iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** VI **Month of publication:** June 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.72696

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue VI June 2025- Available at www.ijraset.com*

# Enhancement of AES Security On FPGA: Mitigating Side Channel Attacks

Arcot Someshwaran Tushar[1], Nirmala Devi M[2]
[1]*Department of Electronics and Communication Engineering, PES University, RR Campus, Bengaluru, India*
[2]*Hardware Security Research Lab, Department of Electronics and Communication Engineering, PES University, RR Campus, Bengaluru, India*

***Abstract:*** ***This work proposes a hardware-augmented variant of the Advanced Encryption Standard (AES) to mitigate side-channel attack (SCA) vulnerabilities. A suite of countermeasures, including noise injection, dummy operations, and current smoothing—aimed at normalising power and electromagnetic emissions, has been applied and evaluated. The augmented AES architecture is synthesised and evaluated on a field-programmable gate array (FPGA) platform using Vivado, demonstrating functional correctness and enhanced resistance to physical attacks with little resource overhead. This approach indicates the efficacy of integrating lightweight defences in cryptographic hardware, offering a fair trade-off between security and performance in practical implementations.***
***Keywords: AES, SCA, Countermeasures, Masking, Randomisation, Noise Injection, Dummy operations.***

## I. INTRODUCTION

Advanced Encryption Standard (AES) has become a building block in contemporary cryptographic systems, offering protection to data in various applications ranging from financial transactions to secure communication, embedded systems, and military-grade security systems. Its prevalence is attributed to its mathematical solidity, performance, and approval by the National Institute of Standards and Technology (NIST). However, even though AES is cryptographically secure at the algorithmic level, hardware implementations of AES are susceptible to a class of physical attacks known as side-channel attacks (SCAs). Unlike conventional cryptanalysis, in which an attempt is made to find vulnerabilities within algorithms, SCAs exploit physical leaks—i.e., power consumption variations, electromagnetic radiation, and timing variations—induced during cryptographic processing to extract confidential information like encryption keys. These vulnerabilities assume special, critical importance in embedded and Internet of Things (IoT) environments, where attackers could have physical access to or control of the hardware. Within the wide variety of side-channel approaches, the power analysis attacks—Simple Power Analysis (SPA) and Differential Power Analysis (DPA)—are best understood and these are the most powerful. SPA involves examination of patterns visible in power traces that arise in cryptographic calculations, while DPA uses statistical processing of several power traces with the goal of extracting secret keys, even with added noise. Electromagnetic Analysis (EMA) is also perilous but attacks electromagnetic radiation instead of power lines, usually yielding better spatial resolution with no physical contact. The growing sophistication of such attacks, driven by signal processing, machine learning, and low-cost measurement technology, has reemphasised the need to develop efficient countermeasures that shield AES hardware implementations in real-world applications. Traditional defences like masking and algorithmic obfuscation perform well in theory but either become too computationally costly or burdensome for low-resource hardware platforms. Furthermore, one line of defence is inadequate against well-armed attackers with multiple attack vectors. Thus, in this work, enhancing the security of AES against SCAs without degrading its performance or incurring much higher resource utilisation is suggested. A Suite of three lightweight yet effective approaches—random noise injection, dummy operation insertion, and current smoothing is investigated to mask the correlation between processed data and physical emanations. Each of these methods attacks specific leakage vectors and, in combination, offers a strong multi-tiered defence. The goal of this research is to incorporate these countermeasures into the AES design and assess their real-world effectiveness in the field on an FPGA platform. The proposed modifications are described at the Register Transfer Level (RTL) and are synthesised using Vivado Design Suite, enabling full analysis of area and performance trade-offs. This work also describes a comparison between the standard and modified AES cores to explore the impact of the deployed defences on the consumption of resources and correctness of encryption. By demonstrating that the security enhancement may be obtained at negligible overhead, this paper contributes an effective and scalable solution to the new challenge of side-channel attack protection in crypto hardware.

©IJRASET: All Rights are Reserved 

The main Contributions of this work are :

*1)* An effective defence against Side-channel attacks while minimising performance loss and resource usage

*2)* A generalised approach that can be modified to suit multiple encryption algorithms.

