Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Secure Low Power FPGA Design for Detection of Camouflage Attacks in Soc Devices

[1]Palanivel S., [2] Deeban Chakravarthy R., [3]Sai Sathish P.,[4] Vasanthan S., [5]Prabhu V.
[1]Assistant Professor, ECE, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College
[2,3,4]UG Scholar, ECE, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College
[5]Professor, ECE, Vel Tech Multi Tech Dr. Rangarajan Dr.Sakunthala Engineering College

Abstract: - The semiconductor industry faces new challenges due to piracy and misuse of intellectual property (IP), where people who do not trust IP life will copy, reverse engineer, or extract important information. Locking down logic management, that is, placing additional logic controlled by switches on the creative side of the IP to run when the required switches are not available, is a good way to prevent IP hardware from being blocked from attacks. A new synthesis-based persistent attack method for assessing the stability of system code in existing systems. Each critical input field will be evaluated as a countermeasure, looking for relevant designs to help determine appropriate priority. The built-in prediction model of the proposed system is an important component of the evaluation. The system has machine learning algorithms that try to find attack events as quickly as possible using various attack parameters based on behavior. To achieve this, the system operates in two modes; automatic mode continues to work on the chip until it is activated. The second type is the sleep accelerator type, which works in inactive death and eliminates the resistance that the IC may hold.

Keywords*: IP, PUF, DRAM*

1. Introduction

Physical Unclonable Functions act as a fundamental concept within the hardware security domain, leveraging the natural discontinuities within a device to develop unique and ambiguous responses to situations stimulus [1]. The concept is closely related to human body biometric singularity, exploiting the unique imperfections in silicon creation to provide an unparalleled cryptograph for each integrated circuit [2]. The discontinuities range from variations in signal delay, threshold voltage, gains factors, amongst others. Thus, these imperfections, referred to as noise, form a basis for constructing a distinct encryption key from a one-off integrated circuit [3]. The DS28S60 coprocessor from the Maxim Integrated is a well-suited example for the PUF applications in generating encryption keys due to the unique physical properties that inherently define each IC.the primary distinction lies in the fact that, as opposed to traditional cryptographic techniques that require pre-stored keys, PUFs function based on key creation principles in response to fresh challenges, thus granting this security layer an additional physical hardware component [4-5]. As an instance of this strategy in action, DRAM PUFs utilize the fluctuations in the rate of charge leaking out of DRAM cells, a ratio that is deeply impacted by the details of the manufacturing technology [6]. It not only bolsters security with unique hardware but also presents a useful approach for on-the-spot encryption and secure authentication needs [7] furthermore key storage is not feasible when using PUF technology. As a result of generating encryption keys shortly in response to numerous challenges and erasing them following use, PUFs dramatically minimize the danger of key extraction attacks. Because the key generation process is short-lived, key security is imposingly strengthened, thus making any adversarial actions to breach the system increasingly complex [8-9]. However, the contemporary security environment is continually changing as newly developed machine learning capabilities introduce extra issues to PUF-based systems. Recent literature has already established numerous difficulties and demonstrated strong ML algorithms' capacity to replicate PUF responses, necessitating a new kind of PUF that can withstand these types of attacks [10-11]. As a response to the presented emerging threats, the research community has suggested novel

PUF designs that increase security. They include XOR PUF based solutions, Feedforward PUFs, and others. Nevertheless, these enhancements are consistently associated with enhanced power consumption, creating a considerable challenge for low-power devices' implementation [12-13]. Faced with this challenge, research has been directed towards developing optimized PUF architectures capable of offering increased security without sacrificing power efficiency. This has resulted in the development of hybrid solutions where standard PUF mechanisms are combined with secure cryptographic algorithms. Such solutions aim to achieve synergy with both aspects [14-15]. With the increasing use of PUF technology in almost every field such as IoT devices, secure communication networks to name a few, the need for innovation and experimentation increases exponentially. The search for low-power, high-security PUF designs is one of the most important initiatives in the field and has the power to change the principles of hardware security in the modern world [16][17].

