MANTECH Publications

Journal of Research in VLSI Design Tools and Technology
Volume 10, Issue 3, September-December, 2025

Hardware Security and Trusted Integrated Circuit (Ic) Design: Ensuring Reliability, Resilience, And Integrity in The Era of Semiconductor Globalization

Dr. Ramesh Chandra Patil[1], Ms. Sneha Verma[2]

Associate Professor[1], Assistant Professor[2]

Department of Electronics and Communication Engineering[1,2]

DPG Institute of Technology and Management[1,2]

Email ID: *rameshpatil1997@gmail.com[1], snehaverma2022 @yahoo.co.in[2]*

Abstract

The rapid globalization of the semiconductor industry has brought numerous technological advancements but has simultaneously introduced significant vulnerabilities in hardware design and manufacturing. Hardware security and trusted integrated circuit (IC) design have emerged as crucial disciplines to ensure the confidentiality, integrity, and availability of electronic systems. As modern systems rely on ICs for applications ranging from consumer electronics to defense technologies, securing hardware components from malicious modifications, reverse engineering, intellectual property theft, and side-channel attacks has become a top priority. This paper explores the evolving domain of hardware security and trusted IC design, discussing its underlying principles, existing threats, design methodologies, and challenges. It further examines recent research trends and outlines the future scope for developing secure, trustworthy, and sustainable semiconductor systems.

Keywords*: Hardware Security, Trusted IC Design, Trojan Detection, Side-Channel Attack, Secure Hardware Architecture, Semiconductor Reliability, Cryptographic Hardware, Reverse Engineering, Design-for-Security (DfS), Supply Chain Trust.*

INTRODUCTION

In the modern digital era, the security of electronic systems heavily depends on the trustworthiness of their hardware components. As ICs form the foundation of nearly every computing system, hardware vulnerabilities can compromise even the most sophisticated software security mechanisms. The proliferation of fabless design models, global supply chains, and third-party fabrication facilities has intensified concerns about potential security breaches such as hardware Trojans, counterfeit ICs, and malicious modifications during manufacturing.

Hardware security aims to design, test, and verify ICs to ensure their integrity, authenticity, and confidentiality. Trusted IC design, on the other hand, focuses on establishing confidence in the design and manufacturing processes through secure design methodologies, hardware-based cryptographic modules, and verification frameworks. Together, these disciplines play a vital role in defending critical infrastructure, military systems, and consumer devices against physical and logical attacks.

LITERATURE REVIEW

Early Developments in Hardware Security

The concept of hardware trust first gained attention in the early 2000s when globalization led to outsourcing of chip fabrication to offshore foundries. Researchers began identifying risks of tampering, overproduction, and IP piracy. Early efforts focused on *Physically Unclonable Functions (PUFs)*, which leveraged inherent manufacturing variations to create unique, unclonable hardware fingerprints. These were instrumental in authentication and key generation mechanisms.

Evolution of Trusted IC Design Techniques

With the advancement of semiconductor technologies, design-for-security (DfS) frameworks emerged to integrate security features during design rather than as an afterthought. Logic obfuscation, split manufacturing, and hardware watermarking techniques were developed to counter reverse engineering and IP theft. Additionally, side-channel attack mitigation and secure boot architectures became integral components of trusted ICs.

Recent Advancements and Research Directions

Recent research has focused on developing machine learning-driven methods for Trojan detection, formal verification for hardware trust validation, and secure enclaves within processors. Moreover, post-quantum cryptographic implementations at the hardware level are gaining prominence to protect against emerging quantum-based attacks. These advances signify the evolution of hardware security from reactive approaches to proactive, resilient design methodologies.

