ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

Chaos-Based Bitwise Dynamical Pseudorandom Number Generator On FPGA

Mohammed Shafi Uddin [1], Tanishka Shrama [2], Shaik Noman Hussain [3],

Mohammed Amaan [4], Vamsi Rani [5]

1,2,3,4 Student, Department of Electronics and Communication Engineering, Lords Institute of Engineering and Technology,

5, Assistant professor, Department of Electronics and Communication Engineering, Lords Institute of Engineering and Technology, Hyderabad, Telangana, India- 500091

Abstract

Pseudorandom bit generator (PRBG) is an essential component for securing data during transmission and storage in various cryptography applications. Among popular existing PRBG methods such as linear feedback shift register (LFSR), linear congruential generator (LCG), coupled LCG (CLCG), and dual-coupled LCG (dual-CLCG), the latter proves to be more secure. This method relies on the inequality comparisons that lead to generating pseudorandom bit at uniform time interval. Hence, a new architecture of the existing dual- CLCG method is developed that generates pseudo-random bit at uniform clock rate. A new PRBG method called as "modified dual-CLCG" and it's very large-scale integration (VLSI) architecture are proposed in this paper to mitigate the aforesaid problems. The novel contribution of the proposed PRBG method is to generate pseudorandom bit at uniform clock rate with one initial clock delay and minimum hardware complexity.

I. Introduction

PSEUDORANDOM number generators (PRNG) have many applications among diverse fields such as cryptography [1], communications [2], or procedural generation [3]. Specifically, in the field of instrumentation and measurements, PRNGs are needed in many applications such as statistical sampling, Monte Carlo simulations, evaluating the immunity to noise of digital systems and, in general, testing of physical, biological, and electrical systems: code density tests and determination of Wiener and Volterra kernels in nonlinear systems [4], [5]. Some of the most commonly used PRNGs are based on linear congruential generators (LCG) or linear feedback shift registers (LFSR).

Many of these systems, however, present some correlations or short periods, which make them unsuit able for many applications [6]. In this context, chaos-based Manuscript received September 17, 2018; accepted October 12, 2018. This work was supported in part by MINECO-FEDER under Grant TEC2014-52840-R and Grant TEC2017-85867-R. The work of M. Garcia-Bosque was supported by FPU Fellowship under Grant FPU14/03523. The Associate Editor coordinating the review process was Leonid Belostotski. (Corresponding author: Miguel Garcia-Bosque).

In this paper, we propose a random generator based on the logistic map that, in order to improve its statistical properties, dynamically changes its chaotic parameter. The system has been implemented in a Virtex 7 field-programmable gate array (FPGA), using 510 lookup tables (LUTs) and 120 reg isters. To test the good statistical properties of the proposed generator, its generated sequences have been subjected to the National Institute of Standards and Technology (NIST) tests. The sequences have passed all of these tests, proving that they are undistinguishable from a truly random sequence. The main contribution of this paper is the proposal of a novel chaos-based PRNG that: 1) offers better randomness results than other PRNGs com monly used in simulations such as LCGs and LFSRs; 2) requires a very small amount of resources to be imple mented on an FPGA compared to other previously proposed chaos-based PRNGs

Literature Review:

1. W. B. Jone and D. C. Huang and S. C. Wu and K. J. Lee, An efficient BIST method for small buffers, Proceedings 17th IEEE VLSI Test Symposium. Astonishing progress in Silicon devices and circuits and highly reliable mass manufacturing techniques have prompted unprecedented revolutions in electronics for the last 4 decades to the extent that electronics is growingly permeating numerous aspects of our life. The application world, consumer and infrastructure, is now used to exponential performance improvements and high yield. Complexity and competitiveness of modern electronic systems demand for optimization across multiple disciplines. Joint optimization of device, circuit, packaging, and test are increasingly important for high performance systems. Design for Manufacturing and Testing is more critical but increasingly challenging in complex systems. So what does optimization mean for the future of ever-growing and complex solid state electronics? A daunting challenge worth spending a talk on.