Due to differences in manufacturing processes, the characteristics of each metal–oxide–silicon transistor or wire slightly different in a physical device. These differences allow us to measure the difference in the response of two PUF samples to the same problem, allowing PUFs to be used as dedicated fingerprinting tools Due to the inability to control process changes during integrated circuit (IC) manufacturing, hardware replication of PUFs used in ICs is not possible. it can be intercepted by the attacker only for the short time it takes for the PUF to attack. Electronic equipment are more vulnerable to physical attacks than unpowered ones. PUFs are the perfect cryptographic primitive for match authentication in applications where tamper protection is required because of their qualities. Reliable hardware solutions, like Apple's Secure Enclave that prevents FBI access to iPhones, are pricey for low-end devices and only work on high-end models. Software techniques frequently restrict the offered guarantees.

Although various PPUs introduced, for search an effective and safe PPU continues. Well-known PUFs are easily vulnerable to ML model-based attacks. To improve the robustness of PUF in attack modelling various models have been proposed, including XOR PUF, Wear out PUF Feedforward PUF Insertion PUF, Exploitation PUF. However, the power consumption of these models is often too high for limited-use devices. It has also been proposed to use some secure hash function to hash the PUF response. Likewise, entry-level devices such as sensors or actuators may lack the memory, computing resources, and performance to take full advantage of strong cryptographic hash functions such as SHA-3. Low-power design is a set of ideas and techniques designed to reduce the overall and static power consumption of integrated circuits (ICs).

Reducing the energy consumption of all energy sources, taking into account all energy products, is the goal of low energy production. By maximizing the energy content, the overall energy usage is decreased. Static and dynamic energy are both components of energy balance. AC power supplies and short-circuit power supplies are two types of power supplies. Leakage current, or current passing through a transistor while it is not in operation, is included in static power. Change Time of Operating Frequency Capacitive Load Voltage Breach Present Test: Any equipment that needs to give maximum power will use more power the higher the maximum current, or voltage. On the other hand, the overall power decreases with decreasing voltage. Every variation has undergone extensive testing utilizing both robust and ineffective methodologies to attain the highest performance with minimal power consumption.

2. Design and Analysis

The proposed methodology focused on to overcome various clock issues in system-on-chip devices, physical protection devices are needed to test and analyze various functions of FPGA chips. An in-depth benchmark was created to test FPGA devices with various clock tree synthesizers (sweep generators, configurable clock synthesizers, digital phase-locked loops, etc.). To investigate the concept of physical attack detection in SOC devices, application circuits must be designed and tested. Multitasking clock synthesizers and clock distributors require multiple resources for testing. In your case, it looks like you are running simulations to test how the power meter can detect the effects of physical attacks on the SOC device. This testing will include modeling SOC devices, voltage-based sensors, and various types of physical attacks to test the effectiveness of the interception device. Some of the possible steps in this experiment may include creating a detailed model of the SOC device, including its features and power consumption characteristics. Use a voltage meter as a voltage

indicator to monitor the voltage level of SOC devices. Simulate different types of physical attacks, such as voltage spikes, signal interruptions, or attempts to interfere with hardware. Analyze sensor data to identify anomalies or deviations from expected behavior that may indicate an attack. Evaluate the effectiveness of an intrusion detector by its ability to accurately detect and respond to attacks while minimizing vulnerabilities. This type of simulation is important for evaluating the robustness and stability of SOC devices and can help design more secure hardware system mode

