Tutorial on Side Channel Attacks and Dedicated Countermeasures

– With a Particular Focus on Block Ciphers Software Implementations –

Emmanuel Prouff

French Network and Information Security Agency

Tutorial Proposal: Passive Attacks and Countermeasures for Block Ciphers Software Implementations

Goal: present the state of the art attacks and countermeasures for software implementations of block ciphers, with a special focus on AES.

Attendees Profile: engineers and young researchers in embedded security. Basics in cryptography, mathematics and probability (Bachelors Degree).

Tutorial Agenda (draft):

- Part 0 - Short Introduction to the Side Channel Problematic (illustrated in the Banking Smart Cards Context).

- Part I - General Overview of Side Channel Attacks and Introduction of the Security Definitions

  - Basic (Simple) SCA
  - Template SCA
  - Univariate SCA
  - Multivariate SCA
  - Methods to quantify the resistance of an implementation against SCA

- Part II - SCA Software Countermeasures

  - Few words on Leakage Resiliency
  - Noise Addition
  - Randomization of the processings' order (study of the security gain)
  - Sharing/Masking (study of the security gain)
  - Strategies to Secure an AES Software Implementation
  - Comparison of the state of the art masking techniques (with a special focus on AES)

- Conclusion