International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 5, Sep-Oct-2026, ISSN (Online): 2395-566X

Hardware Security in Vlsi Systems: A Review of Threats, Countermeasures and Trust Across The Integrated Circuit Life Cycle

Patwari Kavyanjali Pramod[1] Kamble Akanksha Laxman[2] Sarjine Saniya Janardan[3]
Prof. S. S. Lohote[4] Prof. M. S. Nalawade[5] Dr. V. M. Dhede[6]
[1,2,3]**Department** Of Electronics And Telecommunication Jaihind College Of Engineering Kuran, Pune, Maharashtra, India
[4]Seminar Guide Department Of Electronics And Telecommunication Jaihind College Of Engineering Kuran, Pune, Maharashtra, India;
[5]Seminar Coordinator Department Of Electronics And Telecommunication Jaihind College Of Engineering Kuran, Pune, Maharashtra, India;
[6]Head Of Department Department Of Electronics And Telecommunication Jaihind College Of Engineering Kuran, Pune, Maharashtra, India

Abstract—Integrated circuits are now designed, fabricated, tested and packaged by many different organisations spread across the world. This distributed supply chain lowers cost but also creates opportunities for an untrusted party to insert malicious logic, copy intellectual property, overbuild chips, recycle used parts as new, or extract secret keys from a working device. Hardware security in VLSI studies these threats and the design techniques that defend against them. This review classifies the threats by the life-cycle stage at which they arise and by the asset they target, and then surveys the main families of countermeasures: hardware Trojan detection, logic locking and obfuscation, split manufacturing, physical unclonable functions, side-channel and fault-injection resistance, and secure boot built on a hardware root of trust. For each family the operating principle, representative studies and known weaknesses are discussed. A life-cycle security architecture is then presented that maps each protection to the stage of design, fabrication, test and field deployment where it applies. The comparison shows that no single technique secures a chip, and that defence in depth across the life cycle is required. Open problems such as attacks on logic locking, the reliability of PUF responses and the cost of security verification are identified as directions for further work.

Index Terms—Hardware security, VLSI, hardware Trojan, logic locking, physical unclonable function, side-channel attack, IP piracy, counterfeit IC.

I. INTRODUCTION

Very large scale integration (VLSI) has made it possible to place billions of transistors on a single die, and these chips now control vehicles, medical devices, communication networks, defence systems and payment terminals. Traditionally, the security of such systems was treated as a software problem, while the hardware underneath was assumed to be trustworthy. That assumption has weakened.

A modern system-on-chip often combines third-party intellectual property (IP) cores, is designed with commercial tools, is manufactured at an offshore foundry, and is tested and assembled by yet another company [1]. Each hand-over is a point where the design or the physical chip can be altered, copied or studied by someone the designer does not control.

The consequences of a hardware compromise are severe because hardware sits below every layer of software protection. A malicious circuit hidden in silicon cannot be removed by a software patch, and a secret key leaked through power consumption bypasses even a mathematically strong cipher [2]. Economic losses are also large: counterfeit and recycled parts entering the supply chain reduce reliability and have been reported in critical sectors [3].This paper reviews the field of hardware security for VLSI systems. Its contributions are:

- A classification of hardware threats by life-cycle stage and by target asset.
- A review of the principal countermeasures with their principles, representative studies and limitations.
- A life-cycle security architecture that places each countermeasure at the stage where it is effective.
- A comparison of techniques and a summary of open research challenges.

Section II introduces the IC supply chain and the security goals. Section III reviews the threats, and Section IV the countermeasures. Section V presents the life-cycle architecture, Section VI compares techniques, Section VII discusses challenges, and Section VIII concludes.

© 2026 IJSRET

II. BACKGROUND

1. **The Ic Supply Chain**

An integrated circuit passes through specification, register-transfer level (RTL) design, logic synthesis, physical layout, mask generation, fabrication, wafer test, packaging, final test, distribution, deployment and end-of-life disposal. In the fabless business model, the design house owns only the early stages; the layout file (GDSII) is sent to a foundry that may be in another country, and testing is often outsourced as well [1]. The designer therefore has limited visibility into what happens to the design after it leaves the company.

2. Security Goals

Hardware security aims to provide four properties. *Confidentiality* keeps secrets, such as cryptographic keys and proprietary design details, from being revealed. *Integrity* ensures that the circuit behaves only as specified and has not been altered. *Authenticity* allows a chip to prove that it is genuine and not a clone or a recycled part. *Availability* ensures that the chip cannot be disabled by a hidden trigger. The relevant adversaries include rogue insiders at the design house, untrusted foundries, malicious third-party IP vendors, counterfeiters and end users with physical access to a device [4].