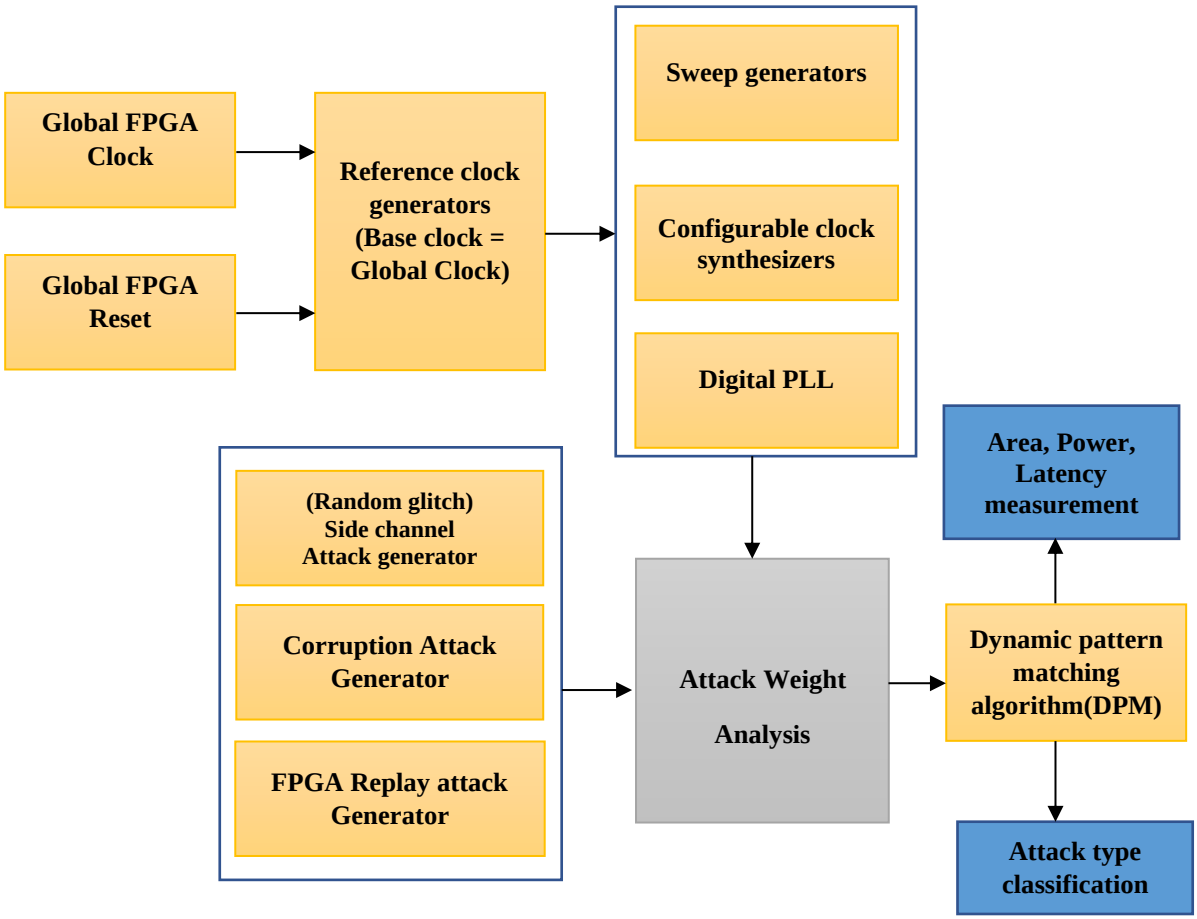

Fig. 1 Operational Workflow Diagram

Reference Clock generator the module is developed to design a reference clock generator derived from global clock, global reset. 20bit clock divider circuit is designed to generate the reference clocks. Test circuit generator from the reference clock generator, sweep generator, clock synthesizer and digital PLL circuits are developed. the design contains configurable architecture with low power techniques used. Design of Attack pattern generator the module contains digital circuits, helpful to generate various patterns of attack scenarios such as side channel attacks, FPGA replay attacks, corruption attacks etc. design of Dynamic pattern matching algorithm the module contains the dynamic pattern matching algorithm evaluated for the purpose of detection and validation of side channel attacks, FPGA replay attacks, corruption attacks etc. Integration the fine state machine enabled process is designed and connected with the sub modules of the process, further the integration of all modules that work without any correlation.

3. Results and Discussion

The FPGA configuration screen shows the locations of the components. Setting "/synthesizer/clk" to "1" will indicate that the clock signal is valid. Elsewhere, "/synthesizer/clr" is "0", indicating that the client has not been removed. The selection signal "/synthesizer/sel" with the value "00000001" refers to the use of binary code to select a specific option in the electronic component. Clock reference '/synthesizer/ref_clk' is currently disabled ('0'). Although the exact functionality is still uncertain without further details, this analysis provides a good insight into the configuration process of the FPGA synthesizer based on the data provided.

