Smart authentication and evaluation of 3DIC security through LDPC based pattern analysis

Ms. Ratshna M R[1]
Department of ECE
Surya Group of Instituitions
Vikiravandi, Villupuram
rakshy23ece@gmail.com

Mrs. Revathi R[2]
Department of ECE
Surya Group of Instituitions
Vikiravandi, Villupuram
revathisec@gmail.com

***Abstract*— Recent developments in 3D IC technology involve multiple levels of infrastructure management to secure the data assets within the device. The focus has been on maintaining intellectual property data integrity and enhancing IC technology security. A trust assurance-based privacy protection framework has been developed to protect internal ICs from attacks such as reverse engineering, counterfeit attacks, direct privacy breaches, and functional locking attacks. To safeguard integrated devices against external attacks, an efficient framework named "Tree House" has been implemented in the existing system. This framework scans and authenticates users directly, preventing counterfeiting and scanning functional logic testing. The system also focuses on detecting side-channel attacks. Additionally, a secure key-based authentication protocol is available for integrated chips using a low-density generator. Code word access to the integrated ICs is facilitated by dynamic memory design and a fast-flowing synthesizer, enabling testing of operations. Testing and evaluation are conducted using specialized software, and further analysis includes power report analysis and comparative validation.**

***Keywords*— *Chip design, Soc attacks, Field programmable gate array, Low power design, Cryptography*.**

I. INTRODUCTION

A side-channel attack is a type of privacy-preserving security breach that involves information leakage from the integrated IC, akin to a black box effect. Unlike traditional attacks that target existing algorithms, side-channel attacks focus on the physical implementation of FPGA devices, exploiting dynamic fluctuations in leakage power, electromagnetic emissions, and variations in sensitive data. These attacks present security threats different from traditional methods and are primarily implemented in cryptography applications[1]. Instead of directly attacking cryptographic algorithms, a strategic focus is placed on detecting information leakage during the execution of cryptographic operations in integrated ICs. Although detectable by algorithms, various types of sidechannel attacks persist, storing information within the integrated IC and slowly corrupting it, providing resilient interruptions[2].

Power consumption fluctuations, electromagnetic emissions, and timing variations create sensitive data vulnerabilities within the system, affecting non-cryptographic keys and impacting algorithmic complexity. The proposed system addresses drawbacks present in existing systems by enabling algorithms to mathematically detect and evaluate side-channel attacks[3]. Safeguarding against such attacks is accomplished through a holistic approach, incorporating hardware design with continuous algorithmic evaluation. Various power analysis attacks are provided, illustrating power consumption patterns of devices. Different cryptographic techniques are tested against these attacks. Integrated ICs physically impact the target device, underscoring the importance of robust security measures.

Timing analysis reveals variations in the time required for the proposed algorithm to execute a given task. However, timing variation attacks exploit these fluctuations, enabling the system to continuously detect changes in timing patterns and subsequently reducing its security attributes. Timing attacks pose a significant threat to cryptographic keys, similar to traditional attacks that directly affect the operation of integrated ICs[4]. These attacks target the resilient variations introduced to clock signals, impacting the entire system and leading to various unwanted power dissipations. Depending on the variations in electromagnetic radiation, techniques like differential electromagnetic analysis are employed to correlate electromagnetic analysis with electromagnetic variations. Magnetic analysis revolves around the integrated IC, generating unwanted emissions and creating disruptive sounds to interfere with the ongoing processes of the ICs[5].

In the proposed system, a supportive approach is adopted, where a high-frequency fast-sweeping synthesizer serves both as a test circuit and a memory device for testing purposes. Side-channel attacks and their patterns are detected using pattern analysis algorithms, facilitating their classification for further analysis.

The rest of the paper is organized with study of existing state of art approaches in Section II, followed with system design through proposed architecture, detailed proposed design methodology in Section III, the implementation results and discussions are made in Section IV, with conclusion and future work follows.