HARDWARE SECURITY THREATS

Table 1: Common Hardware Security Threats and Their Impacts

Type of Threat	Description	Impact on System	Typical Countermeasure
Hardware Trojan	Malicious logic modification in design or fabrication	Data leakage, malfunction, or denial of service	Trojan detection, design validation
Counterfeit ICs	Unauthorized duplication or use of recycled chips	Reliability degradation, failure in critical systems	Secure supply chain, traceability tags
Reverse Engineering	Extraction of circuit design by physical or logical analysis	IP theft, cloning, or design piracy	Logic obfuscation, watermarking
Side-Channel Attack	Exploiting physical leakages (power, EM, timing) to reveal secret data	Cryptographic key exposure	Power balancing, masking techniques
Supply Chain Attack	Compromise of design, fabrication, or test phases	Tampering, overproduction, hidden vulnerabilities	Split manufacturing, trusted foundries

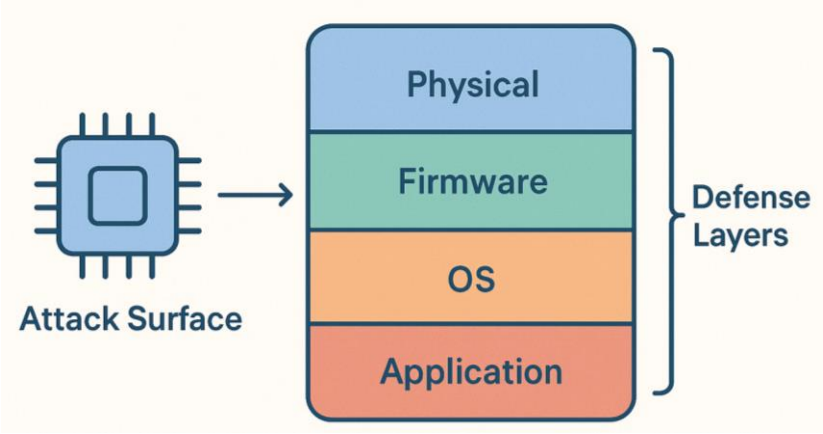


Figure 2: Hardware Attack Surface and Defense Layers

Hardware Trojans

Hardware Trojans are malicious modifications embedded in an IC's design or manufacturing stages. These can remain dormant during testing and activate under specific conditions, leading to data leakage, system malfunction, or denial of service. Detecting Trojans is challenging due to their stealthy nature and minimal footprint.

Counterfeit and Cloned ICs

Counterfeit ICs pose serious risks to system reliability and safety. They may originate from unauthorized production or from recycled components falsely labeled as new. Cloned ICs violate intellectual property and may contain hidden vulnerabilities introduced by untrusted entities.

Reverse Engineering Attacks

Reverse engineering allows attackers to extract a circuit's design from physical or logical analysis. This can reveal proprietary algorithms or cryptographic keys, threatening both commercial confidentiality and national security.

Side-Channel Attacks

Side-channel attacks exploit physical leakages such as power consumption, electromagnetic radiation, or timing variations to infer sensitive data. Such attacks are particularly effective against cryptographic modules implemented in hardware.

SECURE HARDWARE DESIGN TECHNIQUES

Table 2: Secure Hardware Design Techniques and Their Advantages

Security Technique	Main Principle	Advantages	Limitations
Logic Obfuscation	Circuit structure hidden using secret keys	Prevents reverse engineering	Increases design complexity and delay
Hardware Watermarking	Embedding identifiers for IP ownership	Legal proof of authenticity	Limited protection against functional cloning
Split Manufacturing	Dividing fabrication stages between trusted/untrusted fabs	Protects layout secrecy	Increases manufacturing cost

Physically Unclonable Function	Uses manufacturing randomness for unique ID generation	Lightweight and unclonable authentication mechanism	Sensitive to environmental conditions
Hardware Root of Trust	Verifies authenticity during system boot	Ensures system integrity at startup	Requires secure key management

Supply Chain Attacks

The globalized semiconductor supply chain involves multiple vendors and stages, including design, fabrication, assembly, and testing. Each step presents an opportunity for security breaches, making end-to-end trust verification a formidable challenge.