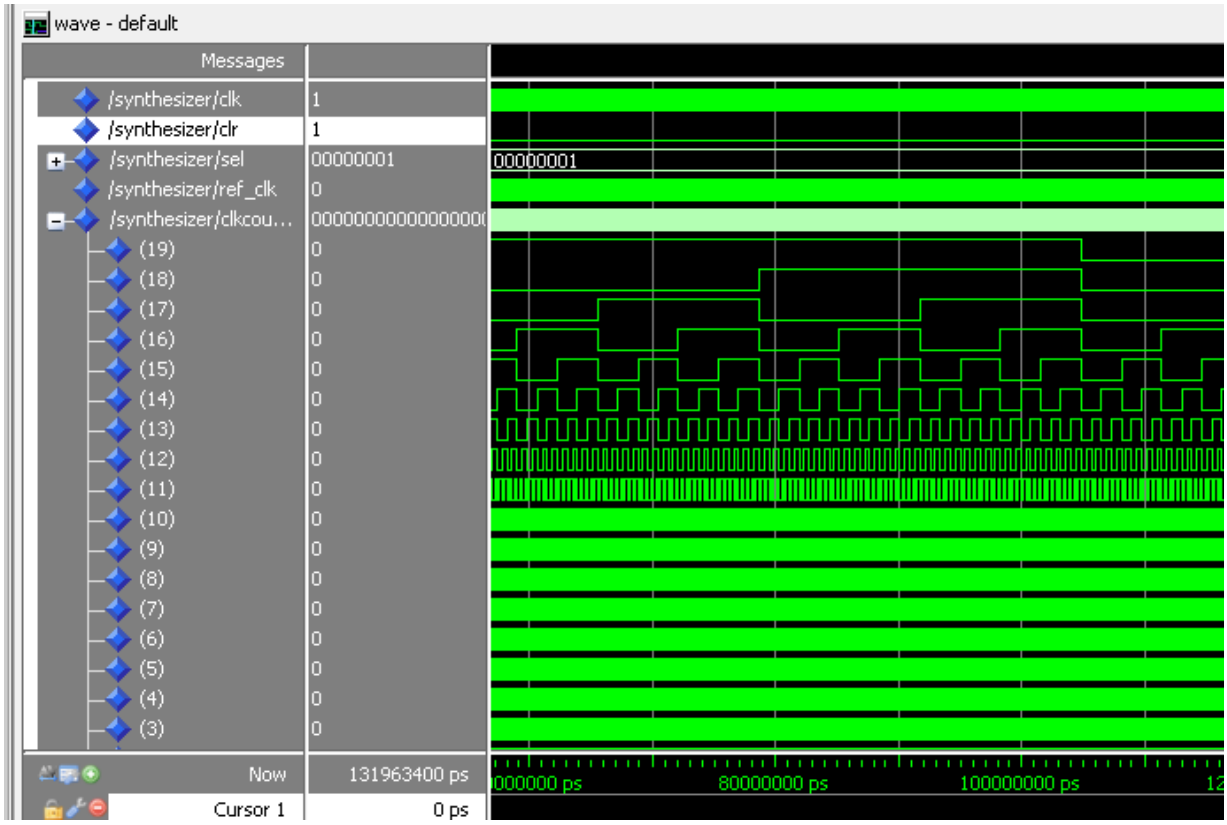

Fig. 2 FPGA Synthesizer Configuration

Block diagram showing data selection (mux) with multiple data inputs (D0-D3) and selection lines (sel). The selection line allows selection from multiple input data by controlling the input data to a single output (Y). the proposed method addresses clock-related issues in SOC devices by testing multiple FPGAs using a combination of power meters and resistors as power meters. The system can use simulation to measure performance by modeling SOC components, integrating sensors, performing analog attacks analyzing sensor data, and measuring performance results. This simulation-based approach provides an efficient, repeatable and controlled environment for testing SOC security devices. The changing nature of communication and the ease of discovery algorithms cannot be ignored. As channel conditions change, signal degradation increases, leading to a higher bit error rate (BER). While strong channel codes can solve this problem, neural network (NN) perceptron's reliance on training data introduces the risk of overfitting. Overcoming these problems requires the use of full semantic information at both the transfer and semantic levels. Intelligent end-to-end (E2E) communication can enable message exchange even in harsh environments by resolving semantic and body noise, ensuring efficient delivery of semantic messages despite channel interference

