OPEN ACCESS

Saudi Journal of Engineering and Technology

Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Side-Channel Attacks and Countermeasures on AES

Nikita Kar Chowdhury[1*], Shraddha Kumari[1], Supriya B[1], Madhushree N K[1], Manju B Mudhol[1]

[1]Electronics and Communication Engineering, Acharya Institute of Technology Bengaluru, India

DOI: https://doi.org/10.36348/sjet.2024.v09i12.003 | **Received:** 18.10.2024 | **Accepted:** 05.12.2024 | **Published:** 15.12.2024

***Corresponding author:** Nikita Kar Chowdhury
Electronics and Communication Engineering, Acharya Institute of Technology Bengaluru, India

Abstract

The Advanced Encryption Standard (AES) is widely regarded as a robust encryption algorithm, ensuring secure communication and data protection. However, physical vulnerabilities such as side-channel attacks (SCAs) pose a significant threat to its implementations. This paper investigates various types of SCAs, including power analysis and electromagnetic analysis, and explores countermeasures like masking techniques to enhance AES resilience. The study includes an implementation of AES in Vivado using Verilog and a detailed analysis of masked and unmasked designs to validate the effectiveness of proposed countermeasures.

Keywords: Advanced Encryption Standard, side-channel attacks, power analysis, electromagnetic analysis

I. INTRODUCTION

In the modern world where people are more connected than ever before, the security of cryptographic algorithms is of great concern. Encryption techniques such as the Advanced Encryption Standard (AES) allow to protect sensitive data efficiently. But, the issues with cryptographic security solutions is that they are usually exposed to side-channel attacks that utilize timing, power, or electromagnetic leaks as their source of attack.

This project aims to achieve the following goals:

The power analysis attack is a potential threat to the AES encryption: Ciphers are a system of converting plain messages into encrypted notes. Illustrated in Fig 1, 1Encryption algorithm s is practical work that has been implemented.

To create and test countermeasures, in particular pervasive techniques to lessen the threat posed by key recovery attacks based on side-channel analysis.

It has been noticed that side-channel attacks tend to defeat the integrity of encryption keys, even when the cryptographic algorithm is conceptually secure by design. Among these attacks power analysis is quite useful and well known, as it takes advantage of looking at the power readings of the device using its power side during encryption to gain access to the sec

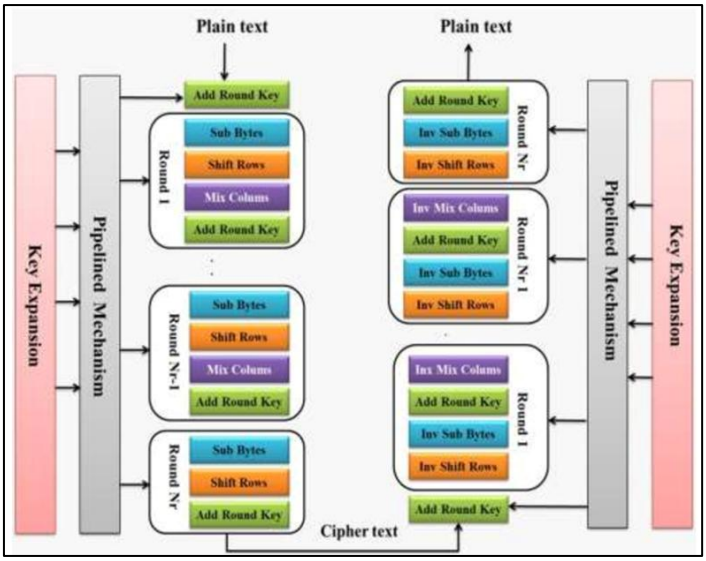

Figure I.1: Block Diagram AES Operation

II. LITERATURE REVIEWS

Congkhapham in the paper titled "A Real-Time Cache Side-Channel Attack Detection System on RISC-V Out-of-Order Processor." The authors look at how RISC-V out-of-order processors can be vulnerable to cache side-channel attacks, which can compromise data security. They review previous research on these types of attacks and the methods used to detect them, noting that many existing solutions struggle to work in real time. The authors propose a new detection system designed specifically for RISC-V processors that improves security by using their unique features. They test the system's effectiveness, focusing on speed and accuracy in identifying attacks. Overall, the paper provides important insights into making RISC-V processors safer and suggests areas for further research.

