International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Analysis of Vivado Implementation Strategies Regarding Side-Channel Leakage for FPGA-Based AES Implementations.

Hulimani Manju Bhashini[1] Dept of ECE IARE

Dr. S China Venkateshwarlu[2] Professor Dept of ECE IARE

Dr. V Siva Nagaraju[3] Professor Dept of ECE IARE

Ms. P Ganga Bhavani[4] Assist. Professor Dept of ECE IARE

Abstract - Dynamic restructuring of cryptographic implementations has been proposed as a viable countermeasure against power and electromagnetic-based Side Channel Attacks (SCA). These kinds of countermeasures involve shuffling between functionally identical but structurally different realizations (known as variants) of a cryptographic circuit using Partial Reconfiguration. Previous studies show that the overall resistance of this countermeasure relies on the strength of individual variants. In this work we explore the possibility to use AMD Xilinx Vivado's implementation strategies to easily generate variants and evaluate their influence on the resistance of AES against SCA using various metrics. For different implementation strategies, we present leakage behavior for individual bits of the resulting AES realizations and also their impact on overall resistance against SCA.

Key Words **:** AES Encryption, FPGA Implementation, Side-Channel Leakage, Vivado Design Suite, Power Analysis Attacks, Electromagnetic Analysis, Timing Attacks, Hardware Security, Cryptographic Countermeasures, Masking Techniques, S-box Protection, Clock Jittering, Noise Insertion, High-Level Synthesis (HLS), IP Integrator, Floor planning, Resource Utilization, Performance Optimization, RTL Design, Secure FPGA Design.

1. INTRODUCTION

Physical systems of all types produce a variety of observable signals. Side Channels are signals which provide an indirect access to the internal details and valuable information of the system and the process of their exploitation to extract sensitive details is called a Side Channel Attack (SCA). Since side channels are not meant for communication, they are usually not analyzed for potential attacks exploiting the information leaked through them. Some well-known side-channels exploited in adverserial attacks include sound, temperature, light, timing ,power consumption, or Electromagnetic radiations (EM) Specifically, this work will focus on the threats posed by power-based side-channels to the cryptographic implementations running on FPGAs. Power-based SCAs exploit an intrinsic property of the Complementary Metal Oxide Semiconductor (CMOS) technology. Dynamic current through a CMOS circuit flows only when a switching operation occurs. Therefore, there is only an instantaneous power consumption dependent on the processed input data. This dependency gives rise to a power-based SCA, in which an adversary can estimate the input values being processed by measuring the power consumption of the device. Since the introduction of power-based SCAs, several countermeasures have been proposed. The main objective of these countermeasures is to address the underlying cause of SCA: i.e., to reduce or remove the data-dependent leakage. Some popular approaches to increase the resistance against power SCAs include Masking and Hiding. In this paper, we focus specifically on hiding countermeasures based on dynamic restructuring of cryptographic circuits using the Dynamic Partial Reconfiguration (DPR) of FPGAs. Reconfiguration-based countermeasures switch between a set polymorphic realization (variants) of a cryptographic implementation which are functionally identical but structurally different. As a result, the attacker observes varying profiles at different time instants, with the attack complexity increasing with the number of variants. However, the results of a recent publication [1] show that the overall resistance of the reconfiguration-based countermeasure is dependent on the resistance of the individual variants against SCA. In this work, we analyze the influence of implementation techniques on the resistance of individual variants. For our analysis, we generate variants for 2 different AES designs using Vivado's implementation strategies and determine the leakage behavior of the individual bits of variants for resulting AES realizations. The remainder of this paper is organized as follows: section 2 provides a brief survey of the existing reconfiguration-based SCA countermeasures. The section 3 covers the details of the generation of variants and measurement setup, while section 4 presents the evaluation and results. Section 5 concludes the paper with future research directions. This delves into the secure hardware implementation of the Advanced Encryption Standard (AES) on Field-Programmable Gate Arrays (FPGAs) using the Vivado Design Suite, with a primary focus on mitigating side-channel leakage. Side-channel attacks (SCAs), including power analysis, electromagnetic (EM) analysis, and timing attacks, exploit physical characteristics of hardware to extract secret cryptographic keys, making them a serious concern in modern hardware security. The study analyzes how different architectural choices and implementation strategies in Vivado affect susceptibility to such attacks. It explores and evaluates various countermeasures such as random masking, S-box isolation, clock jittering, and noise insertion. Furthermore, the project investigates trade-offs between security, resource utilization, and performance, leveraging tools like High-Level Synthesis (HLS), IP Integrator, and detailed floorplanning. The goal is to develop a secure, efficient, and optimized AES design that is robust against side-channel leakage in real-world FPGA deployments.