2. IEEE Standard 1687-2014 - IEEE Standard for Access and Control of Instrumentation Embedded within a Semiconductor Device, IJTAG - Internal Joint Test Action Group, IEEE Computer Society.A methodology for accessing instrumentation embedded within a semiconductor device, without defining the instruments or their features themselves, via the IEEE 1149.1(TM) test access port (TAP) and/or other signals, is described in this standard. The elements of the methodology include a hardware architecture for the on-chip network connecting the instruments to the chip pins, a hardware description language to describe this network, and a software language and protocol for communicating with the instruments via this network.This standard develops a methodology for access to embedded instrumentation, without defining the instruments or their features themselves, via the IEEE 1149.1(TM) test access port (TAP) and additional signals that may be required. The elements of the methodology include a description language for the characteristics of the features and for communication with the features, and requirements for interfacing to the features.

3. D. Bronzi, Y. Zou, F. Villa, S. Tisa, A. Tosi, and F. Zappa, "Automotive three dimensional vision through a single-photon counting SPAD camera," Linear-feedback shift register (LFSR) counters have been shown to be well suited to applications requiring large arrays of counters and can improve the area and performance compared with conventional binary counters. However, significant logic is required to decode the count order into binary, causing system- 12 on-chip designs to be unfeasible. This project presents a counter design based on multiple LFSR stages that retains the advantages of a single-stage LFSR but only requires decoding logic that scales logarithmically with the number of stages rather than exponentially with the number of bits as required by other methods. A four-stage four-bit LFSR proof of concept was fabricated in 130-nm CMOS and was characterized in a time-to-digital converter application at 800 MHz.

4. I. Vornicu, R. Carmona-Galán, and A. Rodríguez-Vázquez, "A CMOS 0.18 μm 64×64 single photon image sensor with in-pixel 11 b timeto- digital converter,"Linear-feedback shift register (LFSR) counters have been shown to be well suited to applications requiring large arrays of counters and can improve the area and performance compared with conventional binary counters. However, significant logic is required to decode the count order into binary, causing system-on-chip designs to be unfeasible. This project presents a counter design based on multiple LFSR stages that retains the advantages of a single-stage LFSR but only requires decoding logic that scales logarithmically with the number of stages rather than exponentially with the number of bits as required by other methods.

5. H. Mo and M. P. Kennedy, "Masked dithering of MASH digital deltasigma modulators with constant inputs using multiple linear feedback shift registers," This project shows that applying a linear feedback shift register (LFSR) dither to a digital delta-sigma modulator (DDSM) cannot always increase its fundamental period. For some DDSMs, the LFSR dither may reduce its period in some cases, instead of increasing it, which worsens the output spectrum. Hence, the project calculates the dithered DDSM's period and analyzes the influence of LFSR dither on the period. Furthermore, for such kind of DDSM, the project explains how to add the LFSR dither to increase the period for a full input range. Finally, experiment is performed to confirm the analysis.

6. F. Villa et al., "SPAD smart pixel for time-of-flight and time-correlated single-photon counting measurements,"Single photon avalanche diodes (SPADs) have been subject to a fast improvement in recent years. In particular, custom technologies specifically developed to fabricate SPAD devices give the designer the freedom to pursue the best detector performance required by applications. A significant breakthrough in this field is represented by the recent introduction of a red enhanced SPAD (RE-SPAD) technology, capable of attaining a good photon detection efficiency in the near infrared range (e.g. 40%

at a wavelength of 800 nm) while maintaining a remarkable timing resolution of about 100ps full width at half maximum. Being planar, the RE-SPAD custom technology opened the way to the development of SPAD 13 arrays particularly suited for demanding applications in the field of life sciences. However, to achieve such excellent performance custom SPAD detectors must be operated with an external active quenching circuit (AQC) designed on purpose. Next steps toward the development of compact and practical multichannel systems will require a new generation of monolithically integrated AQC arrays. In this project we present a new, fully integrated AQC fabricated in a high-voltage 0.18 μm CMOS technology able to provide quenching pulses up to 50 Volts with fast leading and trailing edges. Although specifically designed for optimal operation of RE- SPAD devices, the new AQC is quite versatile: it can be used with any SPAD detector, regardless its fabrication technology, reaching remarkable count rates up to 80 Mcounts/s and generating a photon detection pulse with a timing jitter as low as 119 ps full width at half maximum. The compact design of our circuit has been specifically laid out to make this IC a suitable building block for monolithically integrated AQC arrays.