II. BACKGROUND STUDY

J. Dofe(2016) The author presented a system implementing a potential security threat detection framework. A new triggered payload-based 3D hardware Trojan prediction system was developed, focusing on the power delivery network in 3D

integrated circuits (ICs). This network is utilized for Clock Recovery Oscillators (CRO) and detection through effective side-channel analysis. The novel 3D detection system includes direct communication between two channels, enabling analysis of the 3D structure and evaluation of cross-plane attacks[6].

Zhang et al. (2019) The presented system includes a detailed survey of hardware Trojans applicable to three-dimensional integrated circuits and systems. A comprehensive model of three-dimensional hardware Trojans is analysed using existing performance analysis techniques. A detailed case study is provided, demonstrating the feasibility of using thermal analysis to trigger these three-dimensional Trojans. The activation of three-dimensional Trojans is compared with existing two-dimensional approaches, highlighting the performance of integrated circuits in various environments[7]. ***Nabeel et al. (2020)*** The author introduced a system with a well-developed security ideology based on the physical separation of trusted and untrusted users. The system employs runtime monitoring of the architecture at all levels of integrated chips, providing continuous security analysis. This straightforward method not only prevents security breaches but also ensures reliable supply chain management[8];

Stern et al. (2021) The author presented a novel framework addressing security threats in confidential electronic design circuits. The system focuses on managing confidentiality at both RTL and gate-level graphical design stages. It employs a logic clocking system with a unique temporary logic element access control to protect digital intellectual property from external attacks. This comprehensive approach ensures reliability and supports industry development by adhering to all engineering standards[9].

Alrahis et al. (2021) The author presented a system for attack transformation and detection using a logic login-based Boolean detection process. This system extracts attacks from the secret key, demonstrating how representative scan techniques can disrupt the dynamic processes within integrated circuits (ICs). The scans are effective even with large key sizes and variable encryption keys, showcasing the system's robustness in breaking the dynamics of the IC processes[10].

Limaye et al. (2022) The author presented a system for detecting malicious intellectual property accessibility by introducing Trojans into the hardware and monitoring the counterfeiting actions within integrated circuits (ICs). The proposed approach uses a dynamic scan-based technique to detect secret keys and evaluate changes occurring in the clock cycle. This method serves as a defence against various scanning techniques used in logical locking systems. The paper examines attacks on integrated devices by implementing SAT attacks and verifies the attack levels using scanning techniques[11].

Considering various drawbacks present in the existing framework includes, Complexity in functional lock testing and power drawbacks are considered for evaluating the new architecture for proposed design [12]-[17].

III. PROPOSED METHODOLOGY

In the existing methodology, trust-based decision-making model is developed to detect the privacy encounters, reverse engineering problems, counterfeiting attacks towards 3D integrated chip design and evaluate the efficiency of developed system. The major challenge in existing system includes, Complexity in functional locking testing and power drawbacks are considered.

A. System architecture

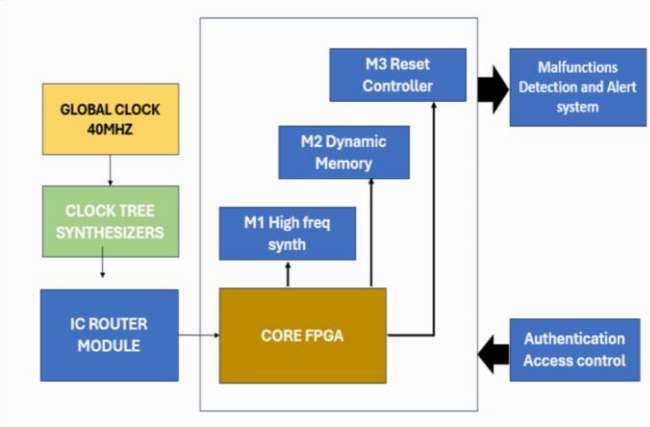

Fig 1. System architecture

Fig 1. Shows the system architecture of proposed side channel attack detection system. The presented approach considers three different scenario of attack testing model such as high frequency fast synthesizer, dynamic memory model and reset controller architecture.

Reset controller, Dynamic memory testing, Fast flowing synthesizer is evaluated. Testing and authentication protocol is implemented to avoid side channel problems.

