TNI Journal of Engineering and Technology
Vol.2 No.2 July - December 2014

A Cost-Effective Hardware True-Random-Bit Generator using High-Dimensional Autonomous Hyperjerk Chaotic System

Worrawut Chikchornwanit and Wimol San-Um

Research Center for Intelligent Electronics Systems

Department of Computer Engineering, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI)

Pattanakarn, Suanluang, Bangkok, Thailand, 10250. Tel: (+662) 763-2600 Ext.2926. Fax: (+662) 763-2700

worrawut@tni.ac.th, wimol@tni.ac.th

***Abstract*— With the rapid advancement of Information and Communication Technology (ICT) in recent years, information security has become a major issue under consideration for both research and practical applications. Cryptography has therefore been utilized as a solution for information security where a True-Random-Bit (TRB) generator is necessary in confidential key generation or in an intrinsic algorithm to the computation. A number of TRB generators have been reported based on stochastic systems, involving resistor noise amplification, digital clock jitter noises, or a heuristic source of randomness. The use of chaotic systems has also been suggested recently for hardware TRB generators owing to a well-defined deterministic circuits and systems. This paper presents a new hardware TRB generator using a high-dimensional autonomous hyperjerk system. The realization of high-dimensional hyperjerk system provides multi-output signal depending on the dimension degree, and offers very simple circuit implementations through a series connection of integrators with a single nonlinearity. The multi-output chaotic signals are digitized prior to the digit-combination process, yielding a 20,000-bit sequence. The statistical tests that prove the randomness are achieved by various standard test methods such as Chi-square goodness-of-fit test, Gap test, Poker test, Coupon-collectors test, Permutation test, Run test for randomness, Wilcoxon signed rank test, Sign test, Jarque-Bera test and Lilliefors test. This work offers not only a cost-effective hardware implementation, but also high-degree of randomness for applications in cryptography used in information security.**

Keywords-component; True Random Bit generator, Hyperchaotic Autonous System, Dynamical System.

I. INTRODUCTION

Chaotic systems have a number of attractive properties, including sensitivity on initial condition and system parameters, ergodicity and attractor properties. Chaotic systems have been characterized as a system that offers a sensitive dependence on initial conditions, i.e. a small perturbation ultimately results in a dramatic change in system states [1]. However, the slightest uncertainty on the initial state leads to an extremely large uncertainty after a short period of time. In particular, chaotic systems have been realized as a True Random Bit Generator (TRNG) for various applications such as confidential key generators for symmetric key crypto-systems and public-key ones. Traditional TRNGs were implemented by random physical phenomenon, including direct noise amplification of a resistor [2] and jitter noise of digital clock signals [3]. In addition, the embedded TRNGs normally realize external devices or heuristic source of randomness. Despite the fact that such limitations can be conquered through proper custom circuits, randomness extraction is still a challenging topic in the designs based on such devices. Chaotic systems have offered a potential alternative, when compared to those of traditional TRNGs, through the use of an analog deterministic circuit which exhibits chaotic behaviors. With such initial uncertainties, system behaviors can be predicted only for a short period of time. In the case of the state variable of chaos system is not available to the observer and the chaos-based system is well constructed, the output of the system cannot be determined.

In this paper, a new hardware TRB generator using a high-dimensional autonomous system is presented. The realization of high-dimensional hyperjerk system provides multi-output signal depending on the dimension degree, and offers very simple circuit implementations through a series connection of integrators with a single nonlinearity. The multi-output chaotic signals are digitized prior to the digit-combination process, yielding a 20,000-bit sequence [4]. Some statistical tests for randomness, including Chi-square goodness-of-fit test, Gap test, Poker test, Coupon-collectors test, Permutation test, Run test for randomness, Wilcoxon signed rank test, Sign test, Jarque-Bera test and Lilliefors test, are also included.