## II. RELATED WORK AND MOTIVATION

Srivastava et al.[3] proposed SCAR, a Power Side-Channel Analysis framework at the RTL level, using graph neural networks (GNNs) to represent the data and control flow of cryptographic circuits. The framework identifies vulnerabilities in human-understandable form using large language models and is highly accurate in leakage point detection, but suffers from scalability and generalization outside RTL forms.

Iyer et al.[6] performed a comprehensive power and electromagnetic side-channel attack evaluation of AES-128 implemented on both FPGA and ASIC platforms. They examined a broad set of threat models that included black-box, gray-box, and white-box designs, and demonstrated the feasibility of exact EM-based side-channel attacks. Although their evaluation were broad in scope, it demonstrated the limited scope of current countermeasures and inefficiency in generalizing findings across inherently different technologies.

Moos et al.[7] presented an empirical hardware analysis of static power side-channel analysis of the PRESENT cipher. Their analysis concluded the way leakage patterns are influenced by temperature and technology parameters and highlighted the environmental parameters in the success of side-channel attacks. Their analysis, however, only considered 150-nm CMOS processes and did not include modern cryptographic primitives like AES.

Alioto, M [1] conducted a trend analysis of hardware security and presented a comprehensive summary of vulnerabilities and corresponding countermeasures at architectural and circuit levels, highlighting the necessity for multi-layered protection, particularly as devices trend towards low-power, high-density integration [4]. Other researchers have suggested the application of combinatorial testing towards the identification of hardware Trojans and suspicious data flows that may lead to leakage; however, these approaches tend to necessitate large design overhead and may be plagued by inefficient scalability with regard to advanced encryption engines.

Bommana, S. R., et al.[8] proposed a method that combines deep learning with dynamic FPGA reconfiguration to mitigate side-channel attacks on AES implementations. With real-time hardware configuration adaptation, the method disrupts power analysis patterns, enhancing security with low performance overhead. Bayoumi M, et al.[9] conducted an extensive survey covering recent trends and challenges in hardware security, namely vulnerabilities in the integrated circuit supply chain and the explosion of IoT devices. It classifies different types of attacks and addresses cutting-edge defence schemes, paying specific attention to the necessity of strong security frameworks.

Piessens, F., and van Oorschot, P. C [10] Present an overview of side-channel attacks, the paper illustrates how the attackers exploit physical leakages like timing and power usage. It also emphasises the importance of knowing such vulnerabilities in order to develop suitable countermeasures in cryptographic systems. Prates, N. et al.[11] presented a defence system for timing-based side-channel attacks on IoT traffic. Through traffic shaping mechanisms, the solution hides timing information and thus avoids potential leakages, improving the security of IoT communications. Gattu, N. et al.[12] discussed power side-channel attacks and suggested detection methods to identify such vulnerabilities. Using power consumption pattern monitoring, the suggested methods attempt to identify anomalies that indicate side-channel attacks, thus making hardware design safer.

He, J. et al.[13] Discuss a variety of electromagnetic (EM) side channels, surveying several EM-focused attacks and their respective countermeasures. It emphasises the challenge in protecting hardware from EM emissions and necessitates the use of effective masking and shielding mechanisms.

Harrison, J., et al.[14] Introduced a deep learning-based side-channel acoustic attack that is capable of reconstructing keystrokes from audio recordings. With high accuracy, even through video conferencing software, it highlights the potential threat of ubiquitous audio recording devices.

Boutros, A., and Betz, V. (2021). The article explains the development of FPGA architectures, outlining principles and breakthroughs that have an impact on performance and security. It sheds light on the way design decisions affect the vulnerability of the system to side-channel attacks. Even with these improvements, most current solutions are either restricted to certain attack vectors or have high overhead and thus are not feasible for low-resource settings. This is the backdrop against which we build our approach: a combined approach of noise injection, dummy operations, and current smoothing that maximises security without reducing operational efficiency.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue VI June 2025- Available at www.ijraset.com*

## III. THREAT MODEL

The threat model under consideration in this work is that the attacker has physical access to the cryptographic hardware implementing the AES algorithm, e.g., devices such as smart cards, embedded processors, or FPGA-based modules. The attacker can perform non-invasive side-channel attacks, e.g., power and electromagnetic (EM) measurements, without altering the internal device circuitry. Three standard attack models are considered: black-box (where only ciphertext is observable), Gray-box (where plaintext inputs can be manipulated or repeated), and white-box (where full input control is available but no secret key access is given). The attacker can record multiple encryption sessions to enable statistical analysis, e.g., Differential Power Analysis (DPA) or Electromagnetic Analysis (EMA). The aim is to recover the AES secret key by taking advantage of side-channel leakages, even if the algorithmic security is preserved.