Takuji Miki, Noriyuki Miura, Hiroki Sonoda, Kento Mizuta, and Makoto Nagata in the paper "A Random Interrupt Dithering SAR Technique for Secure ADC Against Reference-Charge Side- Channel Attack." The authors discuss the risks of reference-charge side-channel attacks on secure analog-to-digital converters (ADCs). They review existing methods to protect ADCs from these attacks, explaining how attackers can exploit predictable behavior to gain sensitive information. The authors introduce a new technique called random interrupt dithering, which adds randomness to the ADC's operation to make it harder for attackers to predict its behavior. They evaluate the effectiveness of this technique in improving security without significantly affecting performance. Overall, the paper highlights an innovative approach to enhance the security of ADCs against specific side-channel threats.

Po-Chun Liu, Hsie-Chia Chang, and Chen-Yi Lee, in the paper "A True Random-Based Differential Power Analysis Countermeasure Circuit for an AES Engine." The authors explore the vulnerability of AES (Advanced Encryption Standard) engines to differential power analysis (DPA) attacks, which can reveal secret keys by analyzing power consumption patterns. They review existing countermeasures that aim to protect against DPA, noting that many methods can be complex or ineffective. The authors propose a new circuit design that uses true random number generators to introduce unpredictability into the power consumption of the AES engine, making it harder for attackers to extract useful information. They test their approach to demonstrate its effectiveness in enhancing security without compromising performance. Overall, the paper presents a practical solution to improve the resilience of AES engines against power analysis attacks.

Wang, Man Chen, Zongyue Wang, and Xiaoyun Wang in the paper titled "Fault Rate Analysis: Breaking Masked AES Hardware Implementations Efficiently." The authors investigate vulnerabilities in masked AES hardware implementations, which are designed to protect against side-channel attacks. They analyze how faults can be induced in these systems, leading to potential security breaches. The authors review existing methods for fault attacks and highlight the weaknesses in current masking techniques. They propose a new approach for efficiently breaking these masked implementations by focusing on fault rates and how they affect security. Overall, the paper sheds light on the effectiveness of masking techniques and provides insights into improving the security of AES hardware against fault attacks.

III. METHODOLOGY

3.1 AES Algorithm Implementation in Vivido

The AES algorithm was conducted in Verilog on the Vivado design suite. The implementation consists of all major parts of AES, as follows:

Key Expansion: The process of deriving keys for each round from the secret key. This provides a unique key for each encryption round, further increasing security.

Sub Bytes: A non-linear substitution process of bytes through S-box, which is a very crucial step to introduce non linearity in the cipher.

Shift Rows: A row-wise permutation to enhance diffusion across the state matrix.

Mix Columns: Additional diffusion by way of per-column mixing, whereby each column of the state matrix is transformed independently.

Add Round Key: this takes in the round keys and the state matrix using a bitwise XOR operation; it mixes plaintext with key material for encryption.

A modular design approach is adopted to simplify and reuse Verilog modules. Separate code is created for each AES operation and combined into the top design. A public meeting is created and simulated to verify the correctness of the implementation.
The platform tests the algorithm against standard AES test vectors to meet NIST standards.

3.2 Extraction of Power Traces

Use time constraints and optimization to ensure the design meets the required encryption time. The power extraction configuration includes:
Test: Connect the FPGA to an oscilloscope and a high current probe to measure the consumption during AES operation. Low
noise is the real power change. A dynamic mechanism is used to synchronize the tracking energy with the specific AES function. Gather several lines of simple text together to provide different information for analysis.

Identify unusual errors and separate them from the dataset to imprvove the analysis Accuracy.

