Parameter Obfuscation: A Novel Methodology for the Protection of Analog Intellectual Property

Dr. Ioannis Savidis, Associate Professor, Drexel University

http://ice.ece.drexel.edu

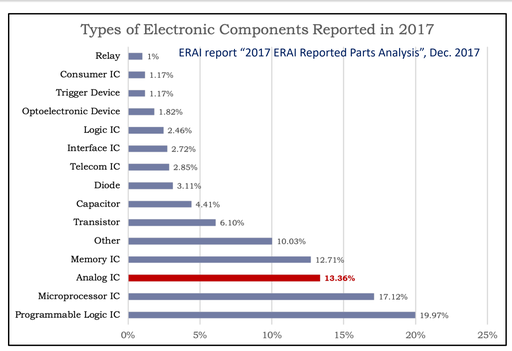
Design & Analysis Lab

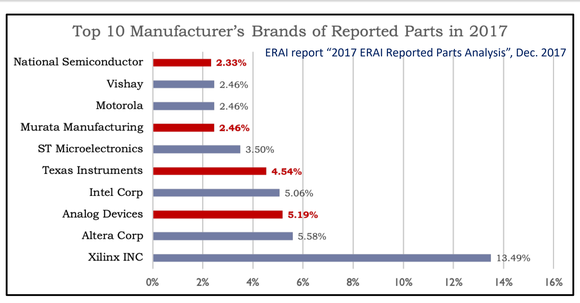
Research Interests

Analysis, modeling, and design methodologies for high performance digital and mixed-signal integrated circuits; Emerging integrated circuit technologies; Electrical and thermal modeling and characterization, signal and power integrity, and power and clock delivery for 3-D IC technologies; On-chip power management; Low-power circuit techniques; Algorithms and methodologies for secure IC design

LABORATORY & TEAM

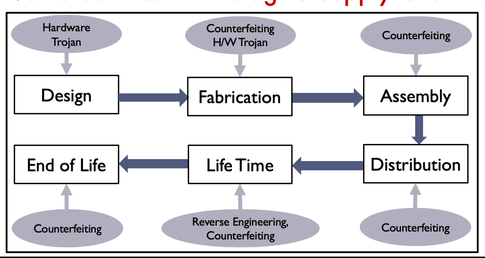
- **Seven Ph.D. students**
  - Kyle Juretus – Secure digital IC design
  - Vaibhav Venugopal Rao – Analog IC IP protection
  - Saran Phatharodom – Digital obfuscation metrics
  - Zhengfeng Wu – ML for analog circuit design
  - Pratik Shrestha – ML for digital circuit security
  - Ziyi Chen – Analog side-channel characterization
  - Shazzad Hossain – Low-power sub-threshold computing

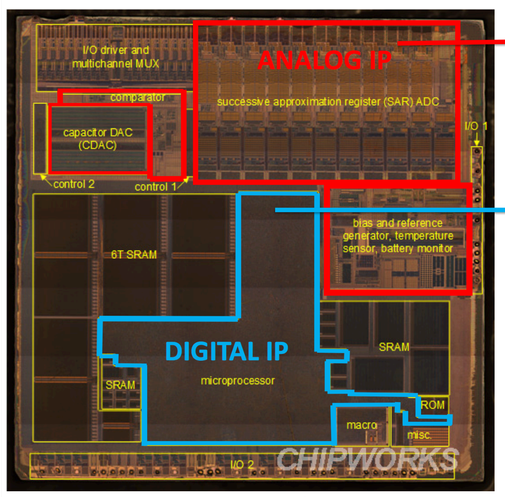




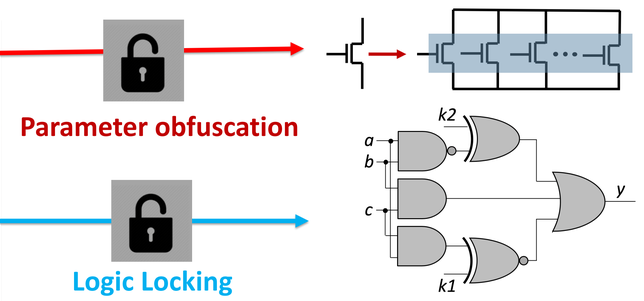
- Analog ICs are the third most counterfeited semiconductor component
- AMS IC manufacturer brands most frequently targeted for counterfeiting