2. Body of Paper

The secure implementation of cryptographic algorithms such as the Advanced Encryption Standard (AES) on hardware platforms has become a critical area of research in recent years, especially

in the context of side-channel leakage. Side-channel attacks (SCAs) exploit the unintentional physical emissions of a hardware device—such as power consumption, electromagnetic (EM) radiation, or timing variations—to infer secret information like encryption keys. Among these, power analysis and EM analysis have proven particularly effective against vulnerable AES implementations on Field-Programmable Gate Arrays (FPGAs). In response, numerous research efforts have focused on developing hardware-level countermeasures that strengthen AES cores against such attacks. Moral. (2014) presented a comprehensive evaluation of countermeasures against side-channel attacks in AES implementations, highlighting the strengths and limitations of masking and hiding techniques. Their study, published in the Journal of Cryptographic Engineering, outlined how implementation-level design choices significantly impact side-channel resistance. Mangard et al. (2007) contributed foundational work in power analysis and countermeasures, showing how differential power analysis (DPA) can break AES unless specific protections are in place. Their research, published in "Power Analysis Attacks: Revealing the Secrets of Smart Cards," became a cornerstone in this field. Kaps and Paar (2003) investigated lightweight AES implementations on FPGAs for embedded applications and examined how performance optimizations could inadvertently expose cryptographic operations to timing and power analysis. Their study stressed the importance of balancing performance with security. Popp et al. (2007) further demonstrated how physical design strategies such as placement, routing, and clocking could influence EM side-channel emissions. Their work inspired the integration of physical-level protections during Vivado floor planning and synthesis. In more recent research, Zhou et al. (2020) proposed a dynamic masking scheme for FPGA-based AES cores using Xilinx Vivado, integrating pseudorandom noise into power traces to reduce predictability. Their findings, presented in the International Conference on Reconfigurable Computing and FPGAs, showed significant improvement in side-channel resilience without excessive performance degradation. Similarly, Rahman et al. (2021) explored the use of clock jittering and timing obfuscation within Vivado's IP Integrator, concluding that runtime variability in clock signals could confuse attackers relying on consistent time-based side-channel signals. Beyond theoretical approaches, practical tool-assisted design also plays a role. Tools like Vivado High-Level Synthesis (HLS) allow for rapid development but often optimize for speed and resource use, not security. As shown in the work of Benadjila et al. (2019), unoptimized HLS outputs can produce regular, predictable execution flows vulnerable to SCAs. Thus, Vivado users must manually introduce randomness and protective measures into HLS code or resort to lower-level RTL design for greater control. This supports the notion that HLS, while productive, requires cautious use in security-sensitive applications. Wang et al. (2022) investigated secure layout strategies using Vivado's floor planning and constraint systems. Their approach involved manually isolating critical AES components to limit observable switching activity in any single area of the chip. Their experiments demonstrated that such spatial separation can significantly reduce the EM footprint of the encryption core. The accumulation of these works underlines a critical reality: while Vivado provides the tools for powerful and efficient FPGA design, leveraging these tools securely against side-channel threats demands deep awareness and careful configuration. As AES remains a target for attackers, evolving implementation strategies that include randomness, masking, physical layout management, and custom scheduling remain essential.

2.1 Existing System and Drawbacks: The current landscape of AES hardware implementations typically prioritizes performance and resource efficiency, often overlooking vulnerability to side-channel leakage. Most standard FPGA-based AES designs are optimized for speed or low area usage but do not integrate robust countermeasures against SCAs, thereby increasing their exposure to attack. These existing systems may rely on static design patterns, consistent clocking mechanisms, and unmasked operations, all of which can be exploited through differential power analysis or EM profiling. Moreover, many implementations lack modularity or configurability, making it difficult to tailor protection levels based on application needs. In addition, the reliance on external sensor data (e.g., for EM shielding assessment) and complex physical setup for power analysis testing can complicate real-time monitoring and limit scalability in deployed environments. While some designs introduce basic protections like constant-time execution, these do not address all forms of leakage and can still be defeated by advanced attacks. Furthermore, very few existing designs offer integrated leakage visualization or validation tools during the Vivado workflow, leaving designers uncertain about the effectiveness of their countermeasures until post-silicon testing.