Logic Obfuscation

Logic obfuscation alters the circuit's structure to make reverse engineering more difficult. By inserting key-controlled gates, the circuit operates correctly only with the proper key, thus protecting against unauthorized use.

Hardware Watermarking

Watermarking embeds unique identifiers into the IC design to prove ownership and detect cloning. This technique helps in legal and forensic verification of IP rights.

Split Manufacturing

In split manufacturing, the front-end-of-line (FEOL) and back-end-of-line (BEOL) fabrication processes are divided among trusted and untrusted facilities, ensuring that complete design knowledge is never available to a single entity.

Physically Unclonable Functions (PUFs)

PUFs use process-induced variations to generate unique signatures for authentication. They provide lightweight security mechanisms suitable for IoT devices and embedded systems.

Secure Boot and Hardware Root of Trust

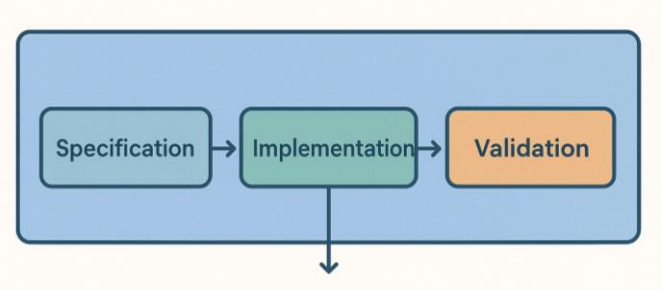
A hardware root of trust forms the foundation for a secure boot process, ensuring that only verified and authenticated firmware is executed. This mechanism prevents system compromise from malicious firmware updates.

CHALLENGES IN HARDWARE SECURITY

Despite extensive research, hardware security continues to face significant challenges:

1. **Complex Supply Chains:** Globalized semiconductor manufacturing makes it nearly impossible to ensure complete trust among all stakeholders.
2. **Detection Complexity:** Hardware Trojans and side-channel vulnerabilities often evade traditional testing due to their subtle and dormant behavior.
3. **Performance vs. Security Trade-offs:** Implementing strong security measures can increase design complexity, area, and power consumption.
4. **Standardization Gaps:** Lack of universal hardware security standards complicates integration and validation across different vendors.
5. **Emerging Threats:** Quantum computing and AI-assisted attacks are evolving faster than traditional defensive strategies.

DESIGN-FOR-SECURITY (DFS) FRAMEWORK



The Design-for-Security (DfS) methodology aims to embed trust features during the early design phases. It emphasizes secure hardware modeling, formal verification, and continuous risk assessment throughout the IC lifecycle.

Secure Design Stages in DfS:

- **Specification Stage:** Security requirements and threat models are defined.
- **RTL Design Stage:** Incorporation of obfuscation, watermarking, and secure key management.
- **Verification Stage:** Use of formal verification tools to detect security flaws.
- **Fabrication and Testing:** Application of split manufacturing and Trojan detection techniques.
- **Deployment:** Activation of secure boot and runtime monitoring for field operation assurance.

APPLICATIONS OF TRUSTED IC DESIGN

Trusted Integrated Circuit (IC) design plays a pivotal role across multiple domains where security, reliability, and performance are critical. The assurance of integrity and authenticity in hardware components is vital not only for data protection but also for operational stability in high-stakes environments. The following subsections elaborate on the major applications of trusted IC design across diverse technological fields.

Defense and Aerospace Systems

In defense and aerospace sectors, hardware security forms the backbone of mission-critical systems such as radar control units, missile guidance electronics, satellite communication modules, and avionics systems. A single instance of tampering or hidden hardware Trojan in these systems can lead to disastrous outcomes—ranging from information leakage to complete mission failure.