Vulnerabilities in Analog IC Supply Chain



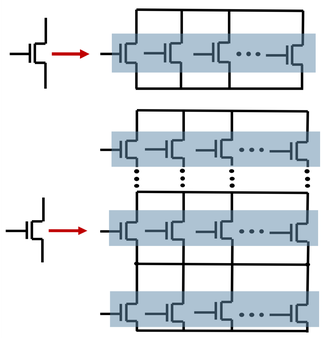


Texas Instruments Touchscreen SoC



- Protecting analog and digital circuits of a cyber physical system increases key space and number of obfuscated functions
- Lack of attack models increases security of analog circuits
- Provides lightweight, multi-function obfuscation methodology

Key Based Parameter Obfuscation Techniques

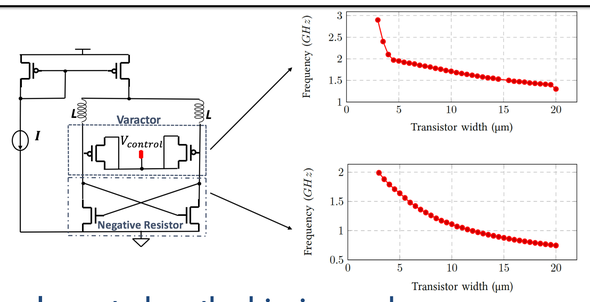


Vector-based obfuscation

$$\left(\frac{W}{L}\right)_{eff} = \left(\frac{W}{L}\right)_1 K_1 + \left(\frac{W}{L}\right)_2 K_2 + \ldots + \left(\frac{W}{L}\right)_n K_n$$

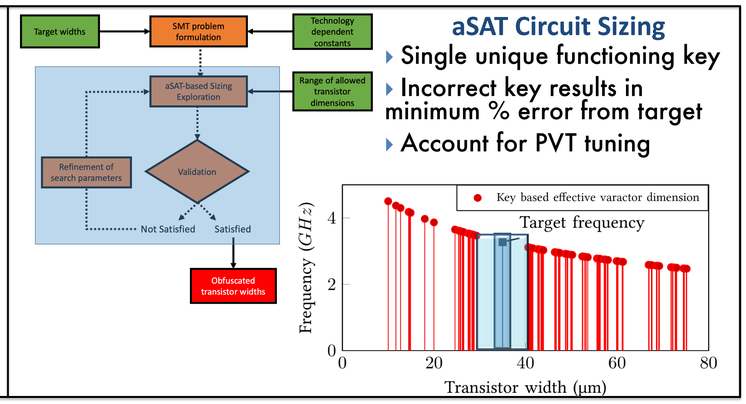
Mesh-based obfuscation

$$\frac{1}{\left(\frac{W}{L}\right)_{eff}} = \frac{1}{\left(\frac{W}{L}\right)_{row_1}} + \frac{1}{\left(\frac{W}{L}\right)_{row_2}} \ldots + \frac{1}{\left(\frac{W}{L}\right)_{row_m}}$$



Implemented on the biasing nodes

- Greater influence on functionality and performance
- Integral part of analog circuits



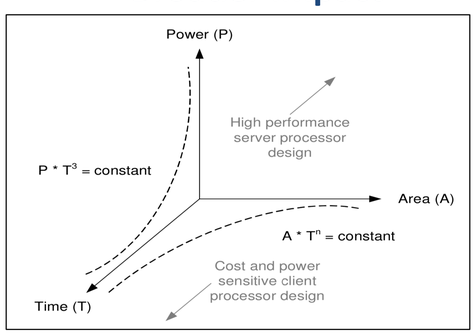
aSAT Circuit Sizing

- Single unique functioning key
- Incorrect key results in minimum % error from target
- Account for PVT tuning

- Parameter obfuscation techniques beneficial for in-house analog circuit design and IP vendors as a solution against various attack vectors
  - IC overproduction
  - Trojan insertion
  - Counterfeiting
- aSAT based transistor sizing methodology reduces analog design time and complexity
  - Determine transistor sizes for given performance specifications
  - Determine obfuscation transistor sizes to produce single unique key and minimum % error for incorrect key

Texas Instruments, Analog Devices, Synopsys, NXP, arm

Broader Impact



- Promotes development of new design methodologies with security as the new constraint along with power, area, and performance
- Promotes development of multi-constraint optimization algorithms

Potential Impact

- Proposed technique protects against overproduction and reverse engineering from untrusted foundries
- Reduces the risk of Trojan insertions as adversary does not have complete circuit understanding
- Masks circuit functionality even for a small key size
  - Ideal for small IoT based circuits
- Complements logic obfuscation techniques to provide increased security of mixed-signal ICs
- Resilient against traditional SAT and side channel attacks

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
October 28-29, 2019 I Alexandria, Virginia