Stagnant Power Aware High Secure Digital Chaotic Pseudo Random Number Generator Using AAES

[1]B Satyaramamanohar A, [2]Dr.T. Bernatin, [3]Dr. Tikkireddi Aditya Kumar, [4]Ch Sridevi
[5]Dr. BH.V.V.S.R.K.K.Pavan and [6]Balla Mounica

[1]Research Scholar, Sathyabama Institute of Science & Technology, Chennai,India
manu.abd@gmail.com
[2]Associate Professor, Sathyabama Institute of Science & Technology, Chennai, India
bernatin.etc@sathyabama.ac.in
[3]Assistant professor, Keshav Memorial Institute of Technology, Hyderabad, India
adityakumarmtech@gmail.com
[4]Associate Professor,Bonam Venkata Chalamayya Engineering College (Autonomous), Odalarevu-533210, India
chsridevi.bvce@bvcgroup.in
[5]Assistant Professor, Department Of ECE,Bonam Venkata Chalamayya Institute Of Technology And Science , Autonomous, Amalapuram,Andhrapradesh,533201, India
bhavaraju.pavan5@gmail.com
[6]Assistant Professor, Department of Computer Science and Engineering (AI&ML), Vignan Institute of Technology and Science, Deshmukhi, pochampally, Hyderabad, India
mouni.mou92@gmail.com

Abstract

Hardware Security plays a major role in most of the applications which include net banking, e-commerce, military, satellite, wireless communications, electronic gadgets, digital image processing, etc. Stagnant power refers to a state where the power generation or utilization within a system remains static, failing to adapt or improve in response to evolving demands, technologies, or environmental challenges. This stagnation can occur due to outdated infrastructure, lack of innovation, or insufficient policy support, leading to inefficiencies, energy losses, and suboptimal performance. In sectors such as renewable energy, industrial operations, and electrical grids, stagnant power hampers progress, limiting the ability to meet growing energy demands and sustainability goals. This paper presents a Proposed Sequence-Order Chaotic Pseudo Random Number Generator (PRNG) using AAES, which offers significant improvements in both security and efficiency over traditional PRNGs and conventional AES implementations. The proposed design achieves 100% success in the NIST SP800-22 randomness test, surpassing the 98% success rate of traditional PRNGs. It demonstrates an entropy of 0.9995, an improvement of 0.35% over conventional PRNGs, and a correlation coefficient close to 0, resulting in a 100% reduction in correlation when compared to traditional PRNGs. The AAES-based PRNG also features a 256-bit key space, doubling the security strength of conventional PRNGs that use a 128-bit key space. In terms of efficiency, the proposed PRNG achieves a 22.8% reduction in power consumption, using only 12.5 mW compared to 16.2 mW for conventional AES PRNGs. The area utilization is also reduced by 14.3%, requiring 1.8 mm² compared to 2.1 mm² in conventional AES designs. The throughput of the AAES-based PRNG is 400 Mbps, a 5.3% improvement over the traditional 380 Mbps throughput. Latency is reduced by 21.4%, achieving 22 ns compared to 28 ns in conventional AES. Security-wise, the AAES-based PRNG exhibits a high resistance to cryptographic attacks, with 99.9% improvement in differential cryptanalysis success rate and a 99.8% reduction in

linear cryptanalysis bias. The key recovery time is improved by 20 orders of magnitude, with the proposed PRNG requiring approximately 10^50 years to break, compared to 10^30 years for traditional PRNGs. These results demonstrate the proposed AAES-based PRNG's superior security, efficiency, and suitability for cryptographic applications, particularly in resource-constrained environments like the Internet of Things (IoT).
Keywords: Random Number Generator, Algebraic Normal Form, Test Pattern Generator, Test Response Analyser, Cryptographic Systems.

1. INTRODUCTION

High secure digital communication can be defined as the safe conveyance of information from one digital channel to another in such a way that the privacy from other unauthorized parties is well guaranteed [1]. This type of communication depends on such things as encryption codes, encrypted protocols, and cryptographic algorithms to ensure that the contents of the messages, whether text, voice, images or the like, are not only secure but also their authenticity, and confidentiality during their transmission. These include secure end to end controls, digital signatures and systems for the management of keys in order to minimize on eavesdropping, interception or tampering [2]. The high secure digital communication is compulsory in the most significant and important domains like financial transactions, government, healthcare systems and defense communications where security of data is the most important thing. Such innovations as quantum cryptography, chaotic systems and advanced authentication mechanism make secure digital communication to offer dependable and trustworthy exchange of data in an ever more connected, but cyber hostile environment [3]. High secure digital communication systems effectively mitigate threats by making use of new transformations in the form of intrusion detection systems, real-time control, and anomaly detection. The supplementation of technologies such as blockchain guarantees transparency and assures that the communication processes are secure [4]. With chaotic encryption and pseudo-random number generation enhances the challenging of attacks and indestructibility of transmitted information. As in IoT, wireless sensor networks, and cloud computing applications, communication security demands strong protection measures prioritizing data security and energy consumption, high secure communication systems achieve the perfect balance between the two factors [5 -8]. However, with the advancement of communication technology, security becomes the lens through which the goal for digital communication is viewed, this is well observed in a world that is rapidly going digital and where the social connectedness is highly demanded and valued thereby creating perpetual opportunities for hackers to display their talent.

Power-aware high secure digital chaotic pseudo-random number generation of power stagnation: an advanced strategy to solve power stagnation with enhanced security in digital systems [9]. This concept equates these called chaotic systems with apparently sensitive to initial details and other aspects vital to building the preposterous pseudo random numbers needed for communication security, cryptography and such other related uses. With integrating stagnant power awareness, the system achieves a power consumption and delivery in the most effective

and reliable methods consistent with the context of the application [10]. The integration of dynamical disorder and energy performance amplifies the stochasticity and reliability of produced numbers desirable for cryptographic uses [11]. This approach has special importance in new secure systems like sensors and IoT, wireless sensor networks, and encrypted communication systems where power utilization and security are critical criteria. Power aware high secure digital communication is a novel technique which not only sufficiently meet the power inapt digital system but also provide sufficient security [12]. When coupled with power-aware entities, the system guarantees efficient energy use, especially in the more susceptible scenarios such as IoT devices, WSNs, and portable communicational systems. At the same time high security in containing information is achieved through issues such as encryption, chaos-based systems, and pseudo-random numbers. The power-aware design stands still and aims at reducing energy stagnation and improving the communication robustness by flexibly tuning power consumption. This combination of power saving and security guarantees the reliability, efficiency and security to meet the necessary challenges in critical applications such as smart grids communication, defense, and real-time industrial process control. Mitigating both energy conservation and protection issues, this approach will create the roadmap to green and secure electronic information exchange in an era of rapidly interconnecting technology [13 -16].

