Design of VLSI-Based Hardware Detection System Against Power Side-Channel Attacks

Dr.V.Pushpa[1], AshwinKumar A[2], Gowtham S[3], Sanjay C[4]
[1, 2, 3, 4] Dept of Electronics and Communication Engineering
[1, 2, 3, 4] Loyola Institute Of Technology

Abstract- *The rapid growth of System-on-Chip (SoC) technologies has increased their vulnerability to advanced physical and power side-channel attacks, which can compromise the security of integrated circuits. Conventional countermeasures often involve complex fabrication processes and high area overhead, making them difficult to implement and verify. This paper presents a VLSI-based hardware detection system designed to identify and mitigate power side-channel and physical attacks in real time. The proposed approach integrates clock-based and voltage-based sensing mechanisms along with dynamic pattern matching to detect anomalies caused by attacks such as voltage manipulation, replay attacks, and unauthorized probing. The system is implemented using FPGA-based architecture and validated through simulation using ModelSim. Experimental results demonstrate that the proposed detection framework achieves high accuracy with low overhead, ensuring minimal impact on system performance. The design offers a scalable and efficient solution that can be seamlessly integrated into existing SoC architectures, enhancing hardware security and reliability in modern embedded systems.*

Keywords: FPGA, Power Side-Channel Attacks, SoC Security, VLSI Design, Attack Detection.

I. INTRODUCTION

The increasing integration and complexity of System-on-Chip (SoC) devices have made them a critical component in modern electronic systems. However, this rapid advancement has also exposed these systems to various security threats, particularly power side-channel attacks and physical attacks. These attacks exploit unintended information leakage such as power consumption, timing variations, and electromagnetic emissions to extract sensitive data, thereby compromising system integrity.

Recent advancements in hardware security have highlighted the growing threat of power side-channel attacks (SCAs) on modern cryptographic and System-on-Chip (SoC) implementations. Several research works have focused on identifying vulnerabilities and proposing effective countermeasures at the hardware level.

Yanning Ji and Elena Dubrova (2025) presented a side-channel attack on a masked hardware implementation of CRYSTALS- Kyber, demonstrating that even protected designs are vulnerable when deep learning techniques are applied to power analysis. Their work revealed a high success rate in key recovery, emphasizing the limitations of conventional masking techniques and the need for stronger hardware-level defenses.

Amisha Srivastava et al. (2025) introduced PoSyn, a power side-channel aware synthesis framework that enhances resistance against leakage by optimizing the mapping of RTL components to standard cells. The proposed method significantly reduces attack success rates while maintaining area and timing efficiency, proving that synthesis-level optimization can improve security without major overhead.

Dejun Xu et al. (2025) proposed a hardware-friendly shuffling-based countermeasure for CRYSTALS-Kyber, utilizing a Random Permutation Generator to randomize execution order and reduce leakage points. Their approach demonstrated strong resistance against correlation power analysis with minimal performance degradation.

Jiheon Woo et al. (2026) developed a novel defense mechanism based on optimal noise injection to minimize mutual information leakage between sensitive data and physical observations. Their framework provides a mathematically grounded approach to enhancing resistance against advanced side- channel attacks while maintaining power efficiency.

From the reviewed literature, it is evident that although several countermeasures exist, many of them introduce high complexity, increased hardware overhead, or limited scalability. Therefore, there is a need for a practical, low-overhead, and real-time hardware detection mechanism that can effectively identify multiple types of attacks in SoC environments. The proposed work addresses this gap by introducing a VLSI-based detection framework with integrated sensing and pattern analysis capabilities.

II. PROPOSED SYSTEM AND ARCHITECTURE

To address the limitations of existing hardware security mechanisms, a VLSI-based detection framework is proposed for identifying power side-channel and physical attacks in System-on-Chip (SoC) environments. The proposed system is designed to operate in real time with minimal hardware overhead while maintaining high detection accuracy. The architecture is implemented using an FPGA-based platform and consists of multiple interconnected modules, including a reference clock generator, clock synthesizer, attack pattern generator, benchmark circuits, delay detector, and a logic attack detection unit. These modules work collaboratively to monitor system behavior and detect anomalies caused by malicious activities.

