

SEnSE: Secure Software Implementation of AES



Motivation

Side-channel analysis (SCA) is a powerful technique to attack implementations of cryptographic algorithms. In this project, an existing software implementation of the Advanced Encryption Standard (AES) should be secured against such SCA attacks by using so-called randomization and shuffling countermeasures. Since the software implementation is intended for a highly constrained 8-bit microcontroller, additional costs in terms of code size and execution time should be kept as small as possible (e.g. by adapting the instruction set). After securing the AES implementation, the efficiency of the applied countermeasures should be verified by conducting actual SCA attacks on an FPGA prototype.

Project description

- Goals
 - Secure an existing software implementation of AES on a simple 8-bit microcontroller by keeping the overhead costs as low as possible.
 - Verify efficiency of implemented countermeasures by conducting SCA attacks on an FPGA prototype.
- Tasks
 - Read into the topic
 - Get familiar with the 8-bit microcontroller, the existing AES implementation, and the concept of randomization/shuffling countermeasures
 - Implement countermeasures
 - Optimize design by adapting the instruction set
 - Locate costly instructions
 - Modify instruction set
 - Verify efficiency of applied countermeasures
 - Build measurement setup
 - Perform SCA attacks on secured/non-secured AES implementation on an FPGA prototype

Literature

- C. Herbst et al.: [An AES Smart Card Implementation Resistant to Power Analysis Attacks](#), 2006
- S. Mangard et al.: [Power Analysis Attacks: Revealing the secrets of smart cards](#), 2007

Deliverables

- Project files (.zip, cleaned)
- Documentation (inline)
- Readme (getting started)
- Presentation (10 .ppt slides)

Project schedule

- Start Immediately
- Month 1 Reading, getting familiar with AES implementation / countermeasures
- Month 2 Implementation of countermeasures / verify efficiency
- Month 3 Final deliverables

Master @IAIK Project

Studies: INF SEW TEL

Prerequisites

- Assembly programming and VHDL
- (basic knowledge of JAVA and MATLAB is advantageous)

Advisor / contact

Thomas.Plos@iaik.tugraz.at