National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Privacy and Piracy Issues in Hardware

A Whitepaper

Contributors

Vijaypal Singh Rathor,
Department of Information Technology

ABV-Indian Institute of Information
Technology and Management, Gwalior,
India

Table of CONTENTS

I Introduction 4

II Anatomy of Piracy 6

III Threat Landscape 9

IV Mitigating Privacy Piracy Issues for Hardware 13

V Logic Locking in Privacy/ Piracy Mitigation 16

VI Use Cases of the methods and Technologies that can Help the Industry to itigate the IP Theft 20

VII Industry Perspective 24

VIII Conclusion 26

I

Introduction

Privacy and piracy issues in hardware or Integrated Circuits (ICs) are growing concerns in the digital era[1]. As technology advances, ICs are increasingly integrated into everyday devices, from smartphones to smart appliances, raising significant privacy and security concerns. One major privacy issue is the potential misuse of data gathered through these devices. Modern ICs often come with the capability to collect and process a wide range of data, which, if not adequately protected, could be accessed or shared without the user's consent[2]. Such risks necessitate robust encryption and security protocols to safeguard user information.

Piracy, on the other hand, refers to the illegal reproduction or cloning of hardware or intellectual property (IP) rights, including ICs[1]. This issue undermines IP rights and poses a substantial threat to the semiconductor industry. Cloned ICs, often produced at a lower quality, can infiltrate the supply chain and cause serious reliability and safety concerns. This piracy is driven by economic incentives and the relatively high cost of original and authenticated hardware. Additionally, the electronic industry loses billions of dollars annually due to IP infringements or IP piracy[3-4].

Both privacy and piracy in hardware highlight the importance of implementing secure design practices and effective legislation[2], [5]. As more critical functions depend on integrated circuits, protecting privacy and preventing piracy becomes essential to ensure both consumer trust and the integrity of technological advancements.

Major Concerns Due to Privacy and Piracy Issues in Hardware

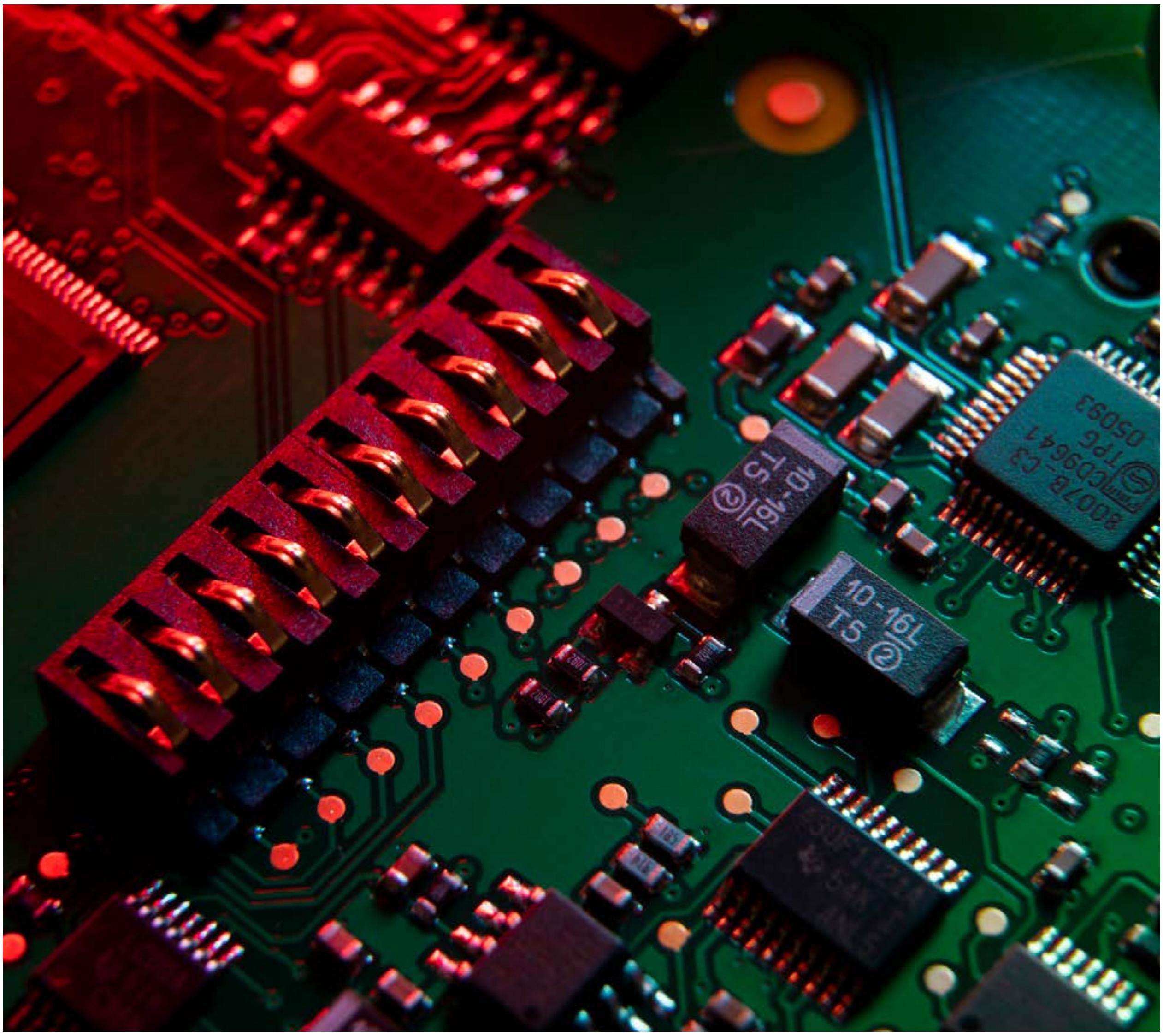
Privacy and piracy have become central concerns in the hardware industry as technology advances. These issues involve several concerns, such as ethical, legal, and technical, that impact both producers and consumers. An overview of these concerns is given below:

- **Information or Data Security:** Devices with integrated circuits collect sensitive information, such as personal preferences and biometric data. A breach in privacy can lead to data leaks, misuse of personal information, or unauthorized surveillance, which ultimately impacts consumer trust. Further, hardware vulnerabilities (such as power or timing analysis) can be exploited or used by hardware Trojans to extract sensitive information like cryptographic keys.

- **Unauthorized Cloning/IP Infringements:** Piracy issues are equally important, especially in the hardware and IC domain. Unauthorized cloning and counterfeiting of integrated circuits have become widespread, mainly due to the expensive nature of authentic components. This creates a direct threat to the profits and intellectual property rights of original manufacturers.

- **Counterfeiting:** Pirated or cloned hardware can contain malicious components or inferior materials, leading to privacy breaches or security vulnerabilities. Moreover, combating piracy requires substantial investment in developing anti-counterfeiting technologies, such as unique identifiers, secure hardware designs, and supply chain tracking mechanisms.

Privacy and piracy issues in hardware present challenges that require a balance between user rights, security, and innovation. These issues highlight the importance of ensuring hardware integrity, secure firmware updates, and proper encryption mechanisms to safeguard against privacy invasions and piracy.



Anatomy of Piracy

Piracy in the context of hardware involves unauthorized replication, distribution, or modification of physical devices, software embedded in hardware, or proprietary designs. It typically starts with reverse engineering, where attackers or counterfeiters analyze the components and functionality of hardware to replicate or modify it without permission. These pirated copies often lack the quality or security of the original, posing risks to users. Piracy can infiltrate the supply chain, affecting industries like consumer electronics, medical devices, and industrial equipment, leading to financial losses, IP theft, and safety concerns.

Origin of Piracy

The origin of threats for hardware piracy comes from various stages of the hardware development, manufacturing, and distribution lifecycle, as shown in Figure 1[6].