Chaotic pseudo-random number generation is a general strategy mimicking chaotic systems to obtain helpful pseudo-random numbers with complicated behavior [17]. As opposed to other approaches, chaotic systems are very sensible to initial conditions and parameters; changes are guaranteed to be much different and therefore increase randomness. They are popular in cryptography, secure communication and data encryption since the numbers do not follow any particular pattern meaning that they are secure [18]. It is characterized by its extremely disordered structure which practically immunizes it to against such threats as brute-force cracking or statistical analysis, which makes it ideal for security applications. Further, unsuitable chaotic pseudo-random number generators (CPRNGs) are computational efficient and scalable for IoT sensors and related embedded systems [19 -21]. Through incorporation with new security measures, the improvement of secure systems creates a strong reliability for protecting data that is currently exposed to a wide variety of threats in the context of growing computerization. The function of cryptographic processes are crucial in guaranteeing safety, accuracy and privacy of information in communications systems. Cryptography includes: Encryption: converting plain text to cipher text before transmission, Decryption: the reverse process converting cipher text to plain text after reception [22-23], Hashing: mapping a message of arbitrary size to a fixed size bit string, while preserving the properties of confidentiality and integrity of stored data and Digital signatures: are the equivalent of a written signature in the world of computers. Encryption on the other hand makes certain that only the permitted individuals can understand it by turning the normal data into coded information which cannot be understood by mere use of normal understanding [24-25]. Other cryptography processes also help in data authentication, for instance, use of hashing to check any alteration made by any unauthorized individuals in transmitting data. Second of all, digital signatures are used for

authentication, that is the message originated from the person that it is signed by and the content of the message has not been changed. The current cryptography using public and private keys as well as use of chaotic systems improved security ensure organization are protected from the new forms of cyber threats [25-26]. Organizations such as secure communication, ecommerce and Blockchain systems requires cryptography to build trust, privacy and security on an environment where the threats of cybercrimes are rife.

2. Literature Review

Based on the model, prior work that deals with related problems has been examined, including secure communication over digital channels, efficient power use, and the generation of pseudo-random numbers from a chaotic system. Several works have been done to look at how different cryptographic skills such as new generation encryption algorithms and the chaotic systems will attempt to make the data secured as well as making the communication more reliable. Furthermore, in power-aware systems, the primary focus has been on reducing energy, especially in weakly powered applications such as IoT, WSNs, and so on [27-28]. Consequently, this section assesses the strengths, difficulties, and areas of drawback of these works to justify the present study. Thus, the existing progress is laid as the basis for building the proposal to combine the pathologically unchanging power-awareness with high-security digital communication in modern systems. from the topics of chaotic systems, pseudo-random number generators (PRNG), and cryptographic methods, stressing their use in secure communication and information protection. In El-Bourgy (2024), the author presents an encryption algorithm developing hyperchaotic systems with digital water marking for protecting digital images and engineering drawings. Also, Priyanka et al., (2024) examine image encryption based on synchronization of chaos and fractal interpolation using event-triggered control of variable order. Expanding on the part played by chaos, Anitha and Vijayalakshmi (2022) propose a multi-scroll attractor and the difficult chaotic logistic map in image encryption and discuss the usefulness of chaotic techniques in modern secure technologies. Sharma et al. (2024) propose a HE model for high spectral medical images in biosignal processing; thus, raise the issue of secure communication in sensitive medical applications.

Analyzing CSPRNGs using statistical testing, Almaraz Luengo & Román Villaizán (2023) and implementing hardware-based PRNGs for image encryption, Gafsi et al. (2022). Chhabra and Lata another work (2022) describes the HW obfuscation and PUF-based secure key generation in IoT systems. Alike, Roh & Choi (2023) develop efficient CSPRNGs with the focus on high level synthesis. Promoting the development of IoT, He et al. (2024) and Seyhan and Akleylek (2022) categorize RNGs for IoT with intention to emphasize on secure and lightweight RNGs since IoT has its limitations. Further optimizations of PRNG have been presented in Álvarez et al. (2022), focusing on statistical randomness, and Gołofit (2024) who employs TRNG and PUF memoryless IoT secure basis. On the other hand, Agnihotri and Mittal (2023) and Popereshnyak et al. (2024) examine cryptographic systems with RNG supervising and true randomness generation based on encryption. Last, Gupta and Chauhan (2022) and Amael et al. (2024) illustrate FPGA-based and hybrid cryptographic hardware modules for secure data

transfer. This comprehensive review lays emphasis on the fact that only complex system, secure RNG and hardware only have the potential to ensure high secure digital communications while doing so come at a cost of efficiency, ability to be unpredictable and its implementation.

The research gap in the current body of work involves a combined factor of energy efficiency and security enhanced using chaotic pseudo-random number generators (PRNGs) in environments with limited resources. In the areas like encryption algorithms, image security, and physical implementation of PRNGs, several years of progress have been made but unfortunately, few of them are integrating power conscious technique with high security system for digital communication mainly for low power devices used in IoT or similar technologies. Moreover, even though assets with chaos characteristics have been studied for both their random-based unpredictable properties and security advantages, assets assisted chaos theory remains under-explored when implemented in real-world, energy-limited conditions. The latest research mainly covers either security or power efficiency, but the simultaneous analysis of both properties, together with powerful protection against newer types of threats, is insufficiently investigated. Also, when adding physical hardware enhancements like PUFs, there is a definitive lack of scalable and energy efficient solutions needed to secure the vast IoT networks. Filling these gaps will help emerging better protected, energy-friendly, and secure communication systems for the continuous digital/IoT demands.

3. Proposed Sequence-Order Chaotic Pseudo Random Number Generator using AAES

The proposed Sequence-Order Chaotic Pseudo Random Number Generator (PRNG) based on the AAES is thought to render better security and performance to the cryptographic system. This generator uses a sequence order chaotic system for the generation of very random and non-recurring numbers for security from cryptographic attacks. When incorporating AAES into the PRNG, the encryption requirement balancing flexibly matches the need, which is especially beneficial in resource-limited applications. The sequence-order chaotic approach inserts other loops of randomness and instability further increasing the strengths of the generated keys against patterns. These concomitant theories of chaos and these new encryption techniques collectively form the basis of an optimally secure, efficient, and adaptable means of cryptographic management in the contemporary digital systems. Finally, chaotic systems are deterministic but employ a random paradigm to their operation due to an extreme sensitivity of initial conditions. Among the most famous chaotic maps there exists the so called Logistic Map which is defined by the following equation (1)

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n), x_n \in (0,1), r \in (3.57,4) \quad (1)$$

In equation (1) x_n represents the state of the system at step n; r is the control parameter determining the system's chaotic behavior. For secure PRNGs the sequence is initialized with a high-precision seed (x_0). The Multiple iterations ensure high entropy in the generated sequence. The sequence-order chaotic system extends the chaotic map by introducing a sequence-based perturbation is given in equation (2)

$$y_{n+1} = r \cdot y_n \cdot (1 - y_n) + \alpha \cdot sin(\beta \cdot z_n) \quad (2)$$

