Fortified-SoC: A Novel Approach Towards Trojan Resilient System-on-Chip Design

Burra Subbarao
Electronics & Commu. Engineering,
SRM University AP, India.
subbarao_burra@srmap.edu.in

Chella Amala
Electronics & Commu. Engineering
SRM University, AP, India.
amala_chella@srmap.edu.in

Banee Bandana Das
Computer Science and Engineering
SRM University, AP, India
banee.bandana@gmail.com

Saswat Kumar Ram
Electronics & Commu. Engineering
SRM University AP, India.
saswatram01@gmail.com

Saraju P. Mohanty
Computer Science and Engineering
University of North Texas, USA.
saraju.mohanty@unt.edu

***Abstract*—This research paper investigates a hardware-type attack on System-on-Chips (SoCs) involving a trigger and a payload. A stealthy and controllable fabrication time attack, A2, is demonstrated, and a circuit is developed based on charge accumulation from rare events within the system. When voltage gets buildup due to charge coupling, the payload has been activated, leading to a privilege-escalation attack. In this research, a specific analog hardware Trojan (A2) detection and mitigation circuit is designed. This Trojan affects the circuit performance by targeting sensitive wires (like reset) in SoCs. This paper presents a method for detecting the Trojan and implementing proper mitigation techniques to safeguard SoCs from malicious attacks.**

***Index Terms*—Hardware Trojan, Hardware security, Internet of Things (IoT).**

I. Introduction

A system's hardware is its foundation. Every piece of software runs on top of a CPU. Software has to have faith that the hardware will implement the specification exactly as intended. For numerous applications, the software cannot detect certain hardware defects or malfunctions [1]–[4]. Even worse, an attack on the hardware could potentially breach all levels of a system that depends on it, violating established security protocols implemented by the software [5]. The shift towards smaller transistors is beneficial for improved performance and reduced power usage; however, the cost of chip production has increased [6], [7]. For instance, the cost of building a fabrication line increases by 15% for every subsequent process node. In the future, it's anticipated that the initial outlay needed to put up a fabrication line for the smallest transistor size will be 20 billion [8]. Many hardware companies prefer to outsource fabrication to spread out the cost of the initial tooling required to support a specific transistor size [9].

Tiny devices have become increasingly prevalent in various applications due to the progress in fabrication processes. These applications include consumer electronics and the Internet of Things (IoTs) [10], [11]. This development can be attributed to the scaling down of MOSFETs, which has significantly contributed to the miniaturization of these devices. The cloud, gateways, and end node equipment (sensor nodes) compose the IoTs [7]. In IoTs, a smart node can detect, analyze, and communicate the required information. We outline steps for detecting and mitigating the described hardware Trojan in SoCs. Firstly, the identification of vulnerable components within the SoCs is crucial. It entails finding sensitive elements such as critical wires or capacitors that the Trojan may exploit [12], [13]. Secondly, a deep understanding of the Trojan's behavior is essential [5]. It involves analyzing how it utilizes charge accumulation on capacitors from infrequent events to activate a privilege escalation attack. Next, sophisticated detection mechanisms need to be developed to identify the Trojan's presence within the SoC [14].

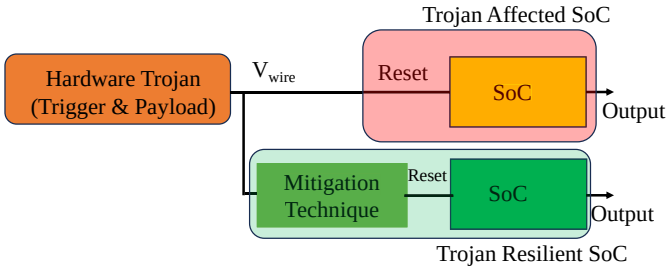

Fig. 1: Trojan Resilient Design

These mechanisms could involve monitoring critical circuit elements for abnormal patterns or voltage fluctuations indicative of the Trojan's activity. Once detected, effective mitigation techniques must be implemented. These techniques may include isolating affected components, enhancing security measures, or redesigning vulnerable circuitry. Validation through rigorous testing is crucial to ensure that detection and mitigation techniques accurately identify and neutralize the Trojan without unintended consequences. Integration into the broader security framework of the SoC is necessary to provide comprehensive protection against hardware-based attacks. Through these measures, SoCs can be fortified against

hardware Trojans, safeguarding them from malicious exploitation [7] and the scenario with and without Trojan resilient design is well presented in Figure 1 to safeguard SoCs.

