ISSN: 2976-7466

Journal of Biosensors and Bioelectronics Research

SCIENTIFIC Research and Community

Review Article

Open Access

Ensuring Security in Semiconductor Design through Verification

Niranjana Gurushankar

Hardware Verification Engineer at Cisco Systems, USA

ABSTRACT

The ever-growing complexity of semiconductor designs, the demand for powerful and feature-rich electronics, presents a significant challenge in ensuring their correctness and security. Security verification has become a critical process in the semiconductor design lifecycle, aiming to identify and mitigate potential vulnerabilities that could be exploited. Given the increasing reliance on semiconductor devices for critical infrastructure and applications, the importance of robust security verification cannot be overstated. This paper explores few of the crucial role verification plays in guaranteeing security within semiconductor design. It examines various facets of this process, including analyzing potential security threats and vulnerabilities. This paper delves into the critical role of verification in ensuring semiconductor security. It also explores various verification techniques, discusses emerging trends, and outlines future directions in this crucial field.

***Corresponding author**

Niranjana Gurushankar, Hardware Verification Engineer at Cisco Systems, USA.

Received: April 07, 2023; **Accepted:** April 14, 2023; **Published:** April 21, 2023

Keywords: Semiconductor Security, Verification, Formal Verification, Simulation-Based Verification, Hardware-Assisted Verification, Post-Silicon Validation, Machine Learning

Introduction

The semiconductor industry is the backbone of modern technology, driving innovation in computing, communication, healthcare, and countless other fields. As semiconductor devices become increasingly complex and integrated into critical infrastructure, ensuring their security is paramount. Security vulnerabilities in semiconductor designs can have catastrophic consequences, ranging from data breaches and financial losses to disruptions in essential services and even threats to national security [1]. The semiconductor industry faced a multitude of security challenges. The increasing sophistication of cyberattacks, coupled with the growing complexity of chip designs, made it more difficult than ever to ensure the security of semiconductor devices. Supply chain vulnerabilities, hardware Trojans, and side-channel attacks were among the major concerns [2]. Formal verification techniques, employing mathematical approaches to rigorously prove the absence of security flaws, are discussed. The paper also covers simulation-based verification, which utilizes simulation to test the design's resilience against different attack scenarios. Furthermore, it delves into hardware-assisted verification, where specialized hardware accelerates and enhances the verification process. In addition, this paper delves into emerging trends in semiconductor security verification. This includes the application of machine learning for vulnerability detection and the development of standardized security verification methodologies. The challenges faced and future directions in this dynamic field are also discussed.

Importance of Security in Semiconductor Design

Semiconductor security is absolutely crucial in today's world, and for good reason. These tiny components, often no bigger than a fingernail, have become the fundamental building blocks of our modern digital existence. They're not just in our smartphones and laptops; they're embedded in practically every electronic device imaginable, from the cars we drive to the medical equipment that keeps us healthy. This pervasive presence means that any vulnerability in these chips can have ripple effects across countless aspects of our lives. Think about our critical infrastructure, the power grids that keep our lights on, the transportation systems that move us around, and the financial networks that underpin our economy. All of these rely heavily on semiconductors for their operation. If these systems were to be compromised due to security flaws in their underlying chips, the consequences could be devastating [3].

Furthermore, semiconductors aren't just responsible for controlling functions; they also store and process massive amounts of sensitive data. Every time we use our phones, browse the internet, or make an online transaction, our personal information flows through these tiny chips. This makes them prime targets for attackers seeking to steal data or disrupt services. And it doesn't stop there. Semiconductor technology is also at the heart of national security applications. Defense systems, intelligence gathering, and secure communication networks all depend on the reliable and secure functioning of these devices. Any weakness in these systems could potentially jeopardize national security [4]. In essence, semiconductor security is vital because it touches upon so many aspects of our lives, from our personal safety and privacy to the stability of our critical infrastructure and national defense. Ensuring that these devices are designed and manufactured with security in mind is no longer just a technical consideration; it's a societal imperative.

Supply Chain Attacks

Addressing the threat of Hardware Trojans requires a multi-faceted approach, including rigorous design and manufacturing practices, enhanced security testing, and increased vigilance throughout the supply chain [5].

