Random Number Generation using Photovoltaic Cell Chaotic Output

Sai Venkatesh Balasubramanian

Sree Sai Vidhya Mandhir, Mallasandra, Bengaluru-560109, Karnataka, India.
saivenkateshbalasubramanian@gmail.com

Abstract

The basic components for most secure computing and communication systems of today are random number generators. The present work purports to a radically novel approach to the design and implementation of random number generators. Firstly, a nonlinear analysis of the photovoltaic cell open circuit voltage is performed, and the presence of chaos is ascertained using standard measures such as Lyapunov Exponents. Following this, the chaotic output is adapted into a bit stream and randomness tests from the NIST Suite are performed. It is seen that the chaotic output indeed passes all the randomness tests. The histogram of the output reveals similarities with Gaussian Normal Distributions, confirming the stochastic nature. Thus, the photovoltaic cell output is a potential power generating random number generator, drastically differing from the conventional power dissipative random number generators.

Keywords: Random Number Generators, Photovoltaic Cell, Chaos, Nonlinear Analysis

1. Introduction

One of the growing and critical concerns in the current era of information explosion is the need for secure information and communication systems that protect data from privacy theft and hacking attacks [1, 2, 3, 4, 5, 6]. There has been tremendous progress in this line of thought, with novel techniques such as cryptography and steganography being developed [7, 8]. However, among such techniques, there is always the concern for power dissipation due to the use of complex circuitry to generate random numbers, which form the backbone for most secure communication systems [9, 10, 11, 12, 13, 14, 15].

The present work looks at this problem in an unprecedented, radically new perspective. The key motivation behind the present work is the observation that the open circuit voltage output of a photovoltaic (solar) cell exhibits a DC offset accompanied by highly dynamic fluctuations [16, 17]. When used for solar energy harvesting, these fluctuations are inevitably averaged out by the use of inverters[18, 19]. However, in the present work, we evaluate and characterize the photovoltaic output fluctuations and show that they are highly chaotic by using standard measures such as Lyapunov Exponents and Kolmogorov Entropy [20, 21, 22, 23, 24, 25, 26]. Further, we convert the open circuit chaotic fluctuations into discrete signals using appropriate sampling, and test the output for randomness using standard tests such as those specified by the NIST Test Suite [12]. It is found that the waveform passes the random tests, and that the solar cell chaotic output can indeed be used as a random number generator. The consequence is that, rather than designing a random number generator circuit that would consume power, the present work uses the naturally inherent stochastic properties of a photovoltaic cell output to generate random numbers, that would generate power as a power-cum-random number generator, rather than consuming power. This property, along with the extreme simplicity of the design forms the novelty of the present work.

2. Detecting and Characterizing Chaos in Photovoltaic Output

The photovoltaic cell open circuit output voltage is typically DC viewed as an offset, accompanied by fluctuations. which have been typically dismissed as noise. However, in the present work, we perform nonlinear characterization of the fluctuations, in order to detect the presence of chaos. In order to achieve this, the experimental setup consisting of a 6V, 50mA rated polysilicon photovoltaic cell connected to a digital storage oscilloscope (TektronixTBS 1052B), in a 100W tubelight lit room, corresponding to a diffused lighting scenario, as shown in Fig. (1).

Using the setup, the open circuit voltage waveform 'Voc' is recorded, and qualitative analysis is done. The analysis consists of the time series waveform, magnitude spectrum, polar plot and the phase portrait. While the time series gives a rough idea of the fluctuations, the Fourier Magnitude spectrum and the polar plot helps to distinguish between the noise floor and the chaotic components present in the waveform [27]. The phase portrait outlines the dynamic behavior of the system [20, 21, 22]. These plots are shown in Fig. (2) for the diffused light scenario case.

