Proposition de recherche doctorale

Design-for-security of analog and mixed-signal circuits and systems

Mots clés :

- Directeur de thèse : Haralampos STRATIGOPOULOS
- Co-encadrant(s) :
- Unité de recherche : Laboratoire d'informatique de Paris 6
- École doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal : Sciences et technologies de l'information et de la communication

Résumé du projet de recherche (Langue 1)

This PhD focuses on hardware trust and security aspects specifically for analog and mixed-signal (AMS) integrated circuits (ICs). The PhD seeks to understand the vulnerability of AMS ICs to security breaches, as well as to propose remedies and methodologies toward designing, fabricating, and deploying trusted and secure AMS ICs. More specifically, the PhD envisions developing a large portfolio of obfuscation methodologies for AMS ICs. Obfuscation aims at encrypting the circuit with a secret key, such that it functions correctly only if the correct secret key is provided. Otherwise, the circuit either fails completely or operates with degraded performances. Obfuscation aims at transforming the circuit such that it is much more difficult to reverse engineer and counterfeit. In essence, obfuscation helps protecting the intellectual properties of the design against adversaries. Reverse engineering is conducted by an adversary to (a) gain information about the internal blocks of the IC (i.e., architecture, netlist, layout masks, implementation details, technological data, etc.) aiming at reducing the adversary's technological disadvantage against the “author” of the IC; (b) gather necessary information for producing a counterfeit circuit; (c) gather valuable information for putting forward a successful and inescapable hardware attack; (d) locate the root-of-trust part of the IC so as to steal secret and sensitive information. Counterfeiting refers to (a) illegal theft of the IC design aiming at producing and selling a similar or identical IC; (b) reselling as new a used, and possibly aged IC; (c) non contractual overproducing of ICs and illegitimate selling of these ICs by an untrusted foundry. The developed obfuscation methodologies will range from generic ones, which are virtually applicable to any circuit class, to circuit class-specific ones, which are applicable to all architectures within a specific circuit class. Comprehensive metrics will be developed to quantify the security protection level achieved, the intrusiveness into the design, the incurred area overhead, etc. Given the expertise of Mr. Elshamy on memristors, this PhD will also investigate the use of memristors in the context of hardware obfuscation and design of security primitives, such as Physical Unclonable Functions (PUFs).