The Curious Case of Trusted IC Provisioning in Untrusted Testing Facilities

Sandip Ray
University of Florida
Gainesville, Florida, USA
sandip@ece.ufl.edu

Atul Prasad Deb Nath
University of Florida
Gainesville, Florida, USA
atulprasad@ufl.edu

Kshitij Raj
University of Florida
Gainesville, Florida, USA
kshitijraj@ufl.edu

Swarup Bhunia
University of Florida
Gainesville, Florida, USA
swarup@ece.ufl.edu

ABSTRACT

Asset provisioning is a crucial step in present-day IC manufacturing process. The nature of on-chip assets can range from crypto keys, IC configurations, and manufacturer firmware to target specific security specifications, policies, and chip debugging information. Given the criticality of the assets, a major part of IC security research is targeted towards the development of their protection mechanisms, especially in post-fabrication deployment phase. However, in this work our curious observation is that a series of novel attack surfaces can stem from asset provisioning at untrusted testing sites and colluding foundries which are not covered by existing threat models and defense schemes. To that end, we study the state-of-the-art protection mechanisms adopted for secure IC provisioning at untrusted testing facilities and highlight their security vulnerabilities. In particular, we show the inadequacy of existing authentication and design obfuscation-based defense mechanisms during asset provisioning through a secure root of trust.

CCS CONCEPTS

• **Security and privacy → Hardware-based security protocols**.

KEYWORDS

IC provisioning; asset provisioning; fabrication-time attacks; fabrication-time defenses; testing-time attacks; testing-time defenses; provisioning attacks; provisioning defenses;

ACM Reference Format:
Sandip Ray, Atul Prasad Deb Nath, Kshitij Raj, and Swarup Bhunia. 2021. The Curious Case of Trusted IC Provisioning in Untrusted Testing Facilities. In *Proceedings of the Great Lakes Symposium on VLSI 2021 (GLSVLSI '21), June 22–25, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3453688.3461758

1 INTRODUCTION

Over the past years, semiconductor design has evolved into a uniquely global enterprise incorporating 3PIP (third-party IP) vendors, IC design houses, fabrication labs, and testing facilities dispersed over multiple countries and continents across the globe. The globalization in microelectronic design supply chain helps ameliorate several challenging factors such as increasing design complexities, aggressive time-to-market, fabrication and validation costs, etc. Note that the exponential shrinkage of transistor nodes over the past decades has enabled the IC designers to pack complex, multi-core and many-core designs with advanced performance in area and power constrained chip designs, with a resultant increase in the price of fabrication. Recent studies show that the price of building a state-of-the-art fabrication laboratory can be about 15-20 billion USD [12]. As a result, majority of the semiconductor chip manufacturing companies are going *fabless* to avoid such prohibitive expenses and outsourcing chip fabrication to a variety of globally distributed remote foundries [8].

With the global horizontal shift in IC Industry, it has become increasingly challenging to ensure the security at every phase of the excruciatingly long and complex global supply-chain. Inclusion of untrusted IPs, remote foundries, and testing sites open the Pandora's box of novel attack surfaces and vulnerabilities. The current business model of outsourced IPs and outsourced fabrication, in addition to the fact that it is difficult to independently vet a fabricated IC, forces designers and OEMs to trust the remote foundries, and testing sites. The unfortunate truth, however, is that neither the vendors nor the foundries and testing sites can be fully trusted. Attackers located at different IP vendors can introduce a variety of malicious modifications to the supplied IPs. Attackers located at the foundries and testing facilities are capable of exploiting a series of attack surfaces and modalities to steal IC assets, overproduce ICs by cloning, illegally alter the ICs for malicious purposes and eventually corrupt the entire chip supply-chain. Organizations involved in the development of ICs targeted for mission-critical application, such as military and defense, adopt custom tailored trusted foundry programs to minimize the threat levels of the global supply-chain [1]. But it is not economically feasible for the majority of manufactures to adopt such custom approaches and build a *chain-of-custody* for every stage of the design flow.

