Trusted and Secure Design of Analog/RF ICs: Recent Developments

Kiruba Subramani, Georgios Volanis, Mohammad-Mahdi Bidmeshki, Angelos Antonopoulos, and Yiorgos Makris
Department of Electrical and Computer Engineering, The University of Texas at Dallas

***Abstract*—Unlike the extensive research effort that has been expended over the last 15 years in understanding the threats of hardware Trojans, piracy and counterfeiting of digital Integrated Circuits (ICs), and in developing appropriate prevention and detection solutions, the topic of security and trust remains in a rather nascent state for their analog/radio-frequency (RF) counterparts. Indeed, as shown in a recent survey, which summarized and presented the available body of knowledge in trusted and secure design of analog/RF ICs, our understanding of the pertinent threats and our ability to thwart them through existing solutions are both rather limited. However, given the widespread use of analog functionality (i.e., physical interfaces, sensors, actuators, wireless communications, etc.) in most contemporary systems, comprehending their vulnerabilities and devising pertinent remedies is urgently required. In this paper, we discuss the limitations of the current state-of-the-art in this field, we highlight recent developments, and we suggest research directions and steps to be taken toward designing, fabricating and deploying trusted and secure analog/RF ICs.**

I. Introduction

Modern semiconductor devices are fabricated through a complex IC supply chain that involves thousands of specialized companies that are situated all over the world. In addition, to tackle the time-to-market pressure, semiconductor companies are relying heavily on third party CAD tools and circuit Intellectual Property (IP) to complete their designs. However, the globalized and highly distributed nature of the third-party entities has resulted in several vulnerable points in the IC supply chain ranging from design, fabrication and even after deployment of the IC, wherein the device can become a target to hardware Trojan attacks, reverse engineering and counterfeiting. As a result, ensuring the security and trustworthiness of modern ICs has become a huge challenge for the semiconductor industry, especially when these devices are used in sensitive applications such as military, infrastructure, banking, automotive and telecommunications.

Research groups from industry, academia and government entities have conducted extensive studies to understand and counteract this problem in the digital domain. However, similar initiatives and research activities are largely missing in the Analog/RF domain, whose components are predominantly used in the front-end of modern wireless and sensor networks. To this end, this survey paper intends to highlight some of the recent developments in the design of trusted and secure analog/RF ICs, an overview of which is provided in Figure 1.

II. Information Leakage through Covert Channel

Analog/RF ICs are predominantly used in modern wireless devices to facilitate the transmission and reception of data packets through a wireless communication channel. Among the various security challenges investigated in a wireless device, the majority focus on vulnerabilities in the software, firmware and baseband domain [1], [2]. To date, however, very few research groups have investigated vulnerabilities in the analog/RF front-end of a wireless device that can facilitate hardware Trojan attacks. Here, the Trojan circuit has primarily been used to exfiltrate secretive information from the targeted device by means of covert communication channels. In the following sections, we summarize recent research efforts focusing on hardware Trojan attack and defense mechanisms that are geared towards information leakage using covert channels.

A. Attacks

Hardware Trojan in an IEEE 802.11a/g Network: Analog/RF hardware Trojan based covert channels have primarily been demonstrated using simple wireless links, rather than standards-compliant devices. Beyond these simple methods, [3] introduced and experimentally demonstrated a hardware Trojan circuit that was implemented in the RF front-end of a WLAN transceiver. The malicious circuit exploits process variation margins of the targeted IC to establish a covert channel that leaks sensitive information. Essentially, the hardware Trojan systematically modifies the termination impedance of a targeted RF component to create variations in its input reflection coefficient and gain, which in turn can be exploited to leak information through imperceptible transmitted power variations. Effectiveness of the Trojan circuit was experimentally assessed in [3], where the authors demonstrated the ability of the Trojan circuit to robustly exfiltrate information without significantly affecting the legitimate communication.

B. Defenses

Traditional post-production tests are ineffective in detecting malicious hardware Trojan circuits because (i) the area and power overhead introduced by the Trojan circuit is negligible, (ii) the Trojan operation does not violate the targeted circuit specifications, and (iii) the Trojan operation characteristics are hidden within the process variation margins. To address this problem, several hardware Trojan defense techniques have been recently proposed in the literature, as discussed below.

