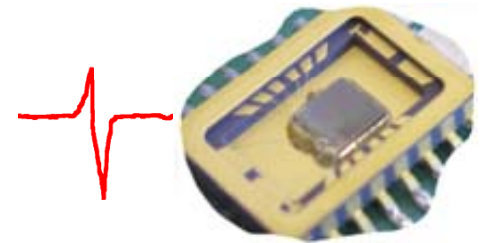


SEnSE: Fault Attacks on an RFID Prototype Chip



Motivation

Fault attacks are powerful techniques to reveal secret information of cryptographic devices. In this project, various fault attacks should be applied to an RFID prototype chip (CRYPTA chip). With the fault attacks, it should be shown whether it is possible to modify data that is written to the memory, to influence the control flow, or to disturb the execution of cryptographic operations on the chip.

Project description

- Goals
 - Get familiar with prototype chip and fault attacks.
 - Build setup and conduct practical attacks.
- Tasks
 - Read into the topic
 - Get familiar with the CRYPTA prototype chip
 - Select most promising fault-attack techniques
 - Build attack setup
 - Conduct practical attacks

Literature

- [Specification of CRYPTA chip](#)
- [Hutter et al., RFID and its Vulnerability to Faults](#)

Deliverables

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

Project schedule

- Start Immediately
- Month 1 Reading, getting familiar chip/fault attacks
- Month 2 Built setup and perform attacks
- Month 3 Final deliverables

Master @IAIK Project

Studies: INF SEW TEL

Prerequisites

- Having fun in playing with hardware components ☺

Advisor / contact

[Thomas Plos@iaik.tugraz.at](mailto:Thomas.Plos@iaik.tugraz.at)