Think of a semiconductor chip's journey like a relay race. It travels across the globe, passing through many different hands

before reaching the finish line. It starts with an idea, a design, crafted in one country. Then, it's off to a specialized factory, often overseas, where it's brought to life. After that, it might be packaged and tested elsewhere before finally being shipped to yet another company to be placed in a phone, a car, or a medical device. This global journey, while efficient, makes securing these tiny but powerful components quite tricky. Each stop along the way introduces potential vulnerabilities, like a chain with many links – a weakness in any one link can compromise the entire chain [6]. This means that security isn't just about the chip itself, but about every stage of its journey. From the initial design to the final product, there are opportunities for bad actors to interfere, potentially stealing information, disrupting functionality, or even introducing hidden threats. This complex web of interconnected processes became a major security concern for the semiconductor industry. It highlighted the need for stronger safeguards at every step to ensure the integrity and trustworthiness of these essential components. There are different stages which were mentioned above, the next few sentences talk about each of the stages in detail.

Design Stage
Even at the initial design phase, there's a risk of malicious actors introducing vulnerabilities, perhaps by inserting hidden "backdoors" or "Trojans" into the chip's design. These could be exploited later to steal data or disrupt functionality [7].

Manufacturing Stage
Manufacturing often involves multiple companies and specialized equipment. This raises concerns about the integrity of the manufacturing process itself. Could someone tamper with the chip during production, perhaps by introducing malicious circuitry or subtly altering its behavior [8].

Distribution and Deployment
As chips move across borders and change hands, there's a risk of counterfeiting, tampering, or theft. This could lead to compromised devices ending up in critical systems, with potentially disastrous consequences. The global nature of the semiconductor supply chain essentially expands the attack surface, providing more opportunities for malicious actors to exploit vulnerabilities. This was a major concern, as the industry grappled with the increasing complexity and interconnectedness of this global network. It highlighted the need for enhanced security measures at every stage of the supply chain to ensure the integrity and trustworthiness of these critical components [9].

Hardware Trojans
Hardware Trojans are a particularly insidious threat in the semiconductor world. Imagine them as tiny, malicious spies embedded within the very heart of a chip, waiting for the right moment to strike.

What are Hardware Trojans?
Essentially, they are hidden circuits intentionally inserted into a chip's design. These circuits are designed to remain dormant most of the time, blending in with the normal circuitry. However, under specific conditions, they can be triggered to leak sensitive information where they might secretly transmit encryption keys, passwords, or other valuable data to an attacker. Second could disrupt functionality, where they could cause the chip to malfunction, leading to errors, crashes, or even complete device failure. In other cases, taking control, where this could allow an attacker to remotely take control of the chip or the device it's in [10].

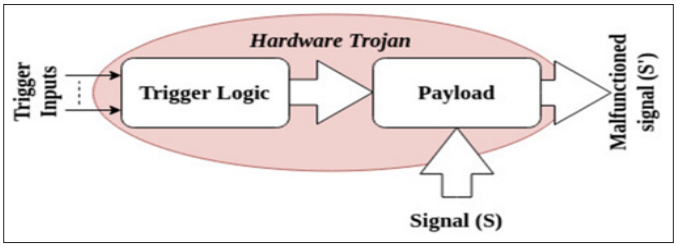

Figure 1: A Survey of Hardware Trojan Taxonomy and Detection [11].

Let's talk about how these trojans are being inserted in the semiconductor. Hardware Trojans can be introduced at various stages as we spoke about the three stages in the previous section of this paper

Design Stage
A malicious actor involved in the design process could subtly alter the chip's blueprint to include the Trojan circuitry [12].

Manufacturing Stage
Someone could tamper with the chip during manufacturing, adding the Trojan during the complex fabrication process [13].

Supply Chain
A Trojan could be inserted at any point in the supply chain, from the initial design to the final assembly of the device [14].