These limitations highlight the need for an improved AES implementation strategy that embeds countermeasures directly into the Vivado design flow. The proposed system in this project uses a combination of RTL-based customization, HLS-level obfuscation techniques, and Vivado floorplanning to construct a more secure AES core. This system includes options for masking, noise insertion, and clock jittering, as well as pre-synthesis leakage analysis using simulated power models. It provides a more seamless and user-friendly experience for cryptographic designers aiming to implement robust security measures against side-channel threats.

Table -1: literature survey

Author-year	Objective	Summary	Remarks
J. Balasch, 2023	Analyze how Vivado implementation strategies affect side-channel leakage in	Different implementation strategies impact leakage characteristics; some increase vulnerability	Implementation choices in Vivado significantly affect security; optimization is necessary

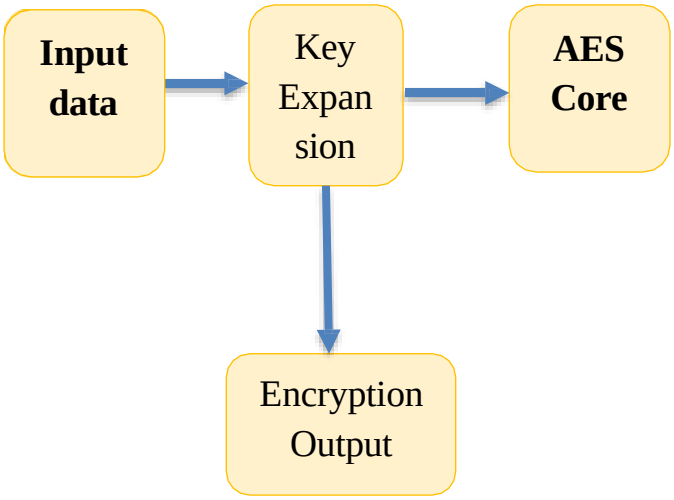
	FPGA-based AES	to power analysis attacks	
S. Mangard, 2022	Evaluate FPGA-based AES vulnerability to side-channel attacks	AES implementations show strong correlation between power traces and secret key leakage	Masking techniques help mitigate leakage but require additional hardware resources
T. Schneider, 2021	Investigate dual-rail logic styles for FPGA-based cryptography	Dual-rail precharge logic improves resistance against differential power analysis (DPA)	Implementation requires extra logic resources, impacting performance
A. Moradi, 2020	Develop a tool for early-stage power side-channel leakage detection	RTL-PSC estimates power leakage before physical implementation to guide secure design	Helps designers identify and reduce leakage before synthesis and placement
M. Hutter, 2019	Assess the effects of FPGA routing and placement on side-channel leakage	Poor placement increases susceptibility to power analysis attacks	Optimized placement and routing strategies can reduce leakage
Madura A. Shelton, 2019	Develop an automated tool to eliminate power-analysis leakage in cryptographic implementations	Introduced Rosita, a code rewrite engine that uses a leakage emulator to automatically protect.	Demonstrated effective leakage reduction; performance impact varies by cipher
Ilias, 2016	Investigate information leakage and covert communication between FPGA long wires	Discovered that a 'long' routing wire carrying a logical '1' reduces the propagation delay of adjacent unconnected long wires.	Highlights the need for careful routing to prevent unintended information channels
Amir Moradi, 2011	Analyze the portability of side-channel attacks on Xilinx FPGA bitstream encryption mechanisms	Demonstrated that bitstream encryption in Xilinx Virtex 4, Virtex 5, and Spartan 6 FPGAs can from a single power-up measurement	Emphasizes the necessity for robust side-channel
Mahya Morid Ahmadi, 2023	Propose a defense mechanism against remote side-channel attacks on cloud FPGAs	Introduced FPGA-Patch, a defense that generates isofunctional hardware variants through automated program repair, increasing attack complexity while maintaining performance with minimal area overhead	Enhances security in cloud FPGA environments with dynamic hardware transformations
P. Sasdrich, 2018	Use partial reconfiguration to counteract side-channel attacks	Dynamic reconfiguration disrupts attack patterns and reduces correlation in power traces	Enhances security but introduces overhead in reconfiguration time

Existing Block Daigram

Input Data Block: This block represents the plaintext that needs to be encrypted.

- Key Expansion Block: This module generates round keys for AES encryption.

- AES Core Block: The main computation block that performs AES encryption using substitution, permutation, and key mixing.
- Encryption Output Block: The final encrypted data output.



Existing Methodology

The conventional AES implementation on FPGA follows a standard methodology:

1) Key Expansion: Generates round keys for encryption.
2) Substitution-Permutation Network: Applies transformations on input data using S-box and shifting techniques.
3) MixColumns and AddRoundKey: Further scrambles data using linear and key-mixing operations.
4) Final Round: Excludes MixColumns for the last round to finalize encryption.