## IV. PROPOSED METHODOLOGY

The proposed method seeks to enhance the security of AES hardware implementations against side-channel attacks (SCAs) through the integration of a variety of low-overhead, hardware-oriented countermeasures. The measures are particularly designed to disrupt the correlation between secret key operations and observable physical leakages, such as power consumption and electromagnetic radiation, without compromising the performance and functionality of the AES algorithm. The method is organised into four main phases: threat analysis, countermeasure design, Hardware Implementation and evaluation.

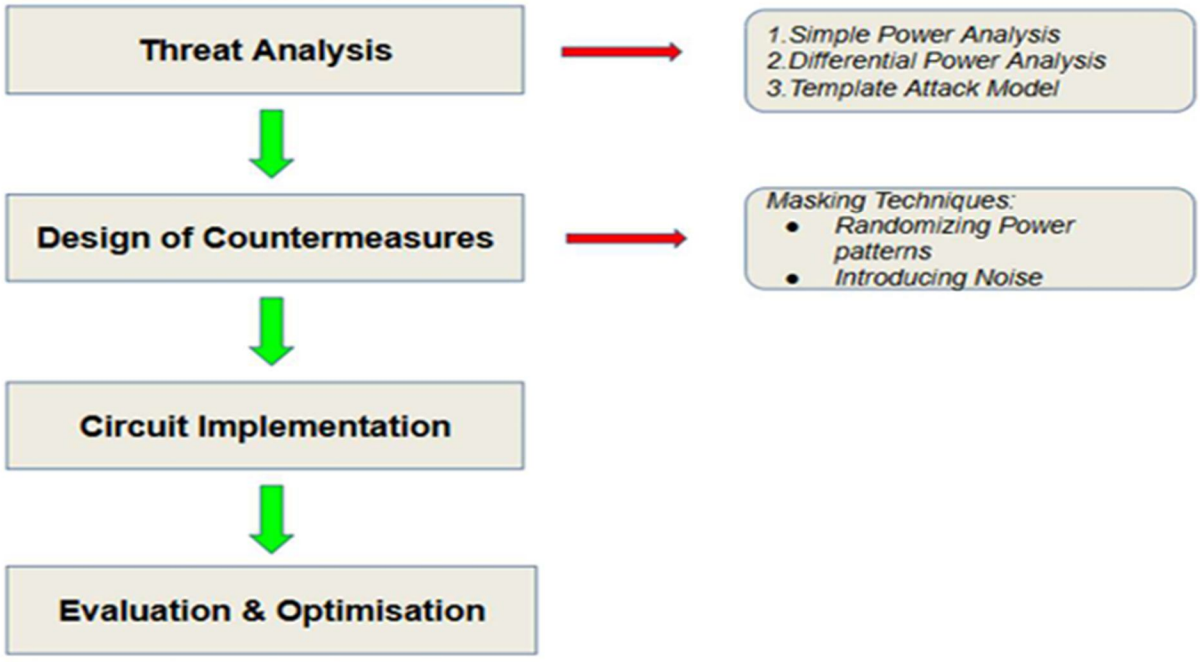



Figure 1: Overview of Methodology

- Threat Analysis: The initial step is the identification of particular side-channel vulnerabilities applicable to hardware implementations of AES, with particular emphasis on power and electromagnetic analysis. According to the given threat model, it is considered that attackers possess physical access and can measure power traces or electromagnetic emissions during the entire encryption process. A vulnerability analysis of the standard AES architecture, with emphasis on areas of high data dependency and observable leakage, namely in the S-Box computations and the key scheduling phases, is conducted. This analysis informs the strategic placement and integration of countermeasures into the AES Datapath to detect hardware Trojans and anomalous data paths that can exacerbate leakage; however, it must be mentioned that such approaches tend to have high design overhead and are not scalable for intricate encryption engines [5]. Even with these innovations, most solutions today are confined to particular attack vectors or have high overhead and therefore are less feasible in resource-constrained settings. This reality is the basis of our solution: one consolidated solution that uses different measures intended to improve security without sacrificing functionality.

