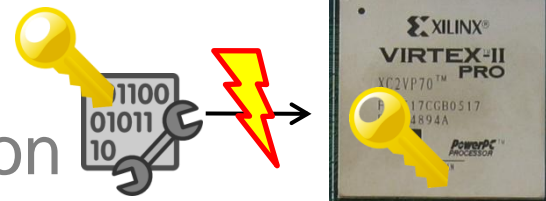


# SCA on FPGAs

## Breaking Xilinx Bitstream Encryption



© 2011 ntb.ch

### Motivation

Modern FPGAs contain security measures that provide a secure channel for a designer to update the configuration of an FPGA, e.g. a firmware update. In case of Xilinx bitstream encryption the designer encrypts the bitstream with a secret key. On powerup the bitstream is decrypted within the FPGA and is then used to configure the FPGA accordingly.

With side-channel analysis (SCA) attacks it should be possible to overcome this security feature and to discover the secret key. This way, an adversary may be able to copy/clone firmware IP and to manipulate such devices.

### Project description

- Goals
  - Break Xilinx bitstream encryption feature by side-channel analysis (SCA) attacks
- Tasks
  - Study literature (SCA & Xilinx)
  - Perform successful SCA attacks on Xilinx FPGA
  - Break Xilinx bitstream encryption

### Literature

- Moradi et al., „ On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks -- Extracting Keys from Xilinx Virtex-II FPGAs”

### Deliverables

- Project files (.zip, cleaned)
- Documentation (paper)
- Presentation (10 .ppt slides)

### Project schedule

- Start Immediately
- Month 1 Study literature, SCA
- Month 2 Investigate bitstream encryption feature of Xilinx FPGAs
- Month 3 Final deliverables

### Master Project

Studies:  INF  SEW  TEL

### Prerequisites

- MATLAB
- Knowledge in Side-Channel Attacks useful

### Advisor / contact

[Mario.Kirschbaum@iaik.tugraz.at](mailto:Mario.Kirschbaum@iaik.tugraz.at)