International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

CHAOS-BASED BITWISE DYNAMICAL PSEUDORANDOM NUMBER GENERATOR

Mr. M. Shravan Kumar Reddy
Assistant Professor
shravan4222@gmail.com
ECE Department, Guru Nanak Institute of Technology, Hyderabad

K. Pravalika
pravalikarathod77@gmail.com
ECE Department, Guru Nanak Institute of Technology, Hyderabad

G. Viishal Gowtham
viishal514@gmail.com
ECE Department, Guru Nanak Institute of Technology, Hyderabad

J. Vivek
vikkyjadhav650@gmail.com
ECE Department, Guru Nanak Institute of Technology, Hyderabad

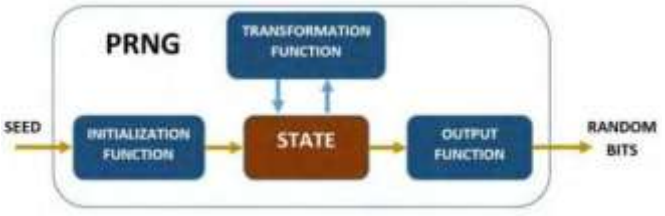
---

Abstract - In this project, a new pseudorandom number generator(PRNG) based on the logistic map has been proposed. To prevent the system to fall into short period orbits as well as increasing the randomness of the generated sequences, the proposed algorithm dynamically changes the parameters of the chaotic system. This PRNG has been implemented in a Virtex 7 field-programmable gate array (FPGA) with a 32-bit fixed point Abstract— In this project, a new pseudorandom number generator (PRNG) based on the logistic map has been proposed. To prevent the system to fall into short period orbits as well as increasing the randomness of the generated sequences, the proposed algorithm dynamically changes the parameters of the chaotic system. This PRNG has been implemented in a Virtex 7 field-programmable gate array (FPGA) with a 32-bit fixed point precision, using a total of 1479 lookup tables (LUTs) and 1445 registers. The sequences generated by the proposed algorithm have been subjected to the National Institute of Standards and Technology (NIST) randomness tests, passing all of them. By comparing the randomness with the sequences generated by a raw 32-bit logistic map, it is shown that, by using only an additional 16% of LUTs, the proposed PRNG obtains a much better performance in terms of randomness, increasing the NIST passing rate from 0.252 to 0.989. Finally, the proposed bitwise dynamical PRNG is compared with other chaos-based realizations previously proposed, showing great improvement in terms of resources and randomness.

INTRODUCTION

Random number generation is a critical component in modern computing applications such as cryptography,

secure communications, simulations, and optimization, where the quality of randomness directly impacts system performance and security. Traditional pseudorandom number generators (PRNGs), including Linear Congruential Generators (LCG) and Linear Feedback Shift Registers (LFSR), are widely used due to their simplicity and efficiency; however, they suffer from limitations such as short periods, predictability, and statistical weaknesses. Chaos theory offers a promising alternative by leveraging properties such as nonlinearity, ergodicity, and high sensitivity to initial conditions to generate sequences that resemble true randomness. Among chaotic models, the logistic map is commonly employed due to its simplicity and strong chaotic behavior, although its digital implementation introduces challenges like finite precision and periodic degradation. To address these issues, this work proposes a Chaos-Based Bitwise Dynamical Pseudorandom Number Generator (CB-BD-PRNG) that integrates chaotic maps with bitwise operations and dynamic parameter updating, enhancing randomness, improving statistical performance, and enabling efficient hardware implementation suitable for secure and real-time applications.