Adaptive Channel Estimation: Modern wireless devices use channel estimation algorithm to determine the channel conditions and effectively retrieve the transmitted signal. In the presence of a hardware Trojan, however, current channel estimation algorithms bundle together the channel non-idealities with the perturbations introduced by a Trojan circuit. To resolve this problem, an Adaptive Channel Estimation (ACE) based defense was proposed in [3] to detect analog/RF Trojans

978-1-7281-2490-2/19/$31.00 ©2019 IEEE

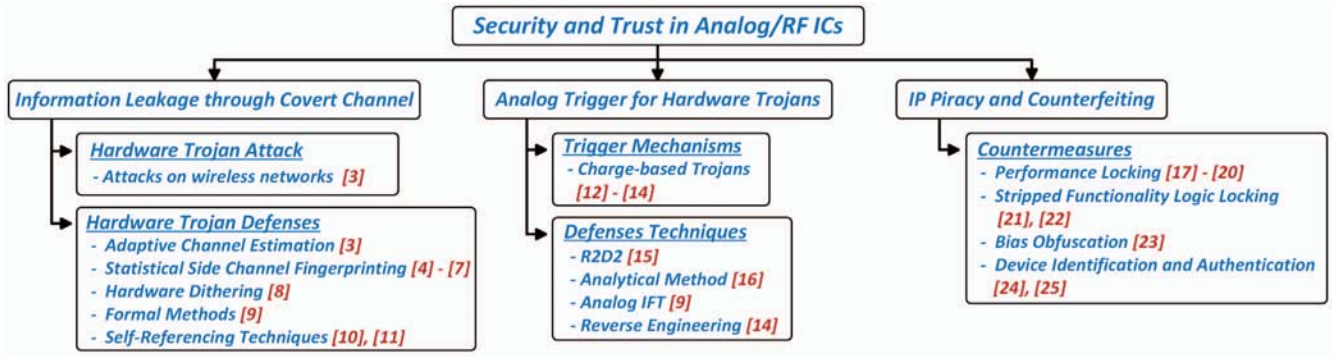

Fig. 1. An overview of recent developments in analog/RF security and trust

that modify the transmission characteristics of a standards-compliant wireless device. The proposed defense leverages the slow-fading traits of an indoor wireless channel to distinguish between channel-induced and Trojan-induced impact on the legitimate signal. Effectiveness of the defense was verified in [3] by conducting experiments in actual channel conditions such as over-the-air and in the presence of interferers.

Statistical Methods: Semiconductor devices have side-channel parameters or fingerprints such as power, delay, temperature, current, etc., which can be used to statistically assess whether an IC belongs to a trusted population or not. Based on this principle, in [4]–[7], the authors proposed a statistical side-channel fingerprinting technique for detecting Analog/RF hardware Trojans in a wireless cryptographic IC. The proposed defense relies on the systematic variations introduced by the hardware Trojan in the transmitted signal characteristics, namely power and frequency, to expose the malicious operation. Effectiveness of the technique has been evaluated using actual silicon measurements from a wireless cryptographic IC that was fabricated in TSMC 350nm technology.

Hardware Dithering: Semiconductor devices typically have a fixed operating point in a multi-dimensional performance space to achieve optimum performance. However, for hardware Trojans that seek to leak information by systematically inducing an offset in the performance space, the fixed operating point serves as a reference for an adversary to extract the leaked information bits. To address this problem, in [8], a run-time hardware Trojan neutralization technique was proposed, such that the operating point of the targeted device is moved around in the performance space in a random fashion. As a result, the reference point used by the adversary to retrieve the leaked bits becomes a moving target, thereby significantly reducing the SNR of the covert channel. This defense technique has been evaluated on a wireless cryptographic IC, where the experimental results show a significant increase of the bit error rate of the covert channel.

Formal Methods: Information Flow Tracking (IFT), which is an effective methodology to detect security threats in the software and digital domain, has also been extended to cover analog/mixed-signal designs [9]. This methodology implements IFT at the transistor-level and works by getting a Verilog netlist of the analog/mixed-signal design and converting it to a formal representation in Coq, in which proof development and checking is performed. This work provides a framework called analog enhanced *VeriCoq-IFT* for converting the design to Coq representation, generating the required security properties and creating their proofs, automatically. A demonstration using this framework showed that such an IFT approach is capable of detecting information leakage paths crossing the analog and the digital domains, including the Trojans in wireless cryptographic ICs described previously in this section.

