Side-Channel Attacks on RFID Tags

PROACT Spring School 2008

Michael Hutter, Thomas Plos

IAIK – Graz University of Technology
michael.hutter@iaik.tugraz.at

thomas.plos@iaik.tugraz.at
www.iaik.tugraz.at

List of Contents

- Introduction
- Implementation weaknesses
- RFID-tag prototypes
- EM analysis on HF tags
  - Measurement setups
  - Results
- HF vs. UHF tags
- Side-channel analysis on UHF tags
  - Measurement setups
  - Results
- Fault analysis on HF and UHF RFID tags
- Conclusion

Introduction

- There are various kinds of attacks on RFID devices
  - Tracking
  - Skimming
  - Eavesdropping
  - Replay and relay

- Use of cryptography to counteract these attacks
  - The implementation of cryptographic primitives is the weakest link in the system
  - Attacks on cryptographic implementations

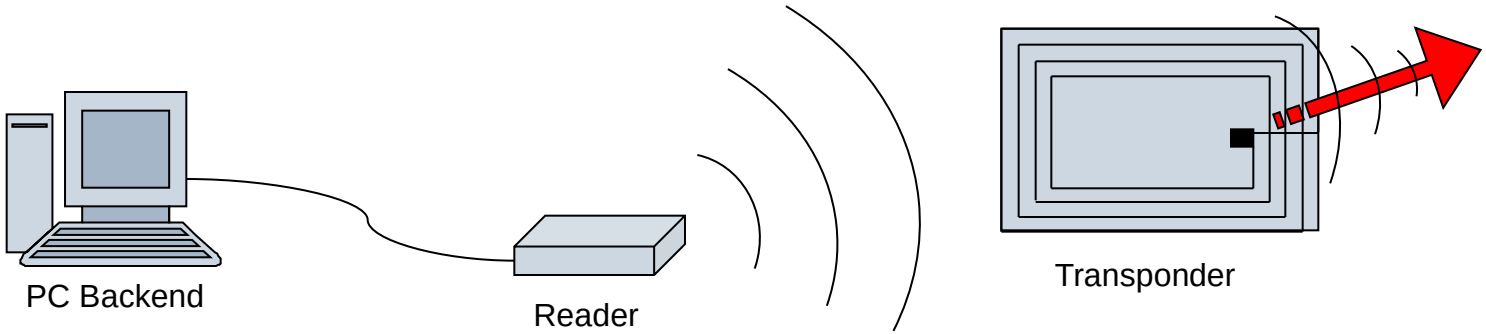
Implementation Weaknesses

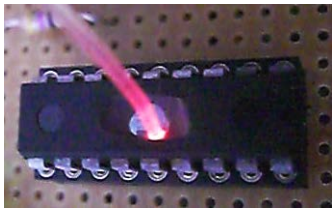
Active attacks

- Fault analysis
- Physical probing

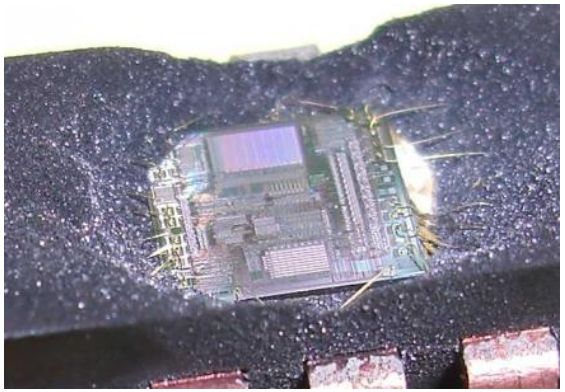
Passive attacks

- Side-channel analysis
  - Power consumption
  - Timing information
  - Electromagnetic radiation