II. HIGH-DIMENSIONAL AUTONOMOUS CHAOTIC SYSTEM

Hyperchaotic attractor is usually characterized as a chaotic attractor with more-than-one positive Lyapunov exponent. The particular dynamical property of such attractor is the expansion in all directions, giving rise to extremely complex chaotic dynamics. Consequently, the hyperchaotic attractor offers a higher degree of randomness and also higher unpredictability. In this work, Lorenz hyperchaotic attractor [5] has been chosen as a basis higher-order autonomous chaotic system for implementing a TRG, i.e.

$$\begin{aligned}\dot{x}_1 &= a\cdot(x_2 - x_1) + x_4,\\ \dot{x}_2 &= -x_1\cdot x_3 + r\cdot x_1 - x_2,\\ \dot{x}_3 &= x_1\cdot x_2 - b\cdot x_3,\\ \dot{x}_4 &= -x_1\cdot x_3 + d\cdot x_4.\end{aligned} \quad (1)$$

where x_1, x_2, x_3, x_4 are system state variables and *a, b, r, d* are adjustable positive parameters. In terms of dynamical analysis, the equilibria of the system (1) can be found through a by setting all equation to zero as follows;

$$\begin{aligned}0 &= a\cdot(x_2 - x_1) + x_4,\\ 0 &= -x_1\cdot x_3 + r\cdot x_1 - x_2,\\ 0 &= x_1\cdot x_2 - b\cdot x_3,\\ 0 &= -x_1\cdot x_3 + d\cdot x_4.\end{aligned} \quad (2)$$

In (2), the system possesses three equilibrium points given by

$$\begin{aligned}P^0(x_{1_E}, x_{2_E}, x_{3_E}, x_{4_E}) &= P(0,0,0,0),\\ P^+(x_{1_E}, x_{2_E}, x_{3_E}, x_{4_E}) &= P\left(+\sqrt{bk}, +\frac{r\sqrt{bk}}{k+1}, +\frac{brk}{b(k+1)}, +a\sqrt{bk}\left(1-\frac{r}{k+1}\right)\right),\\ P^-(x_{1_E}, x_{2_E}, x_{3_E}, x_{4_E}) &= P\left(-\sqrt{bk}, -\frac{r\sqrt{bk}}{k+1}, +\frac{brk}{b(k+1)}, -a\sqrt{bk}\left(1-\frac{r}{k+1}\right)\right).\end{aligned} \quad (3)$$

where the parameter k is designated as $k = ad(1-r)/(r-ad)$. Based on the equilibrium points shown in (3), the system (1) is linearized and the Jacobian matrix (*J*) is defined as

$$J = \begin{pmatrix} -a & a & 0 & 1\\ -z+r & -1 & -x & 0\\ y & x & -b & 0\\ -z & 0 & -x & d\end{pmatrix} \quad (4)$$

Applying the three equilibrium point described in (4) into this Jacobian matrix one at a time and analyzing $|\lambda I - J| = 0$ reveal a similar result of a characteristic polynomial, i.e.

$$m_4\lambda^4 + m_3\lambda^3 + m_2\lambda^2 + m_1\lambda + m_0 = 0 \quad (5)$$

where m_0, m_1, m_2, m_3, and m_4 are constants. In order to investigate the effects of system parameters and basic dynamic properties, numerical simulations have been performed in MATLAB using the initial condition of (x_0, y_0, z_0, w_0) = (0.1, 0.1, 0.1, 0.1). In fact, the initial condition is not crucial, and can be selected from any point that lies in the basin of attractor. In order to find the control parameter *b* that offers the maximum values of chaoticty and complexity. The system (1) can be formulated using the specific value at a = 10, b =8/3, r = 28, d = 1.3. Fig.1 shows the bifurcation diagram of the peak of z (z max) versus the parameter *b*. It is seen in Fig.1 that the system exhibits a period-doubling route to chaos. The chaoticity is a measure of the greatest *LE*, which is the average rate of growth of the distance between two nearby initial conditions that grows exponentially in time when averaged along the trajectory, leading to long-term unpredictability property. In addition, Fig.2 (a) shows the plots of the Kaplan-Yorke Dimension versus the parameter *b*. The chaoticity is a measure of the greatest LE, which is the average rate of growth of the distance between two nearby initial conditions that grows exponentially in time when averaged along the trajectory, leading to long-term unpredictability property. The