The reference clock generator produces multiple clock frequencies using a clock divider mechanism, enabling flexible testing under different timing conditions. The clock synthesizer further refines these signals to generate controlled and configurable clock outputs required for system operation and analysis. These clocking units play a crucial role in identifying timing-based attacks such as clock tampering and synchronization faults.

An attack pattern generator is designed to simulate various real-world attack scenarios, including unauthorized probing, data manipulation, and replay attacks. By injecting controlled attack patterns into the system, the robustness and responsiveness of the detection mechanism can be evaluated effectively.

To analyze system behavior, benchmark circuits are incorporated to process both normal and attack-induced signals. The outputs of these circuits are continuously monitored and compared using a delay detector, which evaluates timing differences between reference and test signals. Any deviation beyond expected thresholds indicates potential abnormal activity.

The logic attack detection unit integrates all modules and performs dynamic pattern matching to identify attack signatures. It analyzes variations in signal patterns, clock behavior, and logical outputs to detect anomalies in real time. A finite state machine (FSM) is used to control the overall operation, ensuring proper synchronization and coordination among all modules.

The proposed architecture provides a scalable and efficient framework for hardware- level security. Its modular design allows easy integration into existing SoC systems without significant performance degradation. By combining clock analysis, voltage monitoring, and pattern-based detection, the system offers a comprehensive solution for detecting a wide range of side-channel and physical attacks in modern VLSI systems.

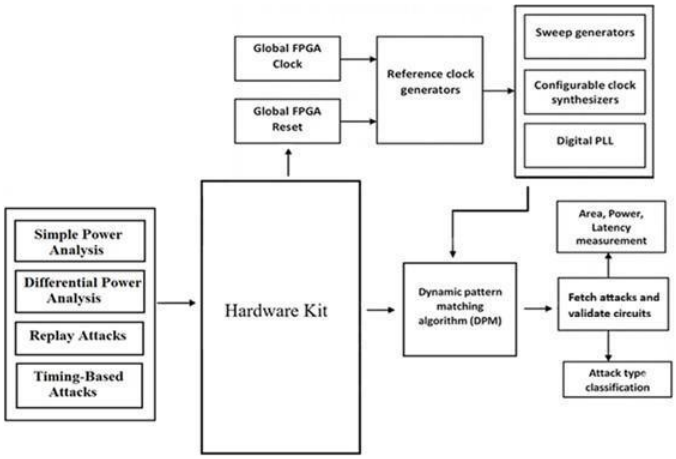

Fig. 1. Proposed FPGA-Based Attack Detection Architecture

III. METHODOLOGY AND IMPLEMENTATION

The proposed hardware detection system is implemented using a modular VLSI design approach to ensure flexibility, scalability, and efficient detection of power side-channel and physical attacks. The complete system is developed and validated using an FPGA-based architecture and simulated in ModelSim. The methodology is divided into key functional modules, each contributing to the overall detection mechanism.

Reference Clock Generator

The reference clock generator serves as the primary timing unit of the system. It is designed using a global clock and reset signal, along with a multi-bit clock divider to generate multiple clock frequencies. This enables the system to operate under varying timing conditions, which is essential for identifying clock-related anomalies such as clock tampering and synchronization faults.

Clock Synthesizer and Test Circuit

The clock synthesizer module generates stable and configurable clock signals required for system operation. It refines the output of the reference clock generator to produce controlled frequencies. The test circuits, including benchmark modules, utilize these clock signals to simulate real-time processing conditions and serve as a reference for analyzing system behavior under normal and attack scenarios.

Attack Pattern Generator

The attack pattern generator is responsible for simulating various types of attacks such as unauthorized probing, data manipulation, and FPGA replay attacks. It introduces controlled attack signals into the system based on configurable inputs. This module plays a crucial role in evaluating the robustness and responsiveness of the detection mechanism under different adversarial conditions.

Dynamic Pattern Matching and Detection Unit

The detection unit continuously monitors system outputs and performs dynamic pattern matching to identify abnormal behavior. It analyzes variations in signal patterns, timing characteristics, and logical outputs to detect inconsistencies caused by attacks. A delay detector is also incorporated to compare reference and test signals, identifying latency variations that indicate potential threats.

