Security and Trust for Wireless Integrated Circuits

Presented by Alán R. Díaz Rizo
Doctoral Advisors: Haralampos-G Stratigopoulos and Hassan Aboushady

Context of the thesis

IC supply chain vulnerabilities and threats

The origin of the hardware security threats is the massively globalized and outsourcing-based Integrated Circuit (IC) supply chain that we see today. The prohibitive cost of owning a first-rate semiconductor foundry forces IC design houses to go *fabless* and outsource their IC fabrication, assembly, and testing. Outsourcing these tasks intensifies the risk of Hardware Trojan (HT) insertion and IC piracy attacks, i.e., cloning, overproducing, remarking, and recycling. Both threats translate into know-how and financial losses for the IC owner. Moreover, complex Systems-on-Chip (SoCs) are built by integrating third-party Intellectual Property (IP) cores from multiple IP providers. However, SoC integrators and IP providers have an imbalanced trust relationship. While IP providers are vulnerable to IP overuse, IP cloning, and IC overproduction, SoC integrators fear integrating HT-infected IPs into their systems.

Consequences of IP/IC piracy and HT insertion

Piracy of ICs has been a major security threat since the past few decades. For instance, in 2011, VisionTech Components sold counterfeit semiconductor chips to more than 1,100 customers in every sector of the electronics industry, including the military [8]. With respect to governments and consumers, in a report [9] out in march 2022, the European Union's law enforcement agency Europol highlighted the risks posed by counterfeit semiconductors to critical infrastructure as well as to people's private devices. Concerning the industry, cloning and overproducing result in know-how and financial losses for the IP/IC owner. IP piracy issues alone incur annual losses up to \$4 billion for the semiconductor industry [10]. In addition to the loss of revenue suffered by counterfeit victims, estimated at \$100 billion annually for the entire electronics industry, due to counterfeit semiconductors, end users and the systems that comprise them can suffer premature or critical failures [11].

The commercialization of HT-infected ICs could permanently damage a company’s reputation and trust. In addition, an IC leaking users' private information puts security and respect for privacy at risk. A HT could be a time bomb that can be triggered under specific conditions controlled by the attacker, leading in a complete denial-of-service while the chip is in the field. Furthermore, considering that the IC supply chain is complex and not necessarily each actor in the chain knows and controls all the stakeholders involved, the infiltration of counterfeit or tampered ICs affects more than one actor. Therefore, its negative effect is difficult to fully assess.

IC supply chain attacks target wireless ICs because wireless ICs have a critical role in society, government and industry, and they exchange sensitive and valuable information through a publicly accessible medium. Therefore, this thesis focuses on wireless ICs and addresses two IC supply chain attacks: IP/IC piracy and HT insertion.

State-of-the-Art (SoA)

Hardware Trojans in RF transceivers

The vast majority of HT designs target digital ICs. For analog ICs, HT insertion is more challenging because analog performance is sensitive to circuit alterations. Targeting RF transceivers, a covert channel is a HT attack in wireless ICs aiming at leaking sensitive information from the transmitter within a legitimate signal transmission. A rogue receiver can listen to the transmission to recover the sensitive information, while the legitimate receiver is inconspicuous and does not realize the information leaking. The HT can be embedded within the digital baseband physical layer (PHY). For instance, in [12], a PHY HT attack is staged in the Forward Error Correction (FEC) block, exploiting the fact that the FEC block offers more error correcting capabilities than the channel needs. In addition, the HT payload mechanism can partially act upon the Analog Front-End (AFE). E.g., two AFE HT payload mechanisms are shown in [13], one that uses a single pole double throw switch and a pair of resistors to alter the input termination impedance of the power amplifier, and another one that reprograms the gain stages.

In parallel, most SoA studies also analyze resilience to various defenses, oftentimes finding a working defense. Defenses range from standard measurements, e.g., Signal to Noise Ratio (SNR), or Bit Error Rate (BER); examining standard compliance; analyzing I/Q constellation diagrams, etc., to more elaborate techniques such as Statistical Side-Channel Fingerprinting (SSCF), i.e., using a one-class classifier to distinguish HT-infected from HT-free devices; Adaptive Channel Estimation (ACE) [13], i.e., leveraging slow-fading characteristics of indoor communication channels to distinguish between channel impairments and HT activity; and channel noise profiling [12].