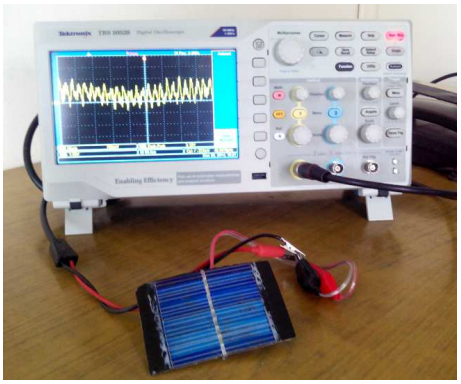

Figure 1: Experimental setup to characterize photovoltaic voltage

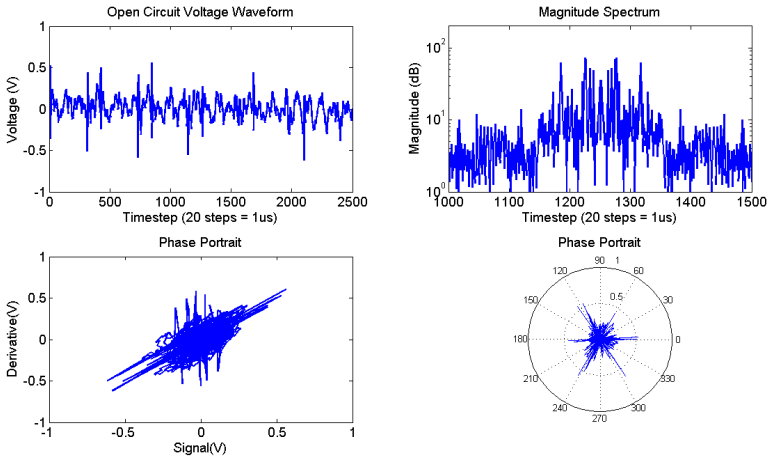

Figure 2: Open Circuit Voltage offset analysis for diffused light scenario

Table 1: Results of NIST Suite Tests for the Chaotic Photovoltaic Output

Statistical Test	P-Value	Proportion	Result
Runs	0.5453	0.9920	Pass
Longest Run	0.2547	0.9930	Pass
Monobit	0.9343	0.9980	Pass
Rank	0.1219	0.9940	Pass
FFT	0.8621	0.9920	Pass
Block Frequency	0.7673	0.9940	Pass
Cumulative Sum	0.1023	0.9700	Pass
Nonperiodic Template	0.2503	0.9880	Pass
Overlapping Template	0.7683	0.9940	Pass
Random Excursions	0.6623	0.9920	Pass
Serial	0.7212	0.9790	Pass
Maurer's Universal	0.2701	0.9910	Pass

The most suitable measure to ascertain the presence of and to characterize chaos in the generated output is the Largest Lyapunov Exponent (LLE), a measure of a system's sensitive dependence on initial conditions [28, 29]. In the present work, Rosenstein's algorithm is used to compute the Lyapunov Exponents λ_i from the voltage waveform, where the sensitive dependence is characterized by the divergence samples $d_j(i)$ between nearest trajectories represented by j given as follows, C_j being a normalization constant [28, 29]:

$$d_j(i) = C_j e^{\lambda_i (i\delta t)} \tag{1}$$

The LLE for the output waveform 'Y' is obtained as 10.0791, the positive value indeed ascertaining the presence of a highly unstable, dynamic chaos.

3. Testing for Randomness in Chaotic Solar Cell Output

In order to test the photovoltaic open circuit output for randomness, the NIST Standard Test Suite (Special Publication 800-22) is used [10, 12]. This suite consists among a number of tests, most significant of which include the Monobit Test, Runs Test, Binary Matrix Rank Test, Template Matching Tests and Maurer's Universal Statistical Test [10, 12]. These tests are performed using MATLAB, by taking the photovoltaic output as a time series, using the sampling frequency of the digital storage oscilloscope. This time series is then converted into a bit stream with an 8-bit resolution.

As a common premise, all the tests focus on the Null Hypothesis framed that the sequence is not random, while testing for uniformity, scalability and consistency [10, 12]. The tests are carried out for 1000 samples in a 1MegaBit dataset, and the expected probability parameter (P-value) should be above 0.0001 with a proportion in the typical range 0.99+/-0.00943 [10, 12]. The results of the tests are tabulated in Table 1.

The results from Table 1 show that the bit sequences obtained from the chaotic photovoltaic output passes the NIST Suite tests, assertively proving its inherent capability to be used as random number generator. In addition to the NIST Tests, the randomness of the Chaotic Signal is also characterized using Histogram plotted in Fig. (3) by taking 100 bins for 2500 samples of the photovoltaic output.

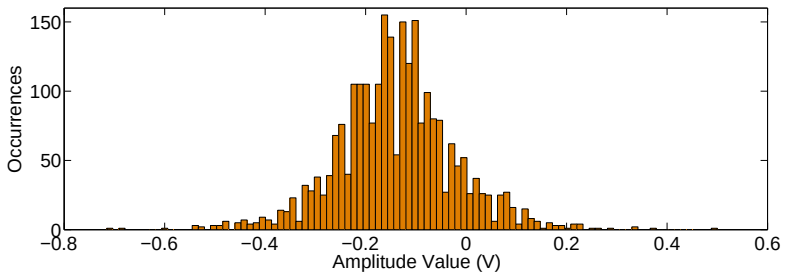

Figure 3: Histogram of Chaotic Photovoltaic Output

From the histogram, it is seen that the distribution of amplitudes approximate a Gaussian based Normal Distribution, with the mean at around -0.1V [10, 12].

4. Conclusion

The open circuit voltage output of a photovoltaic cell is analyzed using the Lyapunov Exponent and the presence of chaos is ascertained, after qualitative analysis using phase portraits, polar plots and spectrum are performed. The generated output is tested for randomness usig the NIST Test suite. It is seen that all the random tests are passed, with sufficient p-values. Finally, a histogram analysis of the chaotic output reveals similarity to Gaussian normal distributions. It is opined that the solar cell chaotic output can thus be used as a random number generator, which provides a radical shift of perspective from power dissipative random number generators to power generating random number generators.

References

[1] M. Hilbert, *How much of the global information and communication explosion is driven by more, and how much by better technology?*, Wiley Journal of the Association for Information Science and Technology, **65**, 856-861 (2014).

[2] G. B. Giannakis, F. Bach, R. Cendrillon, M. Mahoney,J. Neville, *Signal Processing for Big Data*, IEEE Signal Processing Magazine, **31**, 15-16 (2014).

[3] X.Wu, X.Zhu, G.Q.Wu and W.Ding, *Data mining with big data*, IEEE Trans. on Knowledge and Data Engineering **26**,97-107 (2014).

[4] A.McEwan and H.Cassimally, *Designing the Internet of Things*, (Wiley, 2013).

[5] F. Wu, *Advances in Visual Data Compression and Communication: Meeting the Requirements of New Applications*, (CRC Press, US, 2014).

[6] D. Salomon, D. Bryant and Giovanni Motta, *Handbook of Data Compression*, (Springer, California, 2010).

[7] N.Hopper, L.VonAhn and J.Langford, *Provably secure steganography*, IEEE Trans. on Computers **58**,662-676(2009).

[8] P. H. Mahajan, P. B. Bhalerao, *A Review of Digital Watermarking Strategies*, International Journal of Advanced Research in Computer Science And Management Studies, **7** (2014).

[9] L. Shujun, M. Xuanqin and C. Yuanlong, *Pseudo-random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream-Cipher Cryptography*, Springer, **2247**, 316-329 (2001).

[10] A.Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, *Fast physical random bit generation with chaotic semiconductor lasers*, Nature Photonics, **2**, 728-732 (2008).

[11] V. Patidar , K. K. Sud and N. K. Pareek, *A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing*, Informatica, **33**, 441-452 (2009).

[12] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray and S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, (NIST Publications, USA , 2010).

[13] K. D. Wagner, C. K. Chin, and E. J. McCluskey, *Pseudorandom Testing*, IEEE Transactions on Computers, **C-36** (1987).

[14] W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, *An integrated analog/digital random noise source*, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, **44** 521-528 (1997).

[15] L. Blum, M. Blum, and M. Shub. *A simple unpredictable pseudo-random number generator*, SIAM Journal on computing **15** 364-383 (1986).

[16] T. N. Chatterjee. *On the existence of a low-dimensional chaotic attractor in the short term solar UV time series*. Solar Physics. **186**, 421 (1999).

[17] Woyte, V. V. Thong, R. Belmans, J. Nijs. *Voltage fluctuations on distribution level introduced by photovoltaic systems*. IEEE Trans. Energy Conversion. **21**, 202 (2006).

[18] L. Fortuna, M. Frasca, M. G. Xibilia, *Chua's Circuit Implementations: Yesterday, Today and Tomorrow*, World Scientific (2009).

[19] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, U. Parlitz. *Experimental Demonstration of Secure Communications via Chaotic Synchronization*. Int. J Bifurcation Chaos. **2**, 709 (1992).

[20] B. Razavi, *RF Microelectronics*, (Prentice Hall, US, 2011).

[21] K. E. Barner and G. R. Arce, *Nonlinear Signal and Image Processing: Theory, Methods, and Applications*, (CRC Press, U.S, 2003).

[22] E.Bilotta and P.Pantano, *A gallery of Chua attractors*, (World Scientific, Singapore, 2008).

[23] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering* ,(Westview Press, Cambridge, 2008).

[24] M. Ausloos, M. Dirickx, *The Logistic Map and the Route to Chaos: From the Beginnings to Modern Applications*, (Springer, US, 2006).

[25] R. Gilmore and M. Lefranc, *The Topology of Chaos*, (Wiley,US, [2002]).

[26] J. M. T. Thompson and H. B. Stewart, *Nonlinear Dynamics and Chaos* (Wiley,UK, [2002]).

[27] H. Bahouri, J. Y. Chemin, R. Danchin, *Fourier Analysis and Nonlinear Partial Differential Equations*, Springer (2011).

[28] R. G. James, K. Burke, J. P. Crutchfield, *Chaos forgets and remembers: Measuring information creation, destruction, and storage*, Int. J Bifurcation Chaos, **378**, 2124-2127, (2014).

[29] M. T. Rosenstein, J. J. Collins, C. J. De Luca, *A practical method for calculating largest Lyapunov exponents from small data sets*, Physica D, **65**, 117-134, (1993).