B. Design of Fast sweep clock generator The module generates a clock distribution structure using the base global clock. The hardware reset functions as an active high reset. The clock synthesizer, also known as the reference clock generator, creates various control clocks used by the digital elements in the proposed architecture. Flip-flops, clocked gates, multiplexers, and various sequential circuits rely on these clock signals. These clocks originate from the global clock, approximately 40 MHz, as a starting point.

C. Application model development

The proposed system comprises three primary modules: the high-frequency clock synthesizer, the dynamic memory module, and the reset controller. The high-frequency clock generator module is prone to clock errors such as glitches, jitter, and skew. To mitigate these issues, low-power techniques are employed. The dynamic memory module addresses another application scenario. The 3D IC design integrates three distinct applications. The third module, the reset controller, is used to apply asynchronous resets to specific logical blocks. These core modules are implemented using the finite state machine concept.

D. Side Channel attack detections

On the other hand, the malfunction detector and alert system provides authentication results. If a malicious user gains access to the 3D modules that secure the core FPGA, the system will generate an alert in the form of a text message and a flashing light. The type of the attack is evaluated by recalling the attack LUT stored in the temporary memory.

E. Authentication and integration

The system is developed with a digital comparator with respect to look up table (LUT) storing the unique ID generated by Quasi generator (LDPC). The generator code compares with the pre-defined unique code and then allow the user to access the 3D modules. The unauthorized user is denied by the Field programmable logic device (FPGA) by testing the attacks patterns. The attack patterns are dynamic in nature. The continuously varying attack patterns enable the device to analyse the patterns effectively.

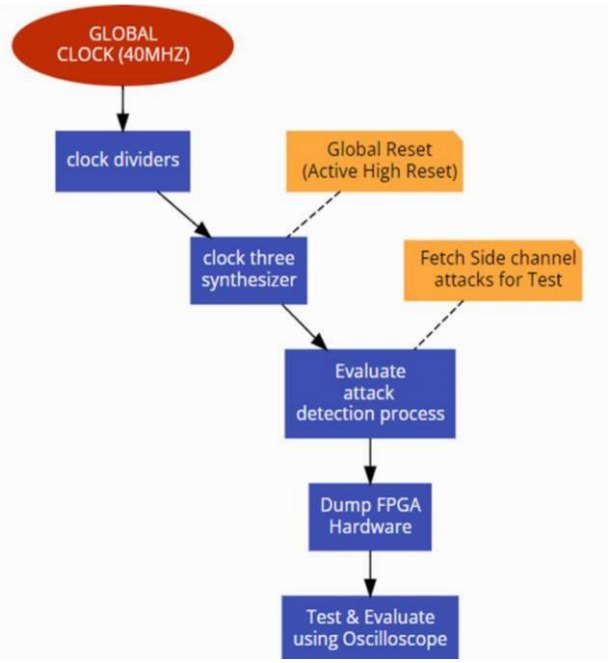

Fig 2. Design flow

Fig 2. Shows the system design flow model in which the pattern of attack frameworks are fetched into the test circuits to analyse the quality of proposed design framework. The simulation result of fast sweep synthesizer outputs before the implementation and after the implementations are developed here. Through partial configuration of FPGA, the proposed design is validated and justified. The complete testing includes the hardware module, followed with digital storage oscilloscope for measuring the frequency is arranged.

IV. RESULTS AND DISCUSSIONS

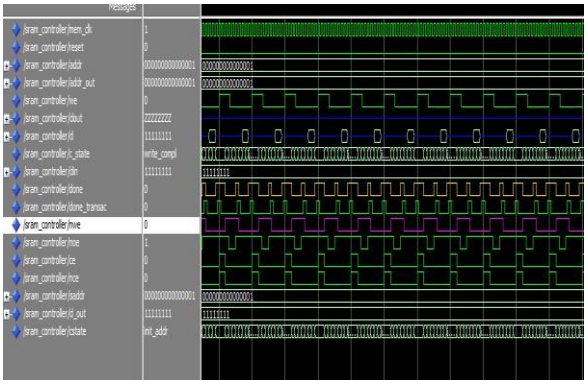

Fig 3. Memory operation

Fig 3. Shows memory operation through reconfigurable IC router module. The proposed three test circuits are simulated and validated through modelsim/Quartus II software.