Fault Analysis

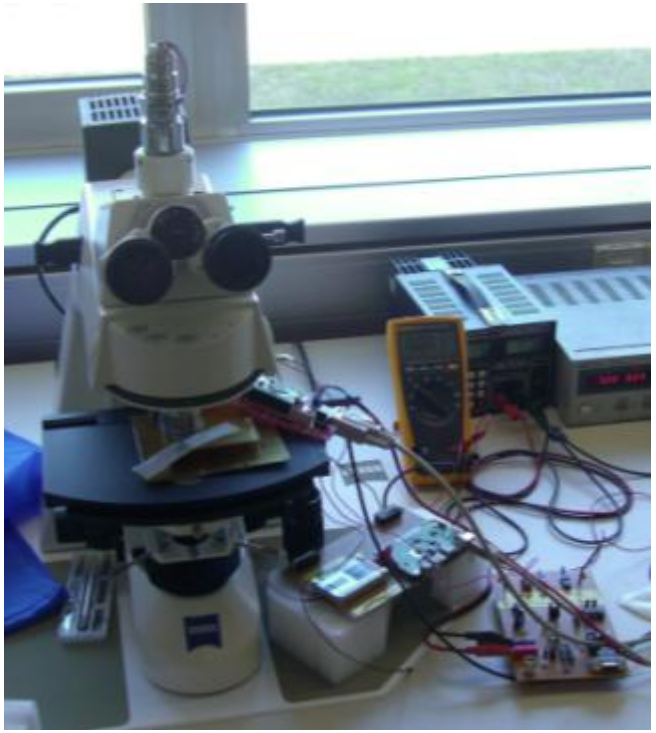


Non-invasive

- Glitch attacks
- Temperature variations

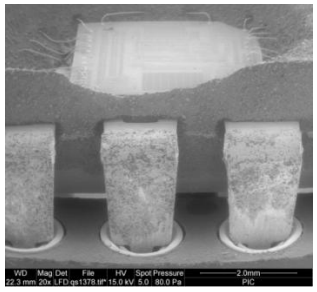
Semi-invasive

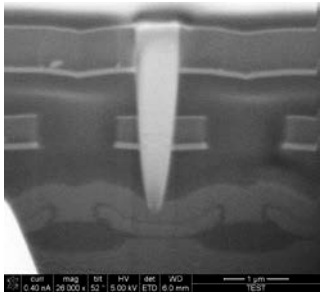
- Optical fault-injection
- EM fault-injection