Trojan-Detection through Self-Referencing: In [10], [11], the authors proposed a run-time Trojan defense that uses self-referencing, instead of golden ICs, to detect the malicious activity. Essentially, in a Trojan infested communication, signal variations introduced by the hardware Trojan are masked by the legitimate circuit response and noise from the communication environment. Since the Trojan operation exhibits a band-limited spectral response, it can be easily distinguished from the environmental noise, which has a flat response. To decouple the primary circuit response, however, the authors use a test stimulus that can be differentiated from the Trojan response using signal processing techniques.

III. Analog Triggers for Hardware Trojans

To evade detection by manufacturing tests, hardware Trojans use trigger mechanisms which are rarely activated during normal operation of an IC. Several studies utilize analog techniques to design such stealthy triggers, which are more difficult to uncover due to their smaller footprints, as compared to their digital counterparts. In this section, we review some of the attack and detection mechanisms introduced in this area.

A. Attacks

A2 [12] uses switched capacitors to design a trigger circuit which is activated when the frequency of toggling on a victim wire goes above a certain threshold. The victim wire normally has a low toggling activity to prevent accidental triggering. The circuit has minimal footprint, close to a typical digital gate, and using this mechanism, A2 implements a Trojan which can escalate the process privilege running in user mode on a microprocessor. Following a similar concept, [13] exploits resistance drift under pulsing current of resistive RAM (RRAM) elements to introduce triggers which are activated after some delay, or operate based on specific voltage thresholds.

A recent study exploits capacitor couplings in deep submicron process technologies to design Trojans with zero active area footprint [14]. This technique only uses rerouting and extending of existing layout tracks to increase the capacitive coupling between a victim and an aggressor wire in a way that a low to high transition on the aggressor can adequately affect the victim wire and flip its digital value. Using this approach, authors in [14] demonstrated, in simulation, Trojans which are capable of leaking a secret key in a cryptographic core, or escalating the user process privilege in a microprocessor IP.

B. Defenses

Since excessive toggling activity on a victim wire is a key characteristic of Trojans such as A2 [12], R2D2 [15] adds on-chip monitors to measure switching activity on potential victim wires during an adjustable time period and raises an alarm if such activity goes above a certain threshold. This method can be effective for detecting A2. However, it adds area and power overhead to a design and requires careful tuning of the time period and frequency threshold to reduce false positive and false negative alarms. Also, based on non-volatility of RRAM elements, the method in [13] can use sporadic pulses which may not be detected by the R2D2 approach.

A recent study [16] introduced an analytical framework for detecting switched capacitor based trigger circuits such as A2. The proposed method starts by searching the design for a minimum capacitance value that is required to realize such trigger circuits. Then, it traces the connectivity of such capacitors back to a user controllable input, if it finds a specific circuit pattern. This methodology is limited in scope and does not consider other types of switched capacitor circuit configurations, which can also serve as Trojan triggers.

Analog information flow tracking [9], which was mentioned before as a formal method in Section II-B, has also been demonstrated to be capable of detecting such malicious designs. Although promising, this approach currently does not consider circuit parameters such as component values, but only focuses on the circuit structure, which may result in false positives in malicious circuit detection.

In [14], the authors propose a reverse engineering based detection methodology by sorting trace lengths in a layout based on the requirement that long trace lengths are necessary for realizing the minimum capacitance needed for such Trojans. As the authors point out, an attacker may be able to find ways to mitigate this requirement, e.g. by using multiple layers or higher voltages, and evade detection by this approach.

IV. IP Piracy and Counterfeiting

A. Threats

IC piracy, which includes counterfeited ICs, overproduction and unauthorized use of ICs, is among the main threats that IP should be protected against. To this end, preventing the operation of fabricated ICs until they are received from the foundry is a potential approach for IP protection. As a result, various IC locking methods have been proposed so far mostly targeting digital ICs. The main idea here is to hide the functionality of the digital IC by adding extra logic gates and key inputs. Only by applying the correct key, the IC will implement the correct Boolean function. On the other hand, locking the design of an analog IC is a more challenging task. Rather than locking functionality, which is very challenging if at all possible while designing analog ICs, locking performance is a potential solution of the problem. It is based on the fact that the performance of an analog IC can be fine-tuned by design parameters, such as transistor dimensions or biases. Specifically, only when a correct key is provided, the IC will operate within its specification limits.

B. Countermeasures

Performance Locking: Lately, several research efforts on security of analog ICs following the performance locking paradigm have appeared in the literature. In [17], a locked configurable memristor-based voltage divider is used to bias the body voltage of the transistors in the input differential pair of a sense amplifier. The correct key will configure the memristor crossbar array, so that a proper voltage is produced by the voltage divider which, in turn, will eliminate the mismatch in the differential pair. However, until memristors become available in conventional CMOS processes, this methodology is of limited utility.