GLSVLSI '21, June 22–25, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8393-6/21/06…$15.00
https://doi.org/10.1145/3453688.3461758

In this paper, we investigate a curious vulnerability arising from collusion between untrusted foundries and untrusted testing facilities. As initial chip testing is typically performed at the foundries and testing sites as part of the structural testing and detection of manufacturing defects, the threat model is viable in current IC design supply chain. Our primary observation is that asset provisioning in untrusted facilities exposes the ICs to a diverse set of attack surfaces that are not covered by traditional IC protection mechanisms. Consequently, the task of IC provisioning in a zero trust model represents one of the weakest links of the supply-chain. The attacks show the futility of existing mechanisms such as PUF-based authentication, logic locking, and watermark hash composites in protecting the IC assets and design secrets during the provisioning phase.

Significant research has been done over the last decade to protect ICs in untrusted remote foundries and testing sites and prevent attacks on chip assets after deployment [2–7, 11]. The primary solutions of chip protection at untrusted foundries and testing sites incorporate unique challenge-response based authentication using PUF circuitry, obfuscation of IC designs, and watermarking ICs to prevent piracy. A large body of security research focuses on the application of PUF-generated CRPs to securely authenticate chips at untrusted facilities. The unclonable nature of PUF CRPs helps the OEMs differentiate between fake and real chips [5, 7]. Logic locking techniques limits attacker's access to the original design by obfuscating it via additional key gates and FSMs (finite state machines) that can only be unlocked with the right set and sequence of keys. It is difficult for an adversary to steal design secrets or reverse engineer an obfuscated design without unlocking it [2, 11]. Watermarking techniques are deployed at ICs to prevent piracy and enable authenticity of IP ownership [6]. Though the major defense mechanisms vary in their implementation, the common goal of the techniques is to authenticate ICs securely and thwart the adversary's access to design secrets and assets to mitigate attacks leading to malicious alterations, cloning, overproduction, and asset leakage.

However, the current defense mechanisms designed for IC protection fail to account for the provisioning aspects of modern ICs. As the ICs remain unlocked and unprotected at an untrusted environment during provisioning, the attackers can fully leverage this phase of the design flow to circumvent the authentication techniques, wrongfully provision clone, overproduced chips, masquerade the fake chips as authentic products, maliciously alter original designs, and steal design secrets. Here, we investigate the curious case of asset provisioning by: (1) studying the state-of-the-art defense mechanisms employed for IC protection and (2) performing their security vulnerability analysis to highlight current limitations in ensuring secure provisioning in an untrusted environment.

The remainder of the paper is organized as following. Relevant background on modern IC supply chain is provided in Section 2. In Section 3, we describe an illustrative IC model augmented with state-of-the-art security features. The threat model of our work in described in Section 4. In Section 5, the existing defense mechanisms for asset provisioning at untrusted testing sites are outlined along with their security vulnerability analysis. We describe the related work in Section 6 and conclude in Section 7.

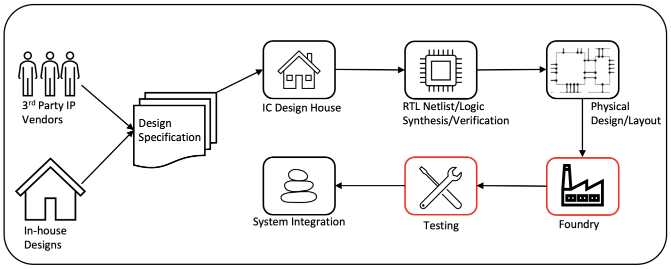

Figure 1: Microelectronic chip design flow with untrusted foundries and testing facilities.

2 MICROELECTRONIC IC SUPPLY CHAIN: PRACTICES AND CHALLENGES

2.1 IC Design Cycle

The major phases of modern-day IC design cycle are shown in Figure 1. With current trends of outsourcing in chip design industry, pre-designed IP blocks are obtained from third-party vendors across the globe. First, the behavioral specifications of these IPs are defined via hardware description languages such as VHDL and Verilog. Then, the behavioral designs are mapped to certain design libraries and node technologies to generate the gate-level netlists. The OEM (Original Equipment Manufacturer) obtains the 3PIPs along with in-house IPs and delivers them to the IC design house for integration. The IC design house integrates the IPs following standardized interfaces and integration protocols. The IC layouts are developed from the integrated netlists and GDSII files are generated. These GDSII file are delivered to the foundries for fabricating silicon chips. The fabricated chips are tested and provisioned at the foundries and testing sites as a part of the initial testing before the system integration and package testing. Only the passed chips are packaged for system integration and re-tested before making them available to the market.

