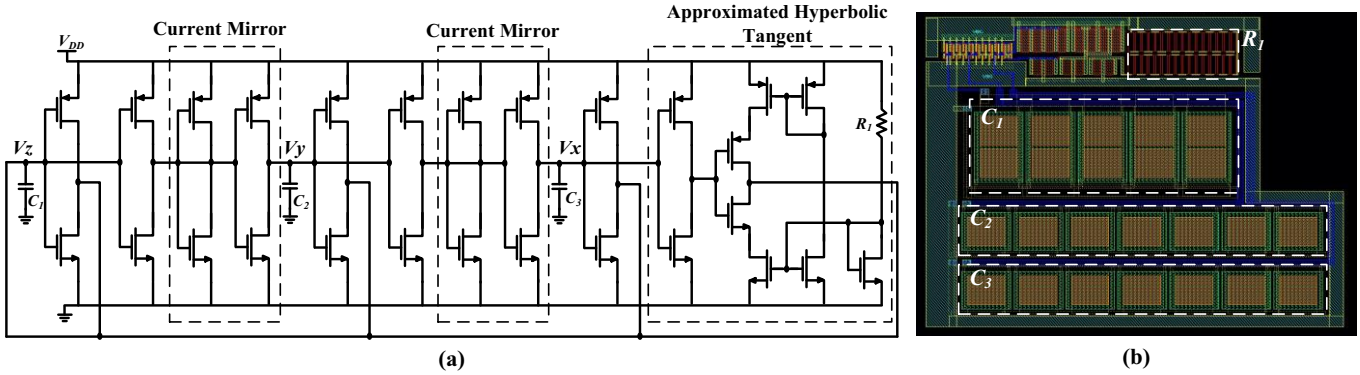

Fig. 1. (a) Schematic and (b) layout diagram of the chaotic oscillator.

Fig. 2. Trajectories of attractor from the oscillator between (a) $v_x - v_y$, (b) $v_x - v_z$ and (c) $v_y - v_z$

where g is a transconductance of tranconductor and adjusting parameter λ is given by C_1/C where $C = C_2 = C_3$. Typically, the chaotic behavior is exhibited in the range of 0.48 - 0.98 of parameter λ [11]. The parameter a, b and c can determine a characteristic of the nonlinear function. In this case such parameters are defined as 50, 50 and 1 in order to execute only on the first-quadrant.

In the circuit implementation, C_1, C_2 and C_3 are fixed as 1, 0.8 and 0.8 pF, respectively (for $\lambda = 0.8$). Fig. 2 depicts the measurement of chaotic strange attractor captured from the oscillator, including (a) $v_x - v_y$, (b) $v_x - v_z$ and (c) $v_y - v_z$ projection.

III. Proposed True Random-Bit Generation

The proposed true random-bit generation comprises three main portions i.e., the chaotic oscillator, a binary sequences generation and a post-processing method. The non-deterministic chaotic signals are generated automatically on single-die chip. Afterwards, the signals are conveyed to the computational software through an analog-to-digital module of microcontroller STM32F7 series.

In the software portion, the chaotic signals from all nodes (v_x, v_y, v_z) are transformed into chaotic binary sequences by a threshold function. In order to increase the randomness dynamical, the simple post-processing method is performed by two-connection of logic components (XOR). As clearly indicates in Fig. 3, that the binary outputs of the system are more robustness after the post-processing method. The schematic diagram of overall system is also shown in Fig. 4.

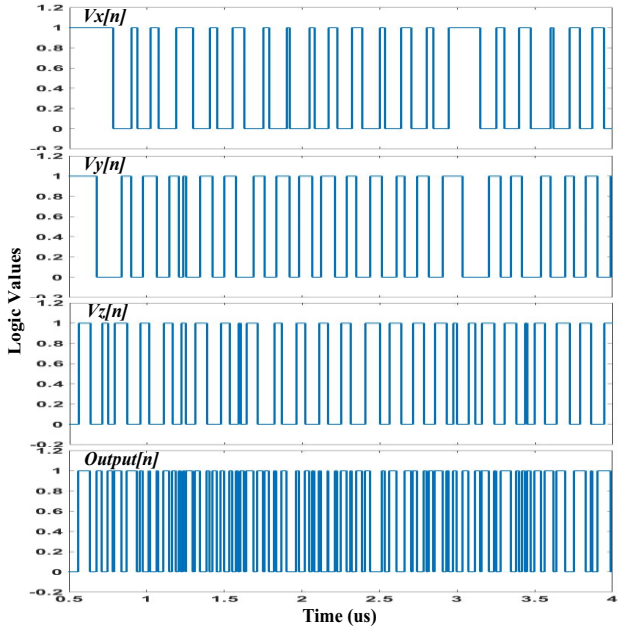

Fig. 3. Chaotic binary waveform and the output of proposed system.