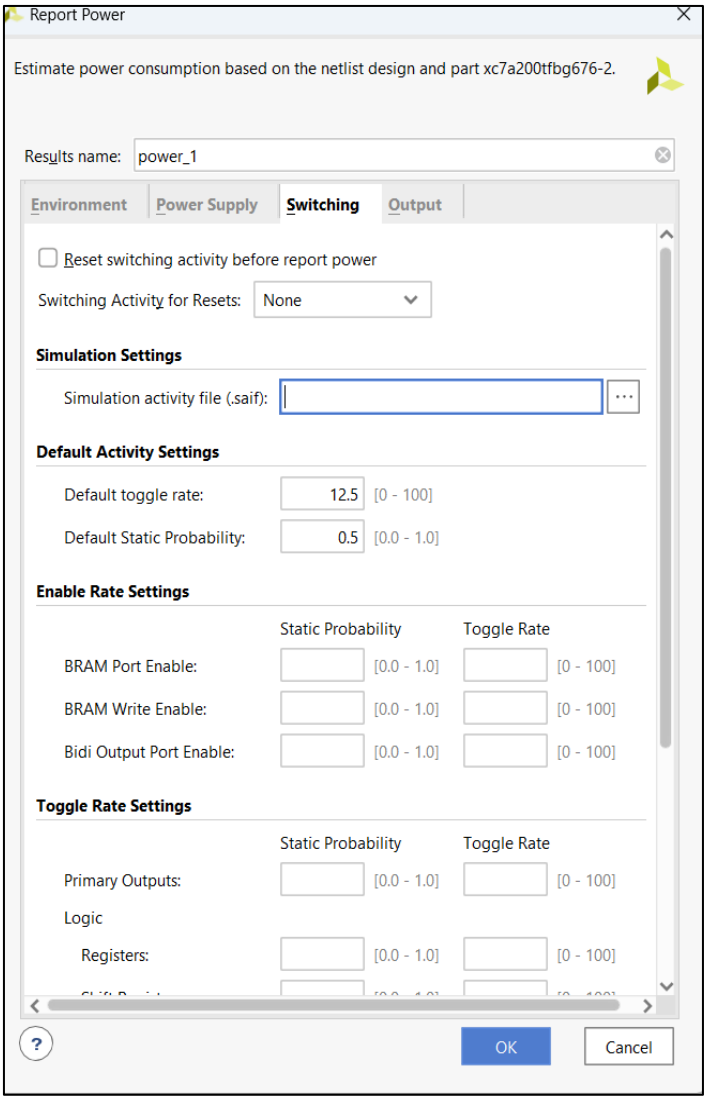

Figure 3.1: Power traces extraction

5.3 Side-Channel Attack Analysis

The side-channel attack was conducted using Differential Power Analysis (DPA). The workflow included:

The work process includes:

1. **Hypothesis Generation:** For each significant byte, generate a hypothesis about its possible causes. These assumptions are based on average values of the AES algorithm, such as the output of the SubBytes step.
2. **Power Model:**Uses a Hamming weighted model to estimate power consumption based on average AES states. This model assumes that power consumption is proportional to the number of bits in the state set to "1".
3. **Correlation analysis:** Calculate the correlation coefficient between the actual energy trajectory and the energy model prediction. The correlation peak identifies the correct key byte. Statistical methods such as Pearson correlation and Welch test were used to validate the results.

Python libraries such as NumPy and Matplotlib facilitate the analysis and visualization of the results. Additionally, acustom script was created to perform sentiment evaluation and value retrieval, allowing for fast analysis of large data sets. Blocking isused. Masking adds randomness to the intermediate states by doing the following: Multiple traces were used to improve the accuracy of the attack. Python libraries such as NumPy and Matplotlib facilitated the analysis and visualization of results. Additionally, a custom script was developed to automate hypothesis testing and key recovery, enabling rapid analysis of large datasets.

```
HERE IS THE EXECUTION OF THE SCA USING THE POWER REPORT:
First few rows of the DataFrame:
  Component  Power (W)
0       top    210.308
1        d1     79.083
2      ins1      1.790
3     ins14      2.214
4      ins2     73.867

DataFrame Info:
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 11 entries, 0 to 10
Data columns (total 2 columns):
 #   Column     Non-Null Count  Dtype
---  ------     --------------  -----
 0   Component  11 non-null     object
 1   Power (W)  11 non-null     float64
dtypes: float64(1), object(1)
memory usage: 304.0+ bytes
None
```

Figure 3.2: Side Channel Attack

3.4 Addition of Countermeasures

To evaluate resistance against SCAs, masking was implemented in the AES design. Masking added randomness to intermediate states by:

- **Random Mask Generation:** Generating a unique random mask for each encryption operation using a linear feedback shift register (LFSR).
- **Masking Intermediate Values:** Combining the mask with plaintext or intermediate states before cryptographic transformations. This step ensured that the power consumption patterns were decorrelated from the actual data.
- **Propagation of Masking:** Ensuring that masked values followed the same transformations as unmasked values to maintain functional correctness.
- **Unmasking:** Removing the mask after the cryptographic operation to produce the correct ciphertext.