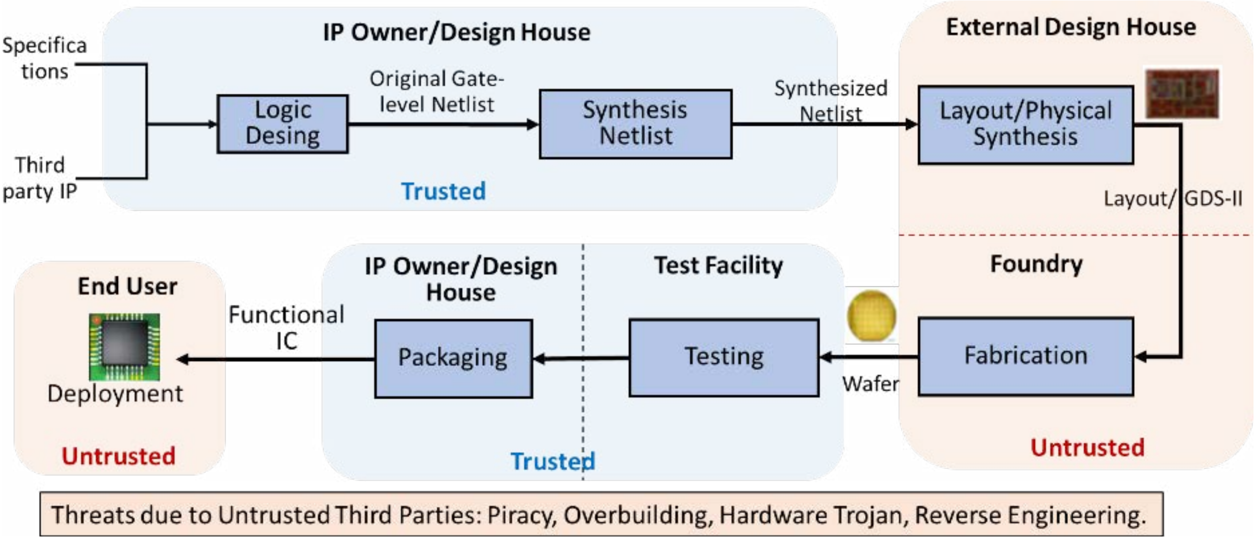


Figure 1. The overview of IC Development stages. The untrusted stages pose threats of piracy overbuilding hardware Trojan and reverse engineering, which causes security and privacy issues in hardware devices.

Hardware piracy involves illegal replication, reverse engineering, modification, or unauthorized use of integrated circuits (ICs) and other hardware components[6], [8]. Below are the primary sources of such threats:

a) Untrusted Third-Party Foundries and Manufacturers

- IC design companies often outsource the manufacturing of chips to third-party foundries due to cost-effectiveness. If these foundries are untrusted, they can potentially overproduce the chips (lead to piracy), sell unauthorized copies, or insert malicious modifications called hardware Trojans.

b) Design Houses and IP Vendors

- Hardware designs typically incorporate Intellectual Property (IP) cores from multiple vendors. An untrusted design house or IP vendor may misappropriate these IP cores, either selling them illegally or sharing them with unauthorized third parties. The lack of proper digital rights management (DRM) and ineffective licensing models can make IP piracy easier, leading to cloned or compromised hardware designs.

c) Unauthorized Reverse Engineering

- Attackers can acquire legitimate hardware from the open market also and reverse engineer it to understand its design and manufacture counterfeit copies. The reverse engineering process can allow attackers to produce replicas or modify the original hardware to include malicious features like hardware Trojans.

Common Methods of Piracy

Hardware piracy refers to illegal reproduction, distribution, or unauthorized use of hardware components or their designs. The most common methods of hardware piracy include:

a) **Reverse Engineering:** Attackers acquire and disassemble legitimate hardware products to understand their operation, circuit design, and functionality. They use this knowledge to make clones or unauthorized copies. Integrated circuits (ICs) often use third-party vendors' Intellectual Property (IP) cores. IP core theft occurs when these design modules are illegally reused or incorporated into new designs without proper licensing or authorization. Companies or individuals may integrate IP cores into their products without paying royalties or obtaining permission, resulting in revenue loss for IP vendors.

b) **Overproduction:** Semiconductor companies often outsource the manufacturing of ICs to third-party foundries. An untrusted foundry may produce more chips than authorized (overproduction) and sell them on the market, often without the owner's knowledge. These excess chips can be identical to the original ones, making distinguishing between authentic and pirated versions difficult.

c) **Counterfeiting:** Counterfeiters create replicas of legitimate hardware components without authorization, using lower-quality materials to mimic the original product. Lower-grade or used components are re-labeled to appear as high-quality or original parts and sold at a premium. These counterfeit components can compromise the reliability and security of the final device.

d) **Hardware Trojan Insertion:** During manufacturing, attackers can modify the hardware to introduce vulnerabilities, such as hardware Trojans. These modifications allow the attackers to alter the behavior of the device or compromise its integrity. A malicious modification may include backdoors that can be used to bypass security features and gain unauthorized access to sensitive data, undermining both privacy and security.

e) **Recycling and Rebranding:** Used electronic components are often harvested from discarded devices and reintroduced into the supply chain as new products. They are typically re-branded to mislead customers into believing they are purchasing new and authentic parts. Refurbished products may be sold as original without any indication that they are recycled, which may involve changing part numbers or making visual modifications to the hardware.

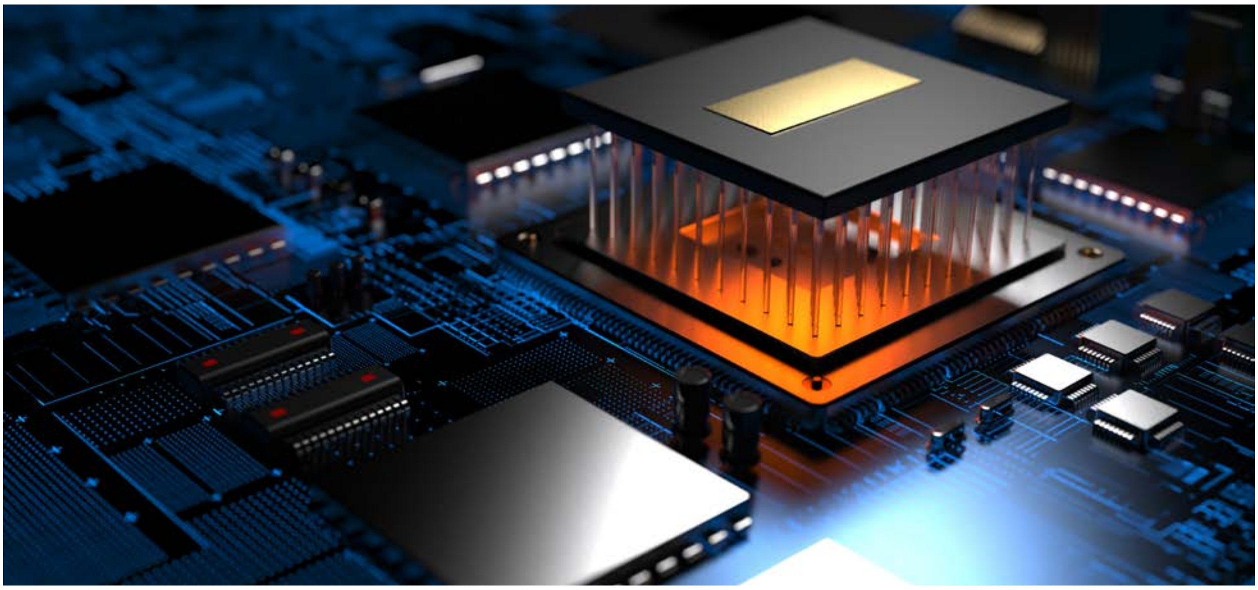
f) **Third-Party Assembly Abuse:** At the assembly stage, unauthorized parties may introduce cloned or counterfeit components into the device. Since the assembly process is often outsourced, such vulnerabilities can be easily exploited. Third-party assembly entities may replace authentic components with lower-grade alternatives, affecting the final product's quality, performance, and safety.

Legal Scenario in India

- The Copyright Act of 1957 serves as the main legislation for protecting intellectual property against piracy. However, with the rapid technological advancements, its provisions were insufficient to address online copyright infringement. Consequently, the Act was amended in 2012 to include various forms of digital piracy under its scope.

