Contact-based Fault Injections and Power Analysis on RFID Tags

Michael Hutter, Jörn-Marc Schmidt, Thomas Plos

ECCTD 2009

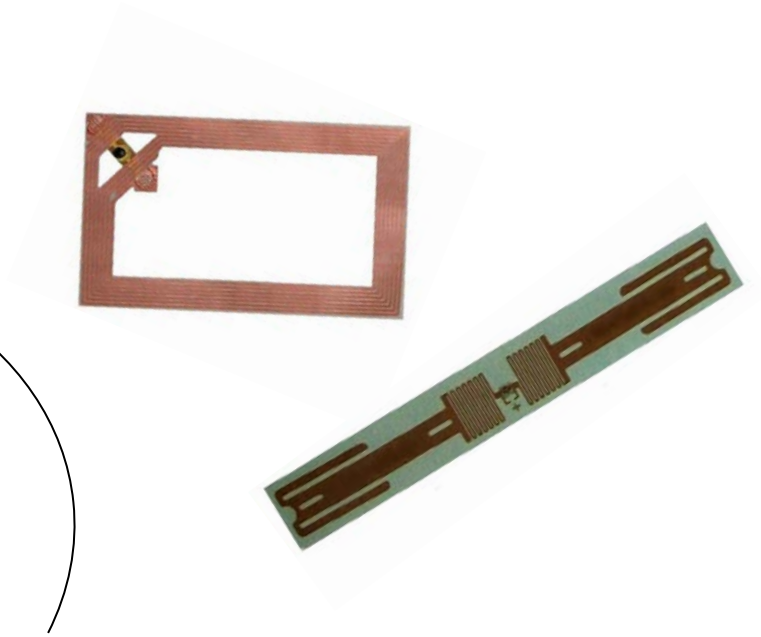
Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology

Presentation Outline

- Introduction
- Implementation attacks on RFID
- Related work
- Contact-based measurement setup
- Fault injection setup and results
- Power analysis setup and results
- Conclusions and future work

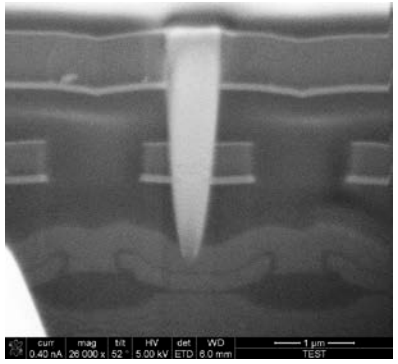
Introduction

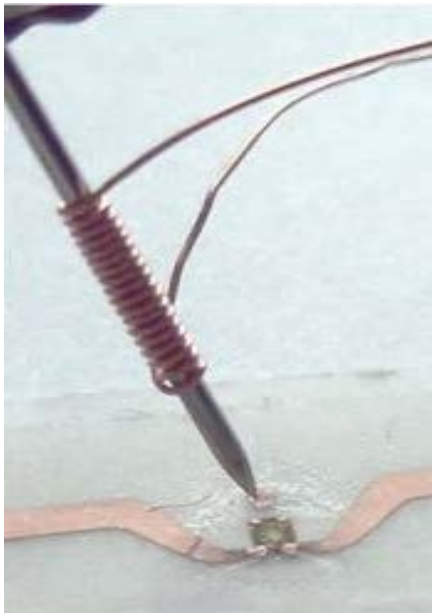
- RFID … **R**adio **F**requency **Id**entification
- Small microchip attached to an antenna
- Reader field is used for
  - Communication
  - Power supply
  - (Clock signal)

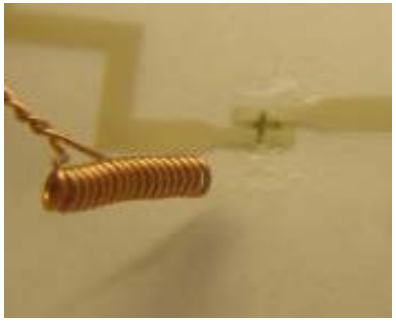


Implementation Attacks on RFID

- Active attacks
  - Fault attacks
- Passive attacks
  - Physical probing
  - Side-channel attacks
    - Power consumption
    - Electromagnetic radiation
    - Timing analysis