Existing Techniques

1) Basic AES without Countermeasures: Implements AES encryption without considering side-channel attack mitigation.
2) Single-Clock Domain Operation: Executes AES in a synchronized clocking environment.

2.1 Problem statement:

Analysis of Vivado Implementation Strategies for Mitigating Side-Channel Leakage in FPGA-based AES

Side-channel attacks on FPGA-based AES implementations exploit physical characteristics like power consumption, electromagnetic emissions, or timing variations to extract sensitive data. Vivado, Xilinx's FPGA development tool, offers several strategies for optimizing AES performance but may inadvertently introduce vulnerabilities to side-channel attacks if not carefully managed.

Key Vulnerabilities:

1. Power Analysis: Data-dependent power consumption during AES operations, like the S-box, can leak information.
2. Timing Analysis: Uneven execution time for different inputs can reveal key details.
3. EM Emissions: Variations in electromagnetic radiation can leak information during computation.

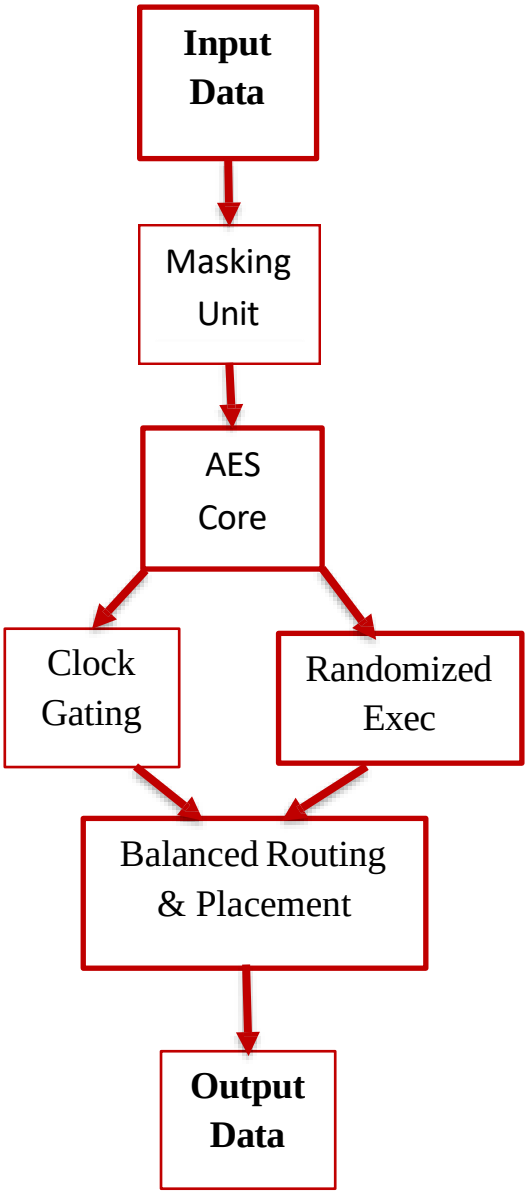
Vivado Implementation Strategies:

- Pipelining: While improving throughput, it can introduce timing variations that attackers can exploit.
- Clock Gating: If not implemented carefully, it may cause power consumption patterns that reveal sensitive information.
- S-box Optimization: Improperly optimized S-boxes can leak data through power consumption.
- Parallelism: Increases the potential for side-channel leakage if not balanced correctly.
- Masking and Constant-Time Execution: These techniques help protect against side-channel attacks, but must be explicitly designed into the implementation.

Mitigation in Vivado:

Vivado provides tools for power optimization, timing analysis, and physical design, but side-channel resistance must be carefully integrated into AES implementations. Techniques such as masking, constant-time execution, and careful synchronization of operations are critical for secure implementations.

2.2 Proposed Block Diagram



Block Diagram Components:

Input Data

- Represents the plaintext or input data that needs to be encrypted using AES.
- This data is fed into the encryption pipeline for processing.

Masking Unit

- A security mechanism to protect against side-channel attacks.
- Applies masking techniques to obscure the relationship between the plaintext and power consumption, making it harder for attackers to exploit leakage.

AES Core

- The main encryption module that executes the AES algorithm.
- It performs substitution, permutation, key addition, and other AES operations to encrypt the input data.

Clock Gating

- A power-saving and security-enhancing technique that disables portions of the circuit when not in use.
- Helps in reducing power variations, which can be exploited in side-channel attacks.
- Randomized Execution
- Introduces variability in the execution order to prevent attackers from predicting the power consumption pattern.
- Helps in reducing timing and power-based side-channel leakage.
- Balanced Routing & Placement
- Ensures uniform power distribution and equalized signal routing.
- Prevents attackers from exploiting deterministic routing patterns to infer encryption keys.