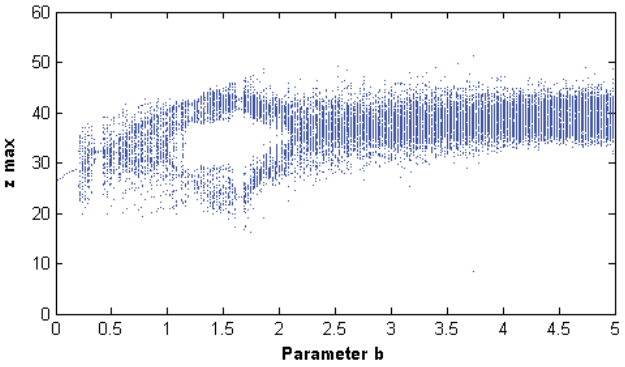
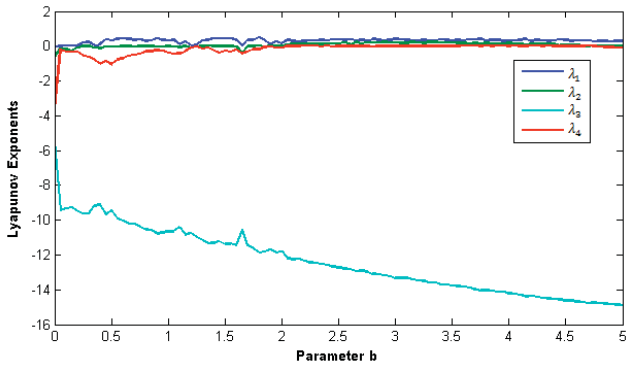
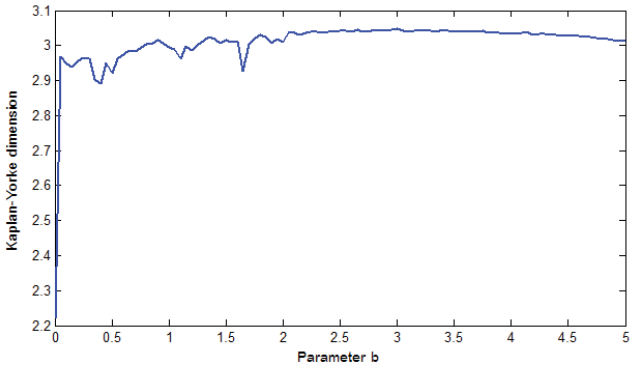


Figure 1. A bifurcation diagram exhibiting a period-doubling route to chaos of the peak of *z* ('z max') versus the parameter *b*.



(a)



(b)

Figure 2. (a) Plots of the maximum positive Lyapunov exponent versus the parameter *b*, (b) Plots of the Kaplan-Yorke Dimension versus the parameter *b*.

Lyapunov exponents can be employed for the estimation of the rate of entropy production and the fractal dimension commonly known as Kaplan-Yorke dimension D_{KY}, i.e.

$$D_{KY} = j + \frac{1}{|LE_{j+1}|}\sum_{i=1}^{j} LE_i = k + \frac{LE_1 + LE_2}{|LE_3|}. \quad (6)$$

where *k* is a non-integer constant, and typically equals to 3 for three-dimensional chaotic systems. In the time domain, Fig. 3

(a) shows apparently chaotic waveforms of signals x and y whilst an apparently continuous broadband spectrum log|*x*| and