- One key provision for combating digital piracy is Section 65A of the Copyright Act, which focuses on the "Protection of technological measures." It aims to prevent individuals from using or uploading pirated content online. The section specifies that anyone who circumvents a technological measure designed to protect rights under the Act shall face up to two years of imprisonment and be liable to fines.

- Additionally, the Information Technology Act of 2000 addresses digital piracy. Section 66 of this Act imposes penalties of up to three years of imprisonment and fines up to Rs 2 lakhs for the illegal online distribution of copyrighted content.



III

Threat Landscape

Major Threats Related to Privacy and Piracy

The threat related to hardware piracy and privacy involves a wide range of attack vectors and risks that can compromise the physical hardware components and the sensitive data they handle. The following outlines the prominent threats:

a) Cloning and Counterfeiting

- **Hardware Cloning:** Attackers create unauthorized copies of original hardware using reverse engineering or unauthorized access to the design. Cloned hardware can pose privacy risks, as it may include malicious components that compromise data integrity.

- **Counterfeit Hardware:** Counterfeiters introduce fake or substandard components into the supply chain, posing risks of malfunction, security vulnerabilities, and privacy breaches. Unsuspecting users may install counterfeit devices with embedded eavesdropping capabilities, allowing attackers to intercept sensitive communications.

b) Reverse Engineering

- Attackers may reverse engineer an integrated circuit (IC) to understand its functionality and replicate the design. This can lead to unauthorized clones, undermining the value of proprietary technologies.

- Reverse engineering can also expose security vulnerabilities, such as encryption keys or proprietary algorithms, which may be used for further attacks compromising user privacy.

c) Intellectual Property (IP) Theft

- **IP Piracy** involves stealing IP cores or design modules used in hardware development. This results in a loss of competitive advantage and revenue for the original designers.

- Unauthorized use of stolen IP can also compromise the privacy and integrity of the hardware, as these stolen designs may be altered to include vulnerabilities.

d) Tampering and Hardware Trojans

- **Tampering** involves the intentional modification of hardware, often by inserting a malicious component or Trojan.
- **Hardware Trojans (malicious inclusion)** may be inserted during the manufacturing process to create backdoors, allowing attackers to exfiltrate sensitive information or execute malicious actions when specific conditions are met. Since the supply chain for hardware components is long and involves multiple intermediaries, an adversary may insert unauthorized components to leak sensitive data, creating significant privacy risks.

e) Unauthorized Overproduction

- **In overproduction**, an untrusted foundry produces extra chips without authorization and sells them in the market. This undermines intellectual property protections and often leads to unauthorized and potentially malicious hardware being integrated into systems.
- These unauthorized components might include subtle modifications that can be used to compromise privacy or launch attacks on systems.

f) Side-Channel Attacks on Pirated Devices

- Hardware components that have been cloned or compromised may be more vulnerable to side-channel attacks, which exploit physical leakage such as power consumption, electromagnetic radiation, or timing information to infer sensitive data.
- Side-channel attacks pose significant risks to privacy, particularly in cryptographic hardware implementations.

g) Third-Party IP Integration and Trust Issues

- Modern hardware systems are built using third-party IP cores. The IP may contain hidden vulnerabilities or backdoors if it is from an untrusted source.
- Such third-party integrations may lead to privacy risks if they contain malicious functionalities intended to siphon off sensitive information.

Hardware Trojan

Hardware Trojans are malicious modifications or additions to integrated circuits (ICs) or hardware components. Hardware Trojans can remain inactive for long periods, activated only under specific conditions, making them difficult to detect during standard testing[6-7]. This stealthiness poses long-term risks, as the Trojan can compromise system security at a critical moment, and it cause significant impact and losses:

Impact of Hardware Trojans on Security and Privacy:

1. Backdoor Access and Data Leakage

- Hardware Trojans can create backdoor access, allowing attackers to bypass security mechanisms.

- Sensitive information can be extracted without detection, compromising confidentiality and privacy. Trojans can be used to eavesdrop on communications or track user activity, leading to severe privacy violations. They can also silently leak personal data such as biometric information or financial records.

2. System Disruption and Denial of Service

- Trojans may include logic to disrupt operations at specific times or under specific conditions, resulting in system malfunctions or denial of service (DoS).

- This can affect critical infrastructures, leading to significant safety and privacy concerns.

3. Privilege Escalation and Control

- Attackers may use Trojans to escalate privileges in a system, giving unauthorized control over devices or networks.

- Such capabilities can lead to complete control of affected systems, compromising user privacy and enabling unauthorized data modification.

4. Impact on Trustworthiness of Supply Chain

- The presence of hardware Trojans is often linked to vulnerabilities in the supply chain. If third-party suppliers introduce malicious changes during the manufacturing process, it can compromise the security of the entire system.

- This raises concerns regarding the integrity and trustworthiness of hardware components, especially those used in sensitive or critical infrastructure.

Possible Losses or Impact on Electronic Industries

Privacy and piracy issues in hardware can cause significant financial, operational, and reputational losses across various industries. These losses stem from data breaches, intellectual property theft, regulatory penalties, and loss of consumer trust[5-9]. Below are the potential impacts of privacy and piracy issues in hardware on industries:

a) Financial Losses:

- Companies may face direct financial losses due to compromised hardware or pirated products. Pirated copies of hardware-based products (e.g., gaming consoles or specialized equipment) can result in lost sales.

b) Intellectual Property (IP) Theft

- One of the most significant losses to industries comes from the theft of intellectual property (IP), particularly in sectors that rely on proprietary hardware technologies like semiconductors, telecoms, and consumer electronics. Hardware piracy can involve the reverse engineering of products, creating counterfeit or pirated versions. The counterfeit chip industry causes billions of dollars in losses annually for manufacturers of semiconductors, as counterfeit components can easily infiltrate supply chains.

c) Reputational Damage

- Privacy violations due to hardware flaws, like insecure IoT devices, compromised processors, or tampered components, can significantly impact a company's reputation. Consumers may lose trust in the brand and switch to competitors. For example, Apple faced consumer backlash after the FaceTime eavesdropping bug allowed unauthorized listening through their hardware, impacting customer trust in Apple's security protocols.

d) Operational Disruptions

- If privacy or security vulnerabilities are discovered in hardware post-deployment, companies may be forced to issue product recalls, replace compromised components, or update firmware. These actions are costly and disruptive. For example, Intel's response to Spectre and Meltdown vulnerabilities involved releasing firmware patches that caused significant performance degradation in some hardware, impacting both consumers and Intel's reputation.

e) Regulatory and Compliance Costs

- Companies that fail to secure their hardware and suffer repeated privacy violations may face increased scrutiny from regulators, leading to ongoing audits, reporting requirements, and compliance obligations.

f) Consumer and B2B Market Losses

- A privacy violation involving hardware, such as a compromised smartphone, wearable, or home IoT device, may lead to a large-scale loss of consumer confidence. This can directly reduce sales as customers seek out more secure alternatives. For example, privacy issues with Google Nest cameras raised concerns about home security and led some users to seek alternative products.

g) National Security Risks:

- Privacy or piracy issues in hardware can lead to government bans on specific products or technologies, as seen with various companies in the defense and telecommunications sectors.

h) Industry-Specific Examples of Losses:

- **Healthcare:** Compromised medical devices or diagnostic equipment can expose patient data, resulting in HIPAA violations and expensive lawsuits. Financial losses due to device recall and remediation of privacy vulnerabilities in hospital equipment.

- **Financial Services:** Hardware breaches in ATMs, point-of-sale (POS) systems, or mobile banking devices can expose sensitive financial data, leading to massive fraud losses and regulatory fines. Significant investment in cybersecurity infrastructure following an attack on hardware systems.

- **Telecommunications:** Losses due to compromised network hardware, such as routers or base stations, which can allow attackers to spy on communication or cause widespread outages. Legal and financial consequences if governments ban compromised telecom equipment suppliers.

- **Manufacturing and Industrial Control Systems:** Hardware piracy in industrial sectors can result in stolen designs for equipment, machinery, or tools, leading to unfair competition and loss of proprietary technology.

