Enter search terms:
Search
in this series
Advanced Search

Notify me via email or RSS

Browse
Collections
Disciplines
Authors

Author Corner
Author FAQ

Links
University Libraries
UMass Amherst
Contact Us

Masters Theses 1896 - February 2014

Off-campus UMass Amherst users: To download campus access theses, 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 thesis through interlibrary loan.

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

Electromagnetic Side-Channel Analysis for Hardware and Software Watermarking

Download

SHARE

Ashwin Lakshminarasimhan

Follow

Document Type
Open Access

Degree Program
Electrical & Computer Engineering

Degree Type
Master of Science (M.S.)

Year Degree Awarded
2011

Month Degree Awarded
September

Keywords
Side-Channel Analysis, Electromagnetic side channel, Trojans, Watermarks

Abstract
With more and more ICs being used in sectors requiring confidentiality and integrity like payment systems, military, finance and health, there is a lot of concern in the security and privacy of ICs. The widespread adoption of Intellectual Property (IP) based designs for modern systems like system on chips has reduced the time to market and saved a lot of money for many companies. But this has also opened the gates for problems like product piracy, IP theft and fraud. It is estimated that billions of dollars are lost annually to illegal manufacturing of Integrated Circuits. A possible solution to this problem of IP theft is to insert small circuits which are like unique IDs that only the owner or the registered verifier will know and detect in case of any conflict. The circuits that are inserted are called watermarks and are in some cases kept very small so as to be hidden. In such cases, we would need detection schemes that work well even with very small watermarks. In this work, we use Electro-Magnetic (EM) based side-channels for the detection of watermarks. Since the 90s, Side-

channel Analyses have attracted significant attention within the cryptographic community as they are able to obtain secret information from smart cards and ICs. The power side-channel analysis is a very powerful method but EM side-channels are very useful as they will not need a resistor in series to the power supply and just needs passive observation of the EM radiations emanated by the IC. This passive monitoring will be a big advantage in the case of automated watermark detection used by a verifier.

In this work, we start with EM side-channel analysis on FPGA for smaller designs. We insert watermarks on a Micro-controller, Smartcard and an FPGA and detect these watermarks using EM side-channel information emanated from the Design under Test. We used environments with different levels of noise interference. We compare the watermarking application using EM side-channels and Power side-channels in these different setups. These watermarks are very small and are hard to attack or remove by an attacker through reverse engineering or side-channel information. Due to the robustness against such attacks and the easy access of EM side-channels when compared to power side-channels, the EM side-channel based watermarks will be a very good solution for the IP theft problem. EM side-channel based watermark detection supports automation which companies of IP cores can make use of. We also extended this work to EM Side-channel Trojans as the concepts are similar

Advisor(s) or Committee Chair
Burleson, Wayne Peter

This page is sponsored by the University Libraries.
© 2009 University of Massachusetts Amherst • Site Policies