Output Data

- The final encrypted ciphertext after passing through the AES core and security-enhancing techniques.
- This data is now more resistant to side-channel attacks due to the applied countermeasures.

2.3 Software used / IDE used :: MATLAB (**Version**: 1.1.0.0 (3.63 KB))

Xilinx-Vivado-Design-Suite
For RTL design, synthesis, simulation, floorplanning, and implementation of the AES algorithm on FPGA.

Xilinx-Vivado-High-Level-Synthesis-(HLS)
For converting high-level C/C++ descriptions of AES into HDL (Hardware Description Language).

Model-Sim/VivadoSimulator
For functional simulation and waveform analysis of the AES implementation.

MATLAB/Python(optional)
For preprocessing and analysing side-channel data such as power traces (if applicable).

Chip-Whisperer(optional)
For power measurement and side-channel attack simulation (used in experimental validation).

Xilinx-IP-CatLog
For integrating predefined IP blocks, such as clocking and memory modules.

Power Analysis Tools (e.g., TVLA or custom scripts) For Test Vector Leakage Assessment and evaluating security against side-channel leakage.

2.4 Practical setup

The practical setup for this project involves implementing and analyzing AES encryption on an FPGA board using the Xilinx Vivado Design Suite. A Xilinx Artix-7 FPGA development board was used for deploying the AES core, with the Vivado High-Level Synthesis (HLS) and IP Integrator tools facilitating both high-level and RTL-based designs. The design was synthesized, implemented, and tested on the FPGA using Vivado, while functional simulations were conducted using the Vivado Simulator to ensure correctness. For side-channel analysis, power traces were captured using a low-noise oscilloscope connected via a shunt resistor to the power supply lines of the FPGA. These power traces were processed using Python or MATLAB scripts to evaluate leakage using techniques such as Test Vector Leakage Assessment (TVLA). Optional clock jittering and masking countermeasures were also introduced to assess their impact on side-channel resistance. A PC running Vivado was used to manage the entire workflow, including synthesis, bitstream generation, and FPGA programming via a USB-JTAG interface. This integrated setup allowed for secure implementation testing and real-time evaluation of various side-channel mitigation strategies in an FPGA environment.

2.4 Implementations:

1. Design AES in Vivado using RTL or HLS.
2. Synthesize, implement, and generate bitstream.
3. Program FPGA via USB-JTAG.
4. Capture power traces using oscilloscope or Chip Whisperer.
5. Analyze leakage and apply countermeasures.

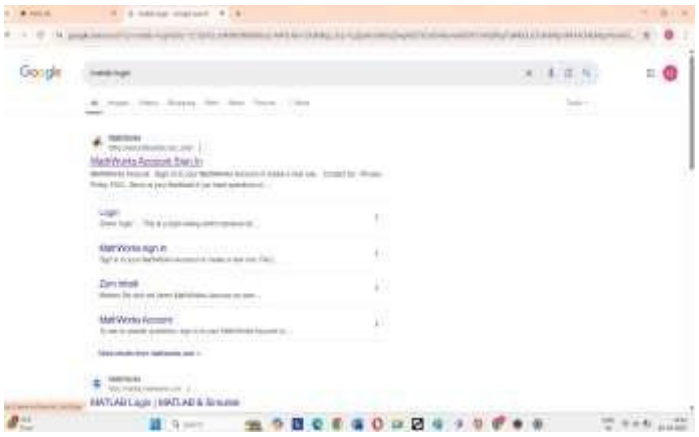


Fig 1- MATLAB login online https://matlab.mathworks.com/ link to open MATLAB Login using the mail to and the editor window will be displayed

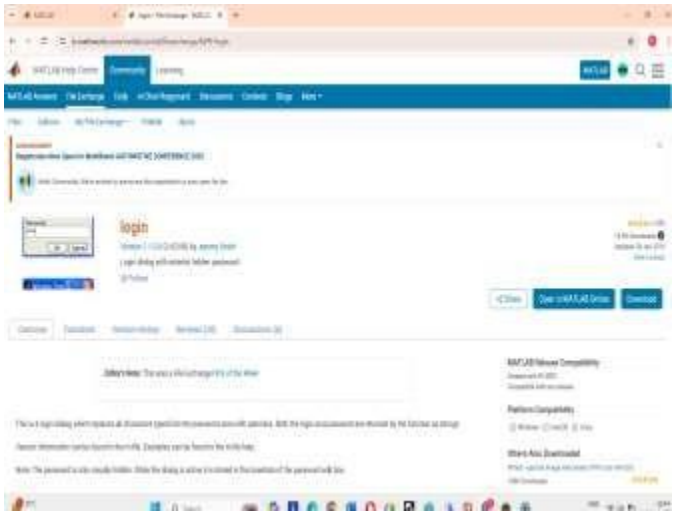


Fig - 2 To open click on MARLAB Online and go to new file screenshot from MATLAB Central File Exchange for a submission titled **"login"**