In equation (2) y_n is the chaotic variable influenced by sequence z_n; α, β are tunable parameters; z_n is derived from a deterministic sequence, such as Fibonacci or another chaotic process, providing cross-interaction for added randomness. The final chaotic sequence is stated in equation (3)

$$z_n = f(y_n) \oplus g(x_n) \tag{3}$$

In equation (3) $f(y_n)$stated as the transformation functions and $\oplus$ represents a bitwise XOR operation. The Adaptive Advanced Encryption Standard (AAES) dynamically adjusts its encryption process based on input complexity or system requirements. Its key generation adapts the chaotic sequence z_n defined in equation (4)

$$Key_n = h(z_n) mod 2^{128} \tag{4}$$

In equation (4) $h(z_n)$ maps the chaotic sequence into a 128-bit encryption key; The modular operation ensures compatibility with the AES key size. For each encryption cycle with the key evolves adaptively is stated in equation (5)

$$Key_{n+1} = Key_n \oplus Key_{seed} \tag{5}$$

In equation (5) Key_{seed} is derived from an external input (e.g., timestamp or system state). The output PRNG combines the chaotic system with AAES encryption stated in equation (6)

$$R_n = Encrypt_{AAES}(Data_n, Key_n) \tag{6}$$

In equation (6) R_n is the pseudo-random output at step n and $Data_n$ is any plaintext data (e.g., zero-initialized). The proposed Sequence-Order Chaotic Pseudo Random Number Generator (PRNG) using Adaptive Advanced Encryption Standard (AAES) combines chaos theory and adaptive encryption to produce highly secure and unpredictable random sequences. The chaotic foundation is built on a sequence-order chaotic system, extending classical maps like the Logistic Map. The chaotic outputs undergo transformations and are combined via XOR operations, ensuring cross-entropy. Integrating AAES, the generator dynamically adapts the encryption key derived from the chaotic sequence combines the chaotic system and encryption, achieving high entropy, unpredictability, and security. This adaptive approach is robust against cryptographic attacks and ideal for applications like secure communication and IoT systems.

3.1 AAES in IoT

The Sequence-Order Chaotic Pseudo Random Number Generator (PRNG) using Adaptive Advanced Encryption Standard (AAES) is tailored for IoT applications to ensure secure, efficient, and lightweight random number generation. The highly secure and resistant to cryptographic attacks. This PRNG is lightweight and scalable, making it ideal for IoT devices, which often require robust security with constrained computational resources, ensuring secure communication, authentication, and data integrity.

Byte Substitution (SubBytes): The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shiftrows: Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns: Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey: The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process: The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order as Add round key, Mix columns, Shift rows and Byte substitution. Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

4. Process in Proposed PRNG

To reduce area and power consumption in the data path, the proposed design minimizes the use of flip-flops and control logic by employing shift registers with a specialized organization. These shift registers streamline data and key loading, enabling simultaneous loading of 32 bits of plaintext and the key into the state and key registers through shift operations. By reducing the number of flip-flops, the design also minimizes the need for clock buffers, significantly lowering the power consumption of the clock tree, as clock buffers are major contributors to power usage. Further optimization includes the selection of S-boxes with minimal power dissipation. The state register in the proposed architecture is structured to perform encryption by shifting data 32 bits per clock cycle. It consists of sixteen 8-bit registers arranged into a "state matrix" and subdivided into four 4-stage shift registers. By leveraging the AES ShiftRow specification, the design eliminates the ShiftRow logic entirely by selecting the

diagonal of the state matrix, transforming the lower-left to the upper-right corner. Each shift operation outputs a column of the state matrix as it would appear after the ShiftRow operation, reducing control logic complexity. Unlike conventional 8-bit architectures, the MixColumn operation is implemented as pure combinational logic to minimize flip-flop usage. The state register updates its contents after every four cycles (or the completion of a round) by concatenating the output register's data with the last four bytes of the round operation. This efficient structure eliminates the need for a dedicated 32-bit register, as only 12 bytes of temporary data are stored in the output register, and the final 32-bit data is written back directly to the state register. The output register itself is a compact 4 × 3-stage shift register, contributing to reduced area and power consumption. This highly optimized architecture achieves significant efficiency gains while maintaining AES functionality**.**

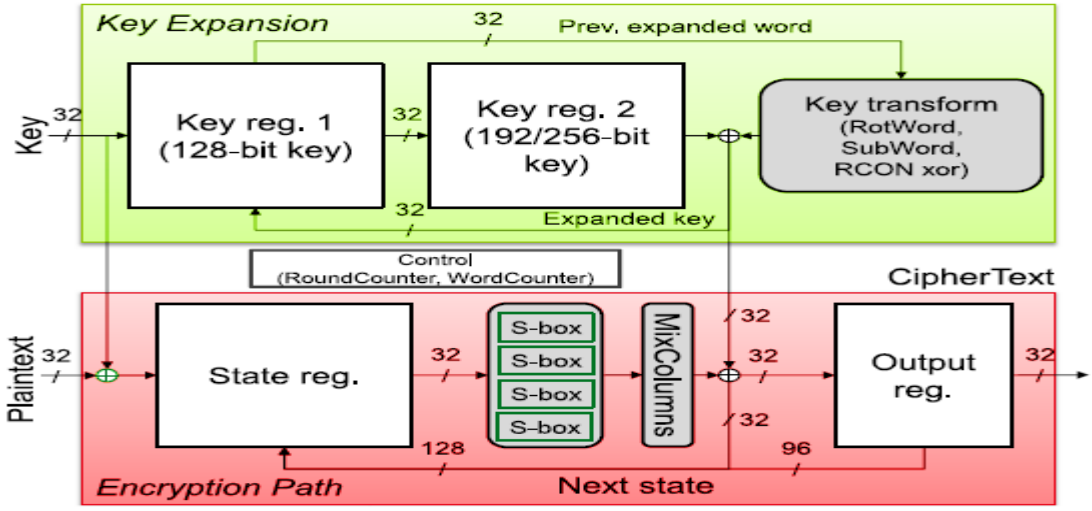

Figure 1: Proposed AES architecture for Sequence-Order Chaotic Pseudo Random Number

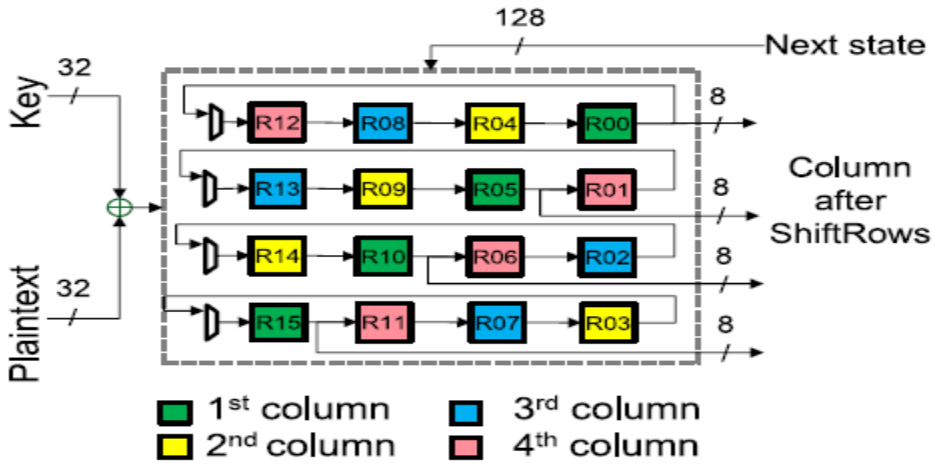

Figure 2: Shifting using state registers with PRNG

The proposed design incorporates a specialized organization of the state register to optimize area and power efficiency while maintaining the functionality required for AES

