Owing to various financial factors, the contemporary semiconductor industry relies on a complex business model, wherein the vast majority of circuit intellectual property (IP) design and integrated circuit (IC) fabrication activities are outsourced to third-party design houses and foundries. The globalized and highly distributed nature of third-party entities results in a semiconductor supply chain model which exhibits several vulnerable points during the design, fabrication, and even the deployment phase of an IC. These vulnerabilities may be exploited by a knowledgeable adversary, thereby introducing various trustworthiness and security threats to the semiconductor industry and the end IC users, namely IP/IC piracy, which includes reverse engineering and counterfeiting, hardware Trojans, side-channel attacks, and fault injection attacks. This thesis focuses on hardware security aspects specifically for analog ICs. In particular, this thesis envisions developing a large portfolio of the first obfuscation methodologies for analog ICs. Obfuscation aims at transforming the original design into one that is functionally equivalent, but the functionality is well hidden by embedding the design in a larger functional space requiring a secret key to unlock its functionality. Obfuscation will be used as a countermeasure for: - Reverse engineering which is conducted by an attacker to (a) gain information about the internal blocks of the IC (i.e., architecture, netlist, layout functionality, implementation details, technological data, etc.) aiming at reducing the attacker’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 which refers to (a) illegal theft of the IC design (i.e., netlist, layout, masks, etc.) aiming at producing and selling a similar or identical (e.g., cloned) IC; (b) reselling as new an old, used, and possibly aged IC; (c) non contractual overproducing of ICs and illegitimate selling of these ICs by an untrusted foundry given that foundries have the fabrication blueprint (e.g. GDS II data). By the end of thesis, we plan to have demonstrated on silicon an obfuscated version of an RF transceiver.