The above discussion raises following concerns in designing Trojan resilient designs as

1) To detect unwanted triggering of pivotal signals/wires in the design by malicious agents.
2) To design circuits that can cater this changes in the design and provide counter mechanism to safe guard the system.

This paper is organized as follows, Section II presents the contribution of the current paper. Section III represents the background of the hardware security issues. Section IV analyzes the proposed work on fortified SoC. Section V depicts the results and Finally, Section VI concludes the paper with future research directions.

II. Contribution of the Current Paper

A. Problem Addressed

The security of integrated circuits is equally important as power, area, and speed in VLSI designs due to the exponential increase in adversaries. The insertion of malicious circuits into the design of the untrusted supply chain is a matter of concern. The unwanted and extra circuits called hardware Trojans can drastically affect the circuit performance by triggering randomly. In this research, to safeguard the designs from such malicious agents and attacks, detection and mitigation techniques are discussed for A2 Trojan.

B. Proposed Solution

In this paper, we proposed and implemented a novel technique to detect and mitigate the effects of Trojan that changes the values of sensitive wire in the SoCs. Here, an A2 Trojan is taken into consideration, which affects the reset wire of any design. Due to the Trojan, an unwanted reset makes the entire system functionality unpredictable with erroneous results.

C. Significance of the Proposed Solution

In this research, the main objective is to provide a more secure alternative for the SoCs to avoid unwanted reset. As the reset is always a sensitive wire in all SoCs, our main focus is to avoid premature reset due to Trojan.

III. Related Work

Many recent works focus on various hardware security issues caused by the worldwide semiconductor industry. A significant concern is the potential for hardware Trojans in circuits, emphasizing the need for vigilance in this domain. Hardware Trojans are not only digital, analog Trojans also exist and can target and trigger circuit events [15]. Because of their small size and ability to be put into even the most delicate wires, Trojan circuits have the power to disrupt a system's whole functioning. These vulnerabilities need to be recognized, and a suitable signal that can reveal the existence of a Trojan must be produced. In the analysis of the received signal, it is crucial to minimize the impact of the Trojan during runtime. The detection and mitigation of Trojan threats in real time can be defined as runtime protection. In works [16], [17], a model was designed to address this issue. The Trojan was seamlessly incorporated and later revealed its presence. In [16], Deng et al. employed a configurable structure with a control mechanism known as BIAS, placed it into the nets, and used run-time detection techniques to successfully detect Trojans. From the studies conducted, it has been evident that an analog Trojan in an integrated circuit can notably decrease the overall system performance. Considering in light of these difficulties, the study focuses on identifying and addressing the security flaws in the system, particularly the A2-based Trojan, during runtime. It aims to provide accurate solutions for enhancing the system's security. In subsequent sections of this research, further elaboration will be given on the activation, identification, and containment of the analog A2-Trojan.

IV. Proposed Work for Fortified-SoC

A hardware attack comprises both a trigger and a payload, where the malicious circuits are intentionally crafted to mimic authentic circuits, allowing them to activate the attack payload. Our research demonstrates the implementation of a fabrication time attack. We have developed a small, stealthy, and controllable circuit. The capacitor in the system stores charge from sporadic events, eventually reaching full capacity when frequent charge-coupled events occur. Once fully charged, the capacitor activates the payload, triggering a privilege escalation attack. For instance, a Trojan may be inserted to influence the design. This section discusses the impact of Trojans on circuit behavior and proposes a mitigation technique. In our design, we incorporate a unique analog hardware Trojan known as A2. The circuit diagram, showcasing the utilization of charge sharing and capacitive coupling, can be well understood by Figure 2.

