A Cost-Effective True Random-Bit Generator using Compact Chaotic Circuit

Asst. Prof. Dr. Wimol San-Um and Mr. Patinya Ketthong[1]
Dr. Surapong Pongpayapinpanich[2]
Lt.Col. Asst. Prof. Dr.Pratya Areekul[3]

[1]Intelligent Electronics Systems Research Laboratory
Computer Engineering Program, Faculty of Engineering,
Thai-Nichi Institute of Technology (TNI)
E-mail Addresses: wimol@tni.ac.th and patinya.ket@gmail.com
[2]Faculty of Engineering Ramkhamhaeng University
[3]Department of Mathematics and Computer Science
Chulachomklao Royal Military Academy (CRMA)

Abstract : A cost-effective true random bit generator using compact chaotic oscillator is presented. The chaotic circuit with minimal counts of eleven electronic components is employed as a source of deterministic random signal. Chaotic signals are digitized by a 10-bit analogue-to-digital converter in a microcontroller prior to a quadri-shift register based post-processing system. Chaos dynamics are presented including waveforms in time and frequency domains, chaotic attractor, and bifurcation diagram. Autocorrelation, histogram, and NIST standard tests suite have been realized for statistical investigations and analysis for randomness of the generated binary sequence, and the sufficient length of 1,000,000 bits successfully passed all NIST standard tests. The proposed true random bit generation system can be implemented through an integration of minimal analogue circuit and simple embedded digital techniques for cryptography in secured communications.

Keywords : True Random-Bit Generator, Chaotic Jerk Oscillator, NIST Tests Suite.

1. Introduction

Information security has become a major issue under consideration for both research and practical applications due to the rapid advancement of Information and Communication Technology (ICT). Cryptography has therefore been utilized as one of a solution to information security where a True-Random-Bit (TRB) generator is necessary for confidential

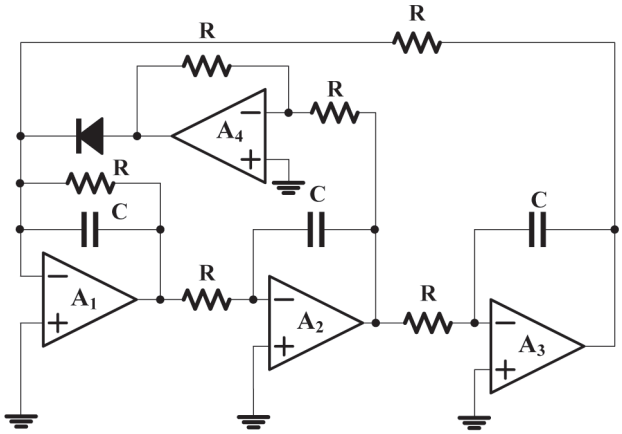

Fig.1 The new chaotic jerk circuit recently proposed by Sprott (2011).

key generation or in some intrinsic computation algorithms [1]. Existing hardware TRBs were commonly implemented by random physical phenomenon such as the amplification of direct resistor noises [2] or jitter noises of digital clock signals [3]. Despite the fact that such limitations can be conquered through proper custom circuits, randomness extraction is still a challenging topic in the designs

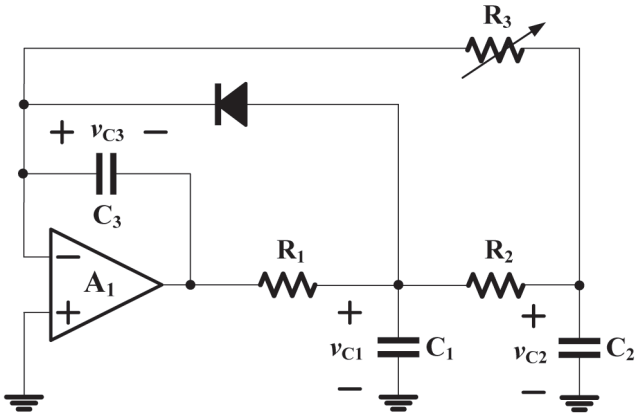

Fig.2 Proposed new compact chaotic jerk circuit with minimal components.