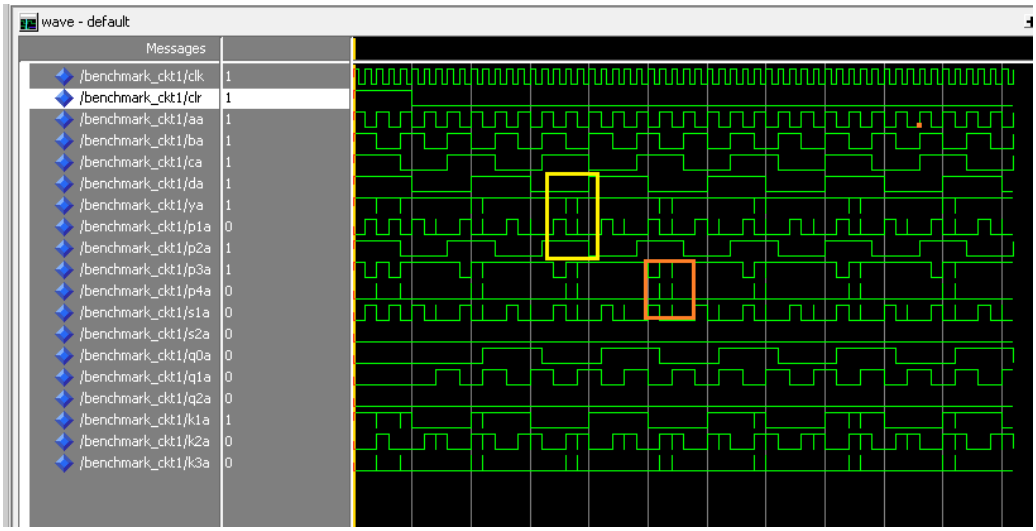

Fig. 3 Pattern Learning Algorithm: Detecting Glitches in a Test Signal

Inspection of program shows simulation of the burr counter algorithm. The algorithm will identify the frame size, check the world time, detect the rising edge of the last signal, increment the burr counter when detected, set the burrs as the correct flag, and continuously monitor. Program showing FPGA synthesizer settings. A value of "1" in "/synthesizer/clk" may indicate an alarm clock. A value of "0" in "/synthesizer/clr" means the synthesizer is not deleted. "/synthesizer/sel" with content "00000001" uses binary code to select a specific option on the device. '/synthesizer/ref_clk' is currently inactive ('0'). Although full functionality is still unclear without further details, this analysis provides a good insight into the configuration process of the FPGAsynthesizer