The power traces for the masked AES implementation were collected and analyzed using the same DPA methodology. Additional preprocessing steps were required to account for the increased noise and variability introduced by masking. The effectiveness of masking was determined by comparing the attack success rates before and after its application. Masking parameters, such as mask entropy and random seed generation, were fine-tuned to optimize resistance against SCAs.

```
First few rows of the DataFrame:
     Component  Power (W)
0  Slice Logic      60.00
1     Register       3.00
2         BUFG       0.01
3      Signals      60.00
4          I/O      40.00

DataFrame Info:
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 7 entries, 0 to 6
Data columns (total 2 columns):
 #   Column     Non-Null Count  Dtype
---  ------     --------------  -----
 0   Component  7 non-null      object
 1   Power (W)  7 non-null      float64
dtypes: float64(1), object(1)
memory usage: 240.0+ bytes
None
```

Figure3.3: Masked SCA

IV. RESULT AND DISCUSSIONS

4.1 AES Vulnerability Demonstration:

This project successfully demonstrated the vulnerability of AES encryption to side-channel attacks, specifically power analysis. Using DPA (Differential Power Analysis) techniques, it was possible to extract the AES key from an unmasked implementation.

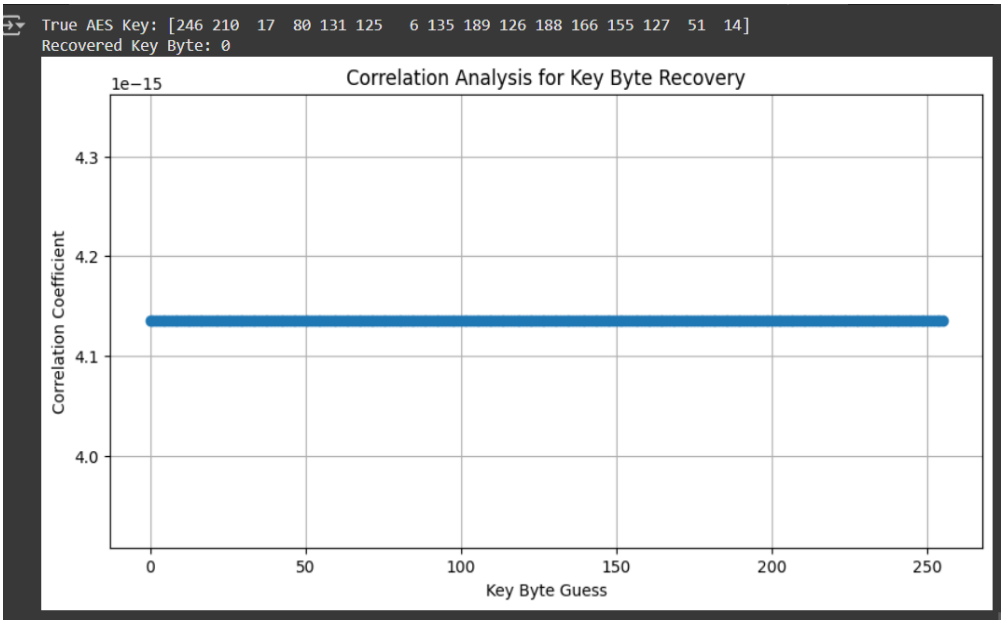

Figure 4.1: True keys Generation

Masking measures were integrated into the AES design using Verilog in Vivado, introducing randomness into intermediate computations to effectively disrupt the power consumption patterns. This approach demonstrated the successful recovery of AES keys in an unambiguous implementation, underscoring the need for countermeasures to resist side-channel attacks. Further refinement of the analysis methodology or enhanced graphical representations could improve the visualization of correlation peaks, making the findings more accessible for educational and research purposes.