1. Body of Paper

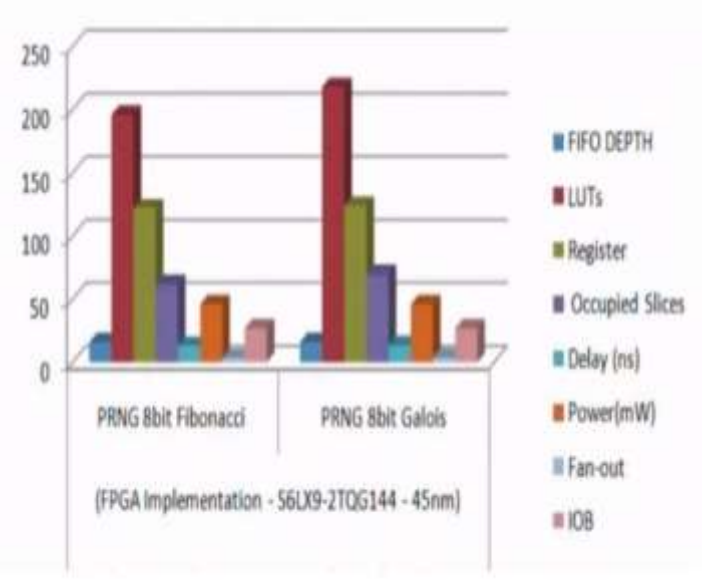
The design of efficient and secure pseudorandom number generators (PRNGs) plays a crucial role in modern applications such as cryptography, secure communications, and simulation systems. Conventional PRNGs, including Linear Congruential Generators (LCG) and Linear Feedback Shift Registers (LFSR), are widely used due to their simplicity and ease of implementation; however, they often suffer from limitations such as short periodicity, linearity, and predictability, which reduce their effectiveness in high-security environments. To overcome these challenges, chaos-based PRNGs have gained significant attention due to their inherent properties of nonlinearity, ergodicity, and high sensitivity to initial conditions. Among various chaotic systems, the logistic map is commonly used for generating random- like sequences, defined by the iterative relation $xi{+}1{=}\ \gamma xi(1\ -\ xi)$, where the control parameter governs the chaotic behavior. Despite these advantages, digital implementations of chaotic systems face issues such as finite precision, quantization errors, and degradation into short periodic cycles, which negatively impact the randomness quality.

To address these limitations, this work proposes a Chaos-Based Bitwise Dynamical Pseudorandom Number Generator (CB-BD-PRNG) that integrates chaotic maps with efficient bitwise operations and dynamic parameter updating. The system initializes with a seed and generates chaotic sequences, which are converted into binary form and processed using operations such as XOR, shifting, and rotation to enhance diffusion and nonlinearity. A dynamic feedback mechanism continuously updates the chaotic parameters based on previously generated outputs, preventing periodic behavior and improving unpredictability. The proposed architecture is implemented on FPGA, utilizing components such as FIFO memory, multiplexers, LFSR modules, and accumulators to achieve efficient hardware realization. Experimental evaluation using the NIST statistical test suite demonstrates that the proposed generator achieves a high passing rate close to the ideal value, indicating strong randomness properties. Additionally, the design requires fewer hardware resources while maintaining high performance, making it suitable for real-time and resource-constrained applications.

Overall, the integration of chaotic systems with bitwise dynamic operations provides a robust and efficient solution for pseudorandom number generation. The proposed CB- BD-PRNG successfully addresses the limitations of both traditional and conventional chaos- based methods, offering improved statistical properties, enhanced security and efficient hardware implementation.

Table-1: Comparison of Chaos based Bitwise Dynamical Pseudorandom Number Generator

	Chaos-Based Bitwise Dynamical Pseudorandom Number Generator on FPGA			
	PRNG 8 bit Fibonacci	PRNG 8 bit Galois	PRNG 32 bit Fibonacci	PRNG 32 bit Galois
FIFO DEPTH	16	16	16	16
LUTs	196	218	2274	2385
Register	122	124	1154	1153
Occupied Slices	62	70	824	859
Delay(ns)	13.202	13.658	55.0548	54.854
Power(mW)	46	46	175	175
Fan-out	3.50	3.70	3.65	3.70



Chaos Based Bitwise Dynamical Pseudorandom

IMPLEMENTATION

The proposed Chaos-Based Bitwise Dynamical of 106 bits have been generated and have been subjected Pseudorandom Number Generator (CB-BD-PRNG) is to the NIST randomness tests, with a significance level of implemented using a hardware-oriented approach on a 0.01 (i.e., 99% of the sequences generated by a truly Field Programmable Gate Array (FPGA) platform to random generator would pass the tests).
achieve high performance and efficiency. The implementation begins with the selection of a suitable chaotic system, specifically the logistic map, which is iteratively computed to generate a nonlinear sequence based on an initial seed and dynamically varying control parameters. The chaotic values are represented using fixed-point arithmetic to enable efficient digital realization while maintaining sufficient precision for chaotic behavior. The generated continuous values are then converted into binary form, allowing further processing at the bit level.