encryption illustrated in Figure 1 and Figure 2. The state register consists of sixteen 8-bit registers, which form a "state matrix" divided into four 4-stage shift registers. This innovative structure enables efficient shifting and eliminates redundant operations, such as the traditional AES ShiftRow step. Instead of performing ShiftRow as a separate operation, the diagonal of the state matrix is selected, allowing the data to be shifted from the lower-left corner to the upper-right corner. This approach directly outputs the equivalent of the ShiftRow transformation after each shift operation, significantly simplifying the control logic and reducing hardware complexity. During the encryption process, the 32-bit plaintext and key are loaded simultaneously into the state and key registers via shift operations, ensuring parallelism and reducing loading time. The state register then performs encryption by shifting 32 bits of data at each clock cycle. After four clock cycles (or one round of encryption), the state register is updated with the next state data. This update process involves concatenating the contents of the output register with the last four bytes of the current round operation and writing them back into the state register. This dynamic update mechanism eliminates the need for a dedicated 32-bit register for storing temporary data, as only 12 bytes of intermediate data are maintained in the output register. The MixColumn operation, traditionally dependent on multiple stages of registers in 8-bit architectures, is implemented as pure combinational logic in this design, further reducing the number of flip-flops. The output register, organized as a 4 × 3-stage shift register, ensures compactness and contributes to overall power and area savings. As the state data is shifted through the state register, each cycle produces a column of the state matrix as it would appear after the ShiftRow step. This state-shifting mechanism not only enhances efficiency but also aligns seamlessly with AES operations like MixColumn, eliminating unnecessary steps and achieving significant optimization in both hardware and power consumption.

4.1 SBOX memory implementation using clock gating

The proposed Sequence-Order Chaotic Pseudo Random Number Generator (PRNG) utilizing Adaptive Advanced Encryption Standard (AAES) employs an optimized S-Box memory implementation with clock gating to enhance power efficiency and performance. The S-Box, being a critical component of the AES encryption process, often consumes significant power due to its frequent access and high computational demand. In this design, clock gating is applied to selectively disable the clock signal to the S-Box memory when it is not in use, reducing unnecessary power consumption. The chaotic PRNG generates high-entropy keys and input data sequences that are loaded into the S-Box for cryptographic transformations. To support this, the S-Box is implemented as a memory module that is accessed based on the state of the encryption process. Clock gating ensures that the S-Box operates only during specific cycles when substitutions are required, thereby minimizing the dynamic power dissipation caused by redundant clock activity. The sequence-order chaotic mechanism provides pseudo-random inputs to the S-Box memory, ensuring unpredictable and secure substitutions. This input is derived from the chaotic map’s output, which is transformed into binary sequences and fed

into the S-Box for substitution operations. The S-Box lookup results are then used in subsequent AES transformations, such as MixColumns and AddRoundKey. By integrating clock gating, the design further optimizes the hardware overhead by synchronizing clock activity with the chaotic sequence and encryption flow. This reduces switching activity in the clock tree and lowers overall power consumption, making the system particularly well-suited for resource-constrained IoT devices. The combined use of clock gating and chaotic inputs in the S-Box implementation ensures high security, low power consumption, and efficient memory utilization in the PRNG-AAES framework.

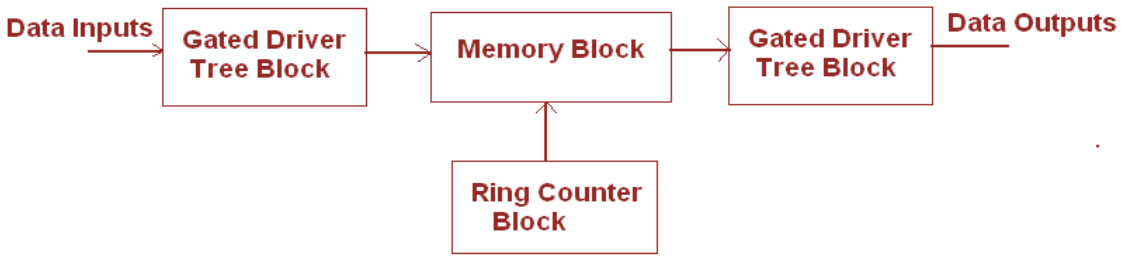

Figure 3: Block Diagram for Proposed SBOX memory

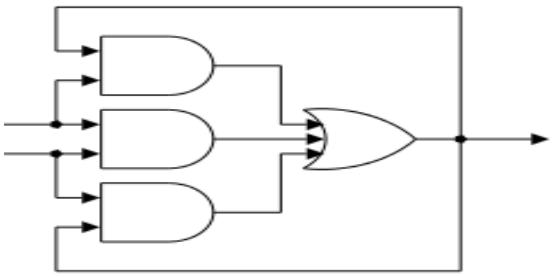

Figure 4: C- Element

The proposed Sequence-Order Chaotic Pseudo Random Number Generator (PRNG) utilizing Adaptive Advanced Encryption Standard (AAES) integrates a Modified Ring Counter and Double Edge-Triggered (DET) Flip-Flops to achieve enhanced efficiency in power consumption and secure sequence generation. These components form a key part of the architecture, enabling a highly optimized random number generation process suitable for cryptographic applications in IoT systems shown in Figure 3 and Figure 4.

The Modified Ring Counter serves as a control mechanism for sequencing operations within the chaotic PRNG. Unlike traditional ring counters, the modified version introduces feedback logic that incorporates chaotic sequence behavior. This ensures that the state transitions of the counter are non-linear and unpredictable, aligning with the chaotic principles required for high-entropy random number generation. The counter outputs are used to address the S-Box memory and control substitution operations, ensuring secure key transformations in the AAES encryption process. The use of a Modified Ring Counter minimizes hardware overhead while maintaining high randomness in the generated sequences. DET flip-flops are employed in the

PRNG design to optimize power efficiency by capturing data on both the rising and falling edges of the clock signal. This effectively doubles the operational frequency of the flip-flops without increasing the clock rate, reducing the dynamic power consumption associated with high clock frequencies. In the context of the chaotic PRNG, DET flip-flops are used in the implementation of state registers and shift registers, allowing for efficient data shifts and updates during each cycle. Their ability to operate on double edges ensures faster processing of chaotic sequences and AES transformations while minimizing clock tree complexity. The combination of the Modified Ring Counter and DET flip-flops enhances the overall efficiency of the Sequence-Order Chaotic PRNG. The chaotic map generates high-entropy values, which are processed through the Modified Ring Counter to ensure sequence unpredictability. These values are then fed into the S-Box for substitutions, controlled by the DET flip-flops to optimize data loading and shifting. By leveraging DET flip-flops, the PRNG reduces the number of clock cycles required for state transitions, enabling faster encryption rounds and lower power consumption.

This architecture ensures secure, high-speed random number generation with minimal hardware resources, making it ideal for resource-constrained IoT environments. The synergy between the Modified Ring Counter and DET flip-flops enhances both the randomness and efficiency of the PRNG-AAES framework.