- **Consumer Electronics:** The flood of counterfeit smartphones, gaming consoles, and wearables leads to substantial revenue losses and damage to brand reputation. Increased costs associated with firmware updates and hardware recalls to patch privacy vulnerabilities.

IV

Mitigating Privacy Piracy Issues for Hardware

Mitigating hardware piracy and ensuring privacy protection requires a combination of technological, procedural, and policy-based approaches to safeguard hardware components and designs from unauthorized copying, tampering, and privacy violations. There are different approaches to mitigate privacy and piracy issues in the hardware[5-6], [9-10]. Below are some effective methods for mitigating privacy and piracy issues in hardware.

Hardware Obfuscation

- **Logic Obfuscation:** Add extra dummy logic, gates, or misleading signals that make it challenging for attackers to reverse-engineer the hardware design. This helps prevent cloning and IP theft and protect the IP.
- **Circuit Camouflaging:** Make the circuit layout look different from its true design, making it difficult for an attacker to determine the actual functionality of individual components, thus complicating the reverse-engineering process.
- **Logic Locking:** Lock or encrypt the design functionality by inserting secret keys into the design. The design functions correctly only when the correct key is applied; otherwise, it provides an incorrect function.

Other Approaches to Mitigate the Privacy and Piracy Issues in Hardware

a) **Hardware Watermarking:** Embed a unique identifier within the hardware design to prove ownership. This identifier is invisible during normal operations but can be revealed under specific testing conditions.

b) **Fingerprinting:** Insert unique features or patterns in each IC, making every copy slightly different. Fingerprinting helps track individual devices and trace their origin if piracy is suspected.

c) **Physical Unclonable Functions (PUFs):** Use PUFs to create a unique signature for each chip, based on inherent variations in the manufacturing process. PUFs serve as a hardware "fingerprint" that is difficult to replicate and can be used to authenticate genuine devices.

d) **Anti-Counterfeiting:** PUFs can be used to differentiate between authentic and counterfeit hardware components during production and in the supply chain.

c) **Blockchain for Anti-Piracy:** Utilize blockchain to establish a secure and immutable record of hardware components' origins and transactions, enhancing the ability to trace the authenticity of components and combat piracy.

d) **Side-Channel Attack Mitigation:** Introduce random noise to make side-channel information, such as power consumption or electromagnetic emissions, more challenging to analyze and exploit. Randomize the order of execution or timing of critical operations to thwart attackers attempting to exploit side-channel leaks for reverse engineering or data extraction.

Hardware Trojan Detection and Prevention

Hardware Trojan detection performs thorough testing, including side-channel analysis and functional testing, to detect anomalies that may indicate hardware Trojans or malicious modifications. To prevent hardware Trojan insertion, Design-for-Trust (DfT) approaches, such as logic locking, IC camouflaging, run time monitoring, etc. approach, can be incorporated into hardware during the design phase[6-7], [9-10]. There are different methods for the detection and mitigation of the Trojan issue in hardware.

a) Detection Methods:

- **Functional/ Logic Testing:** Involves applying a wide range of input vectors to test a circuit's functionality. Formal verification is used to compare the expected logical behavior of the chip against its actual performance. If there are discrepancies or deviations in expected output, it could indicate a Trojan. However, Trojans that remain dormant under regular operation are difficult to detect this way.

- **Side-Channel Analysis:** Insertion of Trojan releases or imposes variations on various physical parameters such as power, Electromagnetic radiation, timing, etc. Therefore, monitoring these parameters during processing facilitates the detection of hardware Trojan. Hardware Trojans often affect the power signature, even when inactive.

- **Machine Learning (ML) Techniques:** ML models can be trained to detect abnormal patterns in power, timing, or other side-channel measurements, improving detection accuracy for stealthy Trojans.

- **Design-for-Trust (DfT) Techniques:** Embedding security mechanisms in the hardware during design (e.g., logic locking) can help detect and prevent unauthorized modifications later in the production process.

b) Mitigation Methods:

- **Design-Time Countermeasures:**

  o **Obfuscation:** Obfuscates critical parts of the hardware design so that an attacker cannot easily understand or modify the circuit. This makes reverse engineering, and thus Trojan insertion, more difficult.

    - **Logic Locking:** Locks certain parts of the circuit with a secret key that is only known at the final stages of manufacturing. If the key is incorrect (as in the case of a tampered chip), the circuit behaves incorrectly or becomes inoperable.

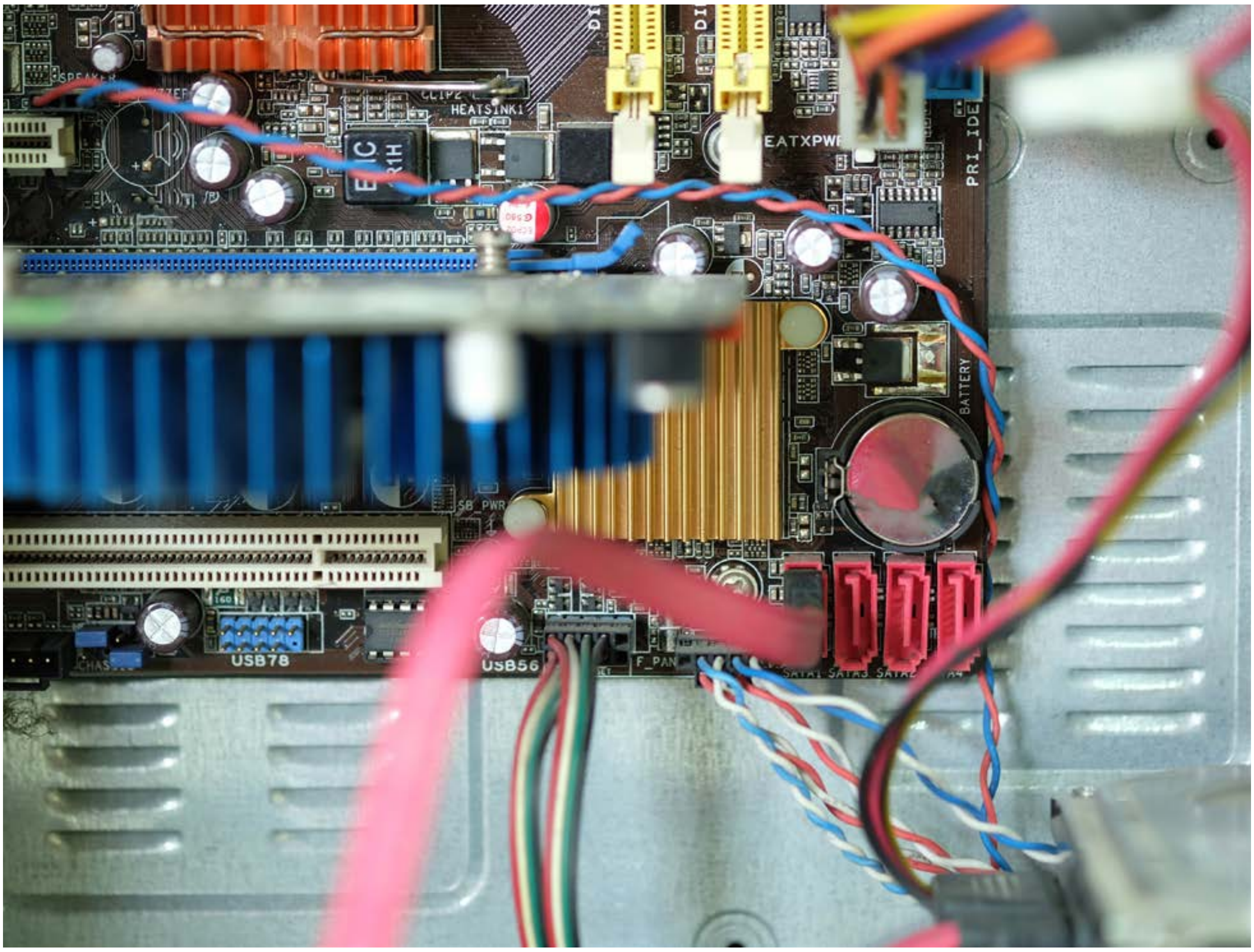
    - **IC Camouflaging:** Masks the design of the integrated circuit by making certain gates look alike but perform different functions, making it extremely difficult for attackers to modify or insert a Trojan during reverse engineering.