2.2 Threats and Vulnerabilities at Untrusted Foundries and Testing Facilities

A detailed classification of attacks originating from untrusted foundries and testing sites is shown in Figure 2. Based on the location of chip, *i.e.*, the foundry or testing facilities, the adversaries can launch a series of attacks with diverse intents and payloads. The chips at untrusted foundry are susceptible to malicious alteration or insertion of malicious piece of circuitry known as hardware Trojans. The Trojans can be exploited at testing facilities or in the later phases of the life cycle to steal design secrets and impair design functionality. In addition, the adversaries at the foundry and testing sites can overproduce IC by cloning and infiltrate the original supply chain with cloned chips. Similarly, the attackers can insert poorly tested out-of-spec chips to the supply chain to corrupt the design flow. Moreover, it is possible for the attackers to snoop the assets during provisioning and steal the design secret through man-in-the-middle attack.

3 STATE-OF-THE-ART IC SECURITY MECHANISMS

In modern-day applications, ICs have become an integral component in achieving the desired design functionality owing to their immense power and area benefits. As technological advancements grow, the deployment of ICs increase in safety critical applications and thus the inclusion of security architectures in the chip design flow is of paramount importance. Owing to the complexity of modern-day IC designs, a streamlined security architecture is not only desirable, but required. The current approach enables designers to design and test their IP for trustworthiness against security vulnerabilities within the bounds of their IP itself, and not considering the implications of the integrated architecture. Figure 3 is an illustrated example of an IC integrated with a dedicated security subsystem. A brief description of on-chip security components and related verification and provisioning process is provided below:

3.1 On-chip Security Architectures

The complexity of modern ICs require security architectures to be implemented in a distributed flow, sprinkled across different components. These distributed security architectures are scattered based on their individual security functionality with the help of security IPs. The two most prevalent security practices include authentication and logic locking. Authentication of IPs can be carried out via a centralized mechanism, or via a distributed design, which is an augmentation of the target IP to facilitate the authentication process. Similarly, the unlocking of obfuscated designs can be carried out via a centralized or distributed mechanism. This section briefly describes the different functionality of these representative security IPs, as depicted in Figure 3.

Watermarking: During the IP design and production, unique watermark based signatures can be added by inserting additional logic gates. These digital signatures can be observed after fabrication process to ensure that attacks such as IP piracy and IC overproduction are avoided. This is achieved by employing a query-based validation of the digital signature deployed at the target IP. This is controlled by the watermark IP. Typical use-cases include fetching the digital signature from the target IP, comparison of the response vectors with the golden signature obtained from the AMI (Asset Management Infrastructure) and then updating the relevant status bits in the AMI based on the outcome of the watermark comparison operation.

PUF-based Authentication: The PUF (Physical Unclonable Function) IP is responsible for the authentication of the target IP. The authentication is carried out using unique challenge-response pairs (CRPs). The AMI provisions the golden response vectors and they are stored on the on-chip NVM. The PUF IP then extracts the response vectors from the target IP by issuing a challenge response vector. The response vector is then compared with the golden response provisioned by the AMI and based on the result of that operation, the target IP is authenticated. The use-cases of the PUF IP includes obtaining provisioned keys from the AMI, obtaining the response vectors from the target IP and carrying out the comparison operation, and then updating corresponding status bits in the AMI repository based on the outcome of the authentication operation.

Logic Locking: Logic locking is one of the most fundamental security steps involved in modern day IC security. The logic locking IP is deployed in unlocking the target IP which are locked via state space obfuscation techniques. It obtains the keys to unlock the IP provisioned by an off-chip AMI or in some cases, stored locally in an on-chip NVM (Non-Volatile Memory). Generic use cases of the logic locking IP include obtaining the provisioned keys from the AMI or NVM (whichever is applicable), acquiring IP-specific metadata such as the type of logic locking algorithm used, the key size, key application fragmentation process based on the bus width, and the application logic based on the number of clock cycles required, etc., and the IP initialization states upon power up and reset conditions.