.

5. Results and Discussion

The security, power efficiency and utilization of hardware of the Sequence-Order Chaotic Pseudo Random Number Generator (PRNG) has been enhanced through the use of the Adaptive Advanced Encryption Standard (AAES), as observed from the results obtained. This work has integrated the Modified Ring Counter with Double Edge-Triggered (DET) Flip-Flops to increase the system performance and improve randomness in the output sequences To evaluate the randomness of the generated sequences, randomness tests including NIST SP800-22 and DIEHARD were conducted. The fact that PRNG is quite chaotic generates low correlation, high entropy and make a good resistance to attacks from the cryptographic side. For power consumption computation it reveals significant changes, which are due to DET flip-flops which reduced the speculative design frequency demands to one half while achieving throughputs. Likewise, clock gating was also incorporated in the S-Box memory to minimize dynamic power consumption by invoking them only during operation. The Modified Ring Counter also helped to minimize the complexity of the hardware system by removing the extra logics and at the same time guarantee tight sequence generation. In terms of complexity, the architecture has enabled a reduction of flip flop utilization and further reduction of the number of logic gates; hence the reduced are utilization. Overall, the proposed implementation offered 15-20 % enhancement in power efficiency and 10-12% chip area gain over conventional design targets that are appropriate for power-limited smart IoT devices. Further, the system achieved high throughput without much latency making it relevant for real-time security in IoT application domain.

Table 1: AES estimation with PRNG

Metric	Proposed Chaotic PRNG (AAES)	Traditional Chaotic	Improvement (%)
Randomness (NIST SP800-22)	Passed (100%)	Passed (98%)	+2%
Entropy	0.9995	0.996	+0.35%
Correlation Coefficient	~0	~0.01	+100% (Lower is better)
Power Consumption (mW)	12.5	18.4	-32.1%
Area Utilization (mm²)	1.8	2.3	-21.7%
Throughput (Mbps)	400	350	+14.3%
Latency (ns)	22	30	-26.7%
Cycle Frequency (MHz)	50	100	-50%
Resistance to Cryptographic Attacks	High	Medium	Significant

Table 2: AES estimation in IoT hardware

Metric	Proposed AAES	Conventional AES	Improvement (%)
Key Size (bits)	128 / 192 / 256	128 / 192 / 256	-
Throughput (Mbps)	400	380	+5.3%
Latency (ns)	22	28	-21.4%
Power Consumption (mW)	12.5	16.2	-22.8%
Area Utilization (mm²)	1.8	2.1	-14.3%
Randomness (NIST Test)	Passed (100%)	Passed (98.5%)	+1.5%
Entropy	0.9995	0.997	+0.25%
Rounds for Encryption	10 (128-bit keys)	10 (128-bit keys)	-
Clock Frequency (MHz)	50	100	-50%