based on such devices. Recently, chaotic systems have been of great attention due to various potential applications. 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 [4]. The use of chaotic signals as sources of randomness in hardware TRBs has been suggested, including, for example, discrete-time chaotic maps [5], switched-capacitor chaotic circuit [6], non-autonomous chaotic circuit [7], and double-scroll attractor [8]. Nonetheless, these circuits are relatively complex requiring large counts of electronic components. As for a promising alternative, simple chaotic circuits in a category of resistor(s), capacitor(s), amplifier(s), and diode(s), have been of much interest due to mini-

mal electronics components and suitability for integrated circuits. Chaotic circuits in such a category [8] have been found in a single third-order ordinary differential equation of a jerk form where the term 'jerk' comes from the fact that successive time derivatives of displacement are velocity, acceleration. Recently, Sprott [9] presents a new chaotic jerk circuit shown in Fig.1 based on the jerk equation is in which chaos occurs for α = 0.27 [10]. Although the circuit in Fig.1 offers relatively simple implementation with equal values of resistors and capacitor, large counts of fourteen electronic components are required involving four op-amps.

In this paper, a new compact resistor-capacitor network based chaotic circuit with minimal counts of eleven electronic components is designed and subsequently utilized as a source of deterministic random signals. The proposed hardware true random bit generation system digitizes the generated chaotic signals by a 10-bit A/D converter in a microcontroller prior to a quadri-shift register based post-processing system. Statistical investigations and analysis for randomness of the generated binary sequence are achieved by autocorrelation, histogram, and NIST standard tests suite.

2. Proposed Compact Chaotic Oscillator

Fig.2 shows the proposed resistor-capacitor network based chaotic circuit. The circuit comprises only single op-amps A1. Resistors (R1, R2, R3) and capacitors (C1, C2, C3) form a low-pass network in a signal path of a closed loop. A diode is employed as a nonlinear device with an inherent exponential function. Unlike the circuit in Fig.1 in which circuit analyses can be achieved straightforward through successive derivatives of three cascade integrators, the circuit analysis of Fig.2 is slightly more complicated, requiring a systematic analysis through Kirchhoff's laws. By setting R=R1=R2 and C=C1=C2, the resulting system of equations is found as follows;

$$\begin{bmatrix} \dot{V}_{C2} \\ \dot{V}_{C1} \\ \dot{V}_{C3} \end{bmatrix} = \begin{bmatrix} -(1/\tau_0 + 1/\tau_2) & 1/\tau_0 & 0 \\ 1/\tau_0 & -2/\tau_0 & 1/\tau_0 \\ -1/\tau_1 & 0 & 0 \end{bmatrix} \begin{bmatrix} V_{C2} \\ V_{C1} \\ V_{C3} \end{bmatrix} + \begin{bmatrix} 0 \\ -I_D/C_2 \\ -I_D/C_1 \end{bmatrix} \quad (1)$$

where time constants $\boldsymbol{T}_0$=C_1R=C_2R, $\boldsymbol{T}_1$=C_3R_3, and $\boldsymbol{T}_2$=C_2R_3. The diode equation is given by ID=I_S(exp[VC_1/(nV_T)]-1), nV_T is a scaled thermal voltage, I_S is a saturation current of a diode. Equation (1) can also be expressed in terms of a normalized dynamical representation using $\boldsymbol{T}$=t/$\boldsymbol{T}_0$ as

(2)

$$\begin{bmatrix}\dot{X}\\ \dot{Y}\\ \dot{Z}\end{bmatrix}=\begin{bmatrix}-(D+1) & 1 & 0\\ 1 & -2 & 1\\ -1/A & 0 & 0\end{bmatrix}\begin{bmatrix}X\\ Y\\ Z\end{bmatrix}+\begin{bmatrix}0\\ -BI_D\\ -CI_D\end{bmatrix} \quad (2)$$

where normalized state variables are $X=V_{C2}/nV_T$, $Y=V_{C1}/nV_T$, $Z=V_{C3}/nV\boldsymbol{T}$, = $dX/d\boldsymbol{T}$, =$dY/d\boldsymbol{T}$, and =$dX/d\boldsymbol{T}$. System constants are $A = \boldsymbol{T}_0/\boldsymbol{T}_1$, $B = \boldsymbol{T}_0/_{C2}$, $C= \boldsymbol{T}_0/_{C3,}$ $D = \boldsymbol{T}_0/\boldsymbol{T}_2$. It is apparent in (2) that the equation is a third-order dynamical system with divergence of flow as follows;

$$\nabla.V=\frac{\partial\dot{x}}{\partial x}+\frac{\partial\dot{y}}{\partial y}+\frac{\partial\dot{z}}{\partial z}=-D-3-BI_D \quad (3)$$