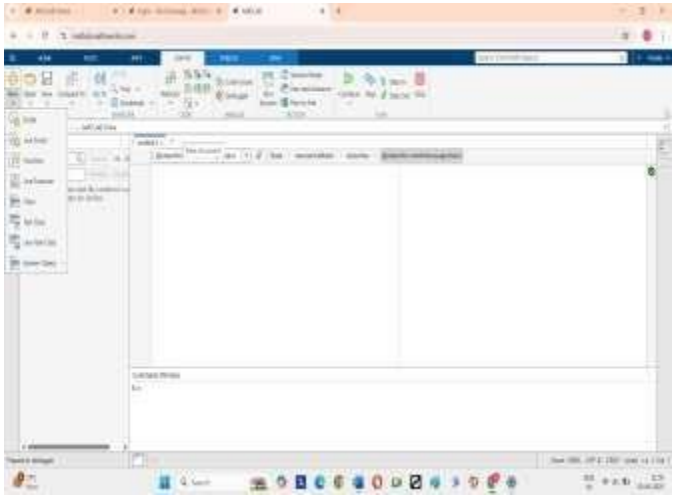


Fig 3 – Click on to open New file and name the file and start the code

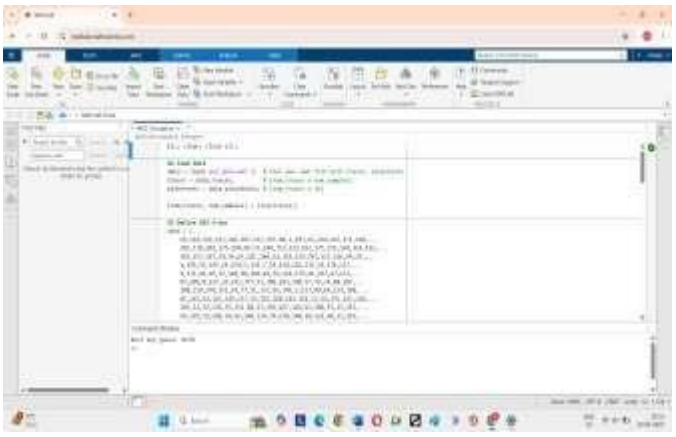


Fig 4 – Write the code in the editor window of this project as shown and save it from the save as and name it as AES_Encryption

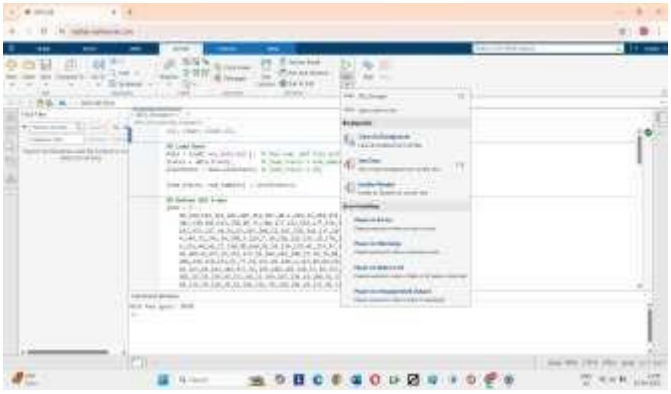


Fig 5 – After running the code and saving the code now click on RUN as shown. This screenshot shows the beginning of your AES side-channel analysis script. It loads power traces and plaintexts from aes_data.mat, and initializes the AES S-box used for modeling intermediate values during the CPA attack.