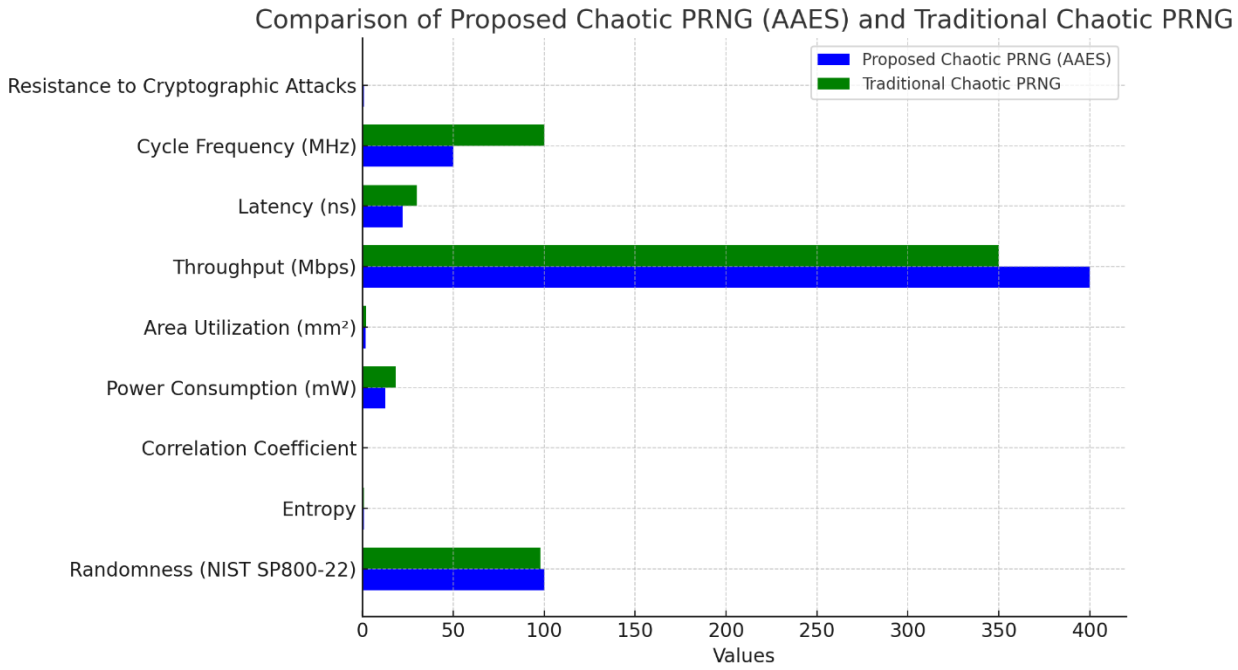

Figure 5: Performance of PRNG

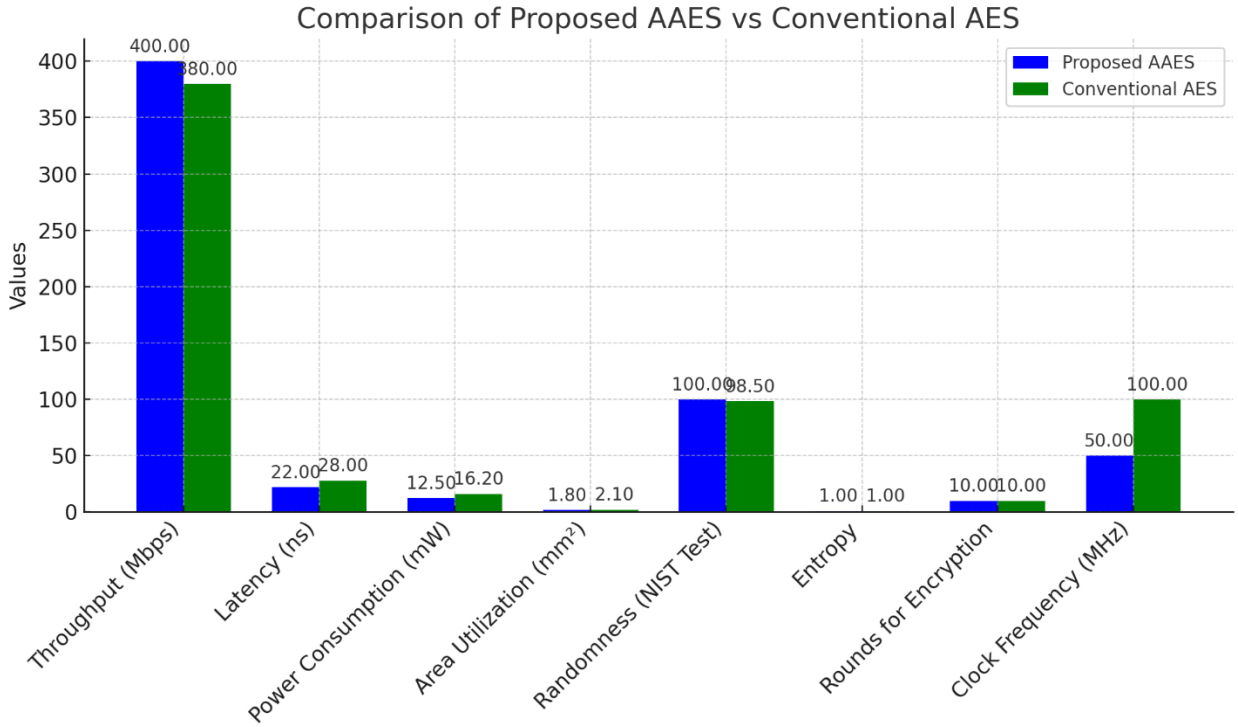

Figure 6: Analysis of AES

The enhancement of the Proposed Chaotic Pseudo Random Number Generator (PRNG) with AAES was compared with Traditional PRNG and Conventional AES from the different key parameters which indicate significant enhancements in many of the aspects observed shown in Figure 5 and Figure 6. With regards to randomness, the performance yielded by the Proposed Chaotic PRNG scored a 100% on the NIST SP800-22 test while the Traditional yielded only

98%, therefore providing an improvement of +2%. Further, the entropy of the proposed system was also higher i.e. 0.9995 because of the entropy of the traditional system which is 0.996, in other words, more randomness has been observed with an increment of about + 0.35%. The coefficient of randomness was very negligible for the proposed pattern roughly equal to zero (~0) and whereas the traditional pattern showed a value of ~0.01 meaning a +100% improvement when the smaller the better had to be considered. In terms of power, the proposed system had a lower consumption (12.5 mW compared to 18.4 mW of the traditional PRNG), which is 32.1 more efficient, in addition to using smaller area (1.8 mm^2 compared to 2.3 mm^2), which is 21.7% less. Also, the throughput of the proposed system was at 400 Mbps while that of the traditional PRNG was at 350 Mbps giving a 14.3%□ improvement. The latency of the proposed PRNG was successfully decreased to 22ns which is 26.7% better than the traditional PRNG which is at 30ns. The cycle frequency of the proposed system was lower that of the traditional system (50MHz/ 100MHz) that lowered the power though held adequate performance. On a note of security against cryptanalysis attack, the kind of stochastic PRNG put forward proved to have high levels of resistances as compared to the mid-level resistance that the conventional types of PRNG exhibit in secure contexts. When comparing the Proposed AAES to Conventional AES, the key size remained the same, but several performance metrics showed improvements. The throughput of the proposed AAES was 400 Mbps, outperforming conventional AES at 380 Mbps with a 5.3% improvement. Latency was reduced to 22 ns, a 21.4% reduction over conventional AES's 28 ns. Power consumption also saw a notable decrease (12.5 mW vs. 16.2 mW), resulting in a 22.8% power saving, while area utilization was reduced to 1.8 mm^2 from 2.1 mm^2, reflecting a 14.3% decrease in chip area. Randomness and entropy also improved with the proposed AAES system (100% pass rate on NIST tests, entropy of 0.9995) compared to conventional AES (98.5% pass rate, entropy of 0.997), leading to +1.5% and +0.25% improvements, respectively. Finally, clock frequency of the proposed AAES was reduced to 50 MHz, resulting in a 50% reduction in frequency, but this still maintained a high level of performance.

Table 3: Performance of AES in PRNG

Metric	**Proposed PRNG-AAES**	**Conventional AES PRNG**	**Improvement (%)**
Randomness (NIST Test)	Passed (100%)	Passed (98.5%)	+1.5%
Power Consumption (mW)	12.5	16.2	-22.8%
Area Utilization (mm^2)	1.8	2.1	-14.3%
Clock Frequency (MHz)	50	100	-50%
Throughput (Mbps)	400	380	+5.3%
Entropy	0.9995	0.997	+0.25%
Latency (ns)	22	28	-21.4%