Equation (3) indicates that the proposed chaotic circuit is a dissipative system with an exponential rate of contraction of $dV/dt=\exp(-D-3-BI_D)$. In other words, a volume element V0 becomes smaller by the flow in time t into a volume element $V_0\exp(-t)$. Each volume containing the trajectories shrinks to zero as $t\longrightarrow\infty$ at an exponential rate of -D-3-BID. System orbits are ultimately confined into a specific limit set of zero volume, and the system asymptotic motion settles onto an attractor of the system.

3. Proposed True Random Bit Generator

Fig.3 shows the proposed hardware true random bit generation system. Initially, the input chaotic signals v_{C1} and v_{C2} are obtained from voltages across the capacitors C_1 and C_2, respectively. Such two voltage signals are buffered in order to maintain the dynamical stability of the chaotic circuit. The summing amplifier has been designed as a signal conditioning circuit in order to (1) adjust the amplitudes of the voltages v_{C1} and v_{C2} to be approximately equal, (2) combine the two signals into a single output vS with appropriate gain, and (3) shift the DC offset of vS for setting the signal swing in the voltage range of 0V to 5V required by the microcontroller specification. The 10-bit A/D converter embedded in the microcontroller has been realized for converting vS into a digital bit stream before transferring to the computer through interfacing board. The post-processing is fully accomplished by a designed program written in C-

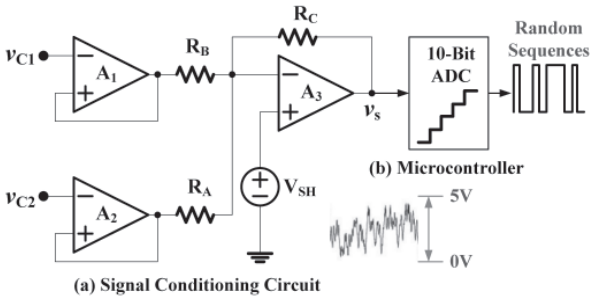

Fig.3 Proposed hardware true random bit generation system.

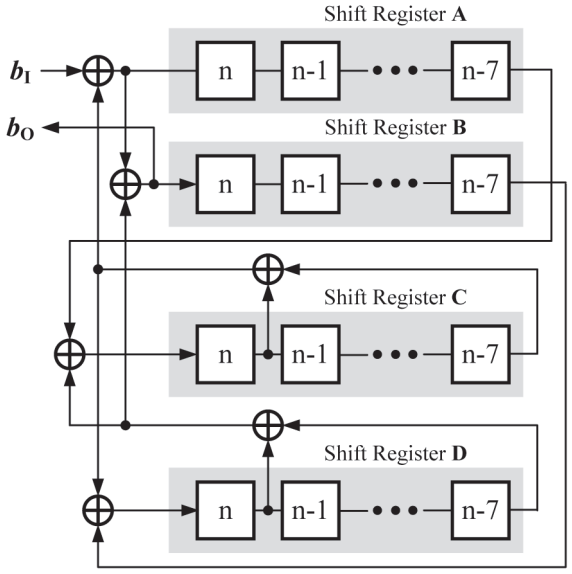

Fig.4 The quadri-shift register (QSR) based post-processing.

language, and the output random binary sequence can be use through this program, depending on specific applications.

In particular for post-processing, there has been a number commonly-used techniques such as XOR corrector, Von Neumann corrector, or Linear Feed-back Shift Registers (LFSRs), this paper realizes a quadri-shift register (QSR) based post-processing [11] with a particular structure of four shift registers A, B, C, and D. This scheme is basically based on XOR operations incorporating with linear shift registers. The principle is to perform XOR operation between the bits coming from the TRB and those bits coming from the delayed bit-stream memorized into a linear shift register. The operation is also repeated several times and a few numbers of XORs are inserted between the different shift registers to increase the complexity of each stage.