3.2 Hardware Security Module as The Root of Trust

The expanse of security vulnerabilities throughout the provisioning pipeline can be reduced to an extent by placing a trusted HSM (hardware security module) at the testing facility. This HSM enables secure communication between the cloud based AMI, the ATE, and the DUT. This serves as a *root of trust* throughout the provisioning

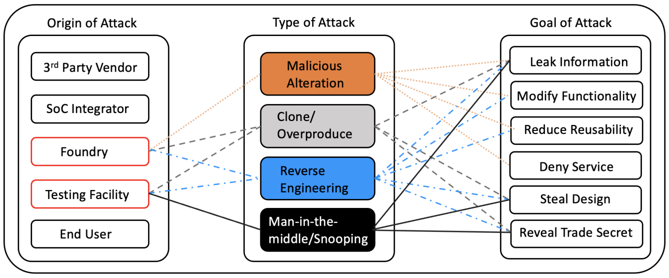

Figure 2: A taxonomy of threats and vulnerabilities originating from untrusted foundries and testing facilities.

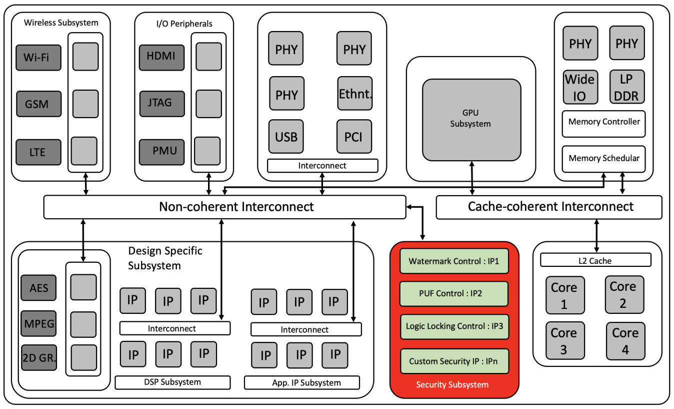

Figure 3: A representative IC designed with security features.

pipeline. However, all security vulnerabilities cannot be thwarted by the use of such a hardware module in a zero trust environment as we discuss how malicious attacks can be launched even despite the presence of a HSM.

3.3 Provisioning from AMI (Asset Management Infrastructure)

Security critical assets such as cryptographic keys and security specifications are usually stored in off-chip database for augmented security. Hence, the need for an secure off-chip asset provisioning infrastructure is critical, especially for standardized security mechanisms. Security IPs that implement functionalities such as authentication, logic locking, and watermarking require golden keys and vectors and these need to be provisioned by a secure and trustworthy enable to enable authentication and unlocking IP functionality when they are powered up for the first time. The PUF IP required the golden response vectors to be provisioned from an off-chip infrastructure similar to the logic locking and watermarking IP. These security operations are performed during the secure boot stage. To enable provisioning of these assets, the HSM is designed to facilitate asset procurement to the DUT (design under test). In the current scope of IC testing, it is a common practice to facilitate the provisioning of such assets from an off-chip cloud based infrastructure.

4 THREAT MODEL

Our threat model considers threats and vulnerabilities stemming from malicious entities located at untrusted foundries and rogue testing facilities. We assume that the adversaries can launch minimally invasive attacks on authentic or cloned chips that require limited to zero knowledge about the design. Consequently, the existing approach of obfuscating the design is not fully efficient against the threat model outlined in our work. For instance, an attacker with minimal access to the chip design files can maliciously introduce observable nodes into the original design without incurring any noticeable area and power overhead. The reverse engineering and alteration effort in this case is insignificant and can be done on a locked design without unlocking it. We also assume that there is potential nexus between the adversaries at the foundry and testing facility. Hence, it is possible for an attacker to exploit an altered chip during testing and provisioning to leak design secrets. However, the hardware security module is considered fully trusted in our threat model. Consequently, any communication through the HSM is deemed secure and trustworthy.

We illustrate the trust level at each participating entities of our threat model in Figure 4. We essentially make the following assumptions:

- The fabrication lab and testing sites are completely untrusted.
- Colluding attackers are present in the untrusted foundry and rogue testing facility.
- The attacker at the foundry can clone fake chips and make minimal alterations to original designs.

Our threat model is completely natural in the context of present-day IC supply chain as the fabricated chips are initially tested and provisioned at remote foundries and testing facilities that cannot be fully trusted.

5 EXISTING DEFENSE MECHANISMS FOR SECURE IC PROVISIONING

Here, we outline the existing defense mechanisms employed for secure IC provisioning in a zero trust environment and highlight the limitations of current approaches.