- **Run-Time Monitoring:** Implements real-time monitoring of the hardware to detect suspicious behavior, such as unauthorized changes in power usage, timing, or functionality.

- **Trusted Foundries:** Using trusted manufacturing facilities that follow strict security protocols reduces the risk of hardware Trojans being introduced during fabrication. This is often necessary for defense and sensitive sectors.

- **Post-Manufacture Testing and Inspection:** Conduct extensive testing of each chip post-manufacture, including functional, power, and timing analysis, to catch any potential Trojans that may have been inserted during production.

In summary, hardware Trojan detection and mitigation require a multi-faceted approach involving both pre-fabrication design techniques and post-manufacturing inspection. Combining these methods helps ensure that hardware is secure from tampering and malicious modifications. In the above-discussed techniques, logic locking is the most effective and emerged as a prominent method to address the piracy and privacy issues in hardware. The next section discusses the different types of logic locking methods mitigating piracy and privacy issues in hardware.



Logic Locking in Privacy/ Piracy Mitigation

Logic locking mitigates security threats by introducing an additional circuitry that requires a secret key for correct operation. This makes reverse engineering or unauthorized use of an integrated circuit difficult, as the correct functionality of the chip is hidden unless the key is provided. Logic locking helps prevent IP theft, overproduction, and tampering by ensuring that any attempts to replicate or modify the circuit without knowledge of the key will result in an unusable or malfunctioning product. It also thwarts attacks by obfuscating critical parts of the design, complicating reverse engineering and piracy, as shown below in Figure 2.

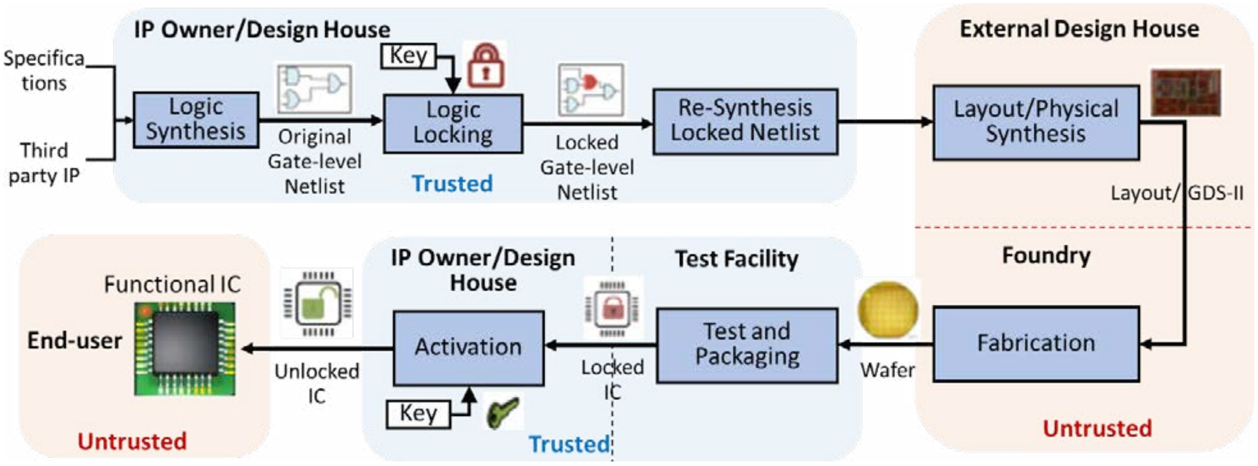


Figure. 2. Employing Logic locking in the development of the IC lifecycle

This section discusses the challenges and current trends in logic locking[8], [11].

Challenges

Logic locking is a technique used in integrated circuits (ICs) to protect against hardware security threats such as reverse engineering, overbuilding, and intellectual property (IP) piracy. However, it presents several challenges, which can be divided into technical, security, and practical implementation aspects:

a) **Key Security:** The security of the logic locking mainly depends on the secrecy of the key. If the key is compromised, the protection is rendered ineffective. Ensuring the key used for logic locking remains secret is a major challenge.

b) **Attack and Evolving Threats Resilience:** As security mechanisms are developed, attackers continually find new methods to break or circumvent them. There are various attacks that can compromise the security of logic locking and pose significant challenges to logic looking.

- **SAT Attacks (Boolean Satisfiability):** Modern logic locking schemes are vulnerable to SAT-based attacks, which can reveal the correct key by evaluating the circuit with a limited number of queries.

- **Removal Attacks:** Attackers may attempt to remove or bypass the locking mechanism, such as by identifying and eliminating the logic gates associated with the locking process.

- **Approximate Attacks:** Attackers may try to unlock the circuit by finding an approximate key that allows the IC to function reasonably well, even if it's not the exact correct key.

a) **Performance Overhead:** Logic locking often introduces additional hardware elements, which can increase the area of the chip, its power consumption, and delay performance. N

b) **Scalability and Compatibility:** Logic locking needs to be compatible with existing IC design flows, which can be difficult if the locking technique significantly alters the structure of the circuit. As circuits become more complex, the locking scheme must scale without introducing excessive overhead or vulnerability.

Addressing these challenges requires balancing security, performance, and practicality in deploying logic locking in ICs. The next subsection presents the current trends in logic locking.

Current Trends

Current trends in logic locking reflect the focus on enhancing security, resilience, and efficiency to mitigate attacks like SAT (Satisfiability) attacks, removal attacks, and machine learning-based reverse engineering[11-14]. Here are the prominent trends in logic locking:

a) SAT-Resilient Logic Locking

- **Development of SAT-resistant Techniques:** A significant trend in logic locking is the development of techniques specifically designed to resist SAT attacks. Methods like SARLock[15] and Anti-SAT[16] have been created to exponentially increase the complexity of solving for the correct key using SAT solvers. By adding specialized logic blocks that make finding the correct key highly complex, these techniques improve resilience against algorithmic attacks.

- **Hybrid Techniques:** Combining conventional XOR-based logic locking with SAT- resistant modules has become popular[17]. This approach leverages the ease of implementing XOR gates along with advanced modules designed to thwart SAT attacks, enhancing both efficiency and security.

- **Provably Secure Logic Locking:** Stripped Functionality Logic Locking (SFLL) is designed to strip some of the circuit's original functionality and lock it, requiring a key to recover this functionality[18]. The main advantage of SFLL is that it provides provable security against several classes of attacks, such as SAT, signal-based analysis, and removal attacks[13]. The focus on provable security addresses the need for clear, demonstrable guarantees of robustness.

b) Machine Learning-Resilient Logic Locking

- **Defense Against ML Attacks:** With the increased use of machine learning (ML) in reverse engineering, new logic locking techniques are being developed to resist ML-based attacks. These methods add randomness or obfuscation patterns that confuse ML models trying to learn the locked circuit's behavior[19].

- **Adversarial Machine Learning:** Researchers are incorporating adversarial learning techniques to generate obfuscation patterns that specifically exploit the weaknesses of ML models. By doing so, they create designs that are inherently misleading to AI-driven attacks, thus improving resilience against automated attacks.

c) Logic Locking with Physical Unclonable Functions (PUFs)

- **Integration with PUFs:** PUFs are increasingly being integrated with logic locking schemes to generate and store keys securely[20]. The PUF-based keys are unique for each device, and even minor physical variations between chips result in different keys, providing a hardware-rooted level of security.

- **Device-Specific Locking:** By combining logic locking with PUFs, the locking mechanism is made unique to each individual device, making it nearly impossible for attackers to use the key from one chip to unlock another.

d) Lightweight Logic Locking for Resource-Constrained Devices

- **Locking for IoT Devices:** Logic locking is being adapted for resource-constrained devices like IoT nodes and embedded systems. The emphasis is on lightweight locking schemes that require minimal area and processing power, making it feasible to protect even low-cost hardware from piracy.