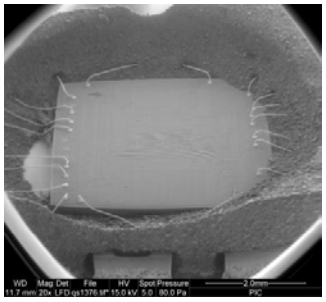


Invasive

- Modify the chip structure

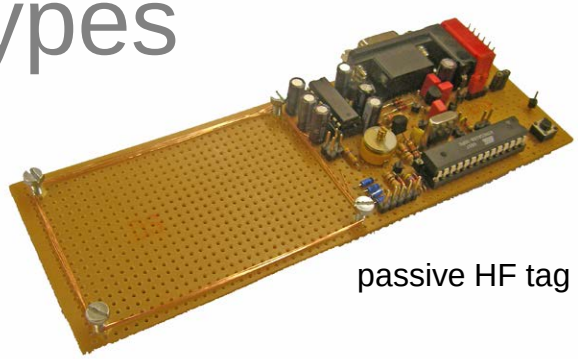






RFID-Tag Prototypes

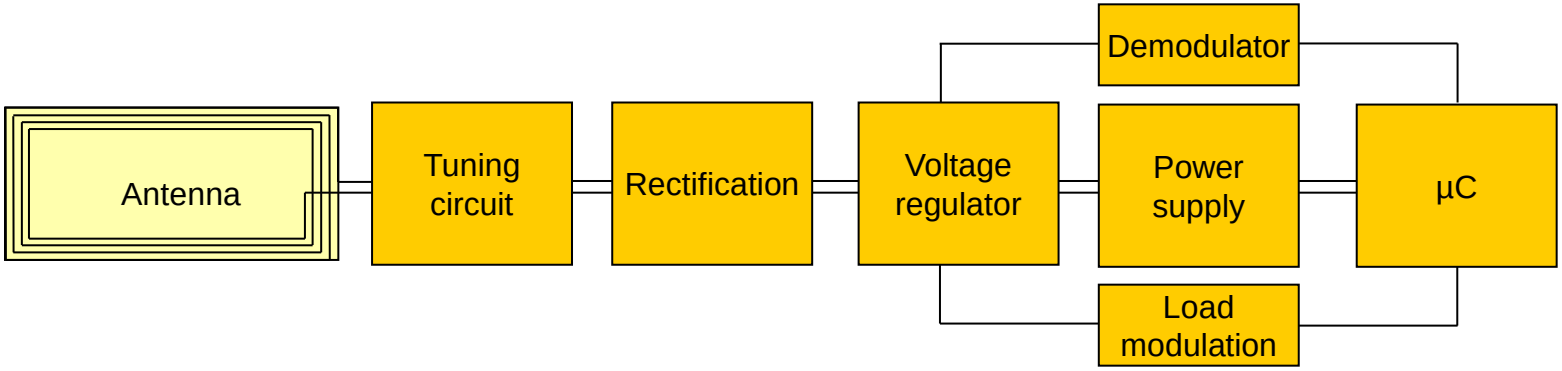
- Can be used for..
  - Demonstrate new RFID applications
  - Performing side-channel analysis
  - Showing weaknesses in RFID systems
  - Evaluate security protocols



