Tutorial proposal – DEPEND 2011

Proposal for a **half-day tutorial (3 hours).** It may be summarized for a shorter embedded tutorial (e.g., 1 hour) if convenient for the Conference organizers.

Title
Taking care of security in hardware design

Abstract
This tutorial discusses the specific design constraints related to secure integrated or embedded systems, with a special emphasis on the most critical elements in such systems, e.g. cryptoprocessors. The main focus is on hardware-based attacks and some possible solutions. After a presentation of the general context, the basics of circuit-level attacks are summarized. Circuit- and architecture-level methods for the design and implementation of robust secure circuits are then explained, including manufacturing test concerns. Characteristics and limitations of the main hardware protection schemes (also called counter-measures) are discussed. Experimental attack data are shown on several implementation technologies (ASIC and FPGA).

Keywords
Integrated systems, embedded systems, security, attacks, DPA, EMA, DFA, counter-measures

Organizer and Presenter
Régis LEVEUGLE
TIMA Laboratory
46 Avenue Félix Viallet, 38031 Grenoble Cedex, France
Regis.Leveugle@imag.fr

Prepared in collaboration with Paolo MAISTRI, CNRS reasearcher in the same laboratory

Short Biography
Régis LEVEUGLE received the PhD degree in Microelectronics from the National Polytechnical Institute of Grenoble (INPG), France, in 1990. He is currently Professor at this institute and member of TIMA laboratory. His main interests are computer architecture, VLSI design methods and CAD tools, dependability evaluation, fault-tolerant architectures, concurrent checking and secure circuit design.
He has 20 years experience in teaching VLSI design, test and dependability. He created four years ago a specific lecture at Master level on the subject of the proposed tutorial. He also presented several tutorials and embedded tutorials in IEEE international conferences on dependability- and security-related subjects (DTIS'06, ICECS'06, ICECS'07, ICECS'08, SCS'09, LASCAS'10). He was co-author of an embedded tutorial on "Ensuring high testability without degrading security" at the 14th IEEE European Test Symposium, Sevilla, Spain, May 2009.
He has authored or co-authored more than 150 scientific papers and served as a reviewer for many journals and conferences. He has been a member of the French evaluation committee for national projects on security. He has also served on more than 80 international conference program and organization committees. He was Program co-Chair for the 2001 IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT'01), vice-General Chair for the 2002 IEEE International On-Line Testing Workshop, General co-Chair for DFT'02, vice-Program Chair for the 2003, 2005 and 2007 IEEE International On-Line Testing Symposium (IOLTS) and Program co-Chair for IOLTS'03 and IOLTS'06. He is a member of IEEE.

Context and objectives
Integrated embedded systems are nowadays used in many applications, including an increasing number of critical ones. Among those, applications directly related to security features (e.g. access control, identity documents, …) are developing fast. But a lot of other applications also face hacker attacks and have strong security constraints. Major examples are banking, cell phones, pay-per-view television. But less critical applications often have some level of security requirements and/or include cryptographic mechanisms. In such applications, integrated circuits are often used as a trusted area in which confidential

data are stored. The most common example of such data is a secret key used to encrypt/decrypt critical information streams or to avoid cloning. Unfortunately, many attacks have been developed based on the hardware implementation characteristics. Such attacks allow a hacker to steal the secret information manipulated within the circuit, unless efficient protections (also called counter-measures) are implemented in the circuit. An increasing number of engineers and researchers must therefore be aware of these threats and of the real characteristics of practical attacks. In particular, error models considered in the literature are often unrealistic or at least too optimistic.
The main objectives of this tutorial are:

- to make designers understand the different types of implementation-based attacks and their characteristics,
- to discuss the relationship between test techniques and security flaws,
- to present circuit level and architecture level methods for the design and implementation of robust secure circuits,
- to discuss the efficiency and limitations of the main hardware protection schemes,
- to pinpoint the impact of the implementation target (ASIC vs. FPGA),
- to present practical results and experimental data.

Proposed outline

1. Secure circuits
    - Embedded system context
    - Security constraints and evaluation
    - Qualification, common criteria and security evaluation centers
2. Implementation-related attacks on hardware
    - Taxonomy of attacks (including DPA, EMA, DFA)
    - Exploitation examples
    - Design constraints
    - Impact of test mechanisms
    - Error models for main implementation targets – Cell-based design vs. SRAM-based FPGAs
3. Hardware protection schemes against the different types of attacks
    - Principles at circuit and architecture level
        - w.r.t. side-channel attacks
        - w.r.t. fault-based attacks
    - Design examples for usual cryptography algorithms
    - Influence of implementation target on counter-measures (ASIC vs. SRAM-based FPGA)
    - Protected test and evaluation of self-test techniques
    - Influence of design style (e.g. synchronous vs. asynchronous circuit implementation)

All aspects will be illustrated with results and experimental data on concrete and practical examples.

Target audience

Integrated circuit and system designers, both from industry and academia
Researchers and engineers interested in architecture, ASIC or FPGA-based design and security