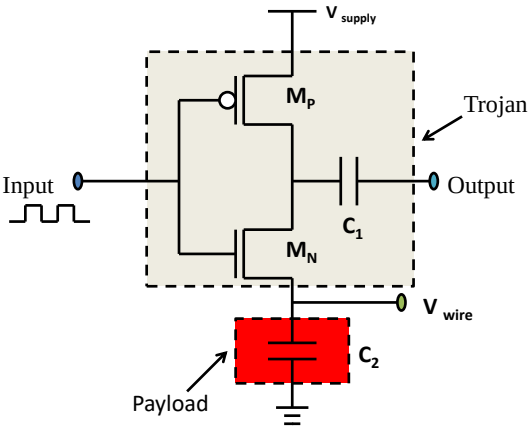

Fig. 2: Illustration diagram of malicious analog Trojan (A2) hardware

This research paper outlines the key contributions as:

1) Our innovative approach involves creating the initial fabrication-time processor attack, which replicates the

typical design-time triggered assaults. We present a method in which a malicious agent during the fabrication process can take advantage of the prevalent empty areas in Application-Specific Integrated Circuit (ASIC) designs to integrate malicious circuits near sensitive wires like reset.

2) This research showcases the initial instance of an analog attack that is more compact than its digital alternative. Our method effectively diverts charge from typical signal transitions to activate its trigger. In addition, our attack relies on a sophisticated and unlikely analog trigger sequence, making it difficult to replicate at the analog level.
3) In this research, we implemented Trojan resilient design, which can detect and mitigate the effect of A2 Trojan in SoCs.

In this design, the payload voltage is accumulated by charging it from the nearest power source (V_{DD}) to the specified V_{wire}. Once the capacitor (payload) reaches full charge, the circuit's performance will be influenced. Our main objective is to detect the A2 Trojan by closely monitoring the voltage build-up on the RST node of an SoC during its normal operation. This procedure of detecting the Trojan and a proper mitigation technique is demonstrated in Figure 3.

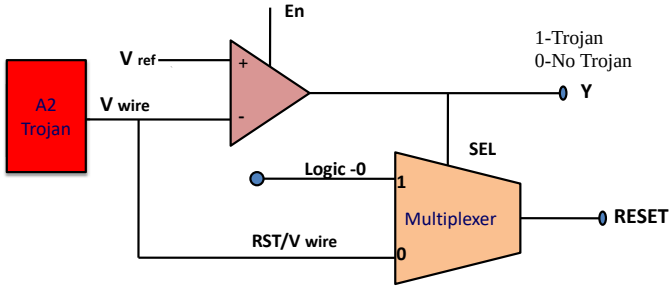

Fig. 3: A novel approach to detect and mitigate the A2 Trojan

The occurrence of the Trojan-triggering event is independent of any specific operation. The Trojan's activation are controlled by continuous events in the system. Once such an event occurs, the Trojan initiates its malicious activities, influencing the system's behavior and potentially compromising the integrity of the system. The detection and mitigation of such Trojans are vital for ensuring the security and reliability of the system.

The detection and mitigation circuit is depicted in Figure 3. The Trojan is designed to charge a payload, and when the voltage on the wire (V_{wire}) reaches a certain threshold, the reset input is activated. This interference disrupts the normal operation of the SoCs, potentially causing premature resets and affecting the overall functionality of the system. Once the payload crosses V_{ref}, V_{wire} can be charged gradually using the voltage from the adjacent wires, which will impact functionality. The Trojan detection circuit's output, denoted as Y, is determined by comparing it with V_{ref}. Y is either 1 or 0, indicating the presence or absence of a Trojan. This signal can be utilized to address the issue. The En signal is high during the entire evaluation period. The detection circuit focuses primarily on identifying the A2 Trojan, as it is similar in structure to the converter circuits used in today's low-power energy harvesting systems [5]. Figure 3 illustrates the detection and mitigation of A2 Trojans once they are inserted and activated by an adversary.

V. Experimental Results

In this research, the NCverilog simulation tool using 90 nm technology library in Cadence is used. It has four modules: RTL design, Functional simulation, Synthesis, and Physical Design. We have done the simulation for the proposed design from Verilog code to GDS-II. The power report for the entire circuit is depicted in Figure 4 in terms of percentage, the leakage power consumed is 3 %, the internal power consumed is 10 %, and the switching power consumed is 87%.