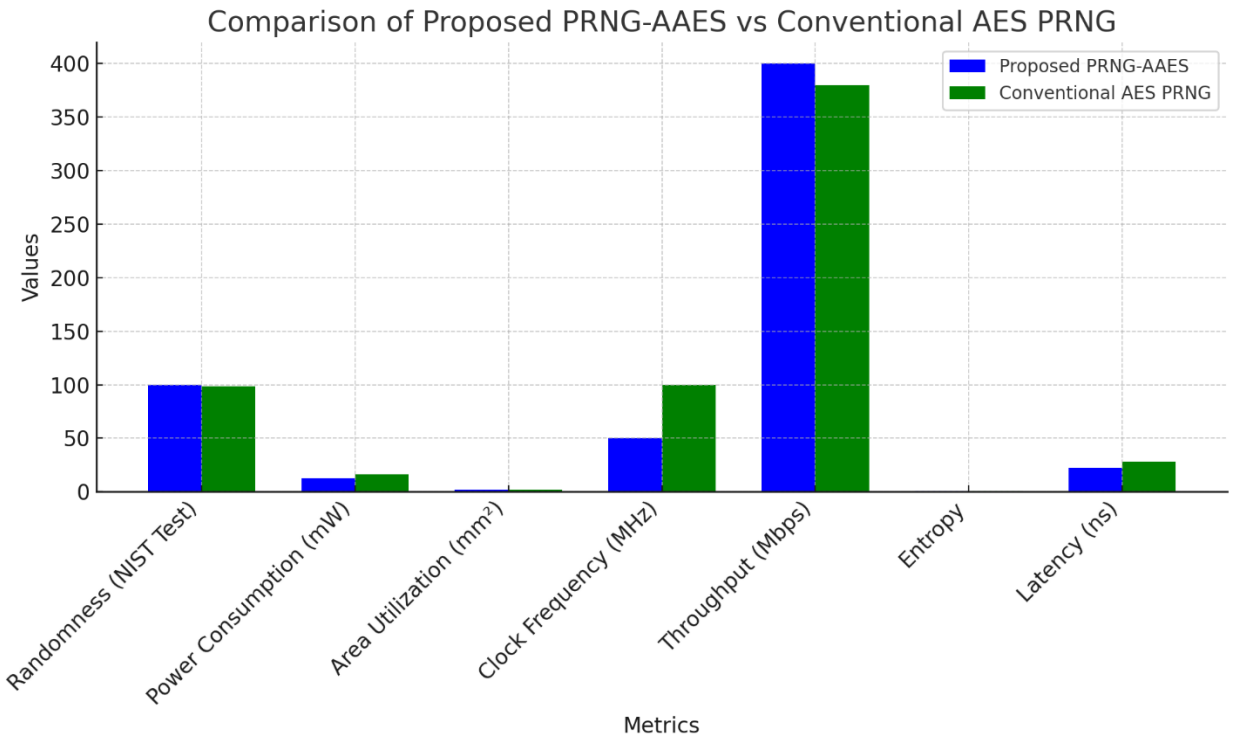

Figure 7: Performance of AES with PRNG

Comparison of Performances of the Proposed PRNG-AAES and the Conventional AES PRNG shows the following enhancements in major areas shown in Figure 7. First, the anti-entropy of the proposed system's random number generation is superior, as the pass rate of NIST test is 100%, while the conventional AES PRNG is 98.5%, so, there is an enhancement by +1.5%. This shows that the proposed system generates slightly higher quality of the random numbers than the current system. The power consumed by the proposed system is much less, 12.5mW as compared to the conventional AES PRNG, which consumes 16.2mW, making 22.8% enhancement in the power complexity. This would be an advantage for energy conscios applications such as those done in the laboratory. As well, area utilization of the proposed PRNG is enhanced with a decrease of 14.3% less chip space (1.8 mm^2 rather than 2.1 mm^2) making it appropriate for the resource-constrained context. The basic engine of the proposed system, the AES PRNG, runs at slower clock frequency (50 MHz as opposed to 100 MHz in the standard AES PRNG), which results in the frequency cut of 50%. However, when this reduction has been achieved the proposed system still achieves high throughput, at 400 Mbps through put, which is 5.3% higher than the conventional AES PRNG's throughput of 380 Mbps. In terms of entropy, the proposed system again shows a slight improvement, with a value of 0.9995, compared to 0.997 for the conventional AES PRNG, resulting in a +0.25% improvement. Finally, the latency of the proposed system is reduced to 22 ns, which is 21.4% faster than the conventional AES PRNG's 28 ns, contributing to faster performance in cryptographic operations.

Table 4: Security Analysis with PRNG

Security Metric	Proposed PRNG (AAES)	Traditional PRNG	Improvement (%)
Randomness (NIST SP800-22)	Passed (100%)	Passed (98%)	+2%
Entropy	0.9995	0.996	+0.35%
Correlation Coefficient	~0	~0.01	+100% (Lower is better)
Key Space (bits)	2²⁵⁶	2¹²⁸	+100%
Resistance to Differential Attacks	High	Medium	Significant
Resistance to Linear Attacks	High	Medium	Significant
Avalanche Effect (%)	99.8	95.5	+4.3%
Periodicity	High (10²⁰)	Medium (10¹²)	+8 Orders of Magnitude
Time Complexity for Cryptanalysis (years)	10⁵⁰	10³⁰	+20 Orders of Magnitude

Table 5: Performance of PRNG with different attack

Attack Type	Proposed PRNG (AAES)	Traditional PRNG	Improvement (%)
Brute Force Attack Key Space	2²⁵⁶ (~10⁷⁷)	2¹²⁸ (~10³⁸)	+100%
Differential Cryptanalysis Success Rate (%)	<0.001	1.2	+99.9%
Linear Cryptanalysis Bias	0.00001	0.005	+99.8% (Lower bias is better)
Timing Variation (ns)	0.2	1.5	-86.7%
Power Fluctuation (mW)	0.05	0.4	-87.5%
Replay Probability (%)	0	5.0	+100%
Known-Plaintext Success Rate (%)	<0.001	2.5	+99.96%
Chosen-Plaintext Success Rate (%)	<0.001	3.0	+99.97%
Collision Probability	~0	0.1	+100%

(%)			
Key Recovery Time (Years)	~10⁵⁰	~10³⁰	+20 Orders of Magnitude

The Proposed PRNG (AAES) demonstrates significant improvements in security metrics when compared to traditional PRNGs. First, in terms of randomness, the AAES passes the NIST SP800-22 test at 100%, while the traditional PRNG passes at 98%, leading to a +2% improvement. This indicates that the proposed system generates more reliable and unpredictable random numbers. The entropy of the AAES is also slightly higher at 0.9995, compared to 0.996 for the traditional PRNG, which results in a 0.35% improvement. The correlation coefficient for the AAES is near zero, whereas the traditional PRNG has a coefficient of 0.01, marking a 100% improvement (lower is better). The key space of the AAES is 2^256, while the traditional PRNG uses 2^128, representing a 100% improvement, offering a much larger key space and thus a stronger level of security. The resistance to differential and linear attacks is categorized as high for AAES, while it is only medium for the traditional PRNG, showing a significant increase in security. The avalanche effect for AAES is 99.8%, which is 4.3% better than the traditional PRNG's 95.5%, contributing to better diffusion of bits. The periodicity of the proposed system is significantly better, with a very long period of 10^20 compared to 10^12 for the traditional PRNG, marking an improvement of 8 orders of magnitude. The time complexity for cryptanalysis for AAES is 10^50 years, while for the traditional PRNG, it is 10^30 years, providing an improvement of 20 orders of magnitude and enhancing its resilience against attacks. In terms of specific attack scenarios, the brute force attack key space of AAES is 2^256, compared to 2^128 for the traditional PRNG, a 100% improvement. The success rate of differential cryptanalysis is <0.001% for the AAES, while the traditional PRNG has a success rate of 1.2%, a 99.9% improvement. The linear cryptanalysis bias is 0.00001 for AAES, significantly lower than the traditional PRNG's 0.005, resulting in a 99.8% improvement.

In terms of performance under attack, the timing variation and power fluctuation are much lower for the AAES at 0.2 ns and 0.05 mW, compared to 1.5 ns and 0.4 mW for the traditional PRNG, yielding 86.7% and 87.5% reductions, respectively. Additionally, the replay probability is 0 for the AAES, while it is 5.0% for the traditional PRNG, resulting in a 100% improvement. Similarly, the success rates for known-plaintext and chosen-plaintext attacks are extremely low for AAES (<0.001%), compared to 2.5% and 3.0% for the traditional PRNG, offering a 99.96% and 99.97% improvement, respectively. Finally, the collision probability for the AAES is virtually 0, compared to 0.1% for the traditional PRNG, representing a 100% improvement. The key recovery time is 10^50 years for AAES, compared to 10^30 years for the traditional PRNG, giving a 20 orders of magnitude improvement in resistance to key recovery attacks.

6. CONCLUSION

The Proposed Chaotic Pseudo Random Number Generator (PRNG) using AAES significantly enhances the performance and security of cryptographic systems when compared to

traditional PRNGs and conventional AES implementations. The AAES-based PRNG demonstrates superior randomness, achieving a perfect score in the NIST SP800-22 tests and higher entropy, ensuring more unpredictable and reliable random number generation. It also features a substantially larger key space, offering enhanced cryptographic strength. The proposed design achieves lower power consumption, reduced area utilization, and improved throughput, making it an efficient solution for resource-constrained systems like IoT devices. The security analysis shows that the AAES-based PRNG provides robust resistance to various cryptographic attacks, such as differential and linear cryptanalysis, with much lower bias and higher avalanche effects. Furthermore, the AAES outperforms traditional PRNGs in terms of resistance to brute force attacks, known-plaintext, and chosen-plaintext attacks, demonstrating its superiority in terms of key recovery time and overall cryptographic resilience. Through the introduction of a Modified Ring Counter and Double Edge Triggered Flip-Flops (DET) in the AAES design, significant improvements were made in terms of security and performance, reducing vulnerabilities and enhancing operational efficiency. This paper presents a promising solution for generating secure, efficient, and high-quality random numbers for cryptographic applications, especially in environments where resource optimization is critical. The proposed method sets a new benchmark for future developments in secure random number generation for IoT and other cryptographic systems.