5.1 Authentication via IC Watermarking

IC watermarking enables a remote query and verification based authentication mechanism to securely identify each chip after fabrication. Via chip watermarking, it is feasible for the OEM to verify the detectability and ownership of the IP cores *i.e.*, the in-house or third-party IP used in the chip. In case of asset provisioning, it is of crucial importance to authenticate the ICs properly.

Assumptions:

- The chips are augmented with watermark control IP to facilitate challenge-response technique.
- A hardware security module is deployed as a *root of trust* at the untrusted testing facility to enable secure communication with watermark server located in remote AMI infrastructre.
- The hardware security module is inaccessible to the attackers and it guarantees the security of communication with remote watermark servers.

Flow of Operation:

The watermark based authentication in an untrusted environment incorporates several components including remote AMI, a trusted hardware security module located at the testing site, and the chip under test that has the watermarked IPs.

- The authentication process usually starts by establishing a secure communication channel between the trusted hardware module and the chip under test. In this scenario, we assume that the secure channel is established via Diffie-Hellmann (DH) key exchange protocol which is a standardized protocol in current practice. The IC under test can use several methods (*e.g.*, PUF generated crypto keys, TRNG generated keys, etc.) to generate the public and private keys for the DH protocol. Similarly, the hardware security module can

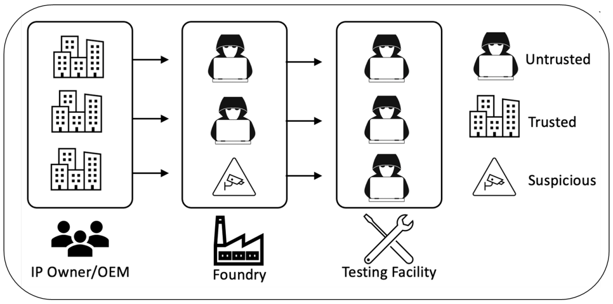

Figure 4: Threat levels at different stages of IC production, testing, and provisioning.

employ various methods to produce the keys including the usage of keys provisioned from the AMI.

- Upon establishment of a secure communication channel, the HSM sends queries to extract the watermarks from the IC. In response, the chip outputs the valid watermark composite hash via watermark control IP. The HSM compares the composite hash with golden references procured from the AMI to validate the chip's authenticity.
- Once there's a match of the watermarks, the provisioning process gets started. The provisioned assets typically include logic locking keys, PUF CRPs, security specifications and policies, authentic firmware etc.

Security Vulnerability Analysis: A major drawback of watermark based authentication is that watermarks are clonable. Hence, an attacker at the testing site can collude with the untrusted foundry to replicate the watermarked IPs and target chips. It essentially means that the attacker can use the stolen watermarked circuitry/IP to masquerade a fake chip as the authentic IC and establish secure communication channel with the HSM to initiate the asset provisioning process. Thus, the attackers at the untrusted testing facility can collude with the malicious entities at the foundry to bypass watermark based authentication. Once the assets are provisioned, the attacker can reverse engineer the chip or use clone chip with internal observable nodes to steal the assets.

5.2 Authentication via On-chip PUFs

PUFs can produce unique, unclonable signatures from chips based on manufacturing process variations. Such signature generation capability makes PUFs a promising candidate for authenticating ICs. The challenge for the PUF circuitry can vary based on the implementation type. PUF-based authentication is crucial during asset provisioning to ensure the authenticity of the chip.

Assumptions:

- The chips are augmented with distributed/centralized PUF circuitry and IP to support CRP based authentication.
- The HSM is deployed at the untrusted testing site to establish secure communication with remote PUF database and subsequent asset provisioning via AMI.
- The hardware security module is fully trusted and it is inaccessible to the attackers.

Flow of Operation:

The PUF-based authentication process requires several components to authenticate the IC, *e.g.*, trusted HSM, cloud-based AMI, and the chip with PUF architecture.

- First, a secure communication channel is established between the chip under test and the HSM using secure key exchange protocol such as DH. The process is similar to the prior description in watermark based authentication.
- Second, the HSM inquires the PUF response of the chip by sending the appropriate challenges obtained from the AMI. Upon reception of the challenge vector from the HSM, the PUF IP of the chip generates the unique responses procured from the PUF circuitry. Based on the implementation of the PUF, the responses can be uninitialized values of SRAM circuitry or values extracted from race conditions of different kinds of specialized circuitry such as ring oscillators, arbiters, etc.
- Third, HSM verifies the PUF responses procured from the IC by comparing those with the golden references obtained from the PUF database. In case of a match, the HSM approve the asset provisioning and the crypto keys and security specifications are sent to the internal storage of the chip. HSM disallows the provisioning in the event of a mismatch.