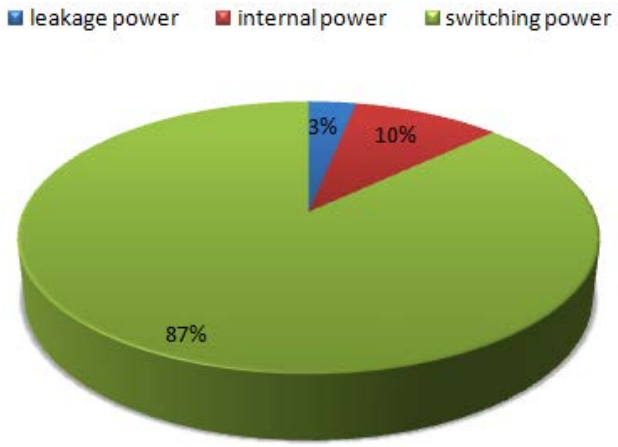

Fig. 4: Power consumption (in %)

The designed circuit consists of two circuits a comparator and a multiplexer. Many studies have employed the full custom approach for chip design [7]; here, we propose to apply the semi-custom approach, which is very helpful in reducing design time and complexity.

Figure 5 represents the schematic of the proposed model to detect and mitigate the Trojan, once triggered. The enable signal will be active till the period when the role of reset is crucial in the SOC. Such that unwanted resets can be avoided and the system can operate without any malfunction. Figure 6

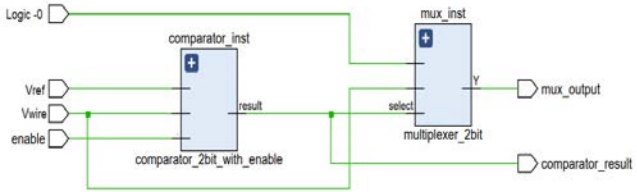

Fig. 5: Schematic of Proposed Design

depicts the simulation result of the proposed concept. The A2 Trojan once builds up the voltage in the wire (V_{wire}), it will make the reset to active. As per the mitigation techniques used, once V_{wire} is triggered by setting up a voltage, it is compared with the V_{ref}. Once Y is one and a Trojan is detected, it makes the reset to maintain its safe value without malfunctioning with the help of a multiplexer. The selection line is used to decide the reset once Trojan gets detected. Figure 7 depicts the layout of the proposed design and finally, the GSD-II is generated for fabrication. The characterization of A2 Trojan is presented in Table I.

Fig. 6: Simulation Result of the Proposed Technique

TABLE I: Characterization Table

Parameters	Implementation of A2 Hardware Trojan
Technology	90 nm
Total Power	$0 - 2.9\ \mu W$
Area	$15.138\ \mu m^2$
Input Voltage Range	$0 - 1$ V

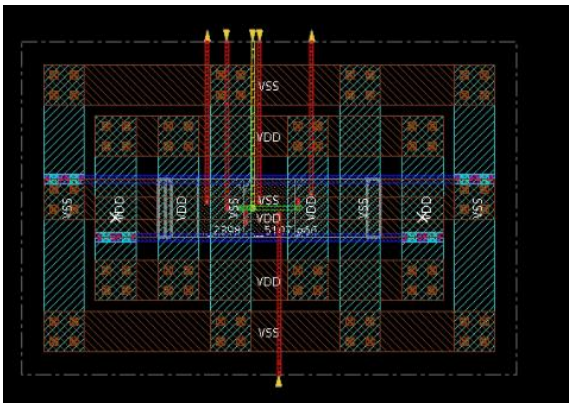

Fig. 7: Layout of Proposed Design

VI. Conclusion and Future Research

This paper highlights the vulnerability of SoCs to hardware-based attacks, particularly focusing on a stealthy and controllable attack called A2. This paper also discusses a methodology involving the creation of malicious circuits that mimic real ones, using a trigger and payload mechanism for privilege escalation. This demonstrates the complexity of modern attacks on semiconductor devices. The proposed hardware Trojan design, based on capacitive coupling principles, shows the need for robust security measures in SoC design and fabrication. The paper also presents ways to detect and mitigate such Trojans, emphasizing the importance of security throughout the entire SoC development life cycle. This research paper consolidates important findings on the susceptibility of SoCs to hardware-based attacks, specifically the A2 attack. In future, AMS simulator is used to validate the entire concept for various applications.