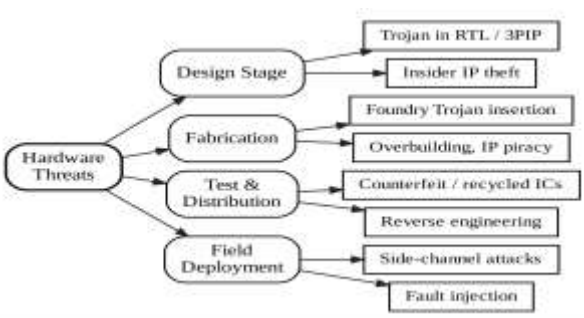


Fig. 1. Classification of hardware threats by the stage of the IC life cycle at which they arise.

III. HARDWARE THREATS

3.1 Hardware Trojans

A hardware Trojan is a deliberate, malicious modification of a circuit. Tehranipoor and Koushanfar classified Trojans by insertion phase, abstraction level, activation mechanism, effect and location [4]. A Trojan usually has a *trigger*, which is a rare condition such as a particular input sequence or an internal counter value, and a *payload*, which leaks information, changes functionality or disables the chip. Because the trigger is chosen to be rare, the Trojan stays dormant during normal functional testing, which is what makes it hard to detect [5], [6].

3.2 Ip Piracy, Overbuilding And Reverse Engineering

An untrusted foundry that holds the complete layout can produce extra chips and sell them without permission, or pass the design to competitors. Reverse engineering allows an attacker to remove the package, image each metal layer and reconstruct the netlist; Torrance and James showed that this is practical even for advanced nodes with the right equipment [7]. Such attacks threaten the designer's revenue and may reveal security mechanisms.

3.3 Counterfeit Integrated Circuits

Counterfeits include recycled chips removed from discarded boards, remarked parts with false grade or date codes, overproduced parts, out-of-specification rejects and clones. Guin *et al.* described how these parts enter the supply chain and why they reduce reliability in critical systems [3].

3.4 Side-Channel And Fault-Injection Attacks

Side-channel attacks extract secrets by observing physical quantities rather than the logical output. Kocher, Jaffe and Jun showed that statistical analysis of power traces collected during encryption can reveal the secret key, a method known as differential power analysis (DPA) [2]. Timing and electromagnetic emanations are exploited in a similar way. Fault-injection attacks deliberately disturb a chip with voltage glitches, clock glitches or laser pulses; Boneh, DeMillo and Lipton demonstrated that a single erroneous output from a public-key computation can be enough to factor the modulus [8].

IV. COUNTERMEASURES

4.1 Trojan Detection

Detection methods fall into destructive inspection, logic testing and side-channel fingerprinting. Logic testing generates patterns that try to activate rare nodes. Side-channel fingerprinting compares the power, delay or current profile of a suspect chip with that of trusted *golden* chips; Agrawal *et al.* showed that statistical analysis of power signatures can expose small extra circuitry [9]. The main difficulty is that process variation creates natural differences between chips that can hide a small Trojan, and that golden references are not always available [6].

4.2 Logic Locking And Obfuscation

Logic locking inserts additional key gates, such as XOR or XNOR gates, into the netlist so that the circuit operates correctly only when the right secret key is loaded after fabrication. EPIC by Roy, Koushanfar and Markov was an early scheme that combined such locking with public-key

© 2026 IJSRET

cryptography so that each chip could be activated only by the designer [10]. Rajendran *et al.* later analysed how well key gates should be placed to resist attacks [11]. However, Subramanyan, Ray and Malik introduced the Boolean satisfiability (SAT) attack, which uses a working, unlocked chip as an oracle and rules out wrong keys with carefully chosen inputs, breaking many early schemes in a short time [12]. This result started a continuing contest between new locking methods and new attacks.

4.3 Split Manufacturing

In split manufacturing the front-end-of-line layers, containing the transistors and lower metal, are made at an untrusted advanced foundry, while the upper metal layers are completed at a trusted facility. The untrusted foundry therefore never sees the complete interconnect. Rajendran, Sinanoglu and Karri studied whether the missing connections could be inferred from layout hints and showed that naive splitting leaks information unless the layout is also modified [13].

4.4 Physical Unclonable Functions

A physical unclonable function (PUF) uses uncontrollable manufacturing variation to give each chip a unique and unpredictable response to an input challenge. Gassend *et al.* introduced silicon PUFs based on delay differences [14], and Suh and Devadas showed how ring-oscillator PUFs could be used for device authentication and secret-key generation without storing the key in non-volatile memory [15]. In practice, PUF responses are affected by temperature and voltage, so error-correction is needed, and some delay-based PUFs can be modelled with machine learning if many challenge–response pairs are exposed.

