A Simple Pseudorandom Bit Generator using Frequency Controlled Digital Chaos

Sai Venkatesh Balasubramanian

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

Abstract

A novel kind of chaos, digital chaos is proposed, and an extremely simple circuit to generate frequency controlled digital chaos using two XOR gates driven by three square signals with mismatched frequencies and duty cycles is designed and implemented in FPGA, with the basic principle that the XOR being a difference circuit, amplifies the mismatches, leading to chaos generation. The presence of chaos is ascertained using Lyapunov Exponent and the effect of driving signal frequency on the chaotic nature is studied. The generated chaotic bit sequence is then tested for randomness using standard tests from the NIST Test Suite. It is found that the generated digital chaotic bit sequence is indeed random, proving capability of the proposed circuit as a pseudo random bit generator for computing and communication applications.

Keywords: Digital Chaos, FPGA, Pseudorandom number Generator, NIST Test.

1. Introduction

The present era is witnessing an explosion of information in terms of both size and coverage [1, 2, 3]. A direct consequence of this is that there is an increased pressure on state-of-the-art computing and communication systems to handle this vast amount of data effectively, without compromising either the capacity or the security aspects [4, 5, 6]. It is in this light that a lot of cryptographic and steganographic techniques have been developed in recent years [7, 8].

The fundamental component in most secure computing and communication systems is a pseudorandom number generator [9, 10, 11, 12, 13]. This component is used as the basis for various operations such as generation of secure 'private' and 'public' keys, and as seed generators for various other encryption and compression techniques [7, 8, 11, 12, 13]. A diverse variety of methods exist for generating such pseudorandom numbers, ranging from designs as fundamental as operational amplifiers (op-amps) and Field Programmable Gate Array (FPGA) based circuits to more complex ones such as chaotic semiconductor LASERs [10, 11, 14, 15]. The generated signals are typically tested for randomness using standard test suites such as the test suite formulated by the National Institute of Standards and Technology (NIST) [12].

The present work purports to a new approach in the design and implementation of pseudorandom bit generators. Specifically, an extremely simple 'digital chaos' generator circuit is designed, which essentially involves two exclusive-or (XOR) gates in tandem, acting on three square wave 'clock' signals, designed using FPGA. It is observed that a mismatch in the frequencies or duty cycles in the input square waves leads to chaos, hence termed 'frequency controlled chaos'. The presence of chaos in the output bit stream is ascertained using the largest Lyapunov Exponent. Finally, the generated bit stream is tested for randomness using standard tests from the NIST suite. It is found from the successful passing of these tests that the generated bit stream possesses sufficient randomness to serve as a pseudo random bit sequence.

The simplicity in design of the frequency controlled digital chaos and hence the pseudorandom bit generator, along with the consistency of randomness observed in the output bit stream forms the novelty of the present work.

2. Design and Implementation of Pseudorandom Bit Generator

2.1. Generation of Digital Chaos

The fundamental element in the proposed pseudorandom bit generator is the frequency dependent digital chaos generation. This is achieved by an extremely simple circuit consisting of 2 XOR gates, as shown in Fig. (1). The three input signals, all of them square waves are represented as A, B and C, whereas the output is Y. Typically, A, B and C have inequal and off-multiple values of frequencies, such that the frequency ratios between any two of them remain non-integers. The key principle is that the XOR Gate, essentially a difference circuit, will amplify the minute differences between the input frequencies, and will in due course, give rise to chaotic output [16, 17, 18, 19, 20, 21, 22]. This principle

directly arises from the sensitive dependence on initial conditions, a fundamental property of chaos, explained by the 'Butterfly Effect' [19, 20, 21, 22].

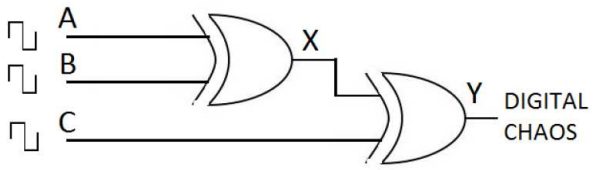

Figure 1: Schematic of the Frequency Controlled Digital Chaos Generator

The proposed schematic is implemented using the Altera Cyclone II 2C20 FPGA, with the base clock frequency set to 27MHz. The input frequencies of A, B and C are set to 26.79 MHz, 9MHz and 3.857MHz, with the duty cycles in percentages as 50, 66.67 and 70 respectively, using appropriate loop counters. The generated output waveform is shown in Fig. (2).