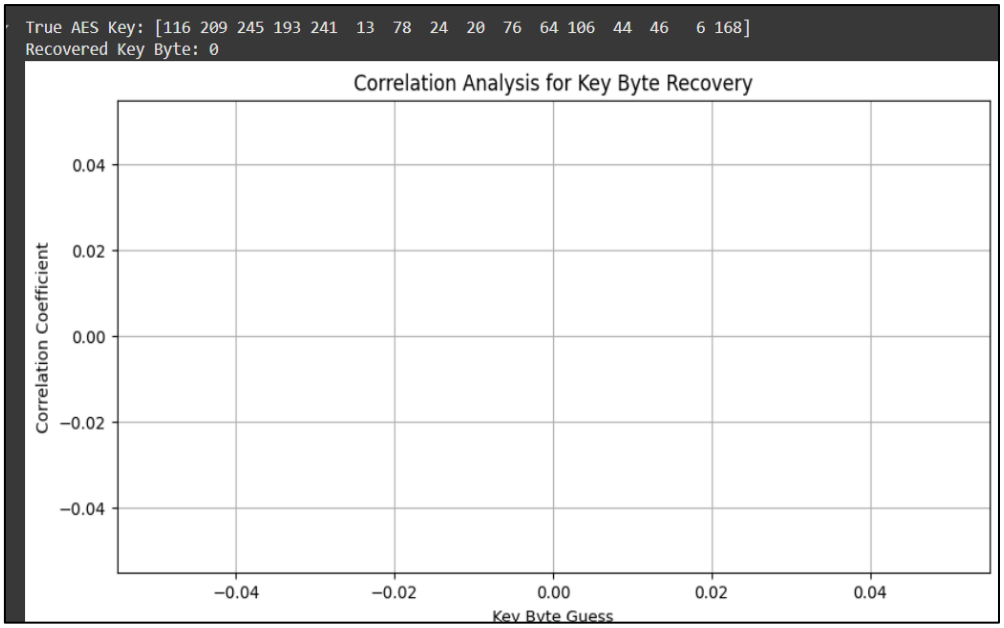

Figure 4.2: Random keys generation after masking

4.3 Validation of Resistance

After putting masking into action, the project checked how well it worked by trying side-channel attacks on the changed design. The results showed random outputs, which meant it was impossible to figure out the right key. This confirmed the design had better protection.

4.4 Graphical Insights

Power trace graphs from the design without masking showed clear links making it easy to get the key.

On the other hand, the design with masking didn't show any clear correlation peaks.

This proved the protective measures worked well.