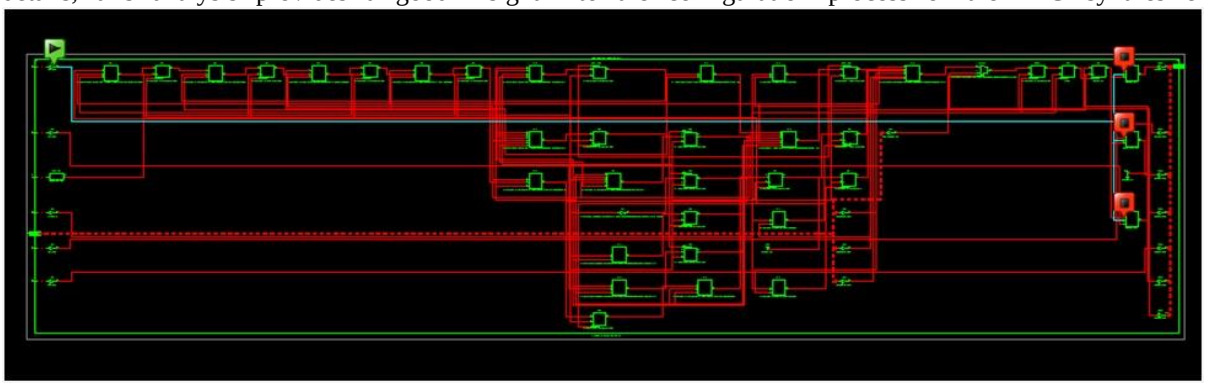

Fig. 4 RTL Schematic View

Device Utilization Summary				
Slice Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Registers	18	11,440	1%	
Number used as Flip Flops	18			
Number used as Latches	0			
Number used as Latch-thrus	0			
Number used as AND/OR logics	0			
Number of Slice LUTs	16	5,720	1%	
Number used as logic	16	5,720	1%	
Number using O6 output only	10			
Number using O5 output only	0			
Number using O5 and O6	6			
Number used as ROM	0			
Number used as Memory	0	1,440	0%	
Number of occupied Slices	9	1,430	1%	
Number of LUT Flip Flop pairs used	17			
Number with an unused Flip Flop	3	17	17%	
Number with an unused LUT	1	17	5%	
Number of fully used LUT-FF pairs	13	17	76%	

Fig. 5 Device Utillization Summary

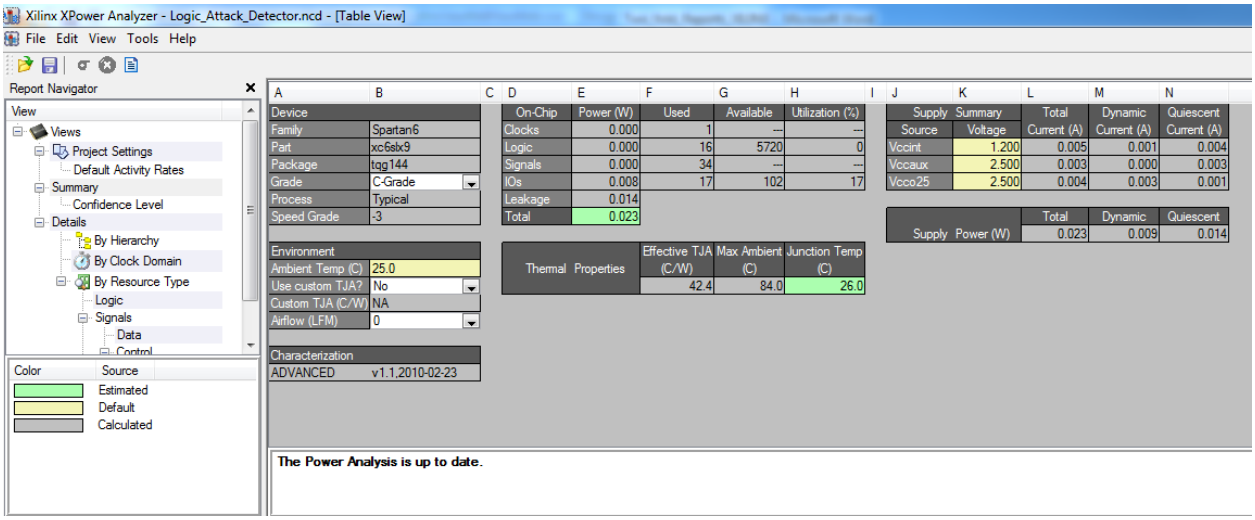

Fig. 6 Power Analysis After Implementation

4. Conclusion

Digital circuits are often affected by external interference. Here we discuss protecting single-chip devices from design faulty detection patterns. System design and evaluation based on the observation line of the weak object is created by the LFSR module. As key authentication, the model can produce the performance of the system measured by power analysis. Digital circuits are sensitive to external interference and need protection to ensure proper operation.