Three methods [18]–[20] explore the idea of combinational locking of biasing currents in analog circuits. In [18], the bias is obfuscated by using multiple branches of biasing transistors connected in parallel. The number of on-transistors is controlled by a digital key and, theoretically, only the correct key can bias the circuit to the desired operating point. However, there exist multiple correct keys and the analog IC performance degradation from the application of incorrect keys could be small. To ameliorate these limitations, the locking of biasing currents is combined with Satisfiability Modulo Theory (SMT) techniques in [19], [20]. In [20], instead of parallel connected transistors, a mesh based topology of transistors is proposed. In [19], a configurable current mirror is designed and by, additionally, applying a hardware metering technique a unique key per chip is ensured.

Two more recent works [21], [22] employ a logic locking technique, called stripped functionality logic locking, on the digital section of the mixed-signal IC. In [22], a Sigma-Delta Analog to Digital Converter (SD-ADC) is used as a case study. The digital part of the SD-ADC consists of a mixer and a decimation filter. The aim is to lock the signal-to-noise ratio (SNR) performance of the SD-ADC by locking the sub-circuit that drives one bit line of the decimation filter. In [21], the digital circuit that is used to tune the analog IC after fabrication is locked such that only by providing the correct key the effect of process variations is eliminated, and the analog IC performs as desired.

Nevertheless, in all the aforementioned methods, the key remains in the digital domain and only indirectly affects design performance by controlling the interconnect between devices that make up the biasing network. In [23], a method is proposed for protecting analog ICs against unauthorized use

by obfuscating their biases through an analog neural network. Essentially, the trained neural network acts as a lock that provides the desired bias voltages to an IC only if the correct analog key is applied at its inputs. In other words, only the input of the neural network that corresponds to the correct key will result in the IC operating within its specification limits.

Device Identification and Authentication: Semiconductor devices experience process variation during manufacturing, which introduce inherent performance variations across fabricated devices. As a result, any two devices from a batch of manufactured ICs exhibit different performance characteristics and this effect is predominantly visible in analog/RF ICs. Such inherent variations can be exploited to develop defense solutions than can play a critical role in combating counterfeiting and IP piracy problems in the analog/RF domain. Along these lines, in [24], the authors propose a deep learning based solution to uniquely identify RF transmitters by leveraging the non-linear characteristics exhibited by a power amplifier. Here, the authors have evaluated the trained model under various factors concerning the effects of signal quality, packet length, channel model and modulation type and have demonstrated the effectiveness of the solution. Similarly, in [25], the author proposes to use Process Specific Function (PSFs) for authenticating analog mixed-signal ICs such as data converters. Here, harmonic frequencies and their corresponding magnitude levels in the output waveform of an IC are used to develop the PSF-based device identification model. Accordingly, for a Digital-to-Analog converter, experimental results have revealed that the PSF model has a probability of detection of 90% with a false alarm rate of 10%.

V. Conclusion

After decades of extensive research activities to address the security and trustworthiness problems in the digital domain, the semiconductor industry is starting to realize the repercussions of the same issues stemming from the analog/RF components, which have remained largely ignored so far. Therefore, there is a recent surge in the number of research activities in this area, the majority of which are geared towards understanding and counteracting these problems in the analog/RF domain. Yet, significant research efforts are still needed to develop security and trustworthiness solutions for this domain. This survey paper highlighted some of the recent accomplishments in this area towards the aforementioned goal.

References

[1] K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "Demonstrating and Mitigating the Risk of an FEC-based Hardware Trojan in Wireless Networks," *IEEE Transactions on Information Forensics and Security, doi:10.1109/TIFS.2019.2900906*, 2019.

[2] P. M. Harley, M. Tummala, and J. C. McEachen, "High-Throughput Covert Channels in Adaptive Rate Wireless Communication Systems," in *IEEE International Conference on Electronics, Information, and Communication (ICEIC)*, 2019, pp. 1–7.

[3] K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "ACE: Adaptive Channel Estimation for Detecting Analog/RF Trojans in WLAN Transceivers," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2017, pp. 722–727.

[4] Y. Liu, Y. Jin, and Y. Makris, "Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Method Evaluation," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2013, pp. 399–404.

[5] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, "Silicon Demonstration of Hardware Trojan Design and Detection in Wireless Cryptographic ICs," *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, vol. 25, no. 4, pp. 1506–1519, 2017.