©IJRASET: All Rights are Reserved 

- Countermeasure Design: Three basic countermeasures have been designed to counter the identified threats: (i) Noise Injection, (ii) Dummy Operations, and (iii) Current Smoothing. Noise Injection is the injection of controlled randomness into the EM and power profiles of the AES circuit. It is achieved through the introduction of random noise generators and modules that introduce irrelevant switching activity during encryption. Random delays and artificial power spikes make tracing alignment and correlation difficult across multiple operations. Dummy Operations are used to introduce computation that is not functional into the AES process flow. The operations are inserted in a strategic way by putting them in parallel or interleaving them with true encryption logic to replicate the same switching patterns without influencing output. This masks the true data-dependent patterns in power traces. Current Smoothing is a method applied at the RTL level to smooth the instantaneous power consumption curve of the circuit. By making power consumption more regular over time, it becomes much more difficult to distinguish between key-dependent and independent operations. This method can also be applied in combination with noise injection to enhance resistance to both SPA and DPA.

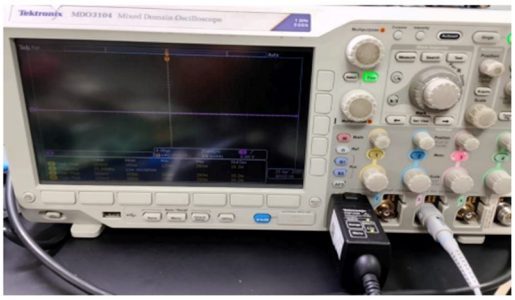



Fig 2 : Tektronix Multi-Domain Oscilloscope & probes

- Hardware Implementation: The RTL design has been implemented on an Artix-7 FPGA (Part Number: XC7A35TCPG236-1). The Experimental setup includes an Artix 7 FPGA board and a Tektronix Multi-Domain Oscilloscope(MDO3104) along with its probes to capture the leakage power from the power rails of the FPGA.
- Evaluation and Validation: The hardened AES design's functional integrity is verified using standard testbenches. Synthesis and resource reports are generated to quantify the area usage of the baseline and hardened implementations. Then, the accurate SCA resistance is typically verified through lab-based trace capture and analysis. Our initial verification goes up to architectural analysis and secondary metrics such as power variation and switching activity. The net effect of the countermeasures will be to significantly increase the effort required for successful side-channel attacks, as shown by the result traces, thereby improving the security and resilience of the design for field deployment.

## V. EXPERIMENTAL RESULTS AND ANALYSIS

The AES encryption algorithm was synthesised using the Xilinx Vivado Design Suite on a Xilinx Artix-7 FPGA chip. The platform was chosen for its performance vs. resource trade-off, which makes it suitable for experimentation as well as for deployment in real-world embedded systems. The design was implemented both in a baseline manner and in a protected version with countermeasures for side-channel leakage mitigation. Synthesis of both designs was done in Vivado, and the resulting logic utilisation of the two designs in terms of Look-Up Tables (LUTs), Flip-Flops, and slices is presented in Table 2. In order to analyse the effectiveness of the side-channel countermeasures adopted, power traces were recorded during the AES encryption process. Power traces were recorded using a high-resolution multi-domain oscilloscope while the designs were executed on the Artix-7 FPGA platform. The baseline and protected designs were exposed to the same test conditions in order to compare them fairly and meaningfully. The recorded traces were analysed and compared visually in order to analyse the extent of information leakage. The power traces of the baseline and protected designs are illustrated in Figures 3 and 4, respectively. The comparative analysis revealed distinct variations in the power signatures, thereby establishing the effectiveness of the protection methods adopted. In addition to the resistance verification against side-channel attacks, there was a thorough functional verification to ascertain the correctness of the AES encryption process. The verification was performed strictly within the Vivado simulation and implementation toolbox. A standard set of AES test vectors was utilised, where known plaintext inputs were presented and the resultant ciphertexts were compared with the expected outputs as dictated by the AES standard. These tests were important to help prevent the built-in security enhancements—such as logic randomisation and masking techniques—from interfering with the natural function of the encryption algorithm.