Anti-Piracy design techniques for RF transceivers

The three major categories of anti-piracy measures used in RF transceivers are split manufacturing, which prevents overproduction and cloning from an untrusted foundry; camouflaging, which obfuscates the hardware to protect the IC against reverse engineering; and locking, which offers end-to-end protection against all potential piracy threat scenarios. Logic Locking (LL) is the strongest locking defense and consists in embedding a lock mechanism inside the IP/IC. The lock mechanism is a circuit that is mingled with the original circuit breaking its functionality unless the correct key is applied. The first LL technique was originally proposed for digital circuits [14]. Since then, several LL defenses and counterattacks were proposed.

LL defenses are classified into three main sets, traditional XOR-based, SAT-attack resilient, and Corrupt-And-Correct (CAC) defenses. LL Attacks are also grouped into three major sets, brute-force and optimization, input-output query, and structural attacks. Traditional XOR-based defenses insert XOR/XNOR key-gates into the design. They are efficient against brute-force and optimization attacks, but vulnerable to I/O query attacks. Attacks based on Boolean satisfiability (SAT), e.g., [15], belong to the I/O query attacks category and can break traditional logic locking approaches, e.g., [14], by recovering the key with little effort. To thwart I/O query attacks, researchers used point-functions as the protection logic. For instance, the Anti-SAT defense [16] thwarts any I/O attack by rendering the SAT attack computationally infeasible. However, the point-function can be identified and removed or bypassed by performing a structural attack. To thwart structural attacks, researchers developed a subset of point-function-based techniques called CAC defenses, e.g., [17]. They rely on their structure to be merged and hidden after logic synthesis. However, this hypothesis was not proven strong and more sophisticated structural attacks were developed that identify and recover the secret key, e.g., [18].

Scientific Results

The findings of this thesis that contribute to the SoA are presented below by publication.

The research results published in [1] made the following contributions to the SoA:

1. A comprehensive study on the evolution of thinking in HT attack models.
2. A novel post-silicon, run-time, and low-cost correlation-based defense to detect HT activity hidden in the synchronization data.
3. A novel HT attack model than can thwart any post-silicon defense mechanism. We proposed the Amplitude Modulation (AM) Short Training Sequence (STS) HT attack for leaking sensitive data out of wireless ICs. The AM STS HT attack acts on the synchronization preamble, does not affect the normal RF transceiver operation or link performance, and only increases the area overhead of the PHY by 0.109%.
4. We demonstrated with hardware measurements the AM STS HT attack from the attacker's perspective where an encrypted message with a 128-bit secret key is being leaked. We analyzed the reliability of the covert channel and demonstrated how the key can be successfully recovered even in the most unfavorable SNR scenario.

The research results published in [2] made the following contributions to the SoA:

1. We demonstrated for the first time locking against piracy of entire RF transceivers at the system-level. The methodology is based on LL of digital blocks in the signal processing chain. The methodology is virtually applicable to any RF transceiver architecture.
2. We showed that generic LL techniques cannot be blindly applied in the context of Analog/Mixed-Signal ICs. To this end, we employed the state-of-the-art SFLL-rem [17] LL technique and showed how to fine-tune it for effective RF transceiver locking.
3. A proof-of-concept is demonstrated with hardware measurements using a Software Defined Radio (SDR). Hardware experiments demonstrated effective BER degradation for incorrect keys while achieving zero performance penalty when applying the single correct secret key, and 3.9% and 0.3% of area and power overheads.
4. We analyzed the resilience against all foreseen key-recovery attacks.

The research results published in [3,4,7] made the following contributions to the SoA:

1. We presented *SyncLock*, a novel and innovative anti-piracy design technique for RF transceivers. *SyncLock* is an RF transceiver-specific LL technique that acts on the synchronization of the transmitter with the receiver. Upon application of an incorrect key, *SyncLock* disables the synchronization, thus the wireless communication link crashes.
2. *SyncLock* is based on two spatially separated hardware-level mechanisms. The first mechanism hides a hard-coded error into the design of the data frame generator corrupting the preamble of the data frame. The second mechanism is located upstream in the signal processing chain into the preamble generator and its goal is to corrupt the preamble so as to cancel out the downstream corruption. The corruption applied by the second mechanism is key-controlled with the key being sourced from a Tamper-Proof Memory (TPM). There exists a single correct key that can counterbalance the two preamble corruptions.
3. *SyncLock* is generally applicable to any RF transceiver architecture, for any wireless communication protocol using correlation-based synchronization algorithms, and for any modulation scheme.
4. *SyncLock* elegantly achieves all locking objectives: (a) locking is transparent to the RF transceiver operation when the correct secret key is applied; (b) applying any invalid key breaks the RF transceiver operation; (c) incurs 1.22% of area overhead; (d) thwarts any known counter-attack in both the analog and digital domains.