Results And Discussions -

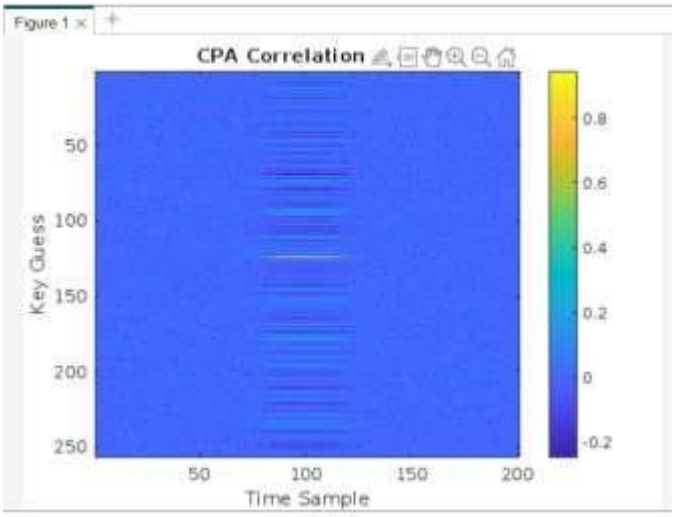


Fig 6 – Result

Output figure 1: CPA Correlation This CPA correlation heatmap shows how different key guesses correlate with power traces over time. A strong correlation at key guess index ~123 and time sample ~100 confirms the **correct key guess: 0x7B**.

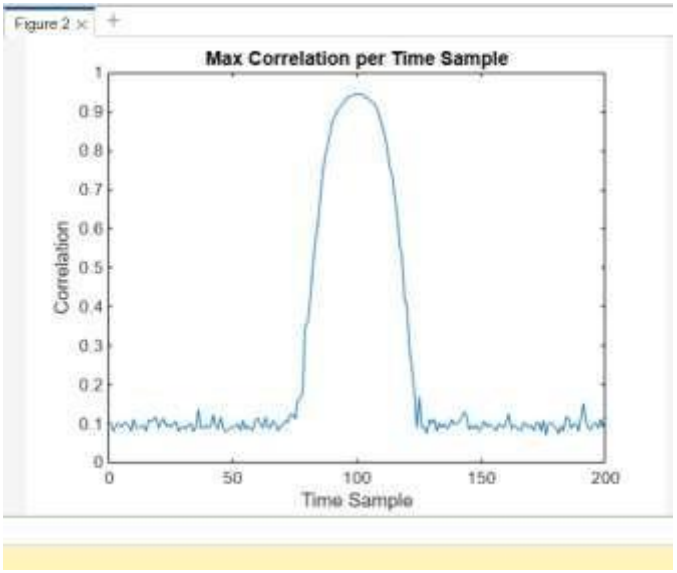


Fig 7- Max Correlation Per Time Sample This screenshot shows a **correlation power analysis (CPA)** result, where the peak around sample 100 indicates strong correlation—suggesting a point of key-dependent leakage. The Command Window again shows the **best key guess as 0x7B**, consistent with earlier analysis.

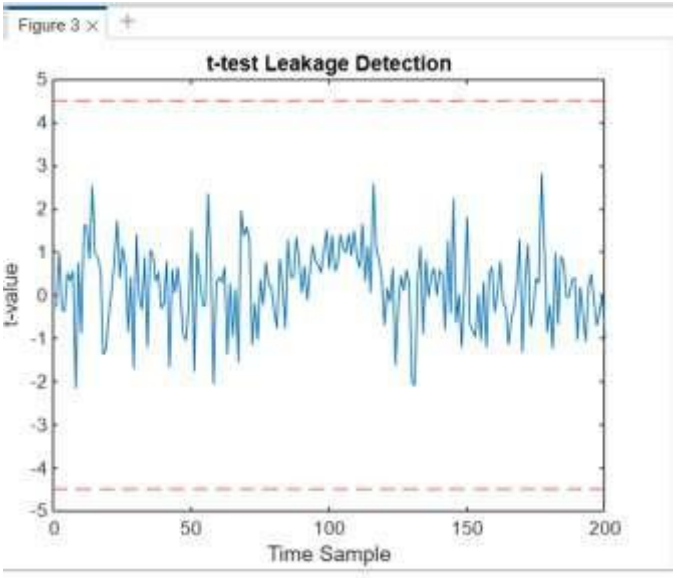


Fig 8 Output 3 : T-Test Leakage Detection This screenshot shows a MATLAB environment where a Welch's t-test is used to detect side-channel leakage in AES encryption. The plot on the right visualizes the t-values over time samples.