IV. Randomness Evaluation

The randomness of the proposed system has been evaluated through 1,000,000 binary sequences. Three statistical methods are employed i.e., histogram, autocorrelation which represent a qualitative measurement, and NIST standard test suite as a quantitative measurement.

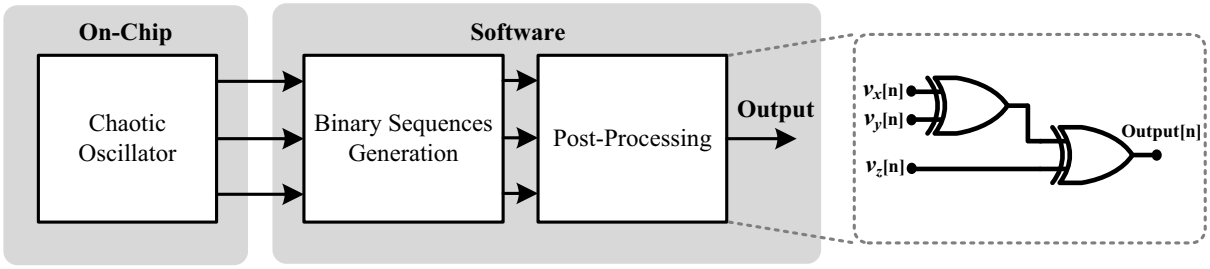

Fig. 4. The overall system of proposed true random-bit generator.

A. Histogram and Autocorrelation

The random characteristics of the output binary sequences are analyzed by MATLAB software. Fig. 5. Illustrates the histogram plot of 1,000,000 bits sequences, suggests that amounts of the binary "0" is nearby binary "1" which is one of the TNRG characteristic. In addition, the autocorrelation of the 1,000,000 bit sequences is also depicted in Fig. 6. It can be considered that there is rarely occurred the periodic region due to the correlations are relatively close to zero for most value.

B. NIST standard test suite

Generally, a high-acceptable statistical tests algorithm has been provided by the National Institute of Standards and Technology (NIST) in order to particularly examine the randomness of binary sequences. In this paper, the widely-used NIST test suite from 800-22rev1a [12] is utilized with typical 1,000,000 random binary sequences. The test suite comprises 15 test methods which imply the random characteristic of the sequences. Where the robustness of the perfect randomness is described by p-value (probability value), for example, a p-value greater than a level of 0.01 suggests that the tested sequences is performing the random behavior with 99% of confidential level. Table 1 summarizes the NIST test results of 1,000,000 binary sequences obtained from proposed system, implies that the sequences passed all the test methods which can be considered as the randomness sequences.

V. Conclusions

The true random-bit generation has been demonstrated and evaluated in this paper. The random source is constructed using the continuous-time chaotic oscillator. Fully fabricated on-chip of the oscillator exhibits chaotic dynamics, indicated by the plot of strange attractor in stage-space-domain. The randomness of binary sequences has been examined through the histogram, the autocorrelation and the NIST statistical test suite. Furthermore, the proposed system has been potentially considered to be the truly random generation, supported by the non-deterministic characteristic and passing all the NIST test methods. This system might be able to an alternative random-bit generator for the various applications such as a secure communication or a high-complexity data encryption.

TABLE I
NIST Standard Test Results of 1,000,000 Bits Generated From Proposed System

Test Methods	p-values	Results
Frequency Test	0.5183	Success
Block Frequency	0.7164	Success
Runs	0.4688	Success
Longest Run of Ones Block	0.1343	Success
Binary Matrix Rank	0.0336	Success
Discrete Fourier Transform	0.3172	Success
Non-overlapping Template Matching	0.0169	Success
Overlapping Template Matching	0.9144	Success
Universal Statistical	0.2664	Success
Linear Complexity	0.2699	Success
Serial	0.9833	Success
Approximate Entropy	0.9468	Success
Cumulative Sums	0.4744	Success
Random Excursions	0.9314	Success
Random Excursions Variant	0.8429	Success

Acknowledgements

The authors are grateful to Bandhit Suksiri for his helping about data acquisition. This work was supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Synopsys, Cadence Design System, Mentor Graphics, Rohm Corporation and Toppan Printing Corporation. Additionally, it was also supported by KAKENHI (23500067) Grant-in-Aid for Scientific Research.