System Integration and Control

All modules are integrated using a finite state machine (FSM), which ensures proper coordination and synchronization across the system. The FSM controls the execution sequence, manages signal flow, and enables real-time monitoring of system behavior. This integrated approach ensures accurate detection while maintaining system stability and performance.

The complete design is implemented using hardware description language (HDL) and verified through functional and timing simulations.

The modular architecture allows easy integration into existing SoC systems, providing a practical and efficient solution for enhancing hardware security against side- channel and physical attacks.

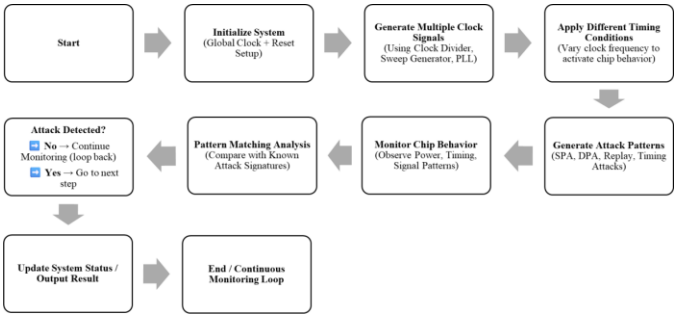

Fig. 2: Data flow of Proposed Attack Detection Methodology

IV. RESULTS AND DISCUSSION

The proposed VLSI-based hardware detection system was successfully implemented and verified using FPGA-based simulation in ModelSim. The primary objective of the results is to evaluate the system's ability to detect power side-channel and physical attacks under different operating conditions.

The simulation results demonstrate the correct functioning of the reference clock generator and clock synthesizer modules, which produce stable and configurable clock signals. These signals enable the system to operate under varying timing conditions, allowing effective identification of timing-based anomalies.

The attack pattern generator was tested by introducing multiple attack scenarios such as replay attacks, timing manipulation, and unauthorized probing. The system responded accurately to these injected patterns, enabling controlled evaluation of detection performance. The monitoring and detection unit continuously analyzed system outputs and identified deviations in signal behavior. The delay detector successfully captured timing differences between reference and test signals, generating appropriate control signals such as 'up', 'down', and 'lock'. These signals indicate synchronization status and help in identifying abnormal system conditions.

The dynamic pattern matching mechanism effectively detected attack signatures by comparing observed signal patterns with predefined reference patterns. When an attack was detected, the system triggered appropriate output responses, indicating successful detection. In the absence of attacks, the system maintained normal operation and continued monitoring without false triggering.

Overall, the results confirm that the proposed system achieves reliable and real-time detection of side-channel and physical attacks with minimal performance overhead. The modular design ensures consistent performance across different test conditions, demonstrating the effectiveness and robustness of the proposed approach.