3. Simulation and Experiment Results

Dynamics properties of Eq. (1) were numerically simulated in MATLAB using Fourth-order Runge-Kutta method with time step size of 1x10-6. Initial conditions were set at (0.1, 0, 0), which lies in the attractor basin. Electronic component values were set to R_1=R_2 =470Ω, C_1=C_2=1μF, and C_3 =10nF. The Diode is 1N4001 using Pspice models I_S = 29.5 x10^{-9} A, V_T = 25.85x10^{-3}V, and n=1.96. As Equation (1) has a single equilibrium point at (0,0,0), the corresponding numerical Jacobian matrix (J) and eigenvalues {λ_1, λ_2, λ_3} are

$$J = \begin{bmatrix} -4430 & 2300 & 0 \\ 2130 & -4260 & -2130 \\ 229890 & 60 & 0 \end{bmatrix} \text{and} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix} = \begin{bmatrix} -13672 \\ 2495 + j8721 \\ 2495 - j8721 \end{bmatrix} \quad (4)$$

It is evident in (4) that such an equilibrium point exhibits the saddle focus node as the eigenvalue λ_1 is a negative real value while the eigenvalues λ_2 and λ_3 are a pair of complex conjugate with positive real part. Fig.5 shows the bifurcation diagram exhibiting a period-doubling

route to chaos of the peak of V_{C2} versus the bifurcating parameter R3 over the region [100Ω, 500Ω]. The chaotic attractors where parameter R_3 is 435 Ω, are show in Fig.6 for a three dimensions view. Chaotic waveforms are show in Fig.7

In the experiments, component values are R_1=R_2=470±1%Ω,C_1=C_2= 1±20% μF, and C_3 =10±5% nF. The Capacitors C_1, C_2 are electrolytic capacitor and C_3 is polypropylene capacitor. The op-amp is uA741 with dual power supply

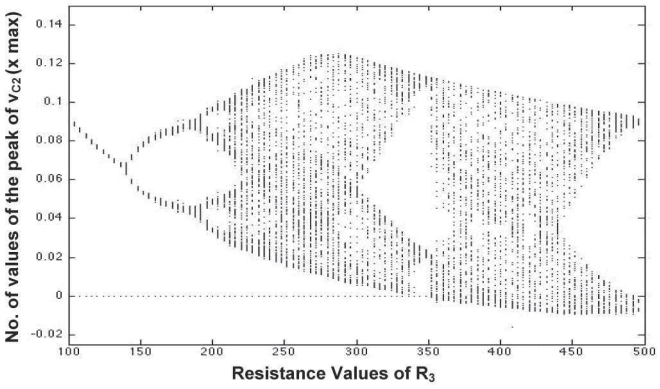

Fig.5 The bifurcation diagram of the bifurcation diagram exhibiting a period-doubling route to chaos of the peak of vC_2 versus the bifurcating parameter R_3.

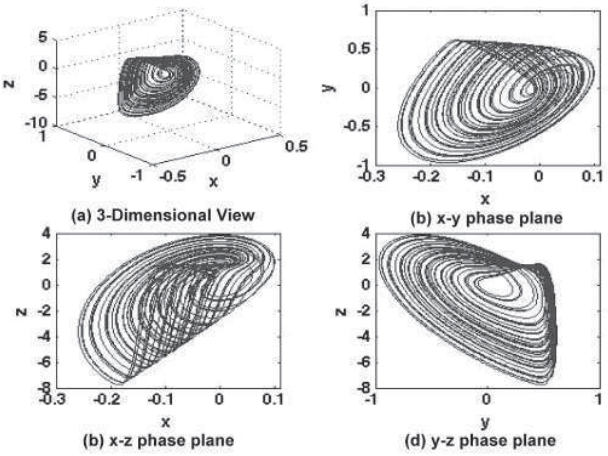

Fig.6 Chaotic attractor where R3 = 435 Ω, (a) Chaotic attractor in 3-dimension view, (b) Chaotic attractor constructed by x and y, (c) Chaotic attractor constructed by x and z, (d) Chaotic attractor constructed by y and z.

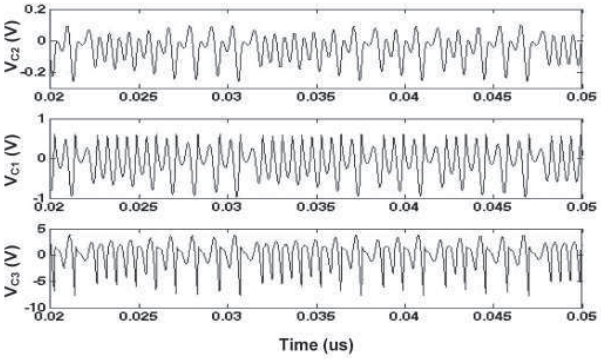

Fig.7 Chaotic waveforms in time-domain where R_3 = 435 Ω.