passive HF tag

semi-passive HF tag

- Implemented Protocols
  - ISO-14443 A/B, ISO-14443-4, ISO-15693, NFC



DemoTag vs. Single-Chip Tag


⇔


Larger parasitic antennas

- discrete hardware-components ⇔ single chip

Separate hardware-design

- Analog front-end and digital chip separated ⇔ “all in one” chip

Low-power consumption

- ~5 mW ⇔ ~5 µW

Clock synchronization

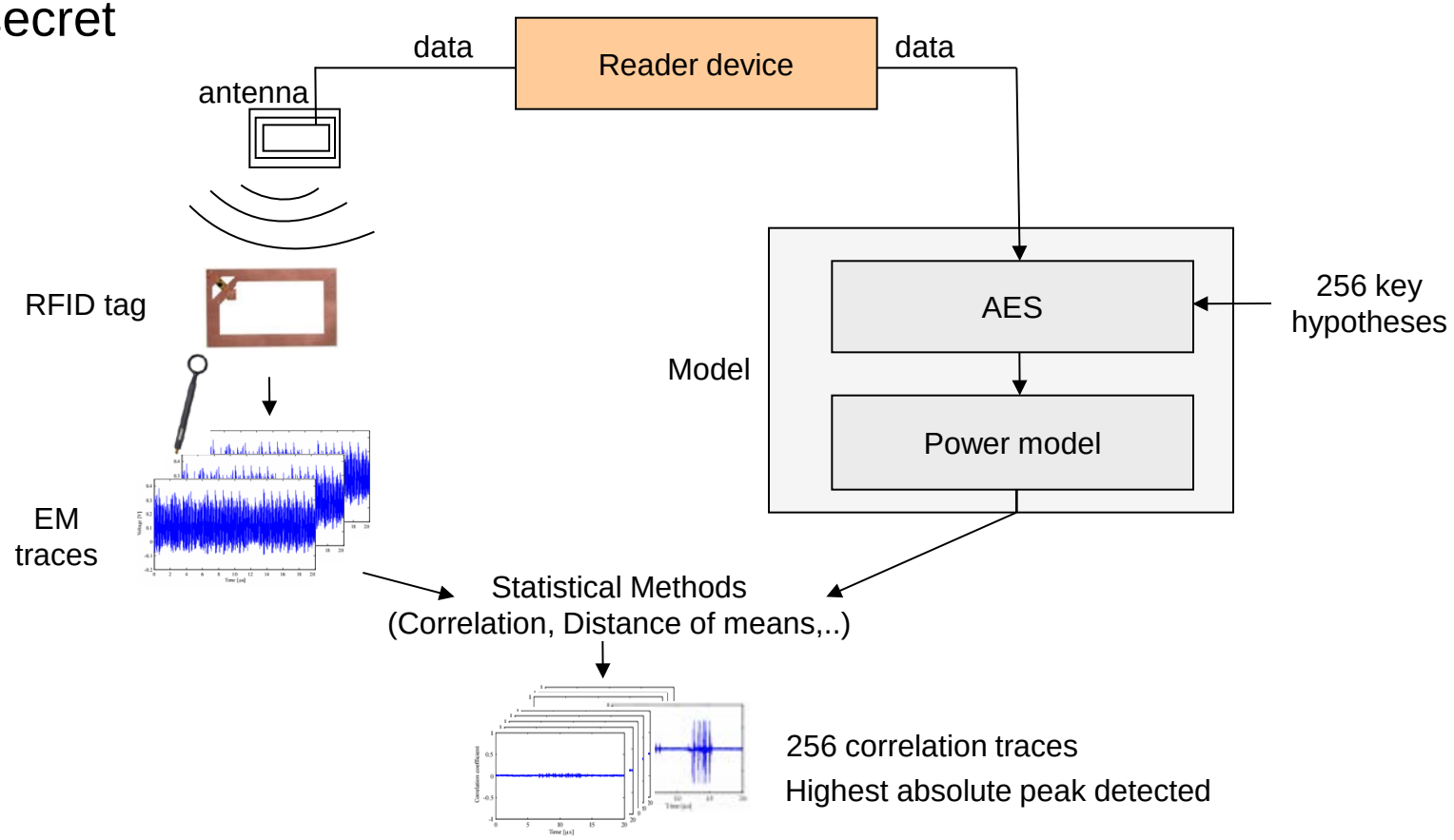
- 13.56 MHz on-chip oscillator ⇔ clock extraction from the field

Trigger signal

- Trigger on the µC output-pin ⇔ need of a demodulator circuit

Differential EM Analysis (DEMA)

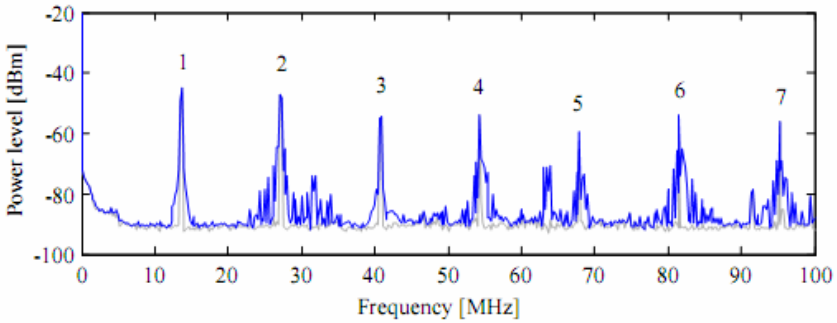
- Target of the attacks is an intermediate value that depends on a secret



Electromagnetic Analysis

- Measuring the chip emissions of the transponder using near-field probes

- Problem: RFID reader produces high noise by emitting a very strong field



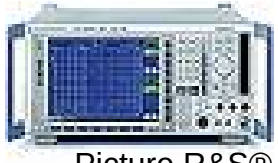
- Challenge: Circumvent the reader signal by
  - Carrier-elimination techniques like the Helmholtz arrangement
  - Frequency-selective measurements using filtering techniques
  - Separation of chip from its antenna