- **Optimized Key Lengths:** Shorter key lengths and optimized key management are being explored to reduce the computational burden while still maintaining an adequate level of security. This trend addresses the balance between security requirements and the limited capabilities of small devices.

e) Logic Locking for Hardware Lifecycle Protection

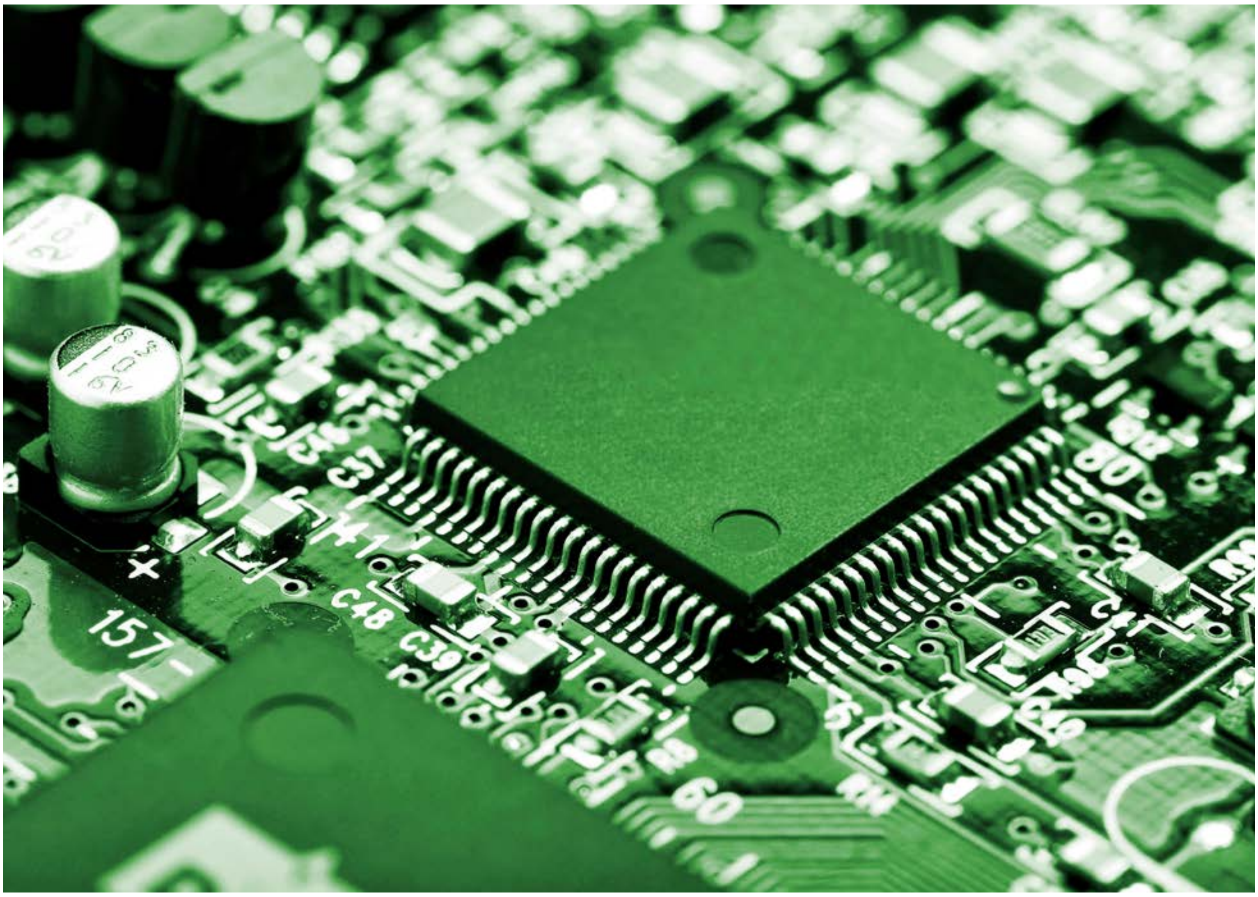
- **End-to-end Hardware Security:** Logic locking is being used not just for manufacturing security but for ensuring end-to-end hardware lifecycle protection. The key is used to unlock the IC only at certain supply chain stages, thereby protecting against overproduction and unauthorized use.

- **Controlled Activation:** A trend is the use of logic locking to implement controlled activation, where the chip is fully functional only after passing through specific verification steps. This prevents foundries from overproducing or selling unauthorized copies.

f) Logic Locking for Emerging Computing Paradigms

- **Quantum-Resilient Locking:** With the advent of quantum computing, there is an increasing focus on designing logic locking mechanisms that are secure against quantum attacks. Quantum-resilient encryption methods, such as lattice-based cryptography, are being integrated with logic locking.
- **Approximate and Neuromorphic Computing:** For approximate computing and neuromorphic Architecture, new types of locks are being designed that leverage the non-deterministic behavior of these systems to obfuscate functionality and resist attacks. This approach is particularly useful in locking hardware that does not have a fixed deterministic output.

The current trends in logic locking reflect a broad focus on enhancing security to counteract evolving threats. Techniques are being developed to counter SAT attacks, ML-based attacks, and quantum computing threats while focusing on resource efficiency for constrained devices. Dynamic, PUF-based, and hierarchical locking mechanisms are improving the adaptability and resilience of logic locking schemes, while new tools and technologies like AI are contributing to more sophisticated and robust designs. These advancements ensure that logic locking remains an effective method for safeguarding hardware IP and maintaining security throughout the supply chain and device lifecycle.



VI

Use Cases of the methods and Technologies that can Help the Industry to itigate the IP Theft

Mitigating Intellectual Property (IP) theft in hardware design and development is crucial for safeguarding proprietary technology and preventing unauthorized exploitation[6]. Here are some use cases of methods and technologies employed to mitigate IP theft:

a) Watermarking in IP Cores

- **Use Case:** A company designing a custom hardware module (e.g., a Digital Signal Processor or DSP) embeds a digital watermark into its HDL (Hardware Description Language) code.
- **How It Helps:** The watermark can be used as a unique identifier that is invisible in standard usage but can be detected if unauthorized use or replication of the IP occurs. This enables the rightful owner to prove ownership in the event of IP infringement.

b) IP Fingerprinting for Traceability

- **Use Case:** A designer embeds fingerprints into each IP core that contains unique information about the licensee and the origin.
- **How It Helps:** If unauthorized use or replication of the IP is suspected, the fingerprint can be used to trace the source, providing a means to prove ownership and detect license violations.

c) Physical Unclonable Functions (PUFs) for Device Authentication

- **Use Case:** A semiconductor manufacturer integrates PUFs into its chips, generating a unique signature for each device during fabrication.
- **How It Helps:** These unique hardware fingerprints help authenticate genuine devices, preventing attackers from creating counterfeit copies of a company's IP. The authentication process ensures that only legitimate hardware containing authorized IP is used in the supply chain.

d) Secure Supply Chain Verification with Blockchain

- **Use Case:** An IoT device company uses a blockchain-based system to track its hardware IP components throughout the supply chain.
- **How It Helps:** Blockchain provides immutable records that prove authenticity, tracking ownership and changes in custody. This ensures that unauthorized entities cannot add counterfeit components or use genuine IP in unapproved products, reducing the risk of IP theft during production and transit.

e) Logic Locking/Encryption

- **Use Case:** A consumer electronics manufacturer uses logic locking/encryption to protect its designs or IP functionality from being cloned and from unauthorized copying/disclosure. The company ships partially functional hardware that requires a secret key to unlock full functionality.
- **How It Helps:** The logic locking/encryption mechanism requires a key provided by the IP owner to unlock/decipher correct functionality. Without the correct key, any attempts to reverse engineer or clone/copy the hardware would produce non-functional copies, thus preventing IP theft or misuse of IP and providing security for both the manufacturer and the third-party IP vendor.

These cases demonstrate that mitigating IP theft requires a combination of hardware and software- level protection, secure supply chain practices, and the use of encryption and authentication methods. Techniques like logic locking, PUFs, blockchain, and secure boot all contribute to a more secure environment that can effectively protect against unauthorized copying, tampering, and exploitation of intellectual property in hardware designs.