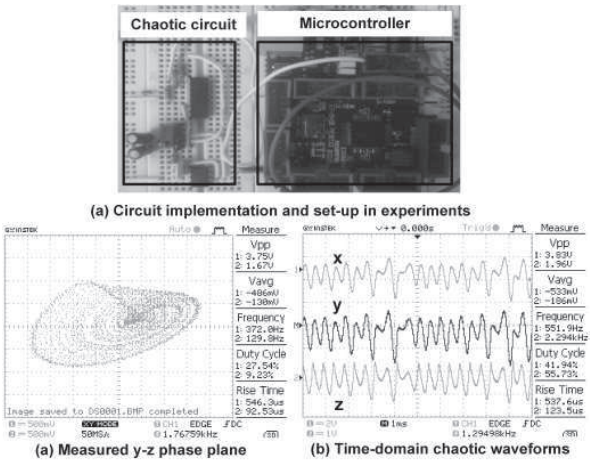

Fig.8 (a) The circuit implementation on-board, (b) Chaotic waveforms in time-domain, (c) Chaotic attractor constructed by v_{C1} and v_{C2}.

voltage of ±12V. The microcontroller is PIC18F8722 with operating clock frequency of40MHz, and MAX232 is used to interface between this microcontroller and computer. The A/D conversion process employs a clock frequency of 1.25 MHz. Fig. 8 (a) shows the circuit implementation on-board in the experiment. Chaotic waveforms in time-domain are demonstrated in Fig.8 (b), including the voltages v_{C1}, v_{C2} and $v_S=v_{C1}+v_{C2}$. It can primarily be seen in Fig. 8 (b) all signals are chaotic as random amplitudes and frequencies are apparent. As for illustrations, the chaotic attractor constructed by v_{C1} and v_{C2} is shown in Fig. 8 (c), resembling a single-scroll attractor topology and corresponding to the simulated result in Fig.6 (b).The results shows that the circuit is ready for use in the post-processing in the succeeding stages.

4. Statistical Analysis

Histogram and autocorrelation were utilized as two basic methods in primary investigations on randomness of a binary sequence with a sufficiently long bit length of N=1,000,000. Fig.9 (a) and (b) show the histograms of pre-processing

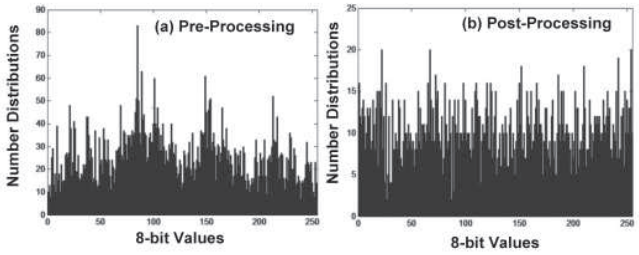

Fig.9 Simulated histograms; (a) Preprocessing,(b) Post-processing.

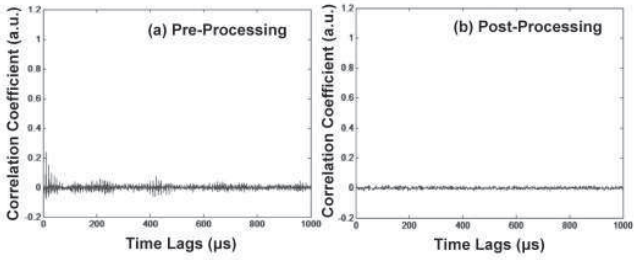

Fig.10 Simulated autocorrelation;
(a) Preprocessing,
(b) Post-processing.

and post-processing binary sequences, respectively. As expected, the binary sequence from the proposed chaotic jerk system in Fig.9 (a) provides bit contributions over encoded numbers in the range [0,255] meanwhile the binary sequence from post-processing system in Fig.9 (b) improve bit contributions efficiently. Figs.10 (a) and (b) depict simulated results of autocorrelation of pre-processing and post-processing binary sequences, respectively. Typically, the correlation of a sequence is employed to examine the similarity between observations as a function of the time separation between data values, and is expected to be unity at zero and close to zero at all other values. It is apparent in Fig.10 (b) that the correlation of post-processing is relatively close to zero for most values.