Recent Work

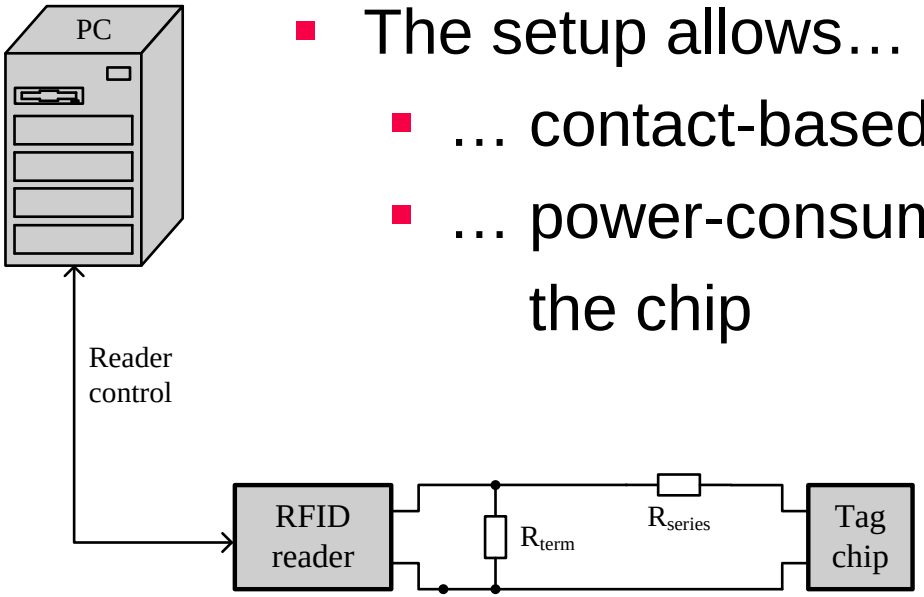
- Oren and Shamir 2006
  - Simple power analysis attacks on UHF tags
- Hutter et al. 2007
  - Differential electromagnetic analysis on HF tags
- Plos 2008
  - Differential electromagnetic analysis on UHF tags
- Hutter et al. 2008
  - Fault attacks on HF and UHF tags
- This work
  - Differential power analysis and fault attacks on UHF and HF tags

Our Analysis

- Performed fault attacks and power-analysis attacks on different RFID tags
  - We induced over-voltage spikes into the chip-antenna connections
- Analyzed HF and UHF tags
  - ISO 15693 and ISO 18000-6C (EPC Gen2)
- Focus on write operation
  - Critical in terms of power consumption and execution time
- Used a contact-based measurement setup