Carrier Cancellation

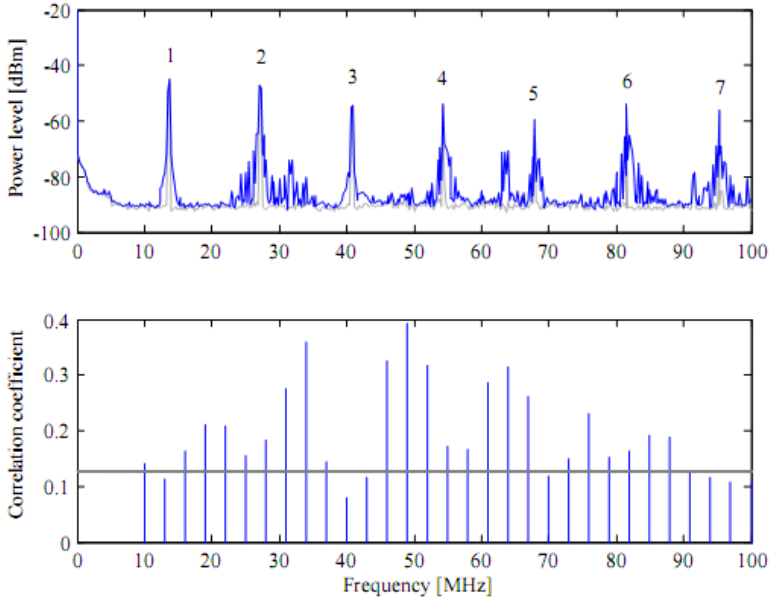
- Helmholtz Arrangement
- Specified in the ISO-10373-6 standard
- Reader coil and two sense coils
- Adjustable resistor
- Carrier attenuation of 40dB
- Used to measure the transformed impedance of passively powered devices

Frequency-Selective Measurements

- Use of filtering techniques to identify data-dependent frequency emissions
- Device Characterization
  - Sweep through the EM spectrum
  - Perform DEMA attacks on each filtered frequency band
- Receiver used for filtering
  - 10MHz .. 10kHz filters



Picture R&S®



Separate Antenna from the Chip

- Isolate chip from its antenna
- Extend the antenna to place the chip outside the reader field
- Detuning: Loss of impedance matching between chip and antenna

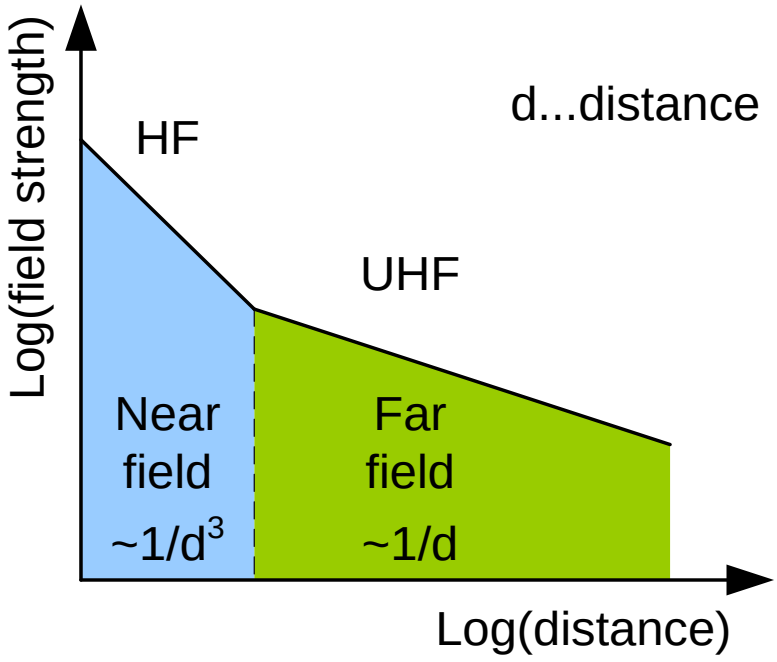
- Put the chip into a shielded environment