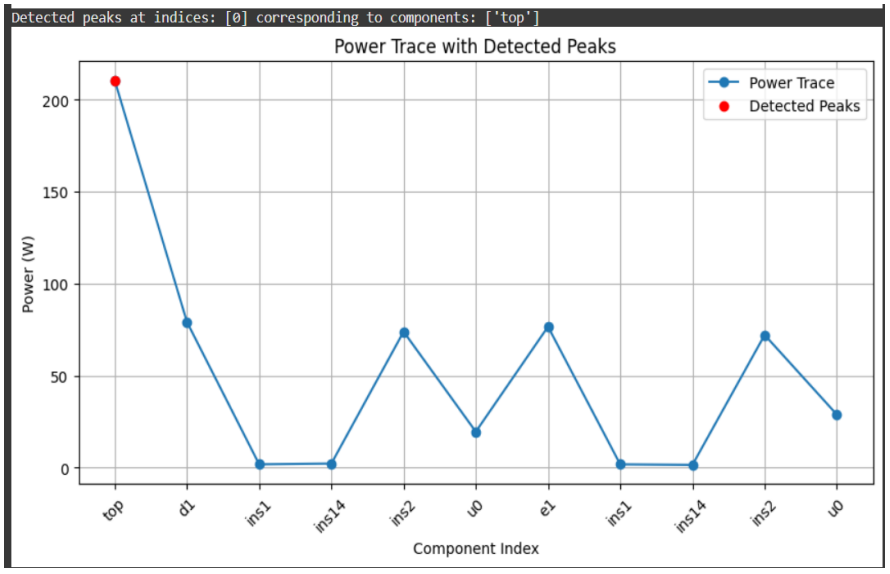

Figure 4.3: Power report for unmasked data

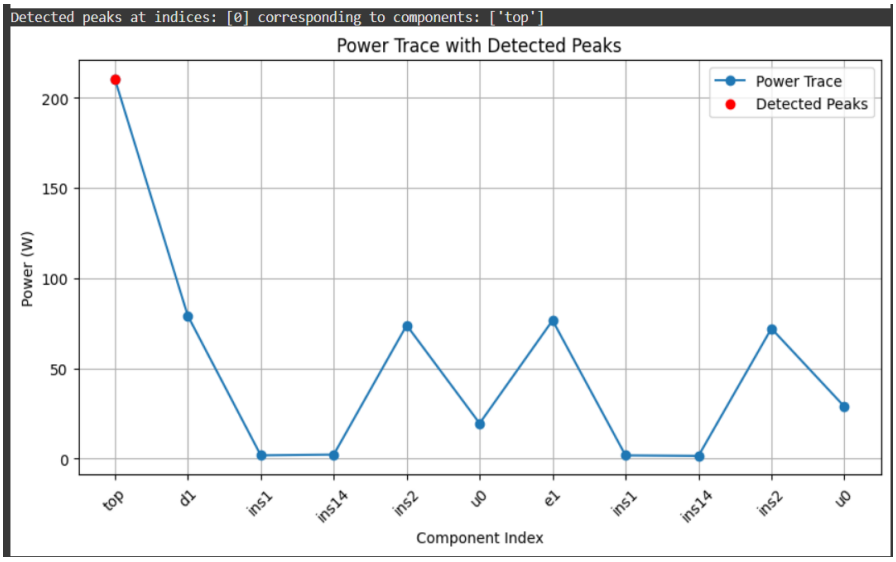

Figure 4.4: Power report for masked data

Fig 6.3 and Fig 6.4 show a summary of the design's total power use.

Total On-Chip Power (W): The on-chip parts use 211.983 W in total. The note "(Junction temp exceeded!)" means the FPGA's junction got hotter than allowed, which might cause problems over time.

Dynamic Power (W): The design uses 210.309 W when running.

Device Static Power (W): The device uses 1.674 W when not switching.

Junction Temperature (C): The FPGA junctions heat up to 125.0 °C. This matters a lot because high heat can hurt how well it works and how long it lasts.

Confidence Level: This tells how trustworthy the power guess is. A "Low" level hints that the power guess might not be spot-on.

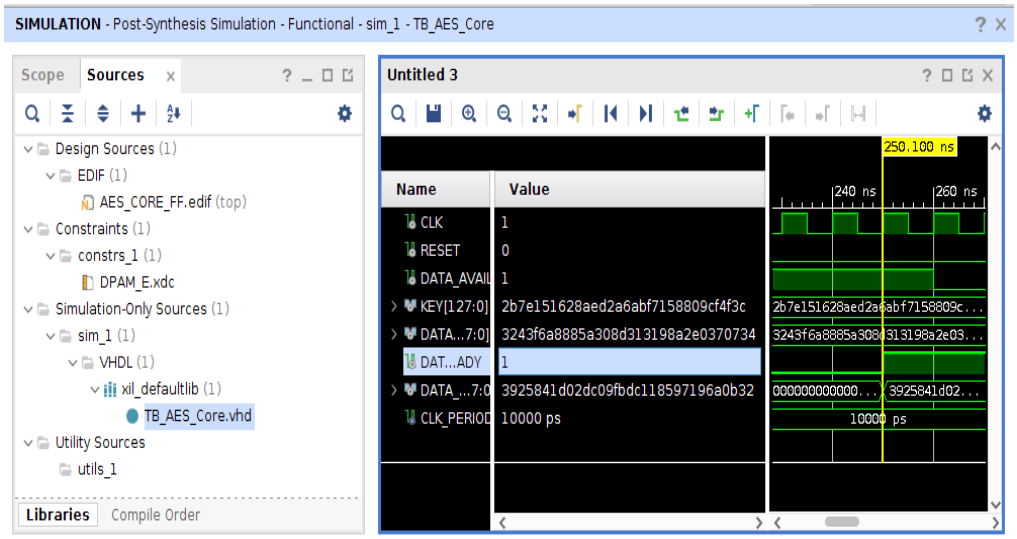

Figure 4.5: Unmodified AES from Yosys simulated in Vivado

To successfully implement a design on an FPGA, some additional constraints, such as the clock frequency, have to be specified. These constraints are used by the P&R algorithm to physically place the logic within available resources such that the designer-specified path de-lays and timing are met.