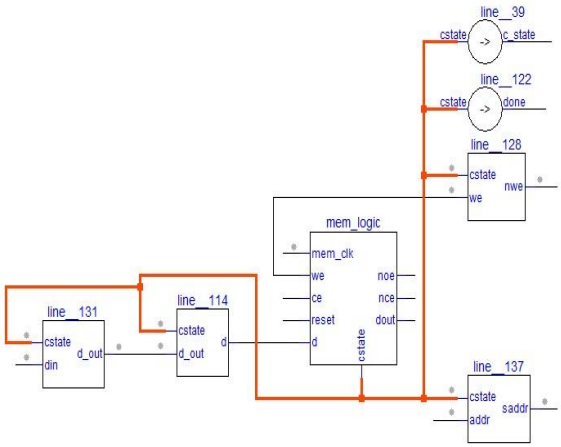

Fig 4. Data flow design

Fig 4. Shows data flow design evaluated with customized network node connected with memory module.

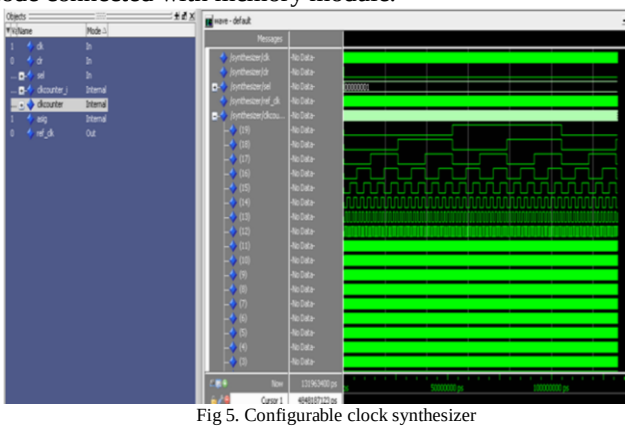

Fig 5. Configurable clock synthesizer

Fig 5. Shows the configurable clock synthesizer circuit result showing the configurable clock pulses.

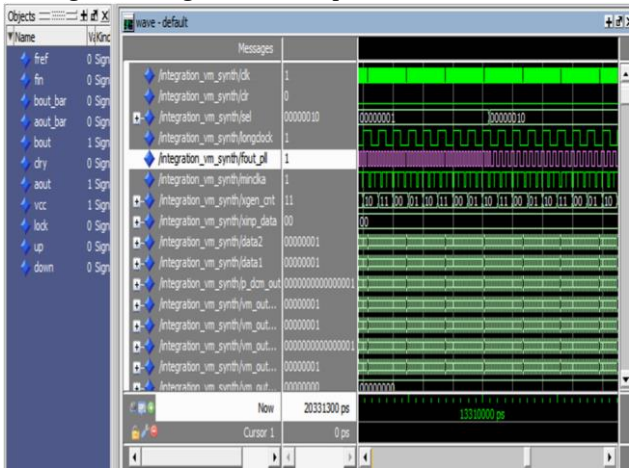

Fig 6. Reconfigurable speed

Fig 6. Shows the digital circuit results with configurable settings. The sysnthesizer result with customized clock frequency is evaluated here.

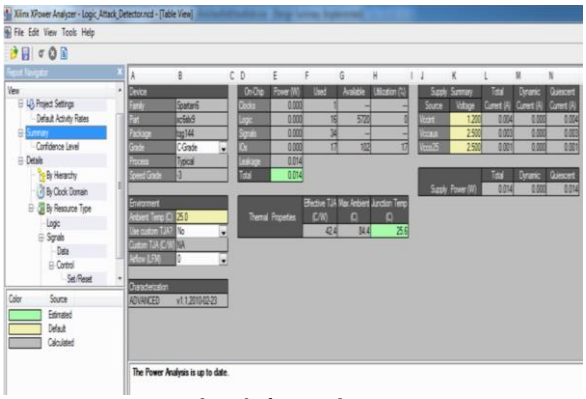

Fig 7 Power analysis before implementation

Fig 7. Shows the power analysis result of proposed implementation before removal of attack present in the synthesizer circuit.