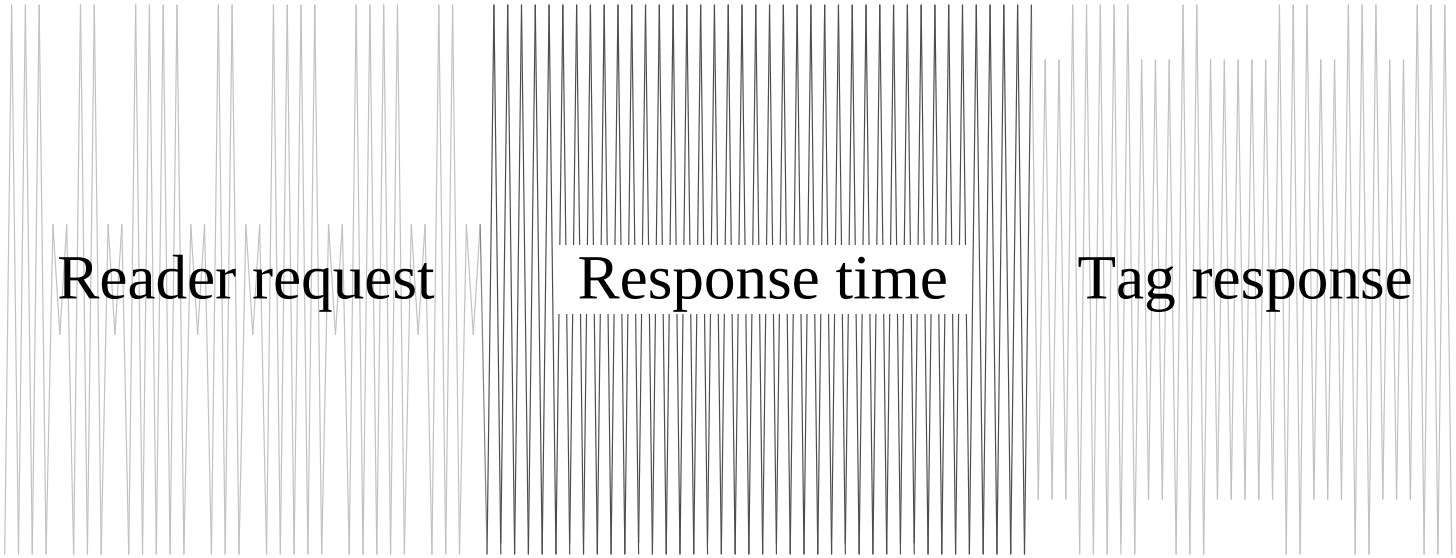
Contact-based Measurement Setup

- The chip of the tag is separated from its antenna
- Chip and reader are directly connected by 2 wires
- No air interface (no inductive/electromagnetic coupling)



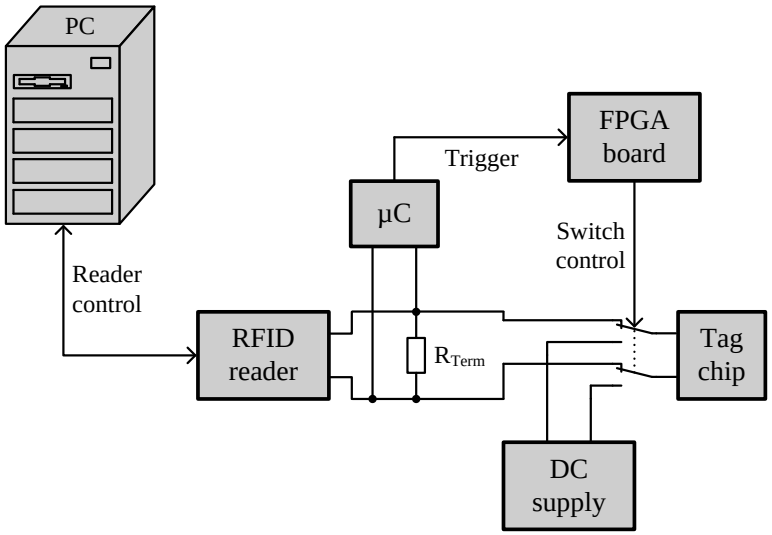
- The setup allows…
  - … contact-based fault injections
  - … power-consumption measurements of the chip