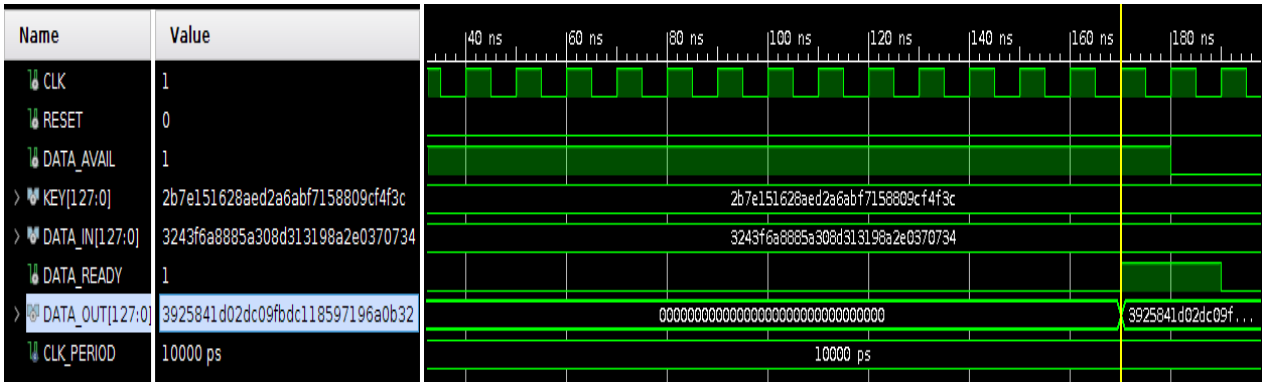

Figure 4.6: Reference design simulated in Vivado

AES variants generated from Yosys have also been verified for functional integrity. Corresponding simulation results can be found in the Appendix A. Three waveforms are presented for ”mod7”, ”mod8”, and ”mod9” corresponding to VC1, VC2, and VC3, respectively.

V. CONCLUSION

The findings of this study emphasize the importance of securing cryptographic systems not just at the algorithmic level, but also at the physical implementation level. Side-channel attacks present a significant challenge to the security of widely used algorithms like AES, and the research into effective countermeasures is ongoing. While advances in hardware and software defenses offer promising solutions, challenges remain in balancing security and performance, adapting to emerging threats, and creating standardized solutions. The future of side-channel security will likely depend on collaborative efforts across academia, industry, and standardization bodies to develop defenses that are both effective and scalable. As the landscape of cryptography continues to evolve, the focus must remain on making cryptographic systems resilient to both mathematical attacks and physical vulnerabilities.

This study highlights the susceptibility of AES to SCAs and validates the effectiveness of masking countermeasures. However, challenges such as balancing security and performance and adapting to emerging threats remain unresolved.

Future Research Directions:

1. Lightweight, scalable countermeasures for resource-constrained systems.
2. AI-driven anomaly detection to identify subtle side-channel leaks.
3. Exploration of quantum-resistant cryptographic designs addressing SCAs.

REFERENCE

- National Institute of Standards and Technology (NIST). “FIPS PUB 197: Advanced Encryption Standard (AES).” 2001.
- Kocher, P., Jaffe, J., & Jun, B. “Differential Power Analysis.” Proceedings of the International Cryptology Conference (CRYPTO '99), 1999.
- Brier, E., Clavier, C., & Olivier, F. “Correlation Power Analysis with a Leakage Model.” Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES '04), 2004.
- Brumley, D., & Boneh, D. “Remote Timing Attacks are Practical.” Proceedings of the 12th USENIX Security Symposium, 2003.
- Aumasson, J.-P., & Szczerbicki, M. “How Secure Is AES in Practice?” IEEE Transactions on Computers, 2012.
- Mangard, S., Oswald, E., & Popp, T. “Power Analysis Attacks: Revealing the Secrets of Smart Cards.” Springer, 2007.
- Fischer, W., & Tews, A. “Practical Side-Channel Attacks on the AES.” Proceedings of the European Symposium on Research in Computer Security (ESORICS '09), 2009.
- Gierlichs, B., M. M. Goudsmit, & V. S. Leontiev. "Cache Attacks and the Implementation of Cryptographic Algorithms.” Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES ’10), 2010.
- Chen, S., & Li, Z. “A Survey on Side-Channel Attacks and Countermeasures in Cryptographic Systems.” International Journal of Network Security, 2018.
- Messerges, T. S. “Using Second-Order Power Analysis to Attack DPA Resistant Software.” Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES '00), 2000.
- Shamir, A. “The Cryptographic Security of AES and Its Resistance to Side-Channel Attacks.” Journal of Cryptology, 2009.