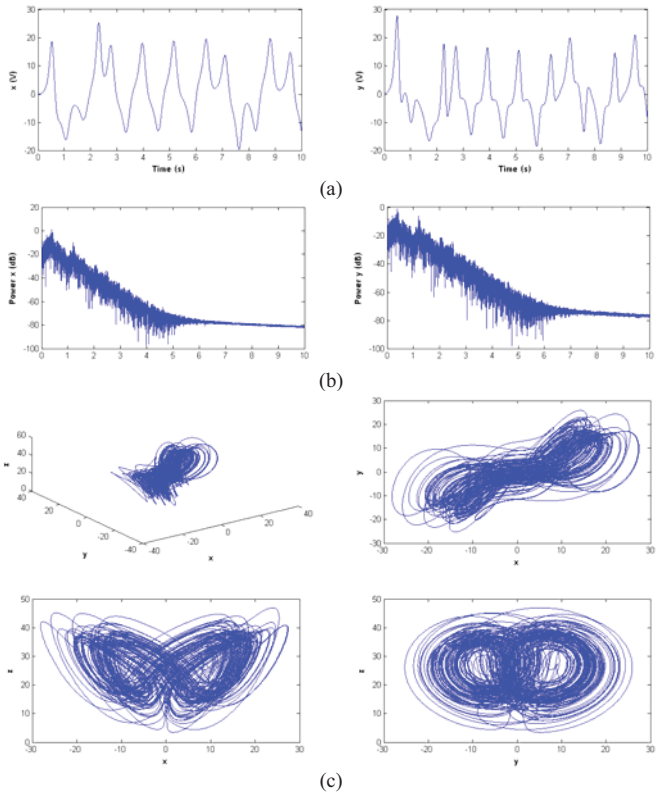


Figure 3. (a) Example of chaotic signals x and y in time domain, (b) examples of spectral characteristics of signal x and y, (c) hyperchaotic attractors.

log|*y*| in the frequency domain is shown in Fig. 3(b). It can be seen from Fig. 3 (a) and (b) that the system exhibits extremely-chaotic behaviors. In addition, by using the Fourth-order Runge-Kutta method to solve the system (1) with time step size of 0.001, the chaotic attractors are displayed in Figs. 3(c) for a three-dimensional view, an *x*–*y* phase plane, an *x*–*z* phase plane and a *y*–*z* phase plane, respectively. It is seen that the attractor of three-dimensional view remains confined to the positive half-space of the *z*-axis.

III. Proposed TRG using Hyperchaotic System

Random bit generators have been employed in applications where the unpredictability is a key requirement. Generally, electronic noises, i.e. thermal and shot noises, and time jitter are usually the only available randomness sources. All noise sources, however, produces a bit stream that usually shows statistical defects due to bandwidth limitation, fabrication tolerances, ageing and temperature drifts, an also deterministic disturbances. Consequently, the noise source should be followed by a strong digital post-processing. Fig. 4 shows the proposed TRG using the Lorenz hyperchaotic system described in (1). The hyperchaotic system is used as a noise-like source, giving randomness through the chaotic signal. It can be considered from (1) that there are four outputs, i.e *x*, y, z, and w, of the hyperchaotic systems. Such a hyperchaotic signal source generates an analog signal, which is input into a digitizer. In order to increase randomness, all outputs have

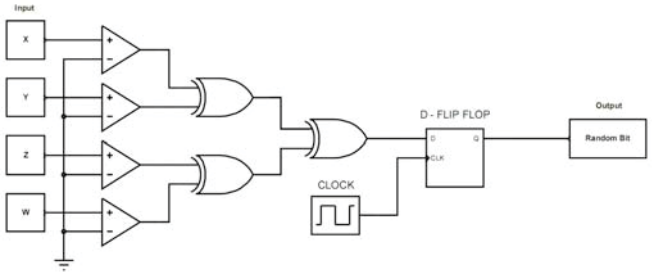


Figure 4. System block diagram of the proposed random bit generator.