Why are These a Significant Threat?
These are difficult to detect, hardware Trojans are often designed to be very small and stealthy, making them extremely difficult to detect using traditional testing methods. These could have devastated impact, Trojans can have a wide range of harmful effects, from compromising sensitive data to causing critical systems to fail. The presence of Trojans undermines trust in semiconductor devices, raising concerns about the security of everything from personal devices to critical infrastructure. The increased complexity of chips is making it harder to identify hidden Trojans within their intricate designs. The complex and geographically dispersed nature of semiconductor supply chains increased the opportunities for Trojan insertion. The risk of state-sponsored actors using Trojans for espionage or sabotage became a growing concern [15].

Side-Channel Attacks
Side-channel attacks are a sneaky and sophisticated way to extract sensitive data from electronic devices, including those containing semiconductors. Unlike traditional hacking methods that try to break through software defenses, side-channel attacks exploit the physical characteristics of the device itself [16]. When a chip is working, it's not just processing data, it's also unintentionally leaking information through various physical channels. This leakage can be in the form of different factors which are discussed below in detail.

Power Consumption
The amount of power a chip uses fluctuates depending on the operations it's performing. By carefully monitoring these power variations, attackers can infer what data is being processed, and even extract sensitive information like encryption keys [17].

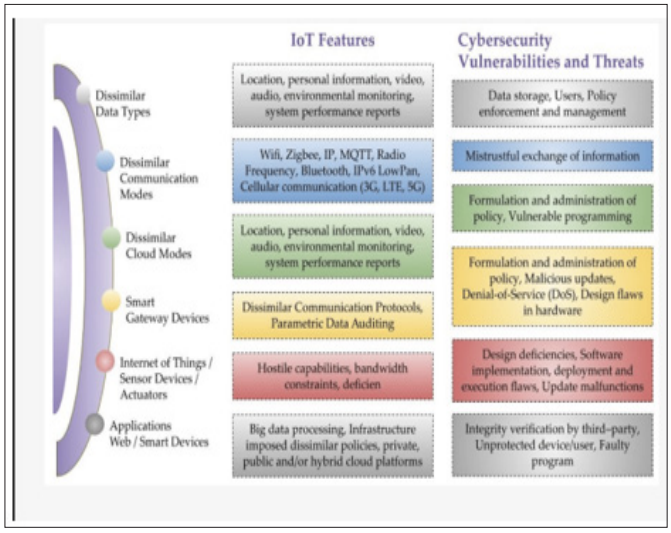

Figure 2: Differential Power Analysis [18].

Electromagnetic Radiation
Electronic devices emit electromagnetic radiation, which can carry information about the device's operations. Attackers can analyze these emissions to glean secrets [19].

Acoustic Emissions
Even the faint sounds produced by a device during operation can leak information. Specialized microphones can pick up these sounds and analyze them for clues about the data being processed [20].

Timing
The time it takes for a device to perform certain operations can also leak information. Attackers can measure these timings to deduce sensitive data [21].

How Side-Channel Attacks Work?
Let's imagine a hacker trying to steal information from a secure chip, like the one in your credit card. Instead of trying to directly hack the chip's software or guess its password, they take a different approach. They use special equipment to carefully monitor the chip's power consumption as it performs different operations, like encrypting data or verifying a transaction. Just like the clicks of a safe's dial, the chip's power consumption subtly changes depending on what it's doing. By analyzing these tiny fluctuations in power, the hacker can start to piece together what's happening inside the chip. They might be able to figure out the secret key it's using to encrypt data, or even extract sensitive information like your credit card number. That's essentially what a side-channel attack does. It exploits the unintentional physical leakage from a chip, like its power consumption or electromagnetic radiation, to gain access to secrets without ever directly breaking into its core. It's a bit like listening to the whispers of a chip to uncover its hidden secrets.

Why Side-Channel Attacks are a Concern?
Side-channel attacks bypass traditional software security measures, making them effective against even well-protected systems. These attacks are often non-invasive and leave no trace on the target device, making them difficult to detect. Side-channel attacks can be used against a wide range of devices, from embedded systems to high-end servers. The attack rate has increased due to an increased usage of cryptography to protect data, side-channel attacks became a more attractive way to bypass these protections. Researchers developed new and more sophisticated side-channel attack techniques, making them more effective and harder to defend against. The proliferation of IoT devices, many of which have weak security, increased the potential targets for side-channel attacks [22].