The outcome of these functional tests is given in Table 1, with successful encryption outputs and complete adherence to AES standards. Through the use of this approach, the project attained an effective side-channel leakage reduction while at the same time maintaining the functional correctness and reliability of the AES implementation under all the test cases.

TABLE 1: AES Functionality Test

| Case No. | Key | Plain Text | Cipher Text | Result |
|---|---|---|---|---|
| 1. | 0x2b7e151628aed2a6abf7158809cf4f3c0000000000 00000000000000000000 | 0x6bc1bee22e409f96 e93d7e117393172a | 0x3ad77bb40d7a366 0a89ecaf32466ef97 | Successful Encryption |
| 2. | 0x102030405060708090a0b0c0d0e0f000000000000 0 00000000000000000000 | 0x69c4e0d 86a7b043 0d8cdb78 070b4c55a | 0x001122334455667 78899aabbccddeeff | Successful Encryption |
| 3. | 0x603deb1015ca71be2b73aef0857d77811f352c073b 6108d72d9810a30914dff4 | 0x6bc1bee22e409f96 e93d7e117393172a | 0xf3eed1bdb5d2a0 3c064b5a7e3db181f 8 | Successful Encryption |
| 4. | 0x2b7e151628aed2a6abf7 158809cf4f3c0000000000 00000000000000000000 | 0xae2d8a571e03ac9c 9eb76fac45af8e51 | 0xf5d3d58503b9699 de785895a96fdbaaf | Successful Encryption |
| 5 | 0x603deb1015ca71be2b73 aef0857d77811f352c073b 6108d72d9810a30914dff4 | 0xf3eed1bdb5d2a03c 064b5a7e3db181f8 | 0x6bc12e409f96e9 3d7e117393172a | Successful Encryption |

Interpretation: This table depicts the functionality of the protected version that provides accurate encryption for multiple cases of plaintext-key pairs, demonstrating that the modifications made to the protected version do not affect the main purpose of the Encryption algorithm, which is encrypting the plaintext to obfuscate the data it contains.

TABLE 2 : Resource Utilisation Report

| Design Variant | LUTs (20800) | FFs (41600) | IOBs(106) |
|---|---|---|---|
| Baseline (No modifications) | 3307(~15.8%) | 2990 (~7.18%) | 76 (71.7%) |
| Protected(With randomisation ,dummy operations & current smoothing) | 3357 (~16.1%) | 2992 (~7.2%) | 76 (71.7%) |

Interpretation: The usage of resources, which in turn depicts area usage, is a minimal amount, which demonstrates that the area usage is not dramatically increased in the protected version, hence making it an area-efficient approach to protect against side channel attacks.

TABLE 3 : Power Utilisation Report

| Design Variant | Power Usage |
|---|---|
| Baseline (No modifications) | ~550mW |
| Protected(With randomisation ,dummy operations & current smoothing) | ~900mW |

Interpretation: There is a marginal increase in the power usage of the protected version ( ~350mW ), which amounts to an increase of ~64percent increase in power. This result shows that the protected version does not compromise a lot on energy efficiency while providing adequate protection against side channel attacks, making it an optimal solution.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

