Thesis title:

Hardware Security and Trust for Mixed-Signal Integrated Circuits

Institution:

Sorbonne Université
French National Centre for Scientific Research (CNRS)
Computer Science Laboratory of Sorbonne University's Faculty of Science and Engineering (LIP6)

Location:

Paris, France

When:

Starting September or October 2023

Funding:

3-year PhD grant, ~2000€ monthly gross salary, social security benefits included.

Advisors:

Haralampos-G. Stratigopoulos, Research Director CNRS, Sorbonne Université, LIP6
Hassan Aboushady, Associate Professor, Sorbonne Université, LIP6

Context:

In the early days of the semiconductor industry, all the design know-how, Electronic Design Automation (EDA) tools, fabrication facilities, and test equipment required to build end-to-end an Integrated Circuit (IC) were to be found within single companies. Today, very few vertically integrated companies combining all the required competencies exist. We observe increasing globalization of the diverse design and manufacturing tasks and outsourcing to third parties [1]. For instance, many companies are founded or have transitioned to be "fabless": they outsource the manufacturing step of their IC design to offshore foundries, many of which are located in separate continents. In this way, they do not need to bear the enormous costs of building, maintaining, and upgrading a chip manufacturing facility that costs beyond $10 billion [2]. Another trend we observe nowadays is the rise of complex Systems-on-Chip (SoCs) where numerous general and specialized functions are integrated onto the same chip. Many companies do not have the know-how to design end-to-end a SoC, thus relying on third-party Intellectual Property (IP) cores for building some of the functions. As an example, Apple is a fabless company that procures IP cores from IP vendors including Arm, delegates fabrication to TSMC or Samsung, and product assembly/test services to Foxconn [3].

A major security threat resulting from this globalized supply chain is IP/IC piracy [4]. Main scenarios are as follows:

1) A company that purchases an IP from an IP vendor to use it in a SoC can illegally reuse the IP for other SoCs without remunerating again the IP vendor.
2) An IP may be cloned and sold illegally by a rogue employee of the company.
3) Cloning of an IC or its IP sub-cores can also be performed by a foundry that receives the IC blueprint for fabrication.

4) A malicious foundry may also produce and sell chips beyond the number agreed on in the contract with the chip design owner, known as overbuilding.
5) A legally purchased chip can be subjected to reverse-engineering to extract the IC netlist and layout and other technology secrets. Nowadays, there exists increased reverse engineering capabilities even for advanced technology nodes [5].
6) There exist recycling facilities where functional but aged chips are scrapped from used boards, then they re-enter the market as “fresh” products.
7) Unauthorized chip use is often considered another form of piracy.

Piracy is a serious threat for the microelectronics industry (i.e., loss of revenues and know-how), governments (i.e., national security threat), and the society as a whole (i.e., counterfeit chips are less reliable). To this end, there is a pressing need for anti-piracy design methods that can protect an IP/IC against potential attackers located anywhere in the supply chain.

This PhD will target the design of mixed-signal, analog-digital ICs with built-in anti-piracy defenses. The goal will be to develop design techniques at transistor-level or at system-level that will make the IC provably resist any attempt to pirate it. Example techniques borrowed from the digital domain include locking, where the IC functionality becomes key-controlled with a secret digital key, and camouflaging or physical obfuscation, where the layout is altered in a way that it will deceive the reverse engineer. Our group owns some of the state-of-the-art results in this field [6-9] and has an active collaboration with the NYU in the USA.

Short Bibliography:

[1] A. Varas, R. Varadarajan, J. Goodrich, and F. Yinug. “Strengthening the global semiconductor supply chain in an uncertain era”. Report. Boston Consulting Group (BCG) and Semiconductor Industry Association (SIA), 2021.
[2] D. Takahashi, “Globalfoundries: Next-generation chip factories will cost at least $10 billion,” https://rb.gy/pjllsf, 2017.
[3] J. Purcher, “Apple Supply Chain News: TSMC & Foxconn plan new chip plants,” https://rb.gy/ot1hfv, 2017.
[4] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, “Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain,” Proc. IEEE, vol. 102, no. 8, pp. 1207–1228, 2014.
[5] M. Holler et al., “High-resolution non-destructive three-dimensional imaging of integrated circuits,” Nature, vol. 543, pp. 402–406, 2017.
[6] J. Leonhard, A. Sayed, M.-M. Louërat, H. Aboushady, and H.-G. Stratigopoulos, “Analog and Mixed-Signal IC Security Via Sizing Camouflaging, " IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 5, pp. 822-835, 2021.
[7] M. Elshamy, A. Sayed, M.-M. Louërat, H. Aboushady, and H.-G. Stratigopoulos, “Locking by Untuning: A Lock-Less Approach for Analog and Mixed-Signal IC Security,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 12, pp. 2130 – 2142, 2021.
[8] 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, " IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 8, pp. 2449-2462, 2022.
[9] A.-R. Díaz Rizo, J. Leonhard, H. Aboushady, and H.-G. Stratigopoulos, “Anti-Piracy Design of RF Transceivers,” IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 70, no. 1, pp. 492-505, 2023.

Expected skills:

We seek a highly motivated talent with a M.Sc. degree or equivalent in Electrical Engineering or Computer Engineering and with background knowledge on circuit design, computer-aided design tools (i.e., Cadence, Synopsis, Mentor), and technical computing languages (i.e., MATLAB).

How to apply:

Send by e-mail a detailed CV to Haralampos-G. Stratigopoulos (e-mail: haralampos.stratigopoulos@lip6.fr).