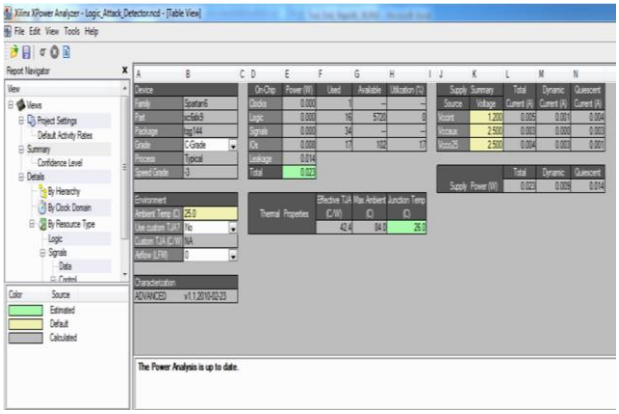

Fig 8. Power analysis after implementation

Fig 8. Shows the power analysis result of proposed implementation after removal of attack present in the synthesizer circuit.

The power is evaluated as below,

0.023-0.014=0.009 W, considering the dynamic power only, as the static power is default.

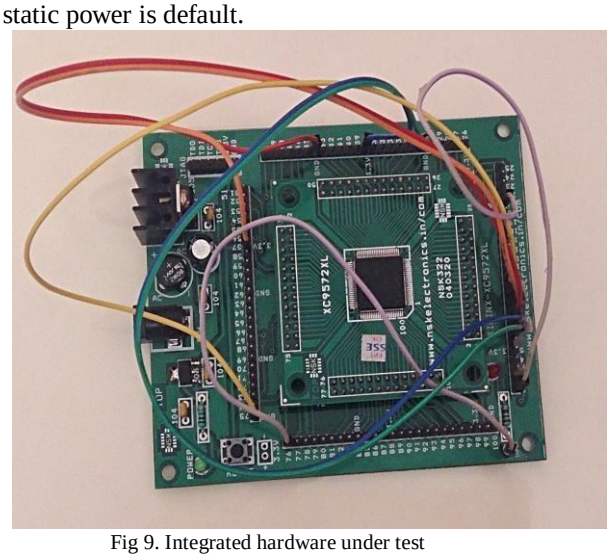

Fig 9. Integrated hardware under test

Fig 9.shows the integrated hardware under test of detection of attack impacted clock synthesizer.

Table 1. Performance results

Slno.	Ref.	Device utilization Report
1	Existing System (Dofe et al.(2016))	86% of FPGA space, with 0.65ns of latency
2	Proposed work	0.65 ns latency 45% of FPGA space is utilized

Table 1. shows the performance results of proposed method, it achieves 0.65ns latency 45% of total FPGA space. Where the existing framework achieved with 86% of FPGA space.

V. CONCLUSION

Recent advancements in 3D IC technology address various levels of infrastructure management to safeguard data assets within the device. There's a concerted effort to preserve the integrity of intellectual property data and bolster the security of IC technology. A trust assurance-based privacy protection framework has been devised to shield internal ICs from a range of attacks, including reverse engineering, counterfeit attempts, direct privacy breaches, and functional locking attacks. To fortify integrated devices against external threats, an effective framework called "Tree House" has been integrated into the current system. This framework directly authenticates users, thwarting counterfeiting and scanning functional logic testing. Moreover, the system is adept at identifying side-channel attacks. Furthermore, a secure keybased authentication protocol is employed for integrated chips via a low-density generator. Access to the integrated ICs is managed through code words, facilitated by dynamic memory design and a fast-flowing synthesizer, thereby facilitating operation testing. Specialized software is utilized for testing and evaluation, with additional analysis including power report analysis and comparative validation. These measures collectively reinforce the security and reliability of integrated devices in the 3D IC technology landscape.

REFERENCES

[1] Y. Kwon, D. Pavlidis, T. L. Brock, D. C. Streit, “A D-band monolithic fundamental oscillator using InP-based HEMT’s,” IEEE Trans. on Microwave Theory and Tech., vol. 41, no. 12, pp. 2336-2344, Dec. 1993.