Logic Locking Approaches to Mitigate IP Theft:

Below are some of the common logic-locking methods used to mitigate hardware piracy and enhance privacy:

a) XOR-Based Logic Locking

- **XOR Gates Integration:** XOR gates are inserted at strategic points in the circuit, requiring a correct key input to produce the desired output[17], [21]. If the wrong key is provided, the circuit produces incorrect results.
- **Key Bit Randomization:** The location of XOR gates and key bits is randomized to maximize the difficulty of determining the correct key through reverse engineering.
- **Challenges:** Basic XOR-based logic locking is vulnerable to satisfiability (SAT) attacks, which can determine the correct key by analyzing the circuit.

b) MUX-Based Logic Locking

- **Multiplexer-Based Integration:** Multiplexers (MUXes) are added to the circuit with one of the inputs connected to the key[21]. The MUX ensures that the correct path is taken only if the correct key is supplied.

- **Obfuscation Through Multiple Paths:** The introduction of MUXes creates multiple possible paths for signal propagation, and only the correct key allows the correct path, increasing the complexity of reverse engineering.

c) Key-Gate or Dummy Logic Insertion

- **Gate-Level Key Integration:** Additional gates are inserted into the circuit, which can only be unlocked using a secret key. The key-controlled gates disrupt the logic functionality if an incorrect key is used[9], [10].

- **Insertion of Dummy Gates:** Dummy signals and gates are used to mislead reverse engineering tools, providing incorrect functionality or hiding the real logic dependencies of the circuit. Therefore, dummy gates that do not contribute to the primary logic are inserted into the circuit. These gates are controlled by parts of the key and are meant to mislead attackers.

d) LUT-Based Logic Locking (Look-Up Table)

- **Use of LUTs:** In this method, some functional blocks of the design are replaced with programmable look-up tables (LUTs)[23]. The LUTs are configured using a secret key, allowing the design to function correctly only with the correct key.

- **Reconfigurable Logic:** The use of LUTs[22] provides flexibility, as they can be reprogrammed, making it more challenging for attackers to understand the true function of the locked design.

e) SAT-Attack Resistant Locking

- **SARLock (SAT-Attack Resistant Logic Locking):** SARLock[15] aims to prevent SAT- based attacks by modifying the logic in such a way that every wrong key leads to incorrect outputs, but only a small subset of key bits can be inferred at a time. This significantly increases the computational complexity for an attacker using SAT solvers to determine the correct key.

- **Anti-SAT Block and Strong Ant-SAT:** An Anti-SAT[16], Strong Anti-SAT[24] block is a specific circuit added to increase the difficulty of key recovery using SAT attacks by exponentially increasing the number of iterations required to find the key.

- **Probably Secure Logic Locking:** Stripped Functionality Logic Locking (SFLL) [18] method strips a portion of the circuit's functionality and locks it using a key. The stripped functionality is restored only when the correct key is provided. SFLL is designed to be secure against different types of attacks, such as SAT and removal attacks.

- **Input Dependent Key-based Logic Locking (IDKLL):** IDKLL-based gate replacement method called GateLock [25] locks the design functionality by replacing the original gates with IDKLL-based locked gates. IDKLL-based locked gates exhibit multiple key sequences as valid keys to unlock the design functionality for all input. In IDKLL-based methods, due to the use of multiple key sequences as valid, it completely mitigates the threat of SAT attack.

Benefits of Logic Locking to Mitigate Various Threats

- **Protection Against Cloning and IP Theft:** Logic locking helps ensure that even if an attacker gains access to a hardware design, they cannot replicate its functionality without the correct key, preventing cloning.
- **Prevention of Reverse Engineering:** Logic locking deters reverse engineering attempts by making the circuit functionally incorrect without the key.
- **Hardware Trojan Mitigation:** Logic locking can prevent unauthorized modifications, such as hardware Trojans since a maliciously modified circuit would need to match the locked design behavior to remain undetected.
- **Privacy Protection:** Logic locking ensures that sensitive data processed by hardware remains private, as only authorized users with the correct key can operate the hardware properly.

VII

Industry Perspective

From an industry perspective, logic locking is viewed as an essential technology to safeguard against various threats in the globalized semiconductor supply chain. The industry is gradually absorbing logic locking as a critical solution to protect intellectual property (IP) and prevent overproduction, reverse engineering, and tampering in globalized semiconductor manufacturing. Adoption is driven primarily by sectors like defense, automotive, and high-end electronics, where security is a priority and IoT. However, concerns around added complexity, performance impact, and cost are slowing broader adoption, especially in cost-sensitive markets. However, its adoption may be slower for industries more concerned with cost and performance unless more efficient, cost-effective solutions emerge. Additionally, with ongoing research on attacks like SAT-based ones, the industry must continuously evolve the technology to stay ahead of adversaries.

How Industry Can Absorb Logic Locking

The successful absorption of logic locking into industry practices requires a multifaceted approach encompassing technological integration, employee training, stakeholder collaboration, and continuous improvement. Here are some strategies on how industries can effectively incorporate logic locking:

a) **Assessment of Current IP Protection Measures:** Industries should conduct a comprehensive assessment of their current IP protection strategies to identify gaps and vulnerabilities that logic locking can address.

b) **Integration with Design Processes:** Logic locking should be integrated into the design flow of hardware development. This includes utilizing logic locking techniques during the initial stages of circuit design to ensure that protection mechanisms are in place from the outset.

c) **Technology and Tool Adoption:** Companies should invest in design tools that support logic locking techniques. This may include EDA (Electronic Design Automation) tools that offer built-in logic locking features.

d) **Developing Security Policies:** Develop policies and guidelines that outline how logic locking should be applied within the organization. This should include best practices for design, implementation, and maintenance.

e) **Collaboration with Research Institutions:** Collaborate with universities and research institutions to explore advanced logic-locking techniques and stay ahead of emerging threats in IP protection.

f) **Industry Standards and Compliance:** Align logic locking practices with relevant industry standards and best practices for IP protection, ensuring compliance with regulatory requirements.

The absorption of logic locking into industry practices requires a proactive and holistic approach, encompassing design, manufacturing, security, and employee engagement. By prioritizing IP protection, investing in the necessary technology, and fostering a culture of security, companies can effectively implement logic locking and safeguard their valuable intellectual property against theft and unauthorized access. This, in turn, will bolster innovation, maintain competitive advantage, and support long-term business sustainability.

Benefits of Logic Locking to the Industry

Logic locking offers numerous benefits to various industries, particularly in protecting intellectual property (IP) and enhancing security. Below are the key benefits from an industry perspective:

a) **Enhanced IP Protection:** Logic locking effectively prevents unauthorized access to hardware designs, making it difficult for competitors to clone or reverse-engineer proprietary technologies.

b) **Revenue Generation and Licensing Control:** Manufacturers can implement tiered licensing models, where different features are unlocked based on the license purchased, providing a new revenue stream.

c) **Supply Chain Security:** Logic locking restricts third-party manufacturers from producing unauthorized or counterfeit products, ensuring that only authorized entities can produce hardware. It helps prevent unauthorized production, ensuring that only contracted units are manufactured and reducing the risk of overproduction.

d) **Competitive Advantage:** Logic locking helps companies retain their competitive edge in the market by protecting innovative designs from being easily replicated.

e) **Improved Security Against Tampering:** Logic locking can make it difficult for attackers to tamper with devices or insert hardware Trojans, ensuring that only authorized versions of the design are in circulation.

f) **Facilitating Collaboration and Outsourcing:** Logic locking allows companies to securely collaborate with external partners by providing access only to specific parts of the design, protecting the overall IP. Companies can safely outsource parts of their design without the risk of losing critical IP, making collaboration more feasible and secure.

VIII. Conclusion

Piracy and privacy concerns in the Integrated Circuit (IC) industry are becoming increasingly critical as ICs power a wide range of essential systems, from consumer electronics to defense and industrial infrastructure. The industry faces challenges such as intellectual property (IP) theft, counterfeit ICs, and hardware trojans, which threaten security and profitability. These issues arise due to global supply chains and pose serious implications for manufacturers and developers, consumers, industries, and national security.

Key Problems:

1. **IP Theft:** Reverse engineering allows unauthorized parties to replicate and modify IC designs, undermining the efforts of original manufacturers.