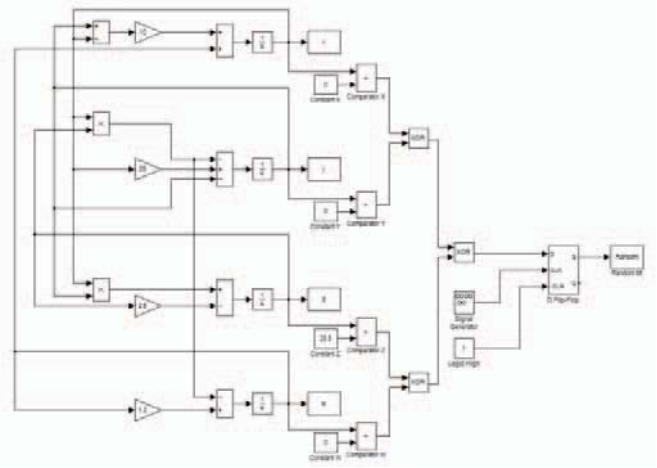


Figure 5. Implementation of the proposed random bit generator using SIMULINK in MATLAB.

been employed through the post processing. The digitizer is implemented by four comparators, sampling the four analog signals and converting the sampled values into a stream of random bits. The non-deterministic source and the digitizer together form the digitized noise source. The random bitsare then fed into the XOR gates, operating as a post-processing to combine into a single bit stream. The frequency of the output bit stream is set by the D-flip-flops. Fig.5 shows the Implementation of the proposed random bit generator using SIMULINK in MATLAB. Fig.6 (a) and (b) shows the output signal before and after sampling through the D-flipflop, respectively. It is seen from Fig.6 that the output is obviously random.

IV. Tests for Randomness

Redundancy in an information source can be caused by two sources, namely a difference in the probabilities of the two binary symbols, and a memory of an information source. The simplest redundancy reduction technique that affects both sources of randomness is XOR correction. It must be stressed that XOR correction can improve statistical properties of the input bit streams only if the input bits are statistically independent. The multi-output chaotic signals are digitized prior to the digit-combination process, yielding a 20,000-bit sequence [5]. Some statistical tests [6-7] for randomness,

including Chi-square goodness-of-fit test, Run test for randomness, Wilcoxon signed rank test, Sign test, Jarque-Bera test and Lilliefors test, are also included.

