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