[6] Y. Liu, K. Huang, and Y. Makris, "Hardware Trojan Detection Through Golden Chip-Free Statistical Side-Channel Fingerprinting," in *ACM Design Automation Conference (DAC)*, 2014, pp. 1–6.

[7] Y. Liu, G. Volanis, K. Huang, and Y. Makris, "Concurrent Hardware Trojan Detection in Wireless Cryptographic ICs," in *IEEE International Test Conference (ITC)*, 2015, pp. 1–8.

[8] C. Kapatsori, Y. Liu, A. Antonopoulos, and Y. Makris, "Hardware Dithering: A Run-Time Method for Trojan Neutralization in Wireless Cryptographic ICs," in *IEEE International Test Conference (ITC)*, 2018, pp. 1–7.

[9] M.-M. Bidmeshki, A. Antonopoulos, and Y. Makris, "Information Flow Tracking in Analog/Mixed-Signal Designs through Proof-Carrying Hardware IP," in *Design, Automation and Test in Europe Conference Exhibition (DATE)*, March 2017, pp. 1703–1708.

[10] F. Karabacak, U. Y. Ogras, and S. Ozev, "Detection of Malicious Hardware Components in Mobile Platforms," in *IEEE International Symposium on Quality Electronic Design (ISQED)*, 2016, pp. 179–184.

[11] F. Karabacak, U. Ogras, and S. Ozev, "Remote Detection of Unauthorized Activity via Spectral Analysis," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 23, no. 6, p. 81, 2018.

[12] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog Malicious Hardware," in *IEEE Symposium on Security and Privacy (SP)*, May 2016, pp. 18–37.

[13] K. Nagarajan, M. N. I. Khan, and S. Ghosh, "ENTT: A Family of Emerging NVM-based Trojan Triggers," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2019.

[14] C. Kison, O. M. Awad, M. Fyrbiak, and C. Paar, "Security Implications of Intentional Capacitive Crosstalk," *IEEE Transactions on Information Forensics and Security, doi:10.1109/TIFS.2019.2900914*, 2019.

[15] Y. Hou, H. He, K. Shamsi, Y. Jin, D. Wu, and H. Wu, "R2D2: Runtime Reassurance and Detection of A2 Trojan," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, April 2018, pp. 195–200.

[16] X. Guo, H. Zhu, Y. Jin, and X. Zhang, "When Capacitors Attack: Formal Method Driven Design and Detection of Charge-Domain Trojans," in *Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2019, pp. 1706–1711.

[17] D. H. Hoe, J. Rajendran, and R. Karri, "Towards Secure Analog Designs: A Secure Sense Amplifier using Memristors," in *IEEE Computer Society Annual Symposium on VLSI*, 2014, pp. 516–521.

[18] V. V. Rao and I. Savidis, "Protecting analog Circuits with Parameter Biasing Obfuscation," in *IEEE Latin American Test Symposium (LATS)*, 2017, pp. 1–6.

[19] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sánchez-Sinencio, and J. Hu, "Thwarting Analog IC Piracy via Combinational Locking," in *IEEE International Test Conference (ITC)*, 2017, pp. 1–10.

[20] V. V. Rao and I. Savidis, "Mesh Based Obfuscation of Analog Circuit Properties," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2019, pp. 1–5.

[21] N. G. Jayasankaran, A. S. Borbon, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, "Towards Provably-Secure Analog and Mixed-Signal Locking against Overproduction," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2018, p. 7.

[22] J. Leonhard, M. Yasin, S. Turk, M. T. Nabeel, M. M. Lourat, R. Chotin Avot, H. Aboushady, O. Sinanoglu, and H. G. Stratigopoulos, "MixLock: Securing Mixed-Signal Circuits via Logic Locking," in *Design, Automation & Test in Europe (DATE)*, 2019.

[23] G. Volanis, Y. Lu, S. G. R. Nimmalapudi, A. Antonopoulos, A. Marshall, and Y. Makris, "Analog Performance Locking through Neural Network-based Biasing," in *IEEE VLSI Test Symposium (VTS)*, 2019, pp. 1–6.

[24] S. S. Hanna and D. Cabric, "Deep Learning Based Transmitter Identification using Power Amplifier Nonlinearity," in *IEEE International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 674–680.

[25] M. J. Casto, "Multi-Attribute Design for Authentication and Reliability (MADAR)," Ph.D. dissertation, The Ohio State University, 2018.