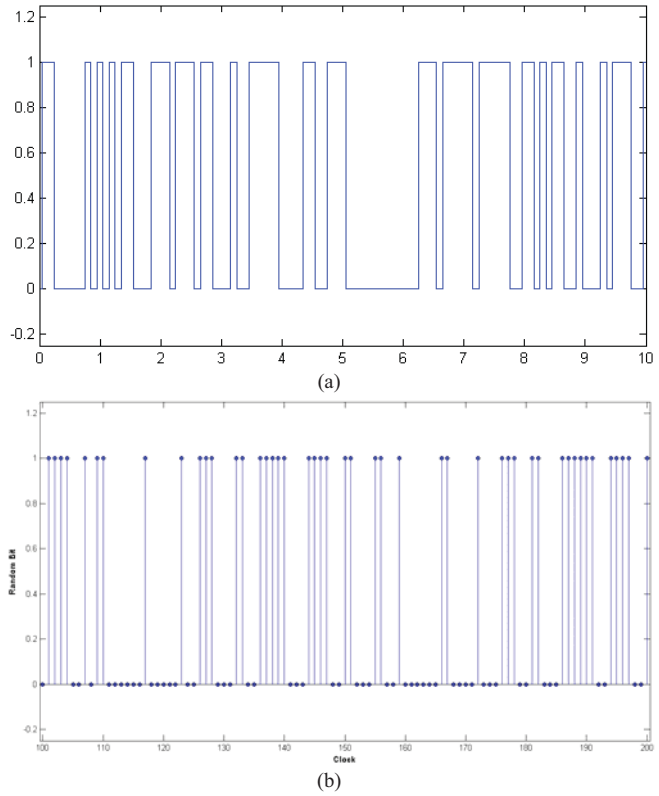


Figure 6. (a) Digitized signal from the our outputs of the Lorenz hyperchaotic system, (b) Sampled signal through D-Flipflop.

```
% Statistical randomness tests for 20,000 bits.
SetTime  = 1000; T = 0.05;
m_Random = s_Random;
m_Clock  = s_Clock;
Pulse    = 1000*T;
Lenght   = (SetTime*1000)/Pulse;
for   Count = 1 : 1 : Lenght
            OutputRandom(1,Count)  =
            double(m_Random(Count*Pulse));
      OutputTime(1,Count) = Count;
end
% Chi-square goodness-of-fit test
[chi2gof_h, chi2gof_p] = chi2gof(OutputRandom);
% Run test for randomness
[runstest_h, runstest_p] = runstest(OutputRandom);
% Wilcoxon signed rank test
[signrank_p, signrank_h] = signrank(OutputRandom);
% Sign test
[signtest_p, signtest_h] = signtest(OutputRandom);
% One-sample and paired-sample t-test
[ttest_h, ttest_p] = ttest(OutputRandom);
% Jarque-Bera test
[jbtest_h, jbtest_p] = jbtest(OutputRandom);
% Lilliefors test
[lillietest_h, lillietest_p] = lillietest(OutputRandom);
```

Figure 7. Statistical tests program in MATLAB.

TABLE I. SUMMARY OF STATISTICAL TESTS FOR RANDOMNESS.

Test Methods	Test Results
Chi-square goodness-of-fit test	Passed
Run test for randomness	Passed
Wilcoxon signed rank test	Passed
Sign test	Passed
One-sample and paired-sample t-test	Passed
Jarque-Bera test	Passed
Lilliefors test	Passed

Fig. 6 (a) shows the digitized signal from the four outputs of the Lorenz hyperchaotic system. Fig. (b) shows the sampled signal through D-Flipflop. Fig.7 shows the statistical tests program in MATLAB. Table 1 summarizes the statistical tests results for randomness. It is iseen in Table 1 that the proposed random bit generator has passed all methods.

V. CONCLUSIONS

This paper has presented a new hardware TRB generator using a high-dimensional autonomous Lorenz system. The realization of high-dimensional hyperjerk system provides multi-output signal depending on the dimension degree, and offers very simple circuit implementations through a series connection of integrators with a single nonlinearity. The multi-output chaotic signals are digitized prior to the digit-combination process, yielding a 20,000-bit sequence. The statistical tests that prove the randomness are achieved by various standard test methods such as Chi-square goodness-of-fit test, Run test for randomness, Wilcoxon signed rank test, Sign test, Jarque-Bera test and Lilliefors test. the proposed random bit generator has passed all methods. This work offers not only a cost-effective hardware implementation, but also high-degree of randomness for applications in cryptography used in information security.

REFERENCES

[1] M. Drutarovsk and P. Galajda, “Chaos based true random number generator embedded in a mixed-signal recon-figurable hardware,” Journal of Electrical Engineering, Vol. 57, pp. 218−225, April 2006.

[2] AIS 31, “Functionality classes and evaluation methodol-ogy for true (physical) random number generators ver 3.1,” Bundesmat fur Sicherheir in der Information technik (BSI), Bon, Germany, September 2001.

[3] M. E. Yalcin, J. K. Suykens, and J. Vandewalle, “True random bit generation from a double scroll attractor,” IEEE Transactions on Circuits and Systems I: Funda-mental Theory and Applications, Vol. 51, pp. 1395-1404, July 2004.

[4] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. aranouovo, “A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC,” IEEE Transactions on Computers, Vol. 52, pp. 403-409, April 2003.

[5] M. E. Yalcin, J. K. Suykens, and J. Vandewalle, “True random bit generation from a double scroll attractor,” IEEE Transactions on Circuits and Systems I: Funda-mental Theory and Applications, Vol. 51, pp. 1395-1404, July 2004.

[6] G. Gonnet. Repeating Time Test for U(0,1) Random Number Generators. Technical report, Informatik, ETH, Zurich, May 2003. URL http://www.inf.ethz.ch/ personal/gonnet/RepetitionTest.html.

[7] G. Marsaglia. The diehard test suite, 2003. URL http://www.csis.hku.hk/ ~diehard/.