As for standard statistical tests, the NIST statistical tests suite [12] issued by the National Institute of Standards and Technology has been realized in order to evaluate the randomness of binary sequences of N=1,000,000 bits generated by the proposed random bit generator using chaotic jerk circuit. Such tests attempt to extract the presence of a pattern that indicates non-randomness of the sequences through probability methods described in terms of p-value. For each test in this paper, this p-value indicates the strength of evidence against perfect randomness hypothesis, i.e. a p-value greater than a typical confidence level of 0.01 implies that the sequence is considered to be random with a confidence level of 99%. Table 1 summaries NIST test results, indicating that the generated sequence passed all standard 15 tests.

Table 1: A summary of NIST test results.

No.	Test Methods	*p*-value	Results
1	Mono-bit	0.41450	Success
2	Frequency Block	0.06353	Success
3	Runs	0.78357	Success
4	Longest Run of Ones Block	0.98222	Success
5	Binary Matrix Rank	0.67479	Success
6	Discrete Fourier Transform	0.06782	Success
7	Non-overlapping Template Matching	0.13846	Success
8	Overlapping Template Matching	0.62031	Success
9	Universal Statistical	0.09889	Success
10	Linear Complexity	0.20068	Success
11	Serial	0.95650	Success
12	Approximate Entropy	0.63124	Success
13	Cumulative Sums	0.53226	Success
14	Random Excursions	0.08583	Success
15	Random Excursions Variant	0.04633	Success

5. Conclusion

A true random bit generator using a compact chaotic circuit has been presented and the sufficient length of 1,000,000 bits has successfully passed all 15 NIST standard tests at a confidence level of 0.01. The designed chaotic circuit employed as a source of randomness has offered minimal counts of eleven electronic components. Embedded analog-to-digital converter and QSR based post-processing have been realized using a microcontroller and a special TRB program. In comparison to other existing system, the proposed circuit generates a true random bit like other existing technique with much lower cost. For instance, the quantum based-systems require a very expensive quantum generator which is made from a semiconductor while this work utilizes simple discrete components which are commercially available in markets. Therefore, the cost is approximately 80% reduced from other approaches. The proposed system offers a potential alternative to simple hardware true random bit generation for voice, text, image, or video cryptography in secured communications.

References

(1) C. Petrieand and J. Connelly, "A noise-based IC random number generator for applications in cryptography", IEEE Trans. Circuits and Systems I, Vol.47, No. 5, pp. 615-621, 2000.

(2) M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouvo,"A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC", IEEE Trans. on Computers, Vol.52, No.4,2003, pp.403-409.

(3) G.Chen and T.Ueta, "Chaos in Circuits and Systems", World Scientific, 2002.

(4) N.K. Pareek, V.Patidar, and K.K.Sud, "A Random Bit Generator Using Chaotic Maps", Inter. Jour. of Network Security, Vol.10, Issue.1, pp. 32–38, 2010.

(5) M. Drutarovsky and P. Galajda, "A Robust Chaos-Based True Random Number Generator Embedded in Reconfigurable Switched-Capacitor Hardware", Radio engineering Journal, Vol.16, No.3, 2007, pp.120-127.

(6) Mustak , E. Yalcin, Johan A. K. Suykens, and JoosVandewalle, "True Random Bit Generation From a Double-Scroll Attractor", IEEE Trans. on Circuits and Systems I, Vol. 51, Issue. 7, 2004, pp.1395-1404.

(7) J.C. Sprott, "A New Chaotic Jerk Circuit", IEEE Trans.on Circuits and systems II, Vol. 58, No. 4, 2011, pp. 240-243.

(8) F. Pareschi, R. Rovatti, and G. Setti, "Simple and Effective Post-Processing Stage for Random Stream Generated by a Chaos-Based RNG", Proceedings of Inter. Sym. on Nonlinear Theory and its Applications, 2006, pp. 383–386.

(9) National Institute of Standards and Technology, "A Statistical Test Suit for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Special Publication 800-22 Revision 1a, 2010.