Increasing Design Complexity
The increasing complexity of semiconductor designs is a serious issue when it comes to security. It gives us amazing devices with incredible capabilities, but it also makes securing those devices much harder. Modern chips have billions of tiny transistors, the fundamental building blocks of electronics, packed into a tiny space. This complexity creates several challenges as discussed below

Hidden Vulnerabilities
With so many components and connections, it's easier for design flaws or intentional vulnerabilities (like hardware Trojans) to go unnoticed. It's like a city with weak spots in its infrastructure that attackers could exploit [23].

Difficulty in Verification
Verifying a chip's security means making sure it works correctly and doesn't have any hidden weaknesses. But with complex designs, this verification process becomes incredibly challenging and time-consuming. It's like trying to inspect every building, every pipe, and every wire in that massive city [24].

Evolving Attack Techniques
Attackers are constantly developing new and more sophisticated ways to exploit vulnerabilities. As chips become more complex, they offer a wider range of potential attack vectors. It's like a city constantly facing new and unexpected threats [25].

Limited Visibility
With complex designs, it's harder to understand exactly how every part of the chip interacts with the others. This lack of visibility makes it difficult to predict and prevent potential security issues. It's like having blind spots in the city's surveillance system [26].

Methodologies for Enhancing Semiconductor Security
Having identified the key security concerns in the semiconductor industry, let's shift our focus to the promising methodologies that are paving the way for a more secure and trustworthy digital landscape.

Threat Analysis
Identifying potential security threats and vulnerabilities early in the design process is crucial. This involves understanding the potential attack vectors and the assets that need protection.

Let's take an example before designing a new chip, the designer thinks about what kinda issues can be faced to make the chip awesome? The designer starts by brainstorming all the possible ways someone could attack it. You also have to think about sneaky attacks, like those that exploit tiny weaknesses in the chip's physical design [27].

Next, you need to figure out how an attacker might actually get to your chip. Could they attack it through the internet connection? Or maybe by physically tampering with the device it's in? Understanding these "attack vectors" helps you build stronger defenses. Of course, you also need to know what you're protecting. What are the most valuable things on your chip? This could be anything from secret codes to the chip's design itself. You need to make sure these "assets" are extra secure. Now, not all threats are equally dangerous. Some are more likely to happen than others, and some would cause more damage if they did happen. So, you

need to assess the risk of each threat. Why is this pre-planning very important? Well, it's much easier to prevent problems than to fix them later. By identifying threats early on, you can design your chip with security in mind from the very beginning. This helps you build a stronger, more resilient chip that can withstand attacks and keep important information safe.

Formal Verification
Formal verification is like having a mathematical guarantee that your chip design is free from certain types of flaws. It's a much more rigorous approach than traditional testing [26]. Instead of just testing a chip with various inputs and hoping for the best, formal verification uses mathematical reasoning to prove that the design meets specific security properties. It's like using logic and equations to demonstrate, with absolute certainty, that your chip behaves as intended.

Formal Specification
First, you define the desired security properties of your chip in a precise mathematical language. This is like writing a set of rules that your chip must follow.

Formal Model
Next, you create a mathematical model of your chip's design. This model captures the chip's behavior and interactions in a way that can be analyzed mathematically.

Verification Engine
You use a specialized software tool, called a "verification engine," to analyze the model and check if it satisfies the specified properties. This engine uses powerful algorithms and mathematical techniques to explore all possible scenarios and ensure that the chip's behavior always adheres to the rules.

The common "Formal Verification Technique" involves model checking where the technique explores all possible states and transitions of the chip's model to verify that it never violates the specified properties. It's like systematically checking every possible path in a maze to make sure there are no dead ends or loops [29]. The next is theorem proving, this involves using logical deduction to prove that the chip's design satisfies the desired properties. It's like constructing a mathematical proof to demonstrate that a theorem is true. After discussing the techniques, let us now see why formal verification is important. Formal verification provides a much higher level of confidence in the security of a chip design compared to traditional testing. It can identify security flaws early in the design process, before they become costly or difficult to fix. Formal verification is particularly useful for complex chip designs where traditional testing methods may not be sufficient. It is often used for critical systems where security is paramount, such as aerospace, medical devices, and financial systems [30].