4.5 Side-Channel And Fault Countermeasures

Defences against power analysis either hide the signal, for example with dual-rail logic or noise generation, or mask the data by splitting each secret value into random shares so that power consumption is statistically independent of the key. Encryption engines such as those implementing AES [16] are the most common targets and therefore the most common place for these protections. Fault attacks are countered by sensors that detect glitches or light, by duplicated computation with comparison, and by checking results before output, as suggested by the analysis of Boneh *et al.* [8].

4.6 Secure Boot And Hardware Root Of Trust

A hardware root of trust is a small, immutable block that holds keys and verifies firmware before it runs. During secure boot, each stage checks the cryptographic signature of the next stage, starting from code in read-only memory. Keys may be stored in one-time-programmable fuses or derived from a PUF [15]. This links the hardware security techniques above to the trust of the complete system.

Table I Summary Of Representative Studies In Vlsi Hardware Security

Ref.	Area	Contribution	Strength	Limitation
[4]	Trojans	Taxonomy of Trojan types and detection methods	Common vocabulary for the field	Survey; no new detection method
[9]	Trojan detection	Power-signature fingerprinting against golden chips	Non-destructive, finds small circuits	Needs golden chips; sensitive to variation
[10]	Logic locking	EPIC key-based activation of each chip	Prevents overbuilding by foundry	Vulnerable to later SAT attacks
[12]	Attack on locking	SAT-based key recovery with oracle	Breaks many locking schemes quickly	Requires a working unlocked chip
[13]	Split manufacturing	Security analysis of FEOL/BEOL split	Shows leakage through layout hints	Extra cost of trusted BEOL facility
[15]	PUF	Ring-oscillator PUF for authentication and keys	No stored key in memory	Noise needs error correction
[2]	Side channel	Differential power analysis	Shows key leakage through power	Attack paper; motivates countermeasures
[8]	Fault injection	Fault analysis of cryptographic protocols	Single fault can expose key	Requires precise fault control

© 2026 IJSRET

4.7 Life-Cycle Security Architecture

Because threats arise at every stage, protection must also be applied at every stage. Fig. 2 presents a life-cycle security architecture that combines the reviewed techniques.

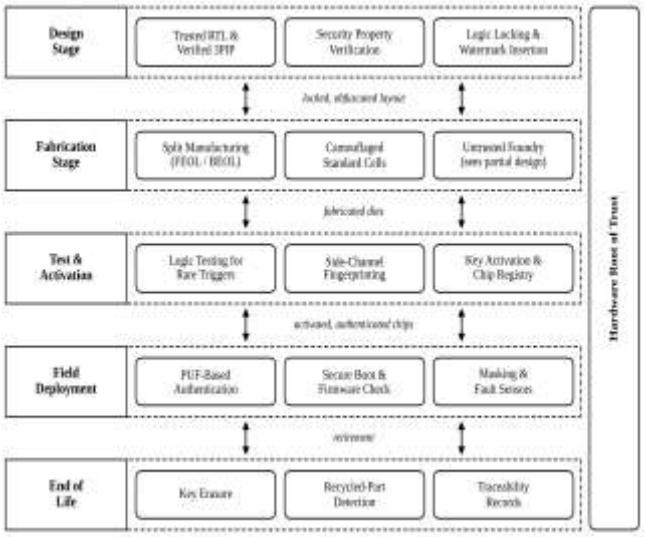


Fig. 2. Life-cycle hardware security architecture mapping countermeasures to each stage of the IC supply chain.

At the **design stage**, trusted RTL and verified third-party IP are combined, security properties are checked with formal and simulation-based verification, and logic locking keys and watermarks are inserted. At the **fabrication stage**, split manufacturing or camouflaged cells may be used so that the untrusted foundry cannot see or understand the complete design [13]. At the **test and activation stage**, the designer or a trusted facility performs Trojan detection with logic testing and side-channel fingerprinting [9], and then unlocks each chip with its key, keeping a record of activated parts to detect overbuilding [10]. At the **deployment stage**, the PUF authenticates the device, secure boot verifies firmware, and the cryptographic cores are protected by masking and fault sensors [2], [15]. Finally, at **end of life**, keys are erased and records allow recycled parts to be recognised [3]. A hardware root of trust spans the whole life cycle and provides the anchor for authentication and key storage.

V. COMPARATIVE ANALYSIS

Table II compares the main countermeasures. Techniques differ in the threat they address, in the stage where they act and in the cost they impose on area, power and design effort.