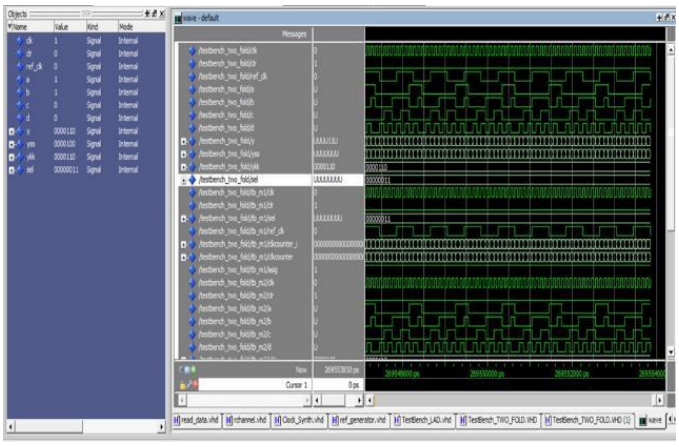

Fig. 3: Clock Signal Output

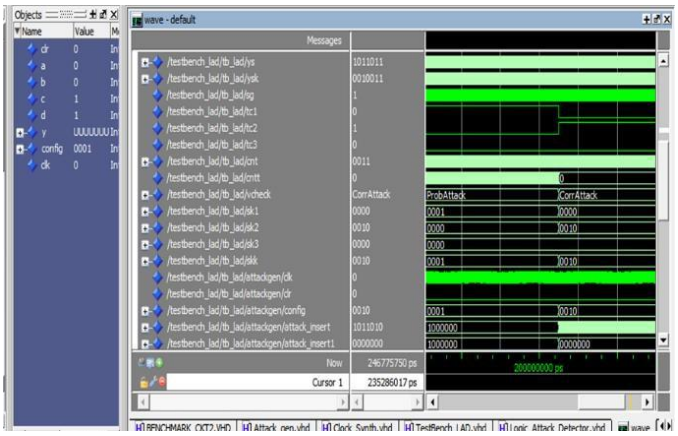

Fig. 4: Attack Injection Waveform

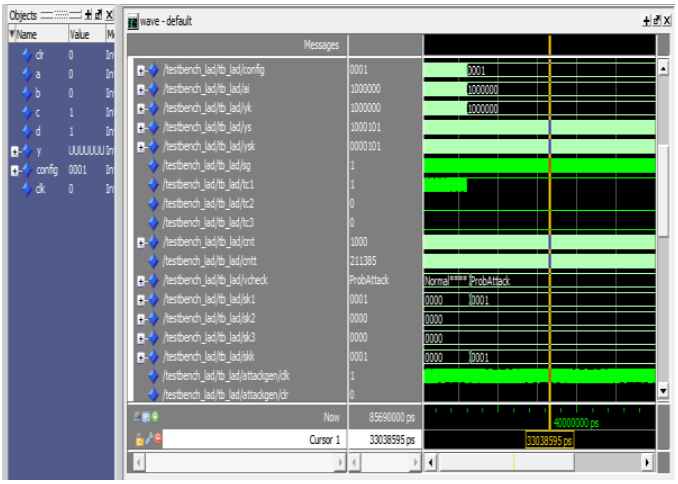

Fig. 5: Detection Output Signal

V. CONCLUSION AND FUTURE WORK

In this work, a VLSI-based hardware detection system for identifying power side- channel and physical attacks in System-on- Chip (SoC) environments has been successfully designed and implemented. The proposed system integrates clock analysis, attack pattern generation, and dynamic pattern matching techniques to detect abnormal behavior in real time. The use of FPGA-based architecture ensures flexibility, scalability, and efficient validation of the design.

The simulation results confirm that the system can accurately detect various attack scenarios, including timing manipulation, replay attacks, and unauthorized probing, with minimal performance overhead. The modular design approach enables easy integration into existing hardware systems without significant modifications. Overall, the proposed framework enhances the security and reliability of modern VLSI systems against evolving attack techniques.

As future work, the system can be extended by incorporating machine learning- based detection techniques to improve accuracy and adaptability against unknown attack patterns. Additionally, real-time hardware implementation on advanced FPGA platforms and integration with secure cryptographic modules can further strengthen the robustness of the system.

VI. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the management and faculty members of the institution for providing the necessary facilities and continuous support throughout the course of this work. The authors are especially thankful to the project guide for their valuable guidance, constructive suggestions, and constant encouragement, which greatly contributed to the successful completion of this project. The support and cooperation received from the department and peers are also gratefully acknowledged.

REFERENCES

[1] Y. Ji and E. Dubrova, "Deep Learning- Based Side-Channel Attack on Masked CRYSTAL Kyber Hardware Implementation," IEEE Transactions on Information Forensics and Security, 2025.

[2] Srivastava, et al., "PoSyn: Power Side- Channel Aware Synthesis for Secure Hardware Design," IEEE Transactions on Computer- Aided Design of Integrated Circuits and Systems, 2025.

[3] D. Xu, et al., "A Hardware-Friendly Shuffling Countermeasure Against Side- Channel Attacks on CRYSTALS-Kyber," IEEE Transactions on Circuits and Systems, 2025.

[4] J. Woo, et al., "Optimal Noise Injection for Minimizing Information Leakage in Side- Channel Attacks," IEEE Transactions on Information Theory, 2026.

[5] M. Yasin and O. Sinanoglu, (2017) "Evolution of logic locking",IEEE International Conference on Very Large Scale Integration. ATS), 1273–1282.