To enhance the statistical properties of the generated sequence, a series of bitwise operations such as XOR, shifting, and rotation are applied to the binary outputs.
These operations increase diffusion and nonlinearity, thereby eliminating detectable patterns and improving randomness. A dynamic feedback mechanism is incorporated, where selected output bits are used to update the control parameter of the chaotic map in each iteration,

preventing the system from falling into periodic cycles caused by finite precision effects. The overall architecture consists of multiple hardware modules, including FIFO memory for temporary data storage, multiplexers for control signal selection, Linear Feedback Shift Registers (LFSRs) in both Galois and Fibonacci configurations for auxiliary randomness, accumulators for improving distribution uniformity, and adder circuits for arithmetic operations. The design is described using hardware description language (VHDL), simulated using Model Sim, and synthesized on a Xilinx FPGA platform. The implementation achieves a balance between randomness quality and hardware resource utilization, making it suitable for real-time and resource- constrained applications.

RESULT

The proposed algorithm has been implemented in a Virtex 7 FPGA. A 32-bit word length has been used for the values of γi and xi and a total of m = 8 different values of γi have been used. The elements of the sequence partition have been obtained by generating random integers within the interval ki ∈ using a simple

LCG algorithm. Finally, only the LSB of each xi has been used to generate the pseudorandom sequence. To test the statistical properties of the PRNG, 100 sequences

Configuration	32-bit Logistic Map	32-bit Logistic Map	32-bit Proposed PRNG
LUTS	439	903	510
Registers	46	70	120
Slices	116	235	143
DSPs	13	18	13
NIST passing rate	0.252	0.979	0.989

IMPLEMENTATION RESULTS

CONCLUSION

In this paper, a Chaos-Based Bitwise Dynamical Pseudorandom Number Generator (CB-BD-PRNG) has been proposed and implemented to address the limitations of conventional and existing chaos-based PRNGs. By integrating nonlinear chaotic dynamics with efficient bitwise operations and a dynamic parameter updating mechanism, the proposed system achieves enhanced randomness, improved entropy, and reduced correlation in the generated sequences. The implementation on an FPGA platform demonstrates that the design not only provides high statistical quality— validated through NIST randomness tests—but also maintains efficient hardware utilization in terms of logic resources, delay, and power consumption. Compared to traditional PRNGs such as LCG and LFSR, as well as basic chaotic generators, the proposed method exhibits superior performance in both randomness quality and implementation efficiency. Therefore, the CB-BD-PRNG is well suited for applications requiring secure and reliable random number generation, including cryptography, secure communication systems, and real- time embedded applications.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the management and faculty of Guru Nanak Institute of Technology for providing the necessary infrastructure and support to carry out this research work. We extend our heartfelt thanks to our project

guide and mentors for their continuous guidance, valuable suggestions, and encouragement throughout the development of this work. We also acknowledge the support of our colleagues and peers who contributed directly or indirectly to the successful completion of this project.

REFERENCES

[1] M. Garcia-Bosque, A. Pérez, C. Sánchez-Azqueta, and S. Celma, "Application of a MEMS-based TRNG in a chaotic stream cipher," *Sensors*, vol. 17, no. 3, p. 646, 2017.

[2] M. Borna and M. H. Madani, "New methods for enhancing fine acquisition in dual folding algorithm of long pseudo noise codes," *International Journal of Communication Systems*, vol. 31, no. 1, p. e3377, 2018.

[3] R. van der Linden, R. Lopes, and R. Bidarra, "Procedural generation of dungeons," *IEEE Transactions on Computational Intelligence and AI in Games*, vol. 6, no. 1, pp. 78–89, Mar. 2014.

[4] L. Xu and X. Li, "Dual-channel pseudorandom sequence generator with precise time delay between its two channels," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 12, pp. 2880–2884, Dec. 2008.

[5] L. Kocarev and S. Lian, *Chaos-Based Cryptography*. Berlin, Germany: Springer, 2011.