[2] B. H. Calhoun and A. P. Chandrakasan, "A 256-kb 65-nm subthreshold SRAM design for ultra-low-voltage operation," IEEE Journal of Solid-State Circuits, vol. 42, no. 3, Mar. 2007, pp. 680-688.

[3] J. Chen, L.T. Clark and T.-H. Chen, "An ultra-low-power memory with a subthreshold power supply voltage," IEEE Journal of Solid-State Circuits, vol. 41, no. 10, Oct. 2006, pp. 2344-2353.

[4] Chen, B., Zhou, C., Liu, Y., & Liu, J. (2022). Correlation analysis of runway icing parameters and improved PSO-LSSVM icing prediction. Cold Regions Science and Technology, 193, 103415.

[5] Golshan, K. (2020). Clock Tree Synthesis. In: The Art of Timing Closure. Springer, Cham. https://doi.org/10.1007/978-3-030-49636-4_6

[6] J. Dofe, Q. Yu, H. Wang and E. Salman, "Hardware security threats and potential countermeasures in emerging 3D ICs," 2016 International Great Lakes Symposium on VLSI (GLSVLSI), Boston, MA, USA, 2016, pp. 69-74, doi: 10.1145/2902961.2903014.

[7] Zhang, Zhiming, and Qiaoyan Yu. "Modeling hardware trojans in 3d ics." 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2019.

[8] Nabeel, M., Ashraf, M., Patnaik, S., Soteriou, V., Sinanoglu, O., & Knechtel, J. (2020). 2.5 D root of trust: Secure system-level integration

of untrusted chiplets. IEEE Transactions on Computers, 69(11), 16111625.

[9] Stern, Andrew, et al. "Aced-it: Assuring confidential electronic design against insider threats in a zero-trust environment." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 41.10 (2021): 3202-3215.

[10] Alrahis, Lilas, et al. "ScanSAT: Unlocking static and dynamic scan obfuscation." IEEE Transactions on Emerging Topics in Computing 9.4 (2019): 1867-1882.

[11] Limaye, N. (2022). Learning-Resilient and Cost-Effective Logic Locking for IP Protection: Attacks, Frameworks, and Defenses (Doctoral dissertation, New York University Tandon School of Engineering).

[12] P. Chakraborty, J. Cruz, A. Alaql and S. Bhunia, "SAIL: Analyzing Structural Artifacts of Logic Locking Using Machine Learning," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3828-3842, 2021, doi: 10.1109/TIFS.2021.3096028.

[13] S. Charles, Y. Lyu and P. Mishra, "Real-Time Detection and Localization of Distributed DoS Attacks in NoC-Based SoCs," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 12, pp. 4510-4523, Dec. 2020, doi: 10.1109/TCAD.2020.2972524.

[14] M. Sinha, S. Gupta, S. S. Rout and S. Deb, "Sniffer: A Machine Learning Approach for DoS Attack Localization in NoC-Based SoCs," in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 11, no. 2, pp. 278-291, June 2021, doi: 10.1109/JETCAS.2021.3083289.

[15] T. -H. Tran, B. -A. Dao, T. -T. Hoang, V. -P. Hoang and C. -K. Pham, "Transition Factors of Power Consumption Models for CPA Attacks on Cryptographic RISC-V SoC," in IEEE Transactions on Computers, vol. 72, no. 9, pp. 2689-2700, 1 Sept. 2023, doi: 10.1109/TC.2023.3262926 [16] E. Shereen, M. Delcourt, S. Barreto, G. Dán, J. -Y. Le Boudec and M. Paolone, "Feasibility of Time-Synchronization Attacks Against PMUBased State Estimation," in IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 6, pp. 3412-3427, June 2020, doi: 10.1109/TIM.2019.2939942

[17] B. -A. Dao, T. -T. Hoang, A. -T. Le, A. Tsukamoto, K. Suzaki and C. K. Pham, "Correlation Power Analysis Attack Resisted Cryptographic RISC-V SoC With Random Dynamic Frequency Scaling Countermeasure," in IEEE Access, vol. 9, pp. 151993-152014, 2021, doi:10.1109/ACCESS.2011