Table Ii Comparison Of Hardware Security Countermeasures

Technique	Threat Addressed	Life-Cycle Stage	Overhead	Known Weakness
Trojan detection	Malicious insertion	Test	Test time	Process variation masks small Trojans
Logic locking	Piracy, overbuilding	Design to activation	Low–moderate area	SAT and structural attacks [12]
Split manufacturing	Foundry piracy	Fabrication	Trusted BEOL cost	Layout-hint inference [13]
PUF	Cloning, key storage	Deployment	Small area	Noise, modelling attacks
Masking / hiding	Power side channels	Deployment	Area and power	Higher-order attacks
Fault sensors	Fault injection	Deployment	Small area	Limited coverage of attack types
Secure boot	Firmware tampering	Deployment	Boot time	Depends on key protection

VI. CHALLENGES AND FUTURE DIRECTIONS

Several problems remain open. First, the contest between logic locking and attacks continues: since the SAT attack [12], every new scheme has been examined for structural and approximate attacks, and provably secure locking with low overhead is still an aim rather than a result. Second, Trojan detection lacks a universal method, because a well-designed Trojan can be extremely small and well hidden, and the golden reference may itself be unavailable [6]. Third, PUFs must deliver stable responses over temperature, voltage and

© 2026 IJSRET

ageing while resisting machine-learning modelling. Fourth, security verification is expensive and is not yet part of most standard design flows; adding security metrics to electronic design automation tools would help designers measure protection as they do power or timing [1]. Finally, new technologies such as chiplets, 3-D integration and AI accelerators add new interfaces and new attack surfaces. Future work is expected to address these through security-aware design automation, standardised threat models and life-cycle traceability of parts.

VII. CONCLUSION

Hardware is no longer a trusted foundation by default. This review has described how the globalised IC supply chain exposes chips to Trojans, piracy, reverse engineering, counterfeiting, side-channel analysis and fault injection, and how the research community has responded with Trojan detection, logic locking, split manufacturing, physical unclonable functions, side-channel countermeasures and secure boot. The comparison shows that each technique covers only part of the threat space and has known weaknesses. A life-cycle approach, in which protections are layered from design to end of life around a hardware root of trust, is therefore the most practical way to provide confidentiality, integrity and authenticity for VLSI systems.

REFERENCES

1. M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," Proceedings of the IEEE, vol. 102, no. 8, pp. 1283–1295, 2014.
2. P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advances in Cryptology—CRYPTO '99, Lecture Notes in Computer Science, vol. 1666. Berlin, Germany: Springer, 1999, pp. 388–397.
3. U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," Proceedings of the IEEE, vol. 102, no. 8, pp. 1207–1228, 2014.
4. M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," IEEE Design & Test of Computers, vol. 27, no. 1, pp. 10–25, 2010.
5. R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," in Proc. IEEE Int. High Level Design Validation and Test Workshop (HLDVT), 2009, pp. 166–171.
6. S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan attacks: Threat analysis and countermeasures," Proceedings of the IEEE, vol. 102, no. 8, pp. 1229–1247, 2014.
7. R. Torrance and D. James, "The state-of-the-art in IC reverse engineering," in Cryptographic Hardware and Embedded Systems—CHES 2009, Lecture Notes in Computer Science, vol. 5747. Berlin, Germany: Springer, 2009, pp. 363–381.
8. D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in Advances in Cryptology—EUROCRYPT '97, Lecture Notes in Computer Science, vol. 1233. Berlin, Germany: Springer, 1997, pp. 37–51.
9. D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in Proc. IEEE Symp. Security and Privacy (SP), 2007, pp. 296–310.
10. J. A. Roy, F. Koushanfar, and I. L. Markov, "EPIC: Ending piracy of integrated circuits," in Proc. Design, Automation and Test in Europe (DATE), 2008, pp. 1069–1074.
11. J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Security analysis of logic obfuscation," in Proc. 49th ACM/EDAC/IEEE Design Automation Conf. (DAC), 2012, pp. 83–89.
12. P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in Proc. IEEE Int. Symp. Hardware Oriented Security and Trust (HOST), 2015, pp. 137–143.
13. J. Rajendran, O. Sinanoglu, and R. Karri, "Is split manufacturing secure?" in Proc. Design, Automation and Test in Europe (DATE), 2013, pp. 1259–1264.
14. B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in Proc. 9th ACM Conf. Computer and Communications Security (CCS), 2002, pp. 148–160.
15. G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in Proc. 44th ACM/IEEE Design Automation Conf. (DAC), 2007, pp. 9–14.
16. National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, 2001.

© 2026 IJSRET