Simulation-Based Verification
Instead of testing your chip in the real world, you create a virtual version of it and its surroundings inside a computer. Specialized software tools are used to create a virtual model of the chip and its surrounding environment. This could include other components, software, and even simulated attackers. Then run the simulations where you expose your virtual chip to all sorts of attacks. This could include feeding it bad data, simulating hidden "Trojans" inside it, or even mimicking those sneaky side-channel attacks we talked about. The chip carefully observes how it reacts to these virtual attacks. Does it behave as expected? Does it leak any secrets? Does it crash or malfunction? This helps you identify any weaknesses in the design.

Finally, by analyzing the simulation results, the potential vulnerabilities in the design can be easily identified that might have been missed in the first place.

Why is Simulation-Based Verification Important?
While formal verification can mathematically prove the absence of certain flaws, it might not catch all vulnerabilities, especially those that arise from complex interactions or unexpected scenarios. Simulation helps fill this gap. Simulation allows you to test your chip in a more realistic environment, exposing it to a wider range of potential attacks than might be feasible with formal methods alone. Finding and fixing vulnerabilities in the simulation stage is much cheaper than discovering them after the chip has been manufactured. Simulation allows you to easily test different attack scenarios and modify your design as needed, providing a flexible and iterative approach to security testing. By combining simulation-based verification with other techniques like formal verification, semiconductor designers can significantly enhance the security of their chips and build more resilient and trustworthy devices [31].

Hardware-Assisted Verification
Hardware-assisted verification is like giving your verification process a turbo boost. Instead of relying solely on software simulations, which can be slow for complex designs, this brings in specialized hardware to speed things up and get a more realistic picture of your chip's behavior. This type of verification involves using specialized hardware platforms to run your chip design in a real-world-like environment. These platforms can mimic the behavior of the chip at much faster speeds than software simulations, allowing you to test more scenarios in less time.

There are two different types of hardware platforms considered in the current generation

- **Emulation Platforms:** These are essentially high-powered computers specifically designed for hardware verification. They can emulate the chip's functionality at speeds significantly faster than software simulations, allowing for more extensive testing.
- **FPGA Prototypes:** FPGAs (Field-Programmable Gate Arrays) are reconfigurable chips that can be programmed to mimic the behavior of your chip design. They offer even faster speeds than emulation platforms and allow for real-time interaction with other hardware and software.

Let's discuss how the above two platforms work, first the design needs to be mapped to either the FPGA or the emulator. Secondly connect the platform to the test environment, the hardware platform is connected to a test environment that simulates the real-world conditions the chip will operate in. This could include other hardware components, software, and even simulated attackers. Third step is to run the verification tests on the hardware platform, which executes the design at high speed and provides detailed information about its behavior. Finally, the results are analyzed to identify any functional or security vulnerabilities that can be found in the design.

Hardware-assisted verification provides a way to test chip designs in a more realistic and efficient manner. These hardware platforms offer a more accurate representation of real-world operating conditions, as they can interact with actual hardware and software. This helps uncover vulnerabilities that might not be apparent in

purely software-based simulations. Furthermore, hardware-assisted verification often comes with advanced debugging tools that help pinpoint the root cause of problems more efficiently. This streamlines the process of identifying and resolving issues, leading to faster development cycles. Another advantage is the ability to start software development earlier in the process. Some platforms allow software developers to begin working on code even before the physical chip is manufactured. This parallel development approach can significantly accelerate the overall project timeline.