Advantages of Chaos-Based Bitwise Dynamical Pseudorandom Number Generator On FPGA:

1. High Security Due to Chaos Properties:

   Chaotic systems are highly sensitive to initial conditions and parameters, making them ideal for generating unpredictable sequences.
2. Parallelism and Speed (via FPGA):

   FPGAs can **exploit parallelism**, allowing multiple chaotic maps or bitwise operations to run simultaneously.
3. Fine-Grained Bitwise Control:

   Bitwise dynamics offer **low-level manipulation** of data, enhancing **entropy** and removing statistical biases in the generated sequences.
4. Resource Efficiency:

   FPGA implementations of bitwise chaotic systems can be lightweight, consuming fewer logic blocks and less power compared to traditional PRNGs or microprocessor-based implementations.
5. Hybrid Flexibility:

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

These systems can be easily combined with other entropy sources or cryptographic primitives in FPGA, enabling hybrid architectures for enhanced security.

II. Proposed System

The proposed chaos-based PRNG is designed for high-security, hardware-efficient, and high-speed random bit generation on FPGA. Key aspects include:

1. High Entropy & Security:
   - Chaotic maps introduce non-linearity and unpredictability, making it resistant to cryptanalysis. ○ Suitable for cryptographic key generation, secure communication, and stochastic simulations.
2. FPGA-Optimized Implementation:
   - Uses fixed-point arithmetic instead of floating-point to optimize FPGA logic utilization.
   - LUT-based chaotic function implementation improves speed.
3. Low-Power & High-Speed Design:
   - Chaotic PRNGs require fewer logic gates than traditional LFSR (Linear Feedback Shift Register)-based PRNGs.
   - Parallel implementation increases throughput.
4. Comparative Analysis with Other PRNGs:
   - Compared with LFSR, Linear Congruential Generator (LCG), and hardware-based TRNGs in terms of:
     - Randomness Quality (NIST Test Suite)
     - Speed (Throughput in Mbps)
     - Hardware Utilization (LUTs, Flip-Flops)
     - Power Consumption
     -

Key Features:

- Uses chaotic maps (like Logistic or Tent maps) for randomness.
- Bitwise operations (XOR, shift, etc.) increase complexity and entropy.
- Dynamic parameter changes make output less predictable.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

- Runs on FPGA for high speed and parallel processing.
- Low resource usage, making it suitable for embedded systems.
- Statistically strong output that can pass standard randomness tests (e.g., NIST).
- Reconfigurable — easy to change parameters or logic as needed.
- Secure seeding to prevent repeatable patterns.
- Scalable design — can generate different bit-length outputs.
- Optional feedback or noise to further improve unpredictability.

Block Diagram:

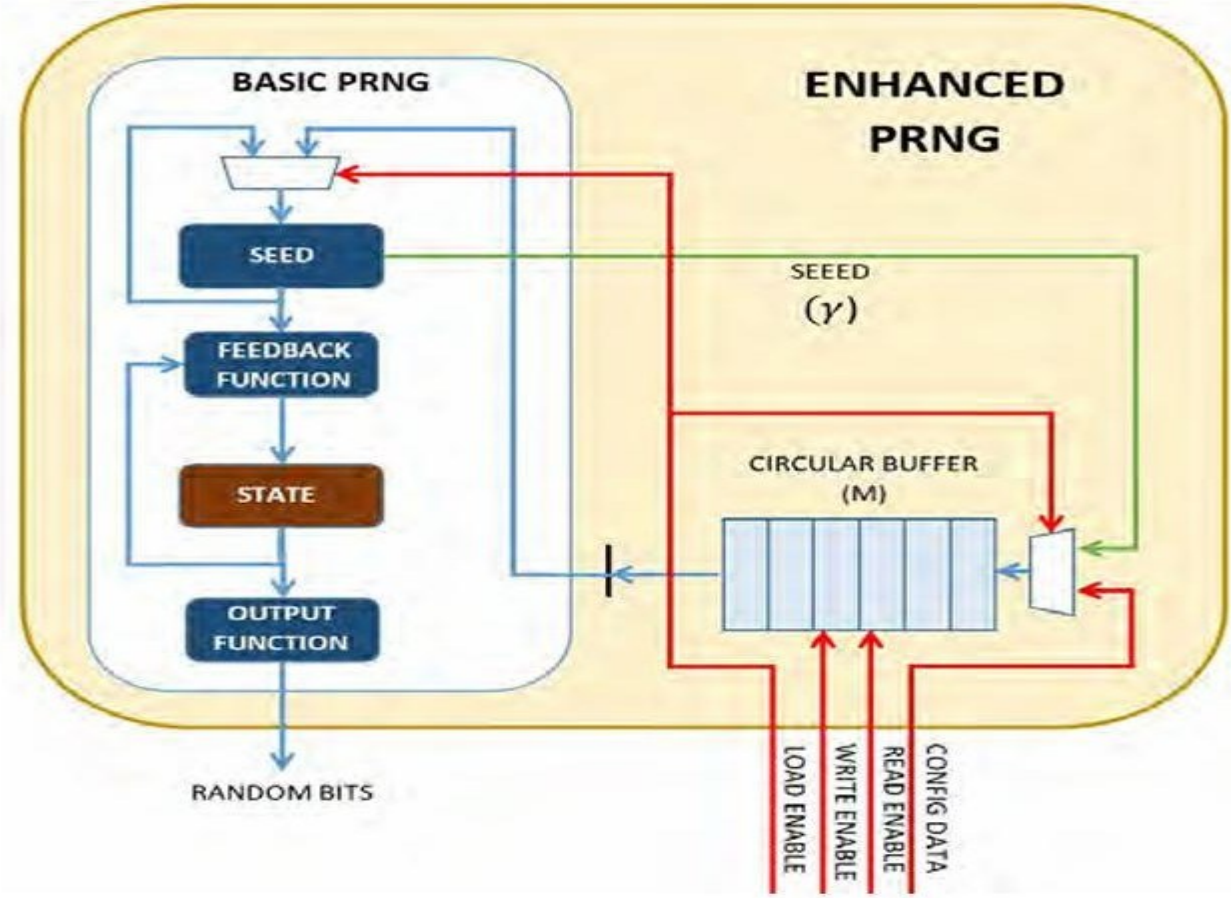

Fig 1- Block diagram for Proposed Chaos-Based Bitwise Dynamical Pseudorandom Number Generator

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

SCHEMATIC DIAGRAM:

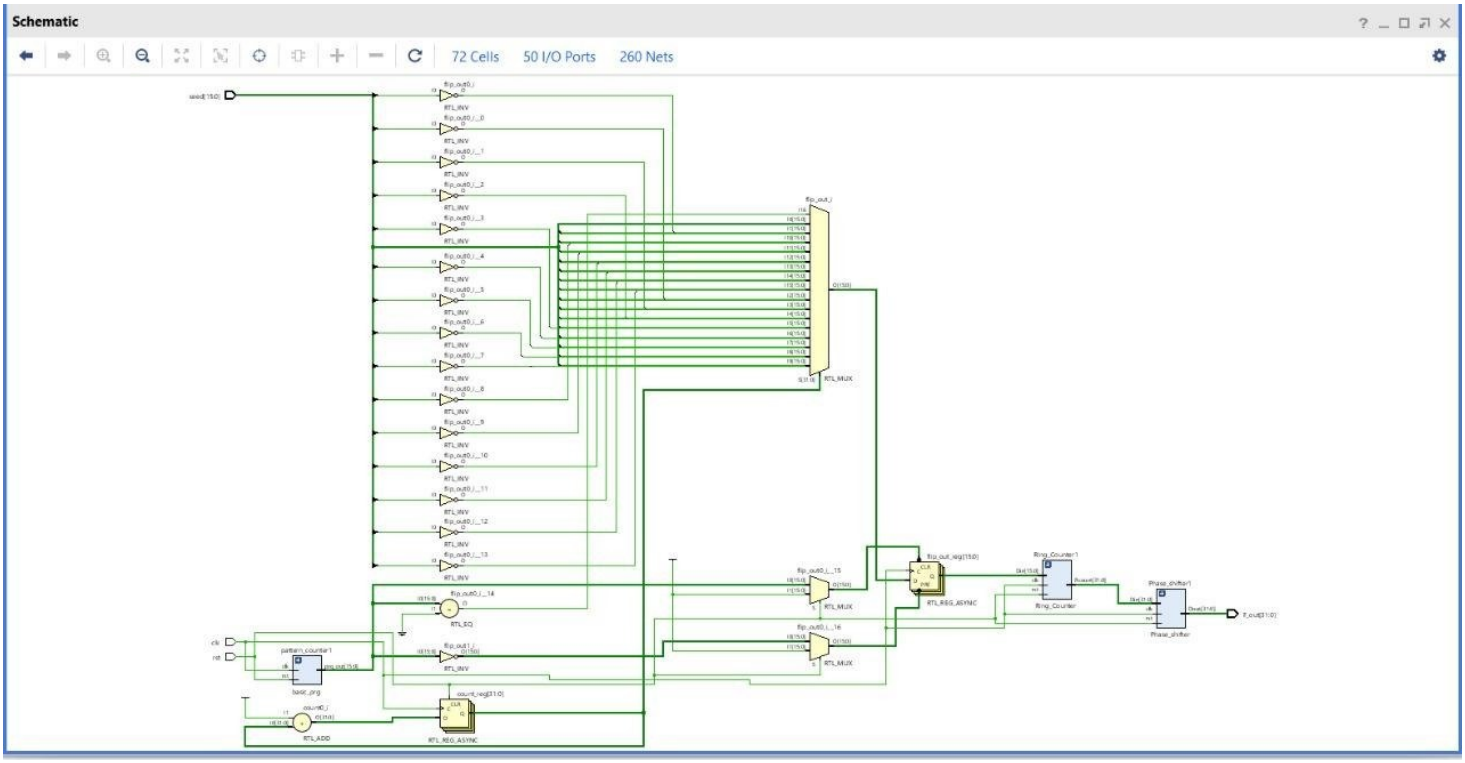

Fig 2 Schematic Diagram for Seed Flipping Architecture

Software Used:

Xilinx Vivado

VHDL/VERILOG designers use Xilinx software to perform Synthesis operations. On FPGA, it is possible to synthesise and customise any simulated code. The process of translating HDL code to a gate level net list is called synthesis. It is a critical component in contemporary design flows.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