Trusted IC design ensures that the chips used in such applications are free from malicious insertions, overproduction, or cloning. Techniques like split manufacturing, hardware watermarking, and PUF-based authentication are widely implemented to secure defense electronics. Moreover, radiation-hardened secure ICs are employed in satellites and spacecraft to enhance reliability under extreme conditions. Defense Research and Development Organisation (DRDO) and Indian Space Research Organisation (ISRO) in India are actively investing in secure chip fabrication units to achieve strategic self-reliance in trusted hardware.

Trusted design thus ensures mission assurance, resilience against cyber-physical attacks, and protection of classified data, making it indispensable in defense-grade applications.

Financial and Cryptographic Devices

The financial sector relies extensively on hardware-level trust to safeguard confidential data, transaction integrity, and user authentication. Devices such as automated teller machines (ATMs), smart cards, point-of-sale (POS) terminals, and cryptocurrency hardware wallets employ trusted ICs to ensure that sensitive information like cryptographic keys and PINs remain secure from tampering and extraction attempts.

In these systems, secure elements (SEs) and hardware security modules (HSMs) are embedded to provide tamper-proof storage and real-time cryptographic operations. Trusted ICs also incorporate secure boot mechanisms, which verify the authenticity of the firmware before system startup, and side-channel resistant architectures that mitigate power and electromagnetic analysis attacks.

For cryptocurrency applications, trusted ICs form the root of trust for private key management, preventing key exposure even in compromised environments. As digital payments and blockchain technologies expand, the demand for certified trusted hardware (such as EAL5+ and FIPS 140-2 compliant chips) continues to rise.

Internet of Things (IoT

The Internet of Things (IoT) ecosystem, comprising billions of interconnected devices, presents one of the largest attack surfaces in modern technology. IoT nodes—ranging from smart home appliances to industrial sensors—often operate under constrained resources such as limited power, storage, and processing capabilities. This makes traditional software-based security solutions impractical.

Trusted IC design provides lightweight and hardware-embedded security mechanisms that protect IoT devices from cloning, counterfeiting, and physical probing attacks. Physically Unclonable Functions (PUFs) are particularly suited for IoT authentication, as they leverage unique hardware signatures to generate cryptographic keys without storing them explicitly. Similarly, hardware-based encryption accelerators ensure secure communication with minimal energy overhead.

In critical IoT infrastructures—like smart grids, healthcare devices, and industrial automation systems—trusted ICs help maintain device identity integrity, secure firmware updates, and real-time anomaly detection. As India moves toward large-scale digitalization through initiatives like *Smart Cities Mission* and *Digital India*, integrating trusted hardware into IoT networks becomes increasingly essential to ensure cyber resilience and data sovereignty.

Autonomous Systems and Automotive Electronics

Autonomous systems, including self-driving cars, drones, and intelligent robots, rely on complex sensor networks and artificial intelligence-driven decision units. Any compromise in the underlying hardware can directly endanger human life and operational safety. Trusted IC design serves as a protective shield against manipulation, spoofing, and unauthorized control in such systems.

In automotive electronics, trusted microcontrollers and secure communication interfaces protect vehicle-to-everything (V2X) networks from attacks that could alter sensor readings, disable braking systems, or falsify navigation data. Hardware-based intrusion detection systems (IDS) monitor real-time data flow for anomalies, while secure firmware verification ensures only legitimate updates are installed.

Additionally, automotive-grade secure ICs adhere to international standards such as ISO/SAE 21434 for cybersecurity and AEC-Q100 for reliability. In electric and connected vehicles, trusted ICs are also used to secure battery management systems and over-the-air (OTA) update mechanisms, safeguarding both driver safety and data integrity.

By embedding trust mechanisms at the hardware level, autonomous and automotive systems achieve robust protection against cyber-physical threats, ensuring safe and reliable operation even in adversarial environments.