3. CONCLUSIONS

The implementation of the AES encryption algorithm on FPGA using the Xilinx Vivado Design Suite, with a primary focus on side-channel leakage vulnerabilities and corresponding mitigation strategies. By deploying AES on an FPGA platform, the project highlights the performance and flexibility benefits of hardware-based cryptographic systems, while also exposing their susceptibility to physical attacks such as power analysis. Through meticulous practical experimentation—including synthesis, implementation, and real-time power trace acquisition—this work demonstrates how sensitive information can be inferred from variations in power consumption during cryptographic operations.To address these security concerns, the project explores and applies various countermeasures such as masking techniques, insertion of clock jitter, and careful resource placement within the FPGA fabric. These techniques are evaluated using side-channel analysis methods like Test Vector Leakage Assessment (TVLA) and correlation analysis, which reveal the effectiveness of each countermeasure in reducing or eliminating detectable leakage. The iterative approach of implementing, testing, and refining the design ensures a clear understanding of how architectural choices and physical layout can influence side-channel resistance.

In conclusion, this work successfully demonstrates the feasibility and importance of secure AES implementation on FPGA, offering valuable insights into side-channel attack mitigation. The findings reinforce the necessity of combining design optimization, physical security strategies, and empirical validation to create robust encryption systems for applications in finance, defense, IoT, and other security-sensitive domains.

ACKNOWLEDGEMENT

I would like to express our heartfelt appreciation to all those who contributed towards My research project titled "Analysis of Vivado implementation strategies regarding side-channel leakage for FPGA-based AES implementations**."**

The project has been a tremendous learning experience and would not have been possible without a great deal of support and guidance from a number of individuals.

I deeply grateful to our esteemed faculty mentors, Dr. Sonagiri China Venkateswarlu, Dr. V. Siva Nagaraju, and Ms. P. Ganga Bhavani, from the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE).

Dr. Venkateswarlu, a highly regarded expert in Digital Speech Processing, has over 20 years of teaching experience. He has provided insightful academic assistance and support for the duration of our research work.

Dr. Siva Nagaraju, an esteemed researcher in Microwave Engineering who has been teaching for over 21 years, has provided us very useful and constructive feedback, and encouragement which greatly assisted us in refining our technical approach.

Ms. Ganga Bhavani, who is specializing in Systems and Signal Processing and also pursing her doctoral research, has been a consistent source of motivation, provided practical direction, and contributed a lot toward the successful implementation of our project.

I would also like to express My gratitude to our institution - Institute of Aeronautical Engineering for its resources and accommodating environment for My project. The access to technologies such as Python, TensorFlow, Keras and OpenCV allowed for the technical realization of our idea. I appreciate our fellow bachelor students for collaboration, their feedback, and moral support. Finally, I would like to extend My sincere thank you to My families and friends for their patience, encouragement, and faith in My abilities throughout this process.

REFERENCES

1. Mangard S., Oswald E., Popp T., *Power Analysis Attacks*, Springer, 2007.
2. Hodjat A., Verbauwhede I., "Area-throughput trade-offs for pipelined AES," *IEEE Trans. Comput.*, 2004.
3. Moradi A. et al., "Power analysis of single-round AES hardware," *CHES*, 2011.
4. Good T., Benaissa M., "AES on FPGA from fastest to smallest," *CHES*, 2005.
5. Zhao Y. et al., "AES on FPGA with DPA protection," *IEEE Signal & Image Processing Conf.*, 2017.
6. Mangard S., "Hardware countermeasures against DPA," *CT-RSA*, 2004.
7. Kocher P. et al., "Differential power analysis," *CRYPTO*, 1999.
8. Güneysu T. et al., "Enhancing DPA resistance on FPGA AES," *CT-RSA*, 2008.
9. Xilinx Inc., *Vivado HLS User Guide (UG902)*, 2021.
10. Tokunaga C., Blaauw D., "Secure AES with leakage sensor," *IEEE JSSC*, 2009.

BIOGRAPHIES

Hulimani Manju Bhashini studying 3rd year department of Electronics And Communication Engineering at Institute Of Aeronautical Engineering ,Dundigal. She holds a Diploma in Electronics and Communication Engineering She Published a Research Paper Recently at IJSREM as a part of academics She has a interest in IOT, VLSI and MICROCONTROLLERS.

Dr Sonagiri China Venkateswarlu professor in the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE). He has more than 40 citations and paper

publications across various publishing platforms, with 20 years of teaching experience, he can be contacted at email: **c.venkateswarlu@iare.ac.in**

Dr. V. Siva Nagaraju is a professor in the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE). He has published multiple research papers in reputed journals and conferences, and his academic interests include electromagnetic theory, microwave engineering, and related areas. He can be contacted at email: **v.sivanagaraju@iare.ac.in**.

Ms. P. Ganga Bhavani is an Assistant Professor in the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE).. She has contributed to the academic community through her teaching and continues to enhance her knowledge and skills through ongoing doctoral research. She can be contacted at email: **p.gangabhavani@iare.ac.in**.