Universität Stuttgart

INSTITUT FÜR
KOMMUNIKATIONSNETZE
UND RECHNERSYSTEME
Prof. Dr.-Ing. Andreas Kirstädter

Bachelor thesis No. 1020

Side channel attack sensibility of Logic-Locked cryptographic circuits

Methods
Measurements
Digital systems design

Topics
Cryptography

Background

Logic Locking protects a circuit against potential attacks in the IC supply chain by inserting additional logic components into the circuit. A quite common symmetric cipher is the Advanced Encryption Standard (AES) which can be implemented as a circuit in hardware. Those cryptographic circuits must be protected against passive physical attacks like side-channel attacks, which can be done using masking.

Problem Description

The target of this thesis is to test if logic locking a masked cryptographic circuit weakens the security of the keys used in the circuit against side channel attacks. For this purpose, DOM-AES, a masked version of an AES-circuit will be tested with and without logic locking, and the ? Test Vector Leakage Assessment? (TVLA) will be used to test the circuits against side-channel attacks.

Aquired Knowledge and Skills

Design of digital cryptographic circuits protected against side-channel attacks (masking), VHDL/Verilog, synthesis of digital circuits, Xilinx FPGA tools, measurements, side-channel-attacks, Student?s t-test, statistics.

Requirements

Digital systems design

Contact

Dipl.-Ing. Matthias Meyer
room 1.334 (ETI II), phone 685-67975, E-Mail matthias.meyer@ikr.uni-stuttgart.de