Security Vulnerability Analysis: A key security aspect of PUF-based authentication is that it prevents the attacker from extracting PUF signatures from the chip. The attacker at the testing site cannot exploit stolen CRPs to launch a masquerading attack with fake chips. However, given the collusion between the malicious entities in the testing facility and the foundry, the attackers can fabricate identical clone chips with internal observable nodes. The minimal alteration of inserting observable nodes in the original chip layout doesn't require detailed knowledge about the design. Hence, the attacker can use such altered, cloned chip to perform secure asset provisioning via HSM and then, extract the assets afterwards with the help of internal observable nodes.

5.3 Design Obfuscation via Logic Locking

Obfuscating IC designs by inserting key gates and finite state machines is a proven solution to limit the attacker's access to the chips fabricated in untrusted foundries. It is challenging for the attacker to reverse engineer a locked IC for cloning and overproducing. Such locking mechanisms give the OEM fine-grained control over the locked ICs in remote foundries and testing sites.

Assumptions:

- The obfuscated chips are manufactured with locking features.
- The HSM authenticates the locked chips via PUF or watermarking based techniques.
- The HSM is fully trusted.

Flow of Operation:

- The secure communication channel between the locked IC and the HSM is established via standard secure key exchange protocol such as DH. The process is similar to the ones described in watermark and PUF-based authentication.
- Once the secure channel is established, the IC is authenticated via watermark or PUF-based challenge-reponse technique. Upon authentication, the logic locking keys are deployed to the chip via HSM to unlock the chip for structural and functional testing.
- Note that the provisioning of unlocking keys is a natural use case as most ICs are initially unlocked and tested at the foundry and testing site for manufacturing defects and fulfilment of functional requirement.

Security Vulnerability Analysis: The weakest aspect of the logic locking based IC protection mechanism is that the chips are unlocked at the untrusted testing site for structural and functional testing. It essentially means the chips are never truly locked during the testing and provisioning phase and the attackers can leverage this weak link of the process to exploit the unlocked, provisioned chips. The degree of exploitation can range from asset leakage and IC piracy to reverse engineering for cloning and overproduction.

6 RELATED WORK

Fabrication and Testing Time Attacks: The attack space during fabrication has been explored extensively over the past decade. We discuss some of the attacks that can bypass the enforced methods for logic locking, PUF based authentication and different encryption techniques. The encrypted design netlist can be attacked and assessed by sensitizing the logic locking bits to the outputs of an unlocked IC via brute force or employing custom test pattern generation frameworks [10]. The scope of security invoked by using a logic locking or encryption based design can also be reduced by using SAT-based tools. These tools explore the overall design space and with every iteration, get that much closer to eliminating the incorrect keys to the locked design and gain access to the original netlist [13]. Hill climbing attacks employ specific test patterns by obtaining the zero hamming distance between the locked design and the test response signals [9]. **Existing Defense Mechanisms:**

There have been numerous proposed techniques to implement logic locking, PUF-based authentication, and watermarking techniques to alleviate the extent of attacks at untrusted foundries and testing facilities [2, 5–7, 11]. The default strategy of implementing logic locking is by using a finite state machine (FSM) based state space obfuscation. In this technique, the design is unlocked by providing a valid input vector that unlocks the FSM and the design under test. The FSM on entering the correct state unlocks the design for normal operation [2]. Random generation and insertion of XOR-based key gates have also been illustrated in the past to unlock ICs at the foundry and testing facilities [11]. PUF based authentication to enable remote locking of ICs using unique authentication IDs generated from the PUFs has been extensively explored [5, 7]. To prevent IP piracy and uncontrolled production, IP watermarking techniques have also been developed to counter these vulnerabilities at the untrusted foundry and testing sites via the use of embedded watermarks for digital signatures [6]. Safeguards like logic locking, authentication and watermarking are only effective to an extent. They do not provide a concrete standard for thwarting attacks in untrusted testing facilities. Thoroughly testing and verifying the design at the testing facility requires the design to be unlocked, so that the functionality and asset provisioning can be verified. This presents a passage for attackers to bypass the enforced security safeguards and compromise the integrity of the entire fabrication process.