Results of HF-Tag Analyses

- Measurements performed on HF-tag prototypes
- Successfully performed DEMA attacks using
  - the Helmholtz Arrangement ✓
  - frequency-selective measurements ✓
- EM analyses pose a serious threat for HF tags and UHF tags…

HF vs. UHF (1)

- HF
  - 13.56MHz (ISO14443, ISO15693, …)
  - Contactless smart cards, ticketing, item identification, …
  - Operates in near field
  - Electric/magnetic coupling
  - Tag-to-reader communication via load modulation
- UHF
  - 868MHz/915MHz (ISO18000-6C)
  - Toll collection, logistics, pallet tracking
  - Operates in far field
  - Electromagnetic coupling
  - Tag-to-reader communication via backscattering



HF vs. UHF (2)

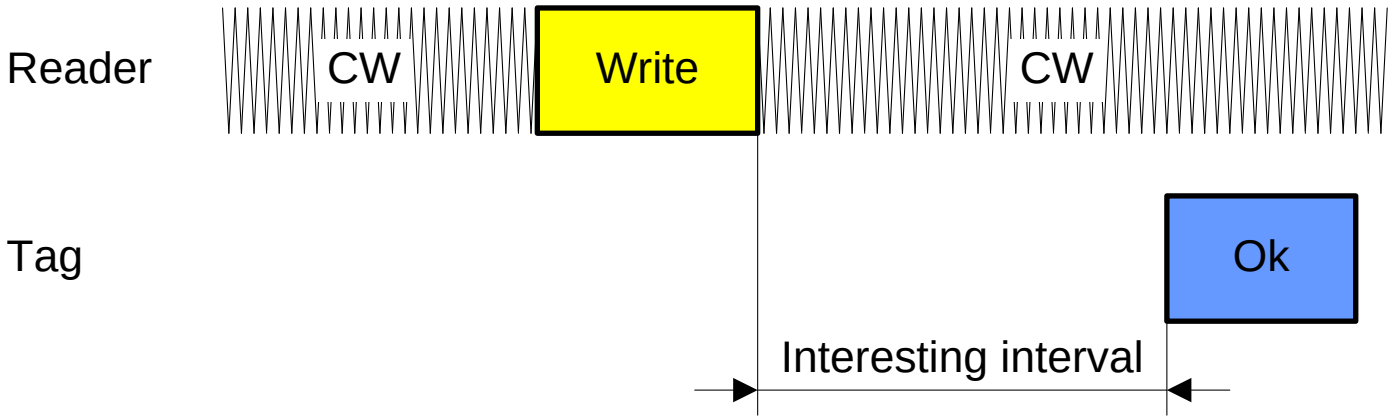
- HF
  - Read range: < 1m
  - Typical power consumption of tags in range of mWs
  - Carrier signal is spurious when analyzing direct emissions of tag IC
- UHF
  - Read range: 5 – 7m (passive transponder) → eavesdropping
  - Typical power consumption of tags in range of μWs → signal directly emitted by tag IC is weaker
  - Carrier signal less spurious when analyzing direct emissions of tag IC (low-pass filtering)
  - Parasitic backscatter