2. **Counterfeit ICs:** Pirated and cloned ICs often flood markets, posing risks of system failures or backdoors that can compromise security in sensitive applications.

3. **Hardware Trojans:** Malicious alterations introduced during IC manufacturing or distribution can lead to system breaches, data theft, or espionage.

Effective Solutions:

1. **Logic Locking:** This emerging technique locks parts of the IC's logic with a secret key, preventing unauthorized access or functionality unless the correct key is applied. Logic locking makes reverse engineering and IP theft much harder, as the IC will not function without the correct decryption mechanism, securing the design even during manufacturing in untrusted facilities.

2. **Enhanced Verification Mechanisms:** Advanced testing methodologies such as side-channel analysis and formal verification should be implemented to detect hardware trojans. These methods identify unauthorized modifications in the IC's design before deployment.

3. **Supply Chain Security:** Implementing a trusted supply chain using blockchain or other authentication technologies will help verify the authenticity of each IC component, ensuring that counterfeit or tampered products don't reach critical systems.

4. **Onshore Manufacturing and Encryption:** Shifting key stages of IC production and design to onshore, secure facilities minimize exposure to external tampering risks. Embedding hardware-level encryption also ensures secure transmission of sensitive data within the IC.

Future Perspective: The future of the IC industry will revolve around design-for-security approaches such as logic locking, which provides robust protection against piracy and IP theft. Combined with AI-powered verification systems and quantum-resistant encryption, these solutions will make ICs more resilient to emerging threats. Governments and industry players must collaborate on standardizing security measures and ensuring the integrity of supply chains. By embedding security at every level—from design to manufacturing IC producers can safeguard their innovations and protect against piracy and privacy breaches in an increasingly digital world.

References

[1] S. Bhunia et al., "Hardware IP Protection against Confidentiality Attacks and Evolving Role of CAD Tool (Invited Paper)," 2022 IEEE/ACM International Conference On Computer Aided Design (ICCAD), San Diego, CA, USA, 2022, pp. 1-9.

[2] Kathole, A.B., Kimbahune, V.V., Patil, S.D., Jadhav, A.P., Vhatkar, K.N. (2024). Challenges and Key Issues in IoT Privacy and Security. In: Prasad, A., Singh, T.P., Dwivedi Sharma, S. (eds)

Communication Technologies and Security Challenges in IoT. Internet of Things. Springer, Singapore. https://doi.org/10.1007/978-981-97-0052-3_3.

[3] "International chamber of commerce, impacts of counterfeiting and piracy to reach us $1.7 trillion by 2015," [Online]. Available: http://www.iccwbo.org/News/Articles/2011/Impactsofcounterfeiting-and- piracy-to-reach-US$1-7-trillion-by-2015/.

[4] SEMI, "Innovation is at risk as semiconductor equipment and materials industry loses up to $4 billion annually due to IP infringement." [Online]. Available: www.semi.org/en/Press/P043775, 2008.

[5] J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending piracy of integrated circuits," Computer, vol. 43, no. 10, pp. 0030–38, 2010.

[6] Rostami, Masoud, Farinaz Koushanfar, and Ramesh Karri. "A primer on hardware security: Models, methods, and metrics." Proceedings of the IEEE 102, no. 8 (2014): 1283-1295.

[7] Xiao, Kan, Domenic Forte, Yier Jin, Ramesh Karri, Swarup Bhunia, and Mohammad Tehranipoor. "Hardware trojans: Lessons learned after one decade of research." ACM Transactions on Design Automation of Electronic Systems (TODAES) 22, no. 1 (2016): 1-23.

[8] Akter, Sonia, Kasem Khalil, and Magdy Bayoumi. "A survey on hardware security: Current trends and challenges." IEEE Access 11 (2023): 77543-77565.

[9] S. Dupuis, P.-S. Ba, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans," in Proc. IEEE 20th International On-Line Testing Symposium (IOLTS), 2014, pp. 49–54.

[10] V. S. Rathor, B. Garg, and G. K. Sharma, "A novel low complexity logic encryption technique for design-for-trust," IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 3, pp. 688–699, 2020.

[11] Kamali, Hadi Mardani, Kimia Zamiri Azar, Farimah Farahmandi, and Mark Tehranipoor. "Advances in logic locking: Past, present, and prospects." Cryptology ePrint Archive (2022).

[12] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2015, pp. 137–143.

[13] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Removal attacks on logic locking and camouflaging techniques," IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 2, pp. 517–532, 2020.

[14] K. Shamsi, M. Li, T. Meade, Z. Zhao, Y. Jin, and D. Pan, "Appsat: Approximately deobfuscating integrated circuits," in Proc. IEEE Symp. Hardware-Oriented Security and Trust, 2017, pp. 95–100.

[15] M. Yasin, B. Mazumdar, J. J. Rajendran, and O. Sinanoglu, “Sarlock: SAT attack resistant logic locking,” in Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2016, pp. 236–241.

[16] Y. Xie and A. Srivastava, “Anti-SAT: Mitigating sat attack on logic locking,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 38, no. 2, pp. 199–207, 2018.

[17] M. Yasin, J. J. Rajendran, O. Sinanoglu, and R. Karri, “On improving the security of logic locking,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 35, no. 9, pp. 1411–1424, 2016.

[18] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. Rajendran, and O. Sinanoglu, “Provably-secure logic locking: From theory to practice,” in Proc. ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1601–1618.

[19] Köylü, Troya Çağıl, Cezar Rodolfo Wedig Reinbrecht, Anteneh Gebregiorgis, Said Hamdioui, and Mottaqiallah Taouil. “A survey on machine learning in hardware security.” ACM Journal on Emerging Technologies in Computing Systems 19, no. 2 (2023): 1-37.

[20] Wei Liang, Bo Liao, Jing Long, Yan Jiang, Li Peng, Study on PUF-based secure protection for IC design, Microprocessors and Microsystems, Volume 45, Part A, 2016, Pages 56-66,

[21] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, “Logic encryption: A fault analysis perspective,” in Proceedings of the Conference on Design, Automation and Test in Europe, 2012, pp. 953–958.

[22] B. Liu and B. Wang, “Embedded reconfigurable logic for ASIC design obfuscation against supply chain attacks,” in Proceedings of the conference on Design, Automation & Test in Europe. European Design and Automation Association, 2014, p. 243.

[23] S. Khaleghi, K. Da Zhao, and W. Rao, “IC piracy prevention via design withholding and entanglement,” in Proc. 20th Asia and South Pacific Design Automation Conference, 2015, pp. 821–826.

[24] Y. Liu, M. Zuzak, Y. Xie, A. Chakraborty, and A. Srivastava, “Strong anti-sat: Secure and effective logic locking,” in Proc. 21st International Symposium on Quality Electronic Design (ISQED), 2020, pp. 199–205.

[25] V. S. Rathor, M. Singh, K. S. Sahoo and S. P. Mohanty, “GateLock: Input-Dependent Key-Based Locked Gates for SAT Resistant Logic Locking,” in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 32, no. 2, pp. 361-371, Feb. 2024, doi: 10.1109/TVLSI.2023.3340350.

National Centre
of Excellence
CYBERSECURITY TECHNOLOGY
AND ENTREPRENEURSHIP

The National Centre of Excellence (NCoE) for Cybersecurity Technology Development is a joint initiative between the Ministry of Electronics & Information Technology (MeitY), Government of India, and the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling up and advancing the cybersecurity ecosystem, focusing on various critical and emerging security areas. Equipped with stateof-the-art facilities, including advanced lab infrastructure and test beds, NCoE facilitates research, technology development, and solution validation for adoption across government and industrial sectors. Adopting a concerted strategy, NCoE endeavors to translate innovations and research into market-ready deployable solutions, thereby contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURITY COUNCIL OF INDIA

☎ +91-120-4990253 | ncoe@dsci.in

https://www.n-coe.in/

4 Floor, NASSCOM Campus, Plot No.
7-10, Sector 126, Noida, UP -201303

Follow us on

@CoeNational

nationalcoe

nationalcoe

NationalCoE