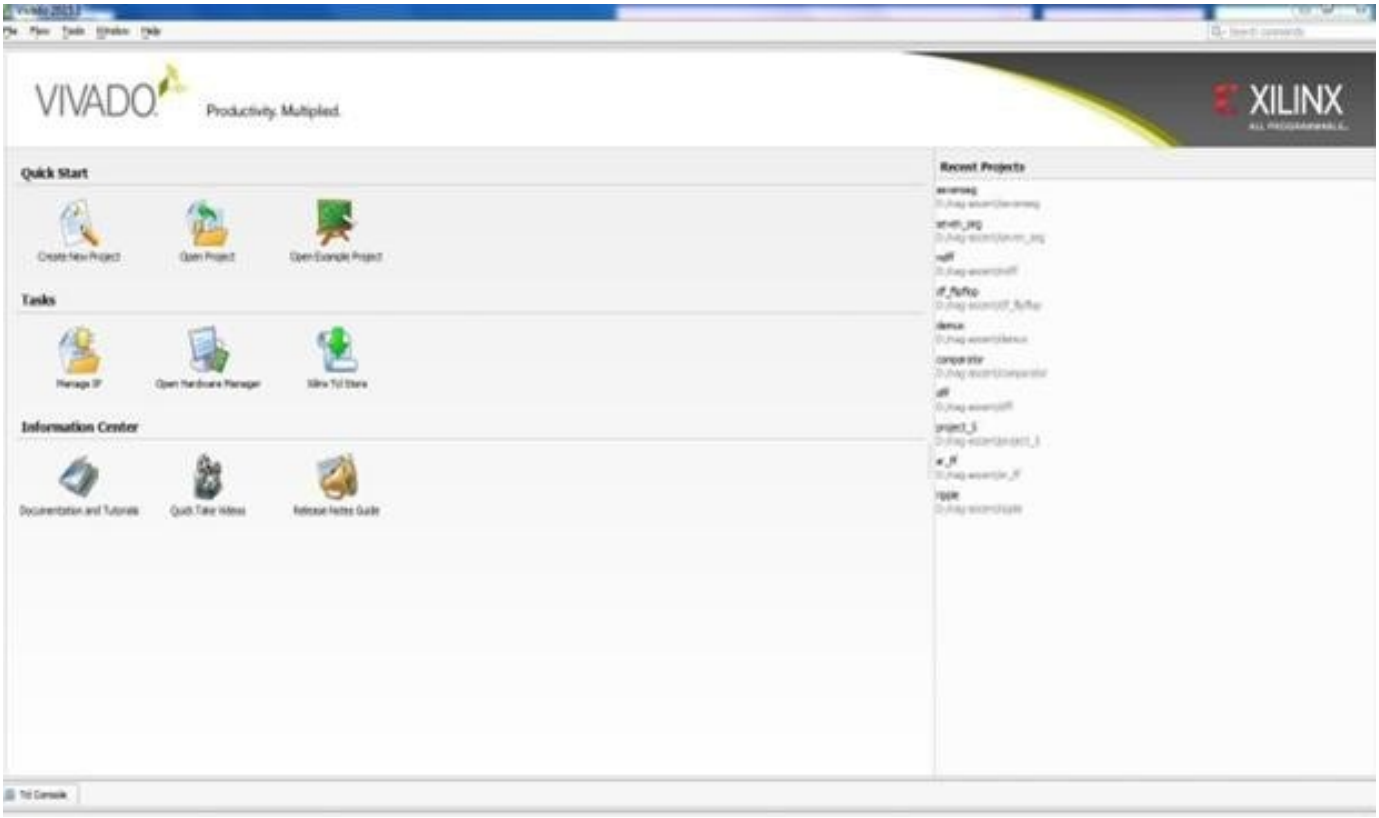

Fig 3- Xilinx Vivado Software Interface

Result:

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

Fig 4. Results on Simulated wave form of CHAOS Based PRNG.

Fig 5: Simulated wave form of PRNG using seed flipping architecture.

Result:

The RTL schematic is abbreviated as the register transfer level it denotes the blue print of the architecture and is used to verify the designed architecture to the ideal architecture that we are in need of development .The hdl language is used to convert the description or summery of the architecture to the working summery by use of the coding language i.e verilog ,vhdl. The RTL schematic even specifies the internal connection blocks for better analyzing .The figure represented below shows the RTL schematic diagram of the designed architecture

Conclusion:

In this project, a new chaos-based bitwise dynamical PRNG and seed flipping based PRNG have been proposed and tested. The system has proven to be capable of generating sequences with good statistical properties, passing the NIST randomness tests by using just a few more resources than the 32-bit logistic map generator. The proposed PRNG

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

achieves better randomness than other commonly used PRNGs such as a 32-order LFSR or a glibc LCG. Finally, a comparison of this PRNG with previously proposed chaos-based PRNGs with seed flipping based PRNG proves the good performance of the proposed system, especially in terms of resources and quality of randomness. In addition proposed PRNG consumed less area and less delay. This PRNG could be used in applications that do not require a high throughput but require a small area utilization or very good statistical properties such as, for example, Monte Carlo simulations.