Parasitic Backscatter

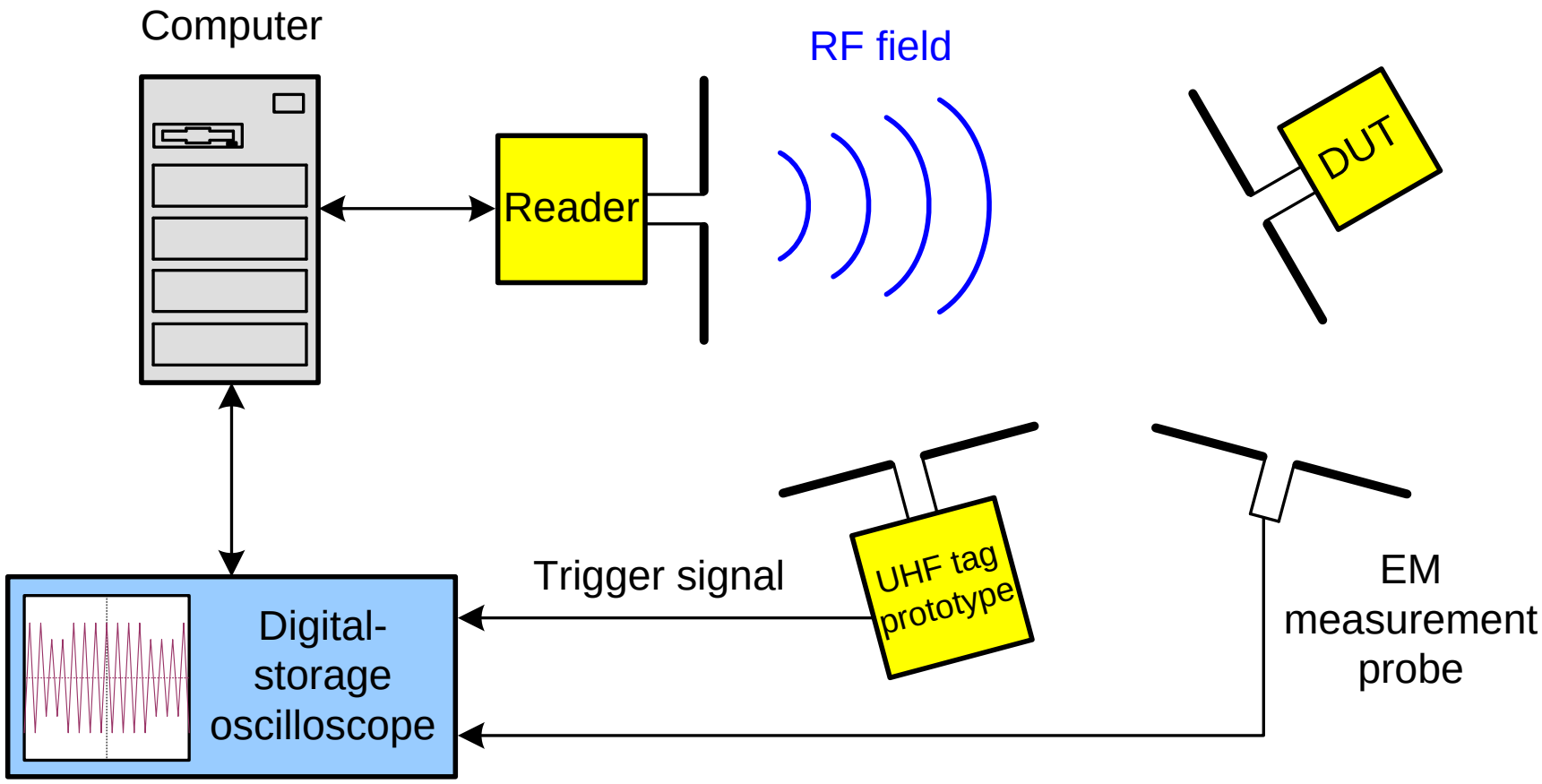
- UHF RFID tags use backscatter modulation for tag-to-reader communication → achieved by changing input impedance Z_T
- Input impedance Z_T is changed:
  - …by switching impedance in parallel to antenna (intended)
  - …but also by varying power consumption of tag IC (unintended)
- Unintended change of Z_T also modulates backscatter → parasitic backscatter
- Observed by Oren and Shamir in 2006

Side-Channel Analysis of UHF RFID Tags

- Examining EPC Generation 2 tags
  - Self-made prototype of a UHF RFID tag
  - Commercially-available UHF RFID tags
- Deploying DEMA to detect susceptibility
- No crypto on current EPC Generation 2 tags → using EEPROM write operation instead