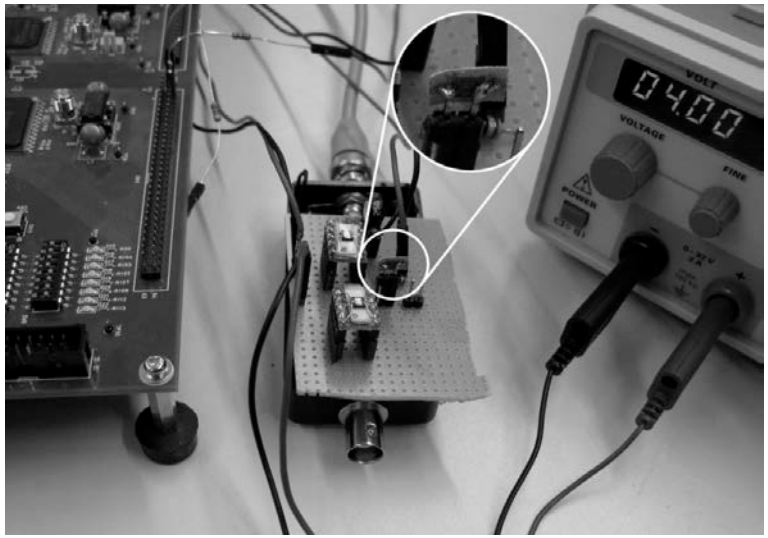
Basic Communication Process



Fault-Injection Setup

- Two high-speed multiplexers connect the chip to a DC voltage (over-voltage injection)
- Trigger device



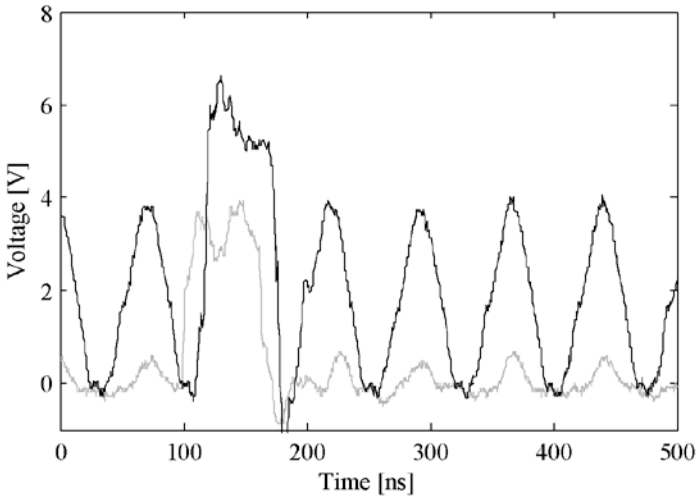


Trigger Signal

- Trigger device
  - SASEBO board used to control the trigger delay and duration
  - A microcontroller is used to listen to the reader communication and to provide a trigger signal after a write command
- Fault injections during the response time of the chip (a few milliseconds)
  - Trigger device was programmed to sweep across the response time (automatic sweep)
  - Injected spikes in steps of 9ns
  - Over-voltage was induced for at least 80ns

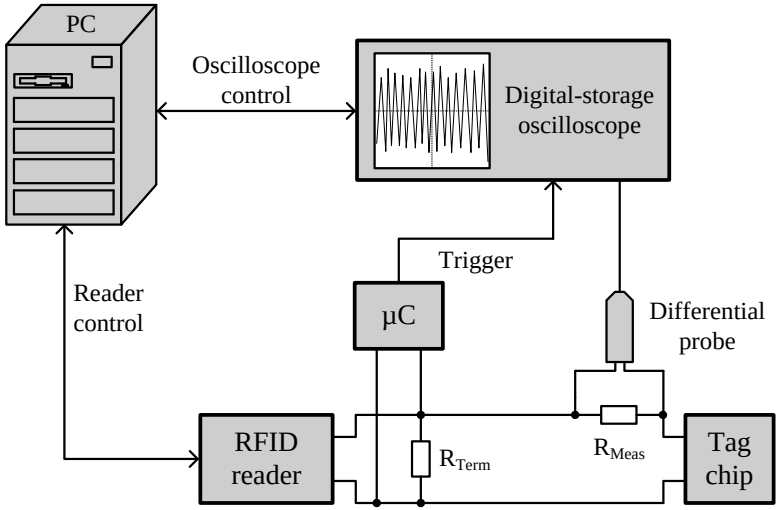
Results

- Faults cause the chip to write faulty values into the memory
- Tags perform a reset during the writing of data
- The faulty value depends on the trigger delay
- Different tags have a different writing time
  → Allows fingerprinting of RFID tags



Power-Analysis Setup

- For HF tags
  - Power is measured over a 100 Ohm resistor
- For UHF tags
  - Power is measured over the internal capacity (0.1pF) of the differential probe (no resistor used)