References

[1] L. Liu, S. Miao, H. Hu and Y. Deng, "Pseudorandom bit generator based on non-stationary logistic maps," *IET Information Security*, vol. 10, pp. 87-94, Feb, 2016.

[2] L. Palacios-Luengas, G. Delgado-Gutiérrez, M. Cruz-Irisson, J. L. Del-Rio-Correa, and R. Vázquez-Medina, "Digital noise produced by a non-discretized tent chaotic map," *Microelectronic Engineering*, vol. 112, pp. 264-268, Mar, 2013.

[3] P. Ketthong and W. San-Um, "A robust signum-based piecewise-linaer chaotic map and its application to microcontroller-based cost-effective random-bit generator," *IEEE International Electrical Engineering Congress (iEECON)*, pp. 1-4, 2014.

[4] W. San-Um and P. Ketthong, "The generalization of mathematically simple and robust chaotic maps with absolute value nonlinearity," *IEEE Region 10 Conference*

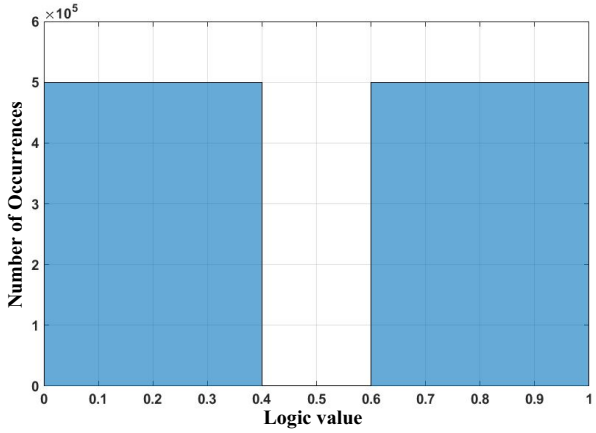

Fig. 5. Histogram plots of output binary sequences.

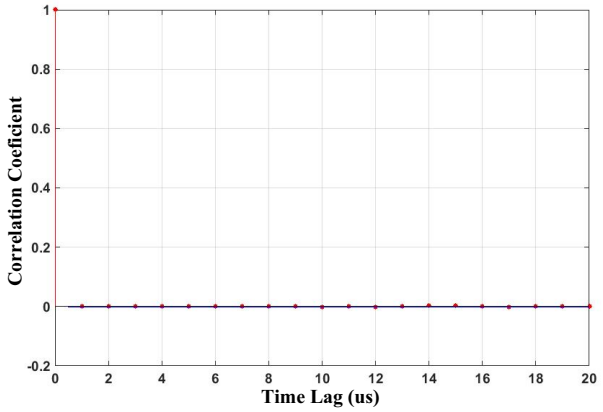

Fig. 6. Autocorrelation of the output binary sequences.

(TENCON), pp. 1-4, Oct., 2014

[5] L. O. Chua, C. W. Wu, A. Huang, and G.Zhong, "A Universal Circuit for Studying and Generating Chaos. II. Strange Attractors," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications*, vol. 40, pp. 745-761, Oct., 1993.

[6] H. Hu, L. Liu, and N. Ding, "Pseudorandom sequence generator based on the Chen chaotic system," *Computer Physics Communications*, vol. 184, pp. 765-768, Dec., 2012.

[7] L.Acho, J.Rolon, and Benitez, "A chaotic oscillator using the Van der Pol dynamics immersed into a Jerk system," *WSEAS Trans. Circuits Syst.*, vol.3, no.1, pp.198–199, 2004.

[8] A. G. Radwan, A. M. Soliman and A. El-Sedeek, "MOS Realization of the Double-Scroll-Like Chaotic Equation," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, pp. 285-288, Feb., 2003.

[9] U. Giiler and S. Ergiin, "Monolithic Implementation of a Double-Scroll Chaotic Attractor and Application to Random Number Generation," *IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, pp. 1037-1040, Dec., 2010.

[10] J. C. Sprott, "A new class of chaotic circuit," *Physics Letters*, pp. 19-23, Feb., 2003.

[11] A. S. Elwakil and M. P. Kennedy, "Construction of Classes of Circuit-Independent Chaotic Oscillators Using Passive-Only Nonlinear Devices," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, pp. 289-307, Mar., 2001.

[12] www.nist.gov. : NIST test suite from a special publication 800-22 rev1a.