7 CONCLUSION

In this paper, we have studied the state-of-the-art defense mechanisms employed for secure IC provisioning at untrusted testing facilities and foundries. We analyzed potential threats and vulnerabilities stemming from colluding adversaries at the testing site and the foundry. More importantly, our analysis suggests that traditional IC protection mechanisms such as IC watermarking, PUF-based authentication, and hardware obfuscation cannot prevent the attackers at rogue foundries and testing sites from stealing IC assets, maliciously altering the chips, and overproducing chips by exploiting the attack surfaces available during asset provisioning. The presence of a HSM at the untrusted environment does not thwart the attackers as the ICs are fully unlocked for during testing and provisioning. The attackers exploit these unlocked, clone chips to securely procure assets from AMI via trusted HSM. Our work highlights one of the weakest links of current IC supply-chain and we believe that security analysis of IC provisioning would encourage the security researchers to further explore and design defense mechanisms capable of mitigating attacks during provisioning at remote untrusted facilities.

REFERENCES

[1] Defense Microelectronics Activity. 2017. *DMEA Trusted IC Program.* https://www.dmea.osd.mil/TrustedIC.aspx/.

[2] R. S. Chakraborty and S. Bhunia. 2009. HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 28, 10 (2009), 1493–1502. https://doi.org/10.1109/TCAD.2009.2028166

[3] Atul Prasad Deb Nath, Srivalli Boddupalli, Swarup Bhunia, and Sandip Ray. 2020. Resilient System-on-Chip Designs With NoC Fabrics. *IEEE Transactions on Information Forensics and Security* 15 (2020), 2808–2823. https://doi.org/10.1109/TIFS.2020.2977534

[4] Atul Prasad Deb Nath, Sandip Ray, Abhishek Basak, and Swarup Bhunia. 2018. System-on-chip security architecture and CAD framework for hardware patch. In *2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC).* 733–738. https://doi.org/10.1109/ASPDAC.2018.8297409

[5] F. Koushanfar. 2012. Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management. *IEEE Transactions on Information Forensics and Security* 7, 1 (2012), 51–63. https://doi.org/10.1109/TIFS.2011.2163307

[6] F. Koushanfar and Y. Alkabani. 2010. Provably secure obfuscation of diverse watermarks for sequential circuits. In *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST).* 42–47. https://doi.org/10.1109/HST.2010.5513115

[7] Aswin Raghav Krishna, Seetharam Narasimhan, Xinmu Wang, and Swarup Bhunia. 2011. MECCA: A Robust Low-Overhead PUF Using Embedded Memory Array. In *Cryptographic Hardware and Embedded Systems – CHES 2011*, Bart Preneel and Tsuyoshi Takagi (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 407–420.

[8] Bill McClean. 2020. *McClean Report: A Complete Analysis and Forecast of the Integrated Circuit Industry.* https://www.icinsights.com/news/bulletins/Fabless-Company-Share-Of-IC-Sales-To-Set-New-Record-In-2020-At-329-/.

[9] S. M. Plaza and I. L. Markov. 2014. Protecting integrated circuits from piracy with test-aware logic locking. In *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD).* 262–269. https://doi.org/10.1109/ICCAD.2014.7001361

[10] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri. 2012. Security analysis of logic obfuscation. In *DAC Design Automation Conference 2012.* 83–89. https://doi.org/10.1145/2228360.2228377

[11] J. A. Roy, F. Koushanfar, and I. L. Markov. 2008. EPIC: Ending Piracy of Integrated Circuits. In *2008 Design, Automation and Test in Europe.* 1069–1074. https://doi.org/10.1109/DATE.2008.4484823

[12] Reuters Staff. 2017. *TSMC says latest chip plant will cost around $20 bln.* https://www.reuters.com/article/tsmc-investment/tsmc-says-latest-chip-plant-will-cost-around-20-bln-idUSL3N1O737Z.

[13] P. Subramanyan, S. Ray, and S. Malik. 2015. Evaluating the security of logic encryption algorithms. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST).* 137–143. https://doi.org/10.1109/HST.2015.7140252