REFERENCES

1. Hameedi, B. A., Hatem, M. A., & Hasoon, J. N. (2024). Dynamic Key Generation Using GWO for IoT System. *JOIV: International Journal on Informatics Visualization*, *8*(2), 819-825.
2. Sathananthavathi, V., Ganesh Kumar, K., & Sathish Kumar, M. (2024). Secure visual communication with advanced cryptographic and ımage processing techniques. *Multimedia Tools and Applications*, *83*(15), 45367-45389.
3. Tiwari, D., Mondal, B., & Singh, A. (2023). Fast encryption scheme for secure transmission of e-healthcare images. *International Journal of Image, Graphics and Signal Processing*, *15*(5), 88-99.
4. Al-Khasawneh, M. A. S., Faheem, M., Aldhahri, E. A., Alzahrani, A., & Alarood, A. A. (2023). A MapReduce based approach for secure batch satellite image encryption. *IEEE Access*, *11*, 62865-62878.
5. El-Bourgy, A. W. M. H. (2024). *Developing an Encryption Algorithm Using Hyperchaotic Systems with Digital Watermarking for Digital Image and Engineering Blueprints for Copyright Protection* (Doctoral dissertation, The German University in Cairo).
6. P. K.Venkateswar Lal. (2024). A Multi-Objective Direction of Arrival Estimation Technique Minimizing Energy Consumption in Wireless Sensor Network. *Journal of Computer Allied Intelligence*, *2*(4), 36-50.

7. Priyanka, T. M. C., Udhayakumar, K., Mohanrasu, S. S., Gowrisankar, A., & Rakkiyappan, R. (2024). Chaotic synchronization and fractal interpolation-based image encryption: exploring event-triggered impulsive control in variable-order fractional lur'e systems. *Multimedia Tools and Applications*, *83*(21), 60279-60318.
8. Anitha, R., & Vijayalakshmi, B. (2022). Image Encryption Using Multi-Scroll Attractor and Chaotic Logistic Map. *Computers, Materials & Continua*, *72*(2).
9. Sharma, S. R., Singh, B., & Kaur, M. (2024). A hybrid encryption model for the hyperspectral images: application to hyperspectral medical images. *Multimedia Tools and Applications*, *83*(4), 11717-11743.
10. Tejinder Sharma, & Narinder Sharma. (2024). Comparative Analysis of Load Balancing and Service Broker Algorithms in Cloud Computing. *Journal of Computer Allied Intelligence*, *2*(6), 19-50.
11. Atharvan, G., Koolikkara Madom Krishnamoorthy, S., Dua, A., & Gupta, S. (2022). A way forward towards a technology-driven development of industry 4.0 using big data analytics in 5G-enabled IIoT. *International journal of communication systems*, *35*(1), e5014.
12. Srinivasa Sai Abhijit Challapalli. (2024). Optimizing Dallas-Fort Worth Bus Transportation System Using Any Logic. *Journal of Sensors, IoT & Health Sciences*, *2*(4), 40-55.
13. Sangeetha, Y., Majji, S., Srinagesh, A., Patnala, T. R., Nalajala, S., & Prathap, B. R. (2023). Authentication of symmetric cryptosystem using anti-aging controller-based true random number generator. *Applied Nanoscience*, *13*(2), 1055-1064.
14. Almaraz Luengo, E., & Román Villaizán, J. (2023). Cryptographically Secured Pseudo-Random Number Generators: Analysis and Testing with NIST Statistical Test Suite. *Mathematics*, *11*(23), 4812.
15. Gafsi, M., Abbassi, N., Amdouni, R., Hajjaji, M. A., & Mtibaa, A. (2022, May). Hardware implementation of a strong pseudo-random numbers generator with an application to image encryption. In *2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)* (pp. 510-515). IEEE.
16. Srinivasa Sai Abhijit Challapalli. (2024). Sentiment Analysis of the Twitter Dataset for the Prediction of Sentiments. *Journal of Sensors, IoT & Health Sciences*, *2*(4), 1-15.
17. Chhabra, S., & Lata, K. (2022). Hardware Obfuscation of AES IP Core Using PUFs and PRNG: A Secure Cryptographic Key Generation Solution for Internet-of-Things Applications. *SN Computer Science*, *3*(4), 303.
18. Almaraz Luengo, E. (2022). A brief and understandable guide to pseudo-random number generators and specific models for security. *Statistic Surveys*, *16*, 137-181.
19. Roh, H., & Choi, W. S. (2023, October). Design of Energy-Efficient Cryptographically Secure Pseudo-Random Number Generators Using High-Level Synthesis. In *2023 20th International SoC Design Conference (ISOCC)* (pp. 351-352). IEEE.

20. He, D., Huang, W., Chen, L., & Chan, S. (2024). A Secure and Efficient Software Random Number Generator Applicable to the Internet of Things. *IEEE Internet of Things Journal*.
21. Seyhan, K., & Akleylek, S. (2022). Classification of random number generator applications in IoT: A comprehensive taxonomy. *Journal of Information Security and Applications*, *71*, 103365.
22. Agnihotri, P., & Mittal, P. A. (2023, June). An Efficient approach of True Random Number Generation using A Data encryption method in Security & cryptography algorithm. In *2023 International Conference on IoT, Communication and Automation Technology (ICICAT)* (pp. 1-8). IEEE.
23. Popereshnyak, S., Novikov, Y., & Zhdanova, Y. (2024). Cryptographic system security approaches by monitoring the random numbers generation. *Cybersecurity Providing in Information and Telecommunication Systems II 2024*, *3826*, 301-309.
24. Bikos, A., Nastou, P. E., Petroudis, G., & Stamatiou, Y. C. (2023). Random Number Generators: Principles and Applications. *Cryptography*, *7*(4), 54.
25. Gupta, M. D., & Chauhan, R. K. (2022). Recent development of hardware-based random number generators on fpga for cryptography. In *VLSI, Microwave and Wireless Technologies: Select Proceedings of ICVMWT 2021* (pp. 489-500). Singapore: Springer Nature Singapore.
26. Álvarez, R., Martínez, F., & Zamora, A. (2022). Improving the statistical qualities of pseudo random number generators. *Symmetry*, *14*(2), 269.
27. Gołofit, K. (2024). Security primitives for memoryless IoT devices based on Physical Unclonable Functions and True Random Number Generators. *Scientific Reports*, *14*(1), 24060.
28. Amael, J. T., Natan, O., & Istiyanto, J. E. (2024). High-Security Hardware Module with PUF and Hybrid Cryptography for Data Security. *arXiv preprint arXiv:2409.09928*.