SCOPE AND FUTURE DIRECTIONS

The scope of hardware security research extends across emerging semiconductor technologies and computing paradigms. Future research directions include:

- **AI-Assisted Security Verification:** Utilizing machine learning for anomaly detection in chip design and runtime monitoring.
- **Post-Quantum Secure Hardware:** Integrating quantum-resistant algorithms into cryptographic accelerators.
- **3D IC and Chiplet Security:** Ensuring trust in vertically stacked and modular chip architectures.
- **Secure Edge Computing:** Developing low-power, trusted hardware for edge devices in 5G and 6G ecosystems.

- **Sustainability Integration:** Designing energy-efficient, eco-friendly secure chips to align with global sustainability goals.

ETHICAL AND SUSTAINABILITY CONSIDERATIONS

The advancement of hardware security must align with ethical standards and sustainable development principles. While automation in hardware verification improves productivity, it may impact employment in traditional design roles. Hence, retraining engineers in secure design and AI-assisted verification is vital. Moreover, the environmental footprint of semiconductor manufacturing demands greener fabrication techniques and recyclable materials to promote ecological balance.

CONCLUSION

Hardware security and trusted IC design have become foundational to modern electronic system integrity. As the global semiconductor ecosystem grows more interconnected and complex, securing the hardware layer is no longer optional—it is a necessity. By integrating robust security mechanisms throughout the design and manufacturing processes, the industry can mitigate risks associated with tampering, piracy, and unauthorized access. Future innovations in AI-driven verification, quantum-resistant architectures, and sustainable semiconductor design will further strengthen trust in hardware systems. Ultimately, ensuring hardware security is not only a technical pursuit but also a strategic imperative for global digital resilience.

REFERENCES

1. Alkabani, Y., & Koushanfar, F. (2008). Active hardware metering for intellectual property protection and security. *Proceedings of the USENIX Security Symposium*, 291–306.
2. Bhunia, S., Hsiao, M. S., Banga, M., & Narasimhan, S. (2014). Hardware Trojan attacks: Threat analysis and countermeasures. *Proceedings of the IEEE*, 102(8), 1229–1247. https://doi.org/10.1109/JPROC.2014.2320510
3. Chakraborty, R. S., Narasimhan, S., & Bhunia, S. (2009). Hardware Trojan: Threats and emerging solutions. *IEEE International High-Level Design Validation and Test Workshop (HLDVT)*, 166–171. https://doi.org/10.1109/HLDVT.2009.5340158

4. Guin, U., Huang, K., DiMase, D., Carulli, J. M., Tehranipoor, M., & Makris, Y. (2014). Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. *Journal of Electronic Testing*, 30(1), 9–23. https://doi.org/10.1007/s10836-013-5439-8
5. Tehranipoor, M., & Koushanfar, F. (2010). A survey of hardware Trojan taxonomy and detection. *IEEE Design & Test of Computers*, 27(1), 10–25. https://doi.org/10.1109/MDT.2010.7
6. Rahman, M. T., Forte, D., & Tehranipoor, M. (2017). A comprehensive survey on hardware Trojan detection. *IEEE Transactions on Emerging Topics in Computing*, 6(4), 370–389. https://doi.org/10.1109/TETC.2015.2506540
7. Rostami, M., Koushanfar, F., & Karri, R. (2014). A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, 102(8), 1283–1295. https://doi.org/10.1109/JPROC.2014.2335155
8. Shamsi, K., Li, M., Zhan, Z., & Rajendran, J. (2017). Cross-layer obfuscation for hardware security and trust. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(5), 830–843. https://doi.org/10.1109/TCAD.2017.2717586
9. Yang, K., Hicks, M., Dong, Q., Austin, T., & Sylvester, D. (2016). A2: Analog malicious hardware. *IEEE Symposium on Security and Privacy (SP)*, 18–37. https://doi.org/10.1109/SP.2016.10
10. Bhunia, S., & Tehranipoor, M. (2019). *Hardware security: A hands-on learning approach.* Elsevier Academic Press.