The LFSR module plays an main role in establishing the golden key authentication that allows the system to be authenticated. Additionally, by analyzing the power, the model can assess the execution of the system and provide a good view of its performance and power. Following these strategies can improve the circuit's ability to withstand external interference and ensure proper functioning in a variety of situations. Designers use various techniques to prevent external influences. One such technique involves the use of shielding to reduce the effects of electromagnetic interference (EMI). Additionally, error detection and correction codes are used to notice and flawless errors that may occur due to interference. Additionally, redundancy is often built into the design to ensure that important functions continue to operate even if some components are affected by outages. Together, these ideas help ensure the reliability and robustness of digital circuits against external interference.

Refrences

[1] S. S. Kumar[1] S. S. Kumar, J. Rajendran, O. Sinanoglu, and R. Karri, "Physically Unclonable Functions for Device Authentication and Secret Key Generation," in Journal of Hardware and Systems Security, vol. 2, no. 2, pp. 97-110, June 2018.

[2] G. E. Suh and S. Devadas, "Silicon Physical Random Functions," in Proceess of the 9th ACM Conference on Computer and Communications Security, pp. 148-160, November 2002.

[3] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "On the Foundations of Physical Unclonable Functions," in IACR Cryptol. ePrint Archive, vol. 2007, no. 227, pp. 1-15, 2007.

[4] L. Bolotnyy and G. Robins, "PUF-based Cryptography: A New Paradigm for Security of Integrated Circuits," in IEEE International Conference on RFID, pp. 58-64, April 2007.

[5] Maxim Integrated Products, Inc "Maxim Integrated DS28S60: Deep Dive into PUF Technology for Secure Cryptographic Key Generation," Maxim Integrated Products, Inc., Application Note 6865, pp. 1-12, March 2019.

[6] M. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "Exploring DRAM PUFs for Cryptographic Key Generation in IoT Devices," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 450-463, May-June 2020.

[7] Z. Chen, S. Feng, Y. Xu, and J. Zhang, "validation and Key Generation Based on DRAM PUFs for IoT Security," in Sensors, vol. 19, no. 14, pp. 3165, July 2019.

[8] S. Sivasaravanababu, V. Prabhu , V. Parthasarathy , G. Saravana Kumar (2023) "A Heuristic-Concatenated Feature Classification Algorithm (H-CFCA) for autism and epileptic seizure detection", Biomedical Signal Processing and Control, DOI.org/10.1016/j.bspc.2023.105245, July 2023,.

[9] H. T. Thangam, G. Gayathri, and T. Madhubala, "XOR PUFs and Beyond: Selective Enhancement of PUF Security," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 7, pp. 1149-1162, July 2015.

[10] K. Juretus and I. Savidis, "Machine Learning Attacks on Physical Unclonable Functions: A New Generation of Cryptographic Challenges," in Proceedings of the IEEE Symposium on Security and Privacy Workshops, pp. 123-127, May 2018.

[11] A. Maiti and P. Schaumont, "Towards Resilient Physical Unclonable Functions: The Design Space of Anti-Machine Learning," in Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1143-1148, March 2019.

[12] Sivasaravanababu, S. & Prabhu, V. & v, Parthasarathy & Mahendran, Rakesh. (2021). An efficient epileptic seizure detection based on tunable Q-wavelet transform and DCVAE-stacked Bi-LSTM model using electroencephalogram. The European Physical Journal Special Topics. 231. 10.1140/epjs/s11734-021-00380-x.

[13] A. Baumgarten, A. Tyagi, and J. Zambreno, "Power Considerations for PUF Circuits in IoT Applications," in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 7, no. 4, pp. 541-553, December 2017.

[14] T. Thangam, G. Gayathri, and T. Madhubala, "Hybrid PUF Designs: Merging Hardware Security with Cryptography," in IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 3, pp. 272-285, May-June 2017.

[15] M. Rostami, F. Koushanfar, and R. Karri, "Secure Hash Function Based development for Physical Unclonable Functions," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1191-1206, June 2016.

[16] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "The Advancement of PUF Security for Internet of Things Devices," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1248-1259, October 2017.

[17] A. Baumgarten, A. Tyagi, and J. Zambreno, "Challenges and Opportunities in Low-Power PUF Design for Secure IoT Deployments," in IEEE Access, vol. 5, pp. 5296-5306, March 2017.