References

[1] M.-L. Li, P. Ramachandran, S. K. Sahoo, S. V. Adve, V. S. Adve, and Y. Zhou, "Understanding the propagation of hard errors to software and implications for resilient system design," *ACM Sigplan Notices*, vol. 43, no. 3, pp. 265–276, 2008.

[2] M. Hicks, C. Sturton, S. T. King, and J. M. Smith, "Specs: A lightweight runtime mechanism for protecting software from security-critical processor bugs," in *Proceedings of the Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems*, 2015, pp. 517–529.

[3] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Securing things: A novel cro applicable in puf and recycled ic detection," 2022.

[4] B. Rohini, A. R. Nayak, and N. Mohankumar, "Enhancing security and trust of iot devices–internet of secured things (iost)," in *Research in Intelligent and Computing in Engineering: Select Proceedings of RICE 2020*. Springer, 2021, pp. 15–24.

[5] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-thing 2.0: Analog-trojan-resilient ripple-less solar harvesting system for sustainable iot," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 19, no. 2, pp. 1–25, 2023.

[6] T. Trippel, K. G. Shin, K. B. Bush, and M. Hicks, "T-ter: Defeating a2 trojans with targeted tamper-evident routing," in *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, 2023, pp. 746–759.

[7] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-thing: A secure aging-aware solar-energy harvester thing for sustainable iot," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 320–333, 2020.

[8] G. Aishwarya, H. Revalla, S. Shruthi, V. P. Ananth, and N. Mohankumar, "Virtual instrumentation-based malicious circuit detection using weighted average voting," in *Microelectronics, Electromagnetics and Telecommunications: Proceedings of ICMEET 2017*. Springer, 2018, pp. 423–431.

[9] J. Vosatka, "Introduction to hardware trojans," *The Hardware Trojan War: Attacks, Myths, and Defenses*, pp. 15–51, 2018.

[10] S. K. Ram, B. B. Das, K. Mahapatra, S. P. Mohanty, and U. Choppali, "Energy perspectives in iot driven smart villages and smart cities," *IEEE Consumer Electronics Magazine*, vol. 10, no. 3, pp. 19–28, 2020.

[11] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. K. Ganapathiraju, "Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 18–28, 2017.

[12] M. M. Bidmeshki, K. S. Subramani, and Y. Makris, "Revisiting capacitor-based trojan design," in *2019 IEEE 37th International Conference on Computer Design (ICCD)*. IEEE, 2019, pp. 309–312.

[13] F. Wang, Q. Wang, B. Fu, S. Jiang, X. Zhang, L. Alrahis, O. Sinanoglu, J. Knechtel, T.-Y. Ho, and E. F. Young, "Security closure of ic layouts against hardware trojans," in *Proceedings of the 2023 International Symposium on Physical Design*, 2023, pp. 229–237.

[14] A. Pavlidis, E. Faehn, M.-M. Louërat, and H.-G. Stratigopoulos, "Runtime hardware trojan detection in analog and mixed-signal ics," in *2022 IEEE 40th VLSI Test Symposium (VTS)*. IEEE, 2022, pp. 1–8.

[15] Y. Hou, H. He, K. Shamsi, Y. Jin, D. Wu, and H. Wu, "On-chip analog trojan detection framework for microprocessor trustworthiness," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 10, pp. 1820–1830, 2018.

[16] D. Deng, Y. Wang, and Y. Guo, "Novel design strategy toward a2 trojan detection based on built-in acceleration structure," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 12, pp. 4496–4509, 2020.

[17] Y. Hou, H. He, K. Shamsi, Y. Jin, D. Wu, and H. Wu, "R2d2: Runtime reassurance and detection of a2 trojan," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2018, pp. 195–200.