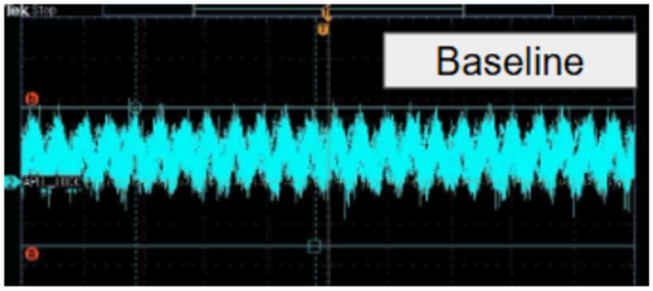



Fig 3 : Power trace from Baseline variant

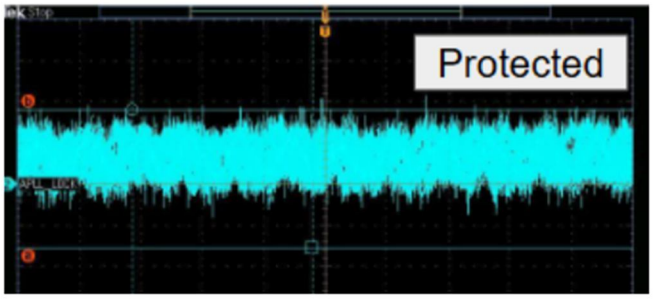



Fig 4: Power traces from Protected Variant

## V. CONCLUSION

This paper presents the design, implementation, and evaluation of a single hardware-focused countermeasure approach against side-channel analysis (SCA) vulnerabilities in cryptographic hardware. The approach utilises three complementary methods—randomisation, noise injection, and current smoothing—within a single framework. The methods were selected because they could mask power consumption profiles in combination and inject sources of randomness into the hardware operation, hence making the hardware more power-side-channel attack proof. The countermeasure suite was implemented on an FPGA platform, and the design was synthesised to analyse the impact on area and timing performance. Power traces were collected from the FPGA under cryptographic load to evaluate the effectiveness of the two-layer protection technique.

The two-layer testing allowed a complete evaluation of how the proposed techniques fare in an actual hardware environment, balancing security enhancement and implementation expense. The findings of the present work highlight the value of an end-to-end, multi-faceted approach to side-channel resistance enhancement that takes advantage of randomness and signal camouflage to shield sensitive operations from unwanted physical probing.

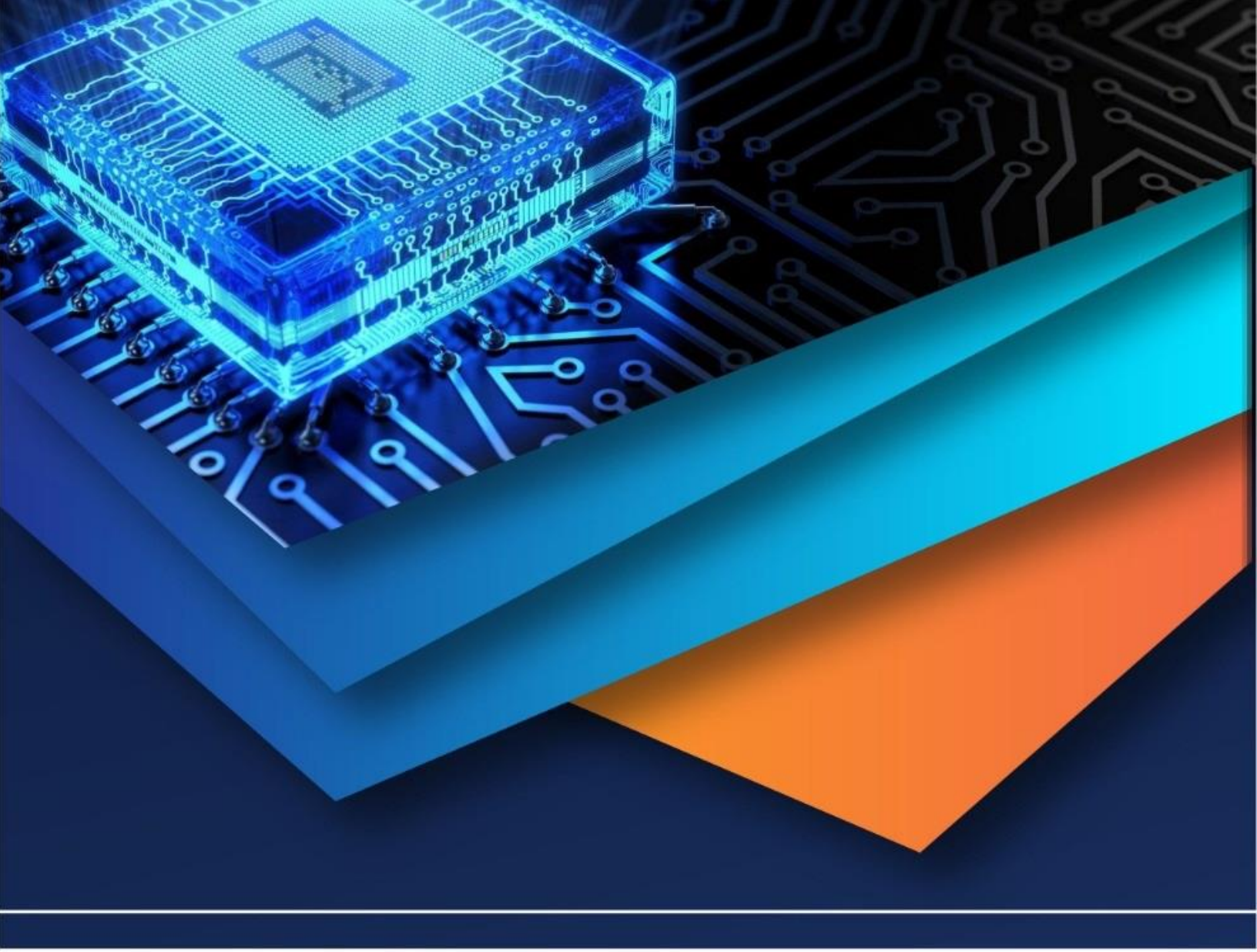
Future work might explore the deployment of the countermeasures in ASIC designs, where power dissipation and performance constraints are varied from those in FPGA-based implementations. Additionally, the integration of machine learning-driven leakage detection into the design process might provide more dynamic guidance for tuning the security-functionality balance

