Seminar

Weize Yu

Department of Electrical Engineering

University of South Florida

Title:

Lightweight Countermeasures for Securing ICs against Power Analysis Attacks

Abstract:

Non-invasive side-channel attacks (SCA) are powerful attacks which can be used to obtain the secret key in a cryptographic circuit in feasible time without the need for expensive measurement equipment. Power analysis attacks (PAA) are a type of SCA that exploit the correlation between the leaked power consumption information and processed/stored data. Differential power analysis (DPA) and leakage power analysis (LPA) attacks are two types of PAA that exploit different characteristics of the side-channel leakage profile. DPA attacks exploit the correlation between the input data and dynamic power consumption of cryptographic circuits. Alternatively, LPA attacks utilize the correlation between the input data and leakage power dissipation of cryptographic circuits. In this talk, on-chip voltage regulators are utilized as lightweight countermeasures against power analysis attacks. Converter-reshuffling (CoRe) technique is proposed as a countermeasure against DPA attacks by using a PRNG to scramble the input power profile. The time-delayed CoRe technique is designed to eliminate machine learning-based DPA attacks through inserting a certain time delay. The charge-withheld CoRe technique is proposed to enhance the entropy of the input power profile against DPA attacks with two PRNGs. The security-adaptive(SA) voltage converter is designed to sense LPA attacks and activate countermeasure with low overhead. Additionally, three conventional on-chip voltage regulators: low-dropout (LDO) regulator, buck converter, and switched-capacitor converter are combined with three different kinds of voltage/frequency scaling techniques: random dynamic voltage and frequency scaling (RDVFS), random dynamic voltage scaling (RDVS), and aggressive voltage and frequency scaling (AVFS), respectively, against both DPA and LPA attacks.