Post-Silicon Validation

Think of post-silicon validation as the "real-world test" for a chip. Even after careful design and simulations, some hidden problems might still exist because a real chip is much more complex than any model. This could be due to other factors that go in before the chip goes to the outside market. Post-silicon validation takes the actual, physical chip and tests it in a real-world environment. This helps uncover any remaining vulnerabilities that might have been missed during earlier design stages. During this testing phase, engineers use various techniques to challenge the chip's security. They might deliberately introduce errors to see how it handles them, measure its physical emissions for any leaked information, and even simulate real-world attacks to see if it can withstand them. It's like putting the chip through a rigorous obstacle course to ensure it's truly robust. This process is essential because it provides a more accurate picture of the chip's security in real-world conditions. It helps build confidence in the chip's reliability and acts as a final safety check before it's released into the market. By catching and fixing any remaining vulnerabilities, post-silicon validation helps prevent potential security breaches and ensures that the chip can function safely and reliably in its intended application.

Future Trends

Given the increasing complexity and criticality of semiconductor devices, alongside the evolving landscape of security threats, the field of semiconductor security verification is ripe with opportunities for future research. Prominent areas are captured below.

The Rise of Machine Learning in Security Verification

The semiconductor industry was increasingly turning to machine learning to enhance security. By training algorithms on vast datasets, these digital detectives could identify potential vulnerabilities in chip designs, even those missed by human eyes. This approach also held the promise of predicting future threats by analyzing past attack patterns, allowing designers to proactively build defenses. Furthermore, machine learning could automate and speed up the verification process, making it more efficient and freeing human engineers for more complex tasks. Ultimately, machine learning offered a powerful new way to create more secure and resilient chips for an increasingly complex digital world.

Standardization and Collaboration

Crucial realization was dawning in the semiconductor world: enhancing security was not a solo endeavor, but a team effort. The industry was recognizing the power of collaboration and standardization. This meant working together to establish common security testing standards and best practices, ensuring everyone was on the same page and following proven methods. It also involved fostering a culture of shared threat intelligence, where companies and researchers could openly exchange information about new vulnerabilities and attack techniques, collectively staying ahead of the curve. Furthermore, it meant baking security into the very DNA of chip design, considering it at every step from the initial brainstorming to the final product. This collaborative approach, with its emphasis on shared knowledge and standardized practices, was seen as crucial for building a more secure foundation for the future of semiconductor technology.

Hardware Security Primitives

The concept of "baking security in" was gaining traction. Instead of relying solely on external security measures, there was a growing movement towards incorporating security features directly into the chip's hardware. This involved creating secure memory regions within the chip, essentially walled-off areas where sensitive data could be stored and protected from prying eyes. It also included building dedicated hardware for encryption and decryption, making it much harder for attackers to crack the chip's security code. Furthermore, researchers were exploring the use of "physical unclonable functions" or PUFs, which leverage the unique physical characteristics of each chip, like a fingerprint, to create secure identification and authentication mechanisms. These hardware-based security measures were seen as a crucial step towards building more resilient and tamper-proof chips.

Addressing Supply Chain Vulnerabilities

Securing the intricate, globe-spanning semiconductor supply chain was paramount. This meant enhancing traceability and provenance, essentially creating a detailed history for each chip, like a passport, to verify its authenticity and prevent counterfeiting. It also involved tightening security measures within manufacturing facilities, implementing stricter protocols to prevent tampering and ensure the integrity of the chips being produced. Furthermore, recognizing that security is a team effort, collaboration with suppliers was crucial, ensuring that every link in the chain, from raw materials to final product, adhered to strong security practices. This holistic approach aimed to create a more secure and trustworthy supply chain, mitigating the risks inherent in the global journey of a semiconductor chip.

Conclusion

In this paper, an overview of the critical role of verification in ensuring semiconductor security was provided, along with a deep dive specifically into the challenges faced. The paper also covered various methodologies for enhancing security, including emerging trends like machine learning and the importance of collaboration across the supply chain. It highlighted key areas for future research that can help in improving the security and trustworthiness of semiconductor devices. Further research is needed to address the evolving challenges in this field and ensure the continued development of secure and reliable semiconductor technology for critical applications.

References

1. Salmani H, Tehranipoor M, Karri R (2010) On detection of hardware Trojans by utilizing Boolean satisfiability. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 29: 1785-1800.
2. Tehranipoor M, Koushanfar F (2010) A survey of hardware Trojan taxonomy and detection. IEEE Design & Test of Computers 27: 10-25.
3. Kuhn MG (2003) Building a secure system out of insecure components. In Proceedings of the 17th Annual Computer Security Applications Conference pp: 354-363.
4. Anderson R (2001) Security engineering: A guide to building dependable distributed systems.
5. Waksman A, Sethumadhavan S (2011) Identifying and mitigating hardware Trojans: Challenges and emerging trends. IEEE Design & Test of Computers 28: 28-38.