## REFERENCES

[1] M. Alioto, "Trends in Hardware Security: From Basics to ASICs," in IEEE Solid-State Circuits Magazine, vol. 11, no. 3, pp. 56-74, August 2019
[2] L. Kampel, P. Kitsos and D. E. Simos, "Locating Hardware Trojans Using Combinatorial Testing for Cryptographic Circuits," in IEEE Access, vol. 10, pp. 18787-18806, 2022
[3] A. Srivastava ;Sanjay Das and Navnil Choudhary, "SCAR: Power Side-Channel Analysis at RTL Level," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 32, no. 6, pp. 1110-1123, June 2024
[4] Luca Crocetti, Luca Baldanzi, Matteo Bertolucci, Luca Sarti, Berardino Carnevale, Luca Fanucci " A simulated approach to evaluate side-channel attack countermeasures for the Advanced Encryption Standard", Integration, vol. 68, pp. 80-86, September 2019
[5] J. R. Rao and B. Sunar, "A very compact S-Box for AES", in Cryptographic Hardware and Embedded Systems – CHES, vol. 3659, pp. 441–455, 2005
[6] V. Iyer, M. Wang, J. Kulkarni and A. E. Yilmaz, "A Systematic Evaluation of EM and Power Side-Channel Analysis Attacks on AES Implementations," 2021 IEEE International Conference on Intelligence and Security Informatics (ISI), San Antonio, TX, USA, 2021, pp. 1-6
[7] T. Moos, A. Moradi and B. Richter, "Static Power Side-Channel Analysis—An Investigation of Measurement Factors," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 376-389, Feb. 2020

[8] S R Bommana, Sreehari V, Syed Ershad and M B Srinivas "Mitigating Side-Channel Attacks on FPGA through Deep Learning and Dynamic Reconfiguration," Scientific Reports, vol. 14, no. 1, pp. 1–13, 202
[9] Akter, S., Khalil, K. & Bayoumi, M. A survey on hardware security: Current trends and challenges. IEEE Access. 11, 77543–77565 (2023).
[10] Piessens, F. & van Oorschot, P. C. Side-channel attacks: A short tour. IEEE Secur. Priv. 22, 75–80 (2024).
[11] Prates, N., Vergütz, A., Macedo, R. T., Santos, A. & Nogueira, M. A defense mechanism for timing-based side-channel attacks on iot traffic. In GLOBECOM 2020-2020 IEEE Global Communications Conference, 1–6 (IEEE, 2020)
[12] Gattu, N., Khan, M. N. I., De, A. & Ghosh, S. Power side channel attack analysis and detection. In Proceedings of the 39th International Conference on Computer-Aided Design, 1–7 (2020).
[13] He, J., Guo, X., Tehranipoor, M. M., Vassilev, A. & Jin, Y. Em side channels in hardware security: Attacks and defenses. IEEE Des. Test. 39, 100–111 (2022).
[14] Harrison, J., Toreini, E. & Mehrnezhad, M. A practical deep learning-based acoustic side channel attack on keyboards. In 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS &PW). 270–280 (IEEE, 2023).
[15] Boutros, A. & Betz, V. FPGA architecture: Principles and progression. IEEE Circuits Syst. Mag. 21, 4–29 (2021).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)