Analog hardware security and hardware Authentication

Hardware security and authentication has become a more and more important concern in the Trust IC design. In this dissertation, a detailed study of hardware Trojans in analog circuits served by extra operating points or modes is discussed and a counterfeit countermeasure method which is based on a PUF authentication circuit is proposed.

Most concerns about hardware Trojans in semiconductor devices are based upon an implicit assumption that hardware Trojans are embedded in the digital hardware and involve a malicious modification of the Boolean operation of a circuit. In stark contrast, analog hardware Trojans can be easily embedded in some of the most basic analog circuits. These Trojans require no architectural modifications, no area or power overhead, and prior to triggering, leave no signatures in any power domains or delay paths. The Power/Architecture/Area/Signature Transparent (PAAST) characteristics can help the Trojan hide from detection with normal Trojan detection methods. They are nearly impossible to detect with the best simulation and verification tools, even if a full and accurate disclosure of the circuit schematic and layout is available. However, the study on PAAST analog hardware Trojan is quite limited. To complement the study on hardware security, example of circuits showing the existence of analog hardware Trojans are given; the PAAST characteristics of this type of hardware Trojans are discussed, heuristic detection methods that can help to detect these analog hardware Trojan are proposed.

Another major and growing problem in the modern IC supply chain is the proliferation of counterfeit chips. A method is proposed that should lower the entry barrier for major suppliers of COTS parts to offer authenticated components to the military and other customers that have high component reliability requirements. The countermeasure is based upon a PUF authentication circuit that requires no area, pin, or power overhead, and causes no degradation of performance of existing and future COTS components.