6. Jin Y, Makris Y (2010) Hardware Trojan detection using path delay fingerprint. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems 18: 1404-1414.
7. Narayan A, Bhunia S (2012) Hardware Trojan detection: An overview. Journal of Electronic Testing: Theory and Applications 28: 1-22.
8. Rajendran J, Sam M, Sinanoglu O, Karri R (2012) Security analysis of integrated circuit camouflaging. In Proceedings of the 2012 ACM SIGSAC Conference on Computer and Communications Security pp: 709-720.
9. Yang K, Karri R, Bhunia S (2013) A survey of hardware security techniques for SoC designs. Journal of Low Power Electronics and Applications 3: 1-33.
10. Waksman A (2013) Hardware Trojan horses: A rising security threat. IEEE Security & Privacy 11: 84-87.
11. Tehranipoor M, Koushanfar F (2010) IEEE Design & Test of Computers 27: 10-25.
12. Bhunia S, Tehranipoor M (2011) Hardware security and trust. Springer Science & Business Media.
13. Li L, Sinanoglu O (2014) On the effectiveness of SAT-based hardware Trojan detection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33: 1502-1515.
14. Zhang X, Tehranipoor M (2011) Case study: Detecting hardware Trojans in third-party IP cores. In Hardware Security and Trust. Springer, Berlin, Heidelberg.
15. Tehranipoor M, Wang X (2011) Introduction to hardware security and trust. In Hardware Security and Trust. Springer, Berlin, Heidelberg.
16. Kocher PC, Jaffe J, Jun B (1999) Differential power analysis. In Annual International Cryptology Conference. Springer, Berlin, Heidelberg pp: 388-397.
17. Mangard S, Oswald E, Popp T (2007) Power analysis attacks: Revealing the secrets of smart cards. Springer Science & Business Media.
18. Kocher PC, Jaffe J, Jun B (1999) In Annual International Cryptology Conference. Springer, Berlin, Heidelberg pp: 388-397.
19. Quisquater JJ, Samyde D (2001) Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In International Workshop on Smart Card Research and Advanced Applications. Springer, Berlin, Heidelberg pp: 200-210.
20. Shamir A, Tromer E (2004) Acoustic cryptanalysis: On nosy people and noisy machines. In International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg pp: 1-18.
21. Kocher PC (1996) Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Annual International Cryptology Conference. Springer, Berlin, Heidelberg pp: 104-113.
22. Oswald E, Paar C (2011) Breaking Mifare DESFire MF3ICD40: Power analysis and templates in the real world. In International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg pp: 207-222.
23. Moore GE (1965) Cramming more components onto integrated circuits. Electronics 38: 114-117.
24. Stoica I, Song D, Popa RA, Patterson D, Bershad B, et al. (2003) A Berkeley view of cloud computing. Communications of the ACM 51: 50-58.
25. Chen Y, Abraham JA (2004) Fault tolerance in VLSI circuits. In Fault-Tolerant Computing. Springer, Boston, MA.
26. Roy S, Ray S, Bhunia S (2012) Classification of logic obfuscation techniques. In Proceedings of the 2012 IEEE/ACM International Conference on Computer-Aided Design IEEE Press pp: 721-728.
27. Thompson K (1984) Reflections on trusting trust. Communications of the ACM 27: 761-763.
28. Clarke EM, Grumberg O, Peled D (1999) Model checking. MIT press.
29. Baier C, Katoen JP (2008) Principles of model checking. MIT press.
30. Kaufmann M, Manolios P, Moore JS (2000) Computer-aided reasoning: An approach. Kluwer Academic Publishers.
31. Bergeron J (2000) Writing testbenches: functional verification of HDL models. Springer Science & Business Media.

Copyright: ©2022 Niranjana Gurushankar. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.