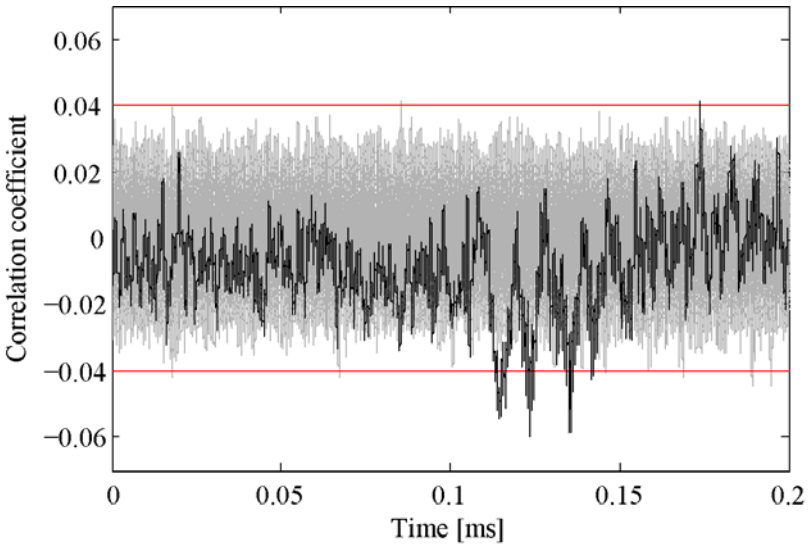


Power-Analysis Attacks

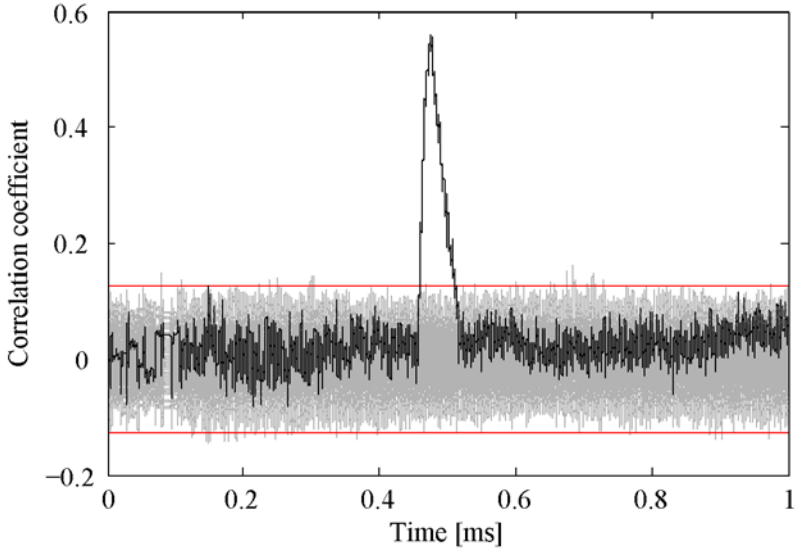
- Trace acquisition
  - 1000 traces for UHF tags and 10000 traces for HF tags were measured
  - Sampling rate: 100 MS/s
- Post-processing techniques
  - Calculated the envelope signal (absolute values + 2 MHz low-pass filter
  - Horizontal and vertical trace alignment
- Target of the attack
  - 8-bit value that was written into memory
- Different Power models applied

Results

- All attacks have been successful



ISO 15693 HF tag



ISO 18006C UHF tag

Summary

- Performed fault and power-analysis attacks on RFID
- Analyzed HF and UHF RFID tags
- Contact-based measurement setup used
- All attacks have been performed successfully

- Security-enabled RFID devices have to include countermeasures to thwart these attacks

Thank you for your attention.

Questions?

Michael.Hutter@iaik.tugraz.at
Jörn-Marc.Schmidt@iaik.tugraz.at
Thomas.Plos@iaik.tugraz.at

http://www.iaik.tugraz.at/content/research/implementation_attacks/