Doctoral Dissertations 1911-2013

Off-campus UMass Amherst users: To download campus access dissertations, please use the following link to log into our proxy server with your UMass Amherst user name and password.

Non-UMass Amherst users: Please talk to your librarian about requesting this dissertation through interlibrary loan.

Dissertations that have an embargo placed on them will not be available to anyone until the embargo expires.

Cryptographic Circuit Design In Nanometer CMOS Technologies

Lang Lin, *University of Massachusetts - Amherst*

Date of Award
2-2012

Document Type
Campus Access

Degree Name
Doctor of Philosophy

Degree Program
Electrical and Computer Engineering

First Advisor
Wayne P. Burleson

Second Advisor
Sandip Kundu

Third Advisor
Csaba A. Moritz

Keywords
Applied sciences, Cryptographic circuit design, Nanometer CMOS, Embedded system security, Hardware trojan, Low-power design, Physical unclonable function, Process variation, Side-channel analysis

Subject Categories
Electrical and Computer Engineering

Abstract
As increasingly important modules in modern embedded systems, cryptographic circuits rely on provable theorems to guarantee hardware security and information privacy. However, perfect security on silicon is very difficult to achieve because traditional implementations of cryptographic circuits are vulnerable to various physical attacks and especially power side-channel analysis attacks. With the rapid advances

of complementary metal-oxide-semiconductor (CMOS) technologies reaching nanometer regimes, more security threats on the hardware level occur due to increased data-dependent leakage power, process variations and interconnect couplings. With the trend of separating design from chip fabrication due to economic incentives, untrusted foundry in the semiconductor supply chain can covertly implant "hardware Trojans" to facilitate physical attacks or even devoid the cryptographic circuits. The present and future design of nanometer cryptographic circuits must take the impacts of process technology and business model into account.

In this work, we have proposed a new security metric PAT and FPGA validation methodologies to evaluate the side-channel attack resistance of nanometer cryptographic circuits. We have demonstrated that process variations and lightweight hardware Trojans can both degrade the embedded system security. To eliminate the side-channel information leakage, the most effective way is to directly build cryptographic circuits with inherent physical randomness such as in the physical unclonable functions (PUFs). We have developed a statistical design methodology and post-silicon validation platform for sub-45nm PUF circuits, and demonstrated improved PUF security with a low-power design in advanced technology nodes. Our test chips in 45nm CMOS silicon-on-insulator technology have negligible side-channel information leakage and can potentially be integrated into modern low-power secure embedded systems.