Publications

[1] A. R. Díaz Rizo, H. Aboushady, and H.-G. Stratigopoulos. “Leaking Wireless ICs via Hardware Trojan-Infected Synchronization.” In: *IEEE Transactions on Dependable and Secure Computing* (2022), pp. 1–16. DOI: **10.1109/TDSC.2022.3218507**.

[2] A. R. Díaz Rizo, J. Leonhard, H. Aboushady, and H.-G. Stratigopoulos. “RF Transceiver Security Against Piracy Attacks.” In: *IEEE Transactions on Circuits and Systems II: Express Briefs* (2022), pp. 1–1. DOI: **10.1109/TCSII.2022.3165709**.

[3] A. R. Díaz Rizo, H. Aboushady, and H.-G. Stratigopoulos.“SyncLock: RF transceiver security using synchronization locking.” In: *2022 Design, Automation and Test in Europe Conference and Exhibition (DATE)*. IEEE. 2022, pp. 1153–1156

[4] A. R. Díaz Rizo, H. Aboushady, and H.-G. Stratigopoulos. “Anti-Piracy Design of RF Transceivers.” In: *IEEE Transactions on Circuits and Systems I: Regular Papers* (2022), pp. 1–14. DOI: **10.1109/TCSI.2022.3214111**.

Publications made in collaboration during the PhD

[5] J. Leonhard, N. Limaye, S. Turk, A. Sayed, A. R. Díaz Rizo, H. Aboushady, O. Sinanoglu, and H.-G. Stratigopoulos. “Digitally Assisted Mixed-Signal Circuit Security.” In: *IEEE TCAD* 41.8 (2022), pp. 2449–2462. DOI: **10.1109/TCAD.2021.3111550**.

[6] A. A. Ibrahim, H. A. Mohamed, A. R. Díaz Rizo, R. Parra-Michel, and H. Aboushady. “Tunable Filtenna With DGS Loaded Resonators for a Cognitive Radio System Based on an SDR Transceiver.” In: *IEEE Access* 10 (2022), pp. 32123–32131. DOI: **10.1109/ACCESS.2022.3160467**.

Patent filed during the PhD

[7] “Method for securing telecommunication transceiver integrated circuit designs against piracy, counterfeiting and unauthorized use.” PCT/FR2022/050437. A. R. Díaz Rizo, H. Aboushady, and H.-G. Stratigopoulos. Mar. 12, 2022.

Reduced Bibliography

[8] D. Takahashi. “Feds close huge chip counterfeiting case.” In: VentureBeat. 2011. url: https://bit.ly/3JjgoHf (visited on 09/25/2011).

[9] European Union Intellectual Property Office. Intellectual Property Crime Threat Assessment 2022. Report. EUROPOL, 2022.

[10] S. Smith. “SEMI: Innovation Is at Risk, Losses of up to $4 Billion Annually due to IP Infringement.” In: Nanotechnology Now. 2008. url: https://bit.ly/3bKz1r0 (visited on 08/08/2022)

[11] U.S. Dep. of Commerce and U.S. Dep. of Homeland Security. *Assessment of the critical supply chains supporting the U.S. information and communications technology industry*. Report, 2022.

[12] K. S. Subraman et al. “Demonstrating and mitigating the risk of an FEC-based hardware Trojan in wireless networks.” In: *IEEE Transactions on Information Forensics and Security* 14.10 (2019), pp. 2720–2734.

[13] K. S. Subramani et al. “Amplitude-modulating analog/rf hardware trojans in wireless networks: Risks and remedies.” In: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 3497–3510.

[14] J. A. Roy et al. “Ending piracy of integrated circuits.” In: *Computer* 43.10 (Oct. 2010), pp. 30–38.

[15] P. Subramanyan et al. “Evaluating the security of logic encryption algorithms.” In: *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE. 2015, pp. 137–143.

[16] Y. Xie et al. “Anti-SAT: Mitigating SAT Attack on Logic Locking.” In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 38.2 (2019), pp. 199–207. doi:10.1109/TCAD.2018.2801220.

[17] A. Sengupta et al. “Truly stripping functionality for logic locking: A fault-based perspective.” In: *IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems* 39.12 (2020), pp. 4439–4452.

[18] Z. Han et al. “Does logic locking work with EDA Tools?” In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021, pp. 1055–1072.