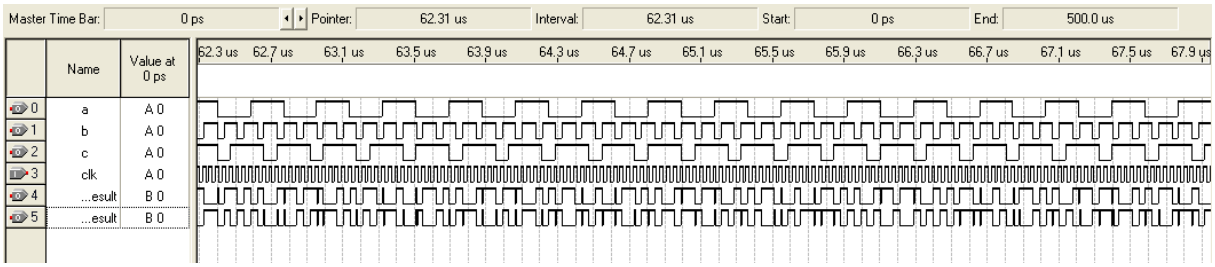

Figure 2: Input Waveforms A, B and C and Output Waveform Y (bottom) of the FPGA Digital Chaos Generator

By using the base clock frequency 27MHz as the sampling rate, the generated output waveform is converted to a bit stream, and the obtained bit stream for the first 2000 samples are plotted in Fig. (3).

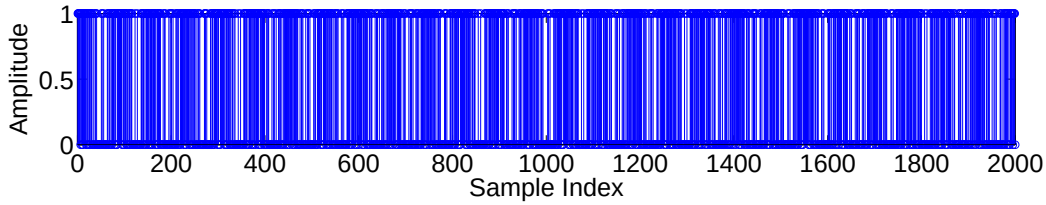

Figure 3: Output Bit Stream (first 2000 samples) of Digital Chaos Generator

2.2. Characterization of Digital Chaos

It had been mentioned earlier that the guiding principle of the digital chaos generator is the use of XOR gates to amplify the input frequency mismatches, aptly termed sensitivity. Thus, 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 [23, 24]. 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 [23, 24]:

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

The LLE for the output waveform 'Y' is obtained as 3.4735, the positive value indeed ascertaining the presence of chaos.

However, the initial proposition suggests that the generated digital chaos is dependent on the input frequencies and duty cycles. Thus, in order to study these effects, the LLE's of various signals obtained using different frequencies (expressed as ratios of first signal A's frequency) and duty cycles for A, B and C are tabulated in Table 1. It is seen that, as proposed, the frequencies and duty cycles indeed affect the nature of chaos, thus leading to the name 'Frequency Controlled Digital Chaos'.

Table 1: Effect of Driving Signal Frequencies (F) and Duty Cycles (D) on the Generated Chaos

F A (MHz)	F A/B	F A/C	D A	D B	D C	LLE
26.79	2.97	6.945	50.0	66.6	70.0	3.4735
26.79	3.33	2.864	50.0	66.6	70.0	3.1724
26.79	2.34	1.273	50.0	66.6	70.0	2.8684
26.79	2.97	6.945	50.0	25.0	80.0	2.9223
26.79	3.33	2.864	50.0	25.0	80.0	3.3632
26.79	2.34	1.273	50.0	25.0	80.0	2.9803

Table 2: Results of NIST Suite Tests for the Obtained Digital Chaotic Output

Statistical Test	P-Value	Proportion	Result
Runs	0.1227	0.9910	Pass
Longest Run	0.2343	0.9930	Pass
Monobit	0.1894	0.9890	Pass
Rank	0.2048	0.9940	Pass
FFT	0.8634	0.9940	Pass
Block Frequency	0.4632	0.9910	Pass
Cumulative Sum	0.2011	0.9900	Pass
Nonperiodic Template	0.0352	0.9880	Pass
Overlapping Template	0.3032	0.9920	Pass
Random Excursions	0.1823	0.9940	Pass
Serial	0.1030	0.9860	Pass
Maurer's Universal	0.3973	0.9910	Pass

3. Test for Randomness of obtained Digital Chaos

The next step is to test the generated digital chaotic bit stream for randomness. In order to achieve this, the NIST Standard Test Suite (Special Publication 800-22) is used [12]. This suite consists among a vast number of tests, significant tests such as the Monobit Test, Runs Test, Binary Matrix Rank Test, Discrete Fourier Transform Test, Template Matching Tests and Maurer's Universal Statistical Test [10, 12]. These tests are performed using MATLAB.

As a common feature, all the tests focus on aspects of the generated pseudorandom bit stream such as uniformity, scalability and consistency. The Null Hypothesis framed is that the sequence is not random [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 2.

The results from Table 2 show that the generated digital chaotic bit sequence passes the NIST Suite tests, thereby assertively proving its inherent capability to be used as pseudorandom bits. In addition to the NIST Tests, the randomness of the Digital Chaotic Signal is also characterized using Histograms. The Histograms of the Digital Chaotic Bit Stream of Fig. (3) is plotted for binary and hexadecimal bases in Fig. (4) and Fig. (5) respectively.

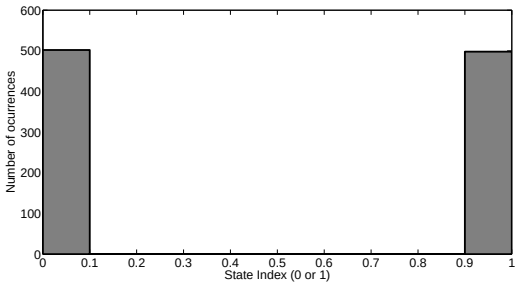

Figure 4: Binary Basis Histogram of Generated Pseudorandom Bit Sequence

From the histograms, it is evident that the generated digital chaotic signal shows fair distribution over all bit and word states in both binary and hexadecimal bases.

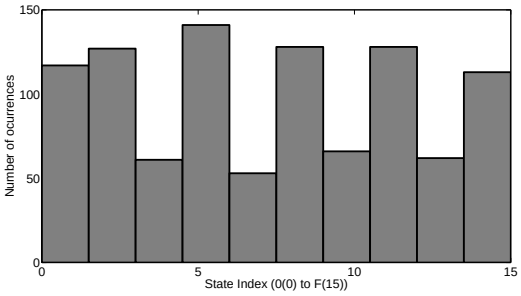

Figure 5: Hexadecimal Basis Histogram of Generated Pseudorandom Bit Sequence

4. Conclusion

Beginning with the fundamental principle that an XOR gate amplifies the frequency mismatches of the driving signals contributing to the sensitivity property, an extremely simple circuit for the generation of 'digital chaos' is proposed sing 2 XOR gates and implemented using FPGA. The presence of chaos is ascertained using Largest Lyapunov Exponent and the effect of driving signal frequencies and duty cycles on generated chaos is studied. The generated chaotic bit sequence is tested for randomness using the NIST Standard Test Suite, and it is found that the digital chaotic signal does indeed pass all the randomness tests, thus proving its capability to be used as a pseudorandom bit sequence in typical communication and computing applications. The extreme simplicity of the proposed design combined with the consistency of the generated digital chaotic signal in passing the randomness tests forms the novelty of the present work.

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] B. Razavi, *RF Microelectronics*, (Prentice Hall, US, 2011).
[17] K. E. Barner and G. R. Arce, *Nonlinear Signal and Image Processing: Theory, Methods, and Applications*, (CRC Press, U.S, 2003).
[18] E.Bilotta and P.Pantano, *A gallery of Chua attractors*, (World Scientific, Singapore, 2008).
[19] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering* ,(Westview Press, Cambridge, 2008).
[20] M. Ausloos, M. Dirickx, *The Logistic Map and the Route to Chaos: From the Beginnings to Modern Applications*, (Springer, US, 2006).
[21] R. Gilmore and M. Lefranc, *The Topology of Chaos*, (Wiley,US, [2002]).
[22] J. M. T. Thompson and H. B. Stewart, *Nonlinear Dynamics and Chaos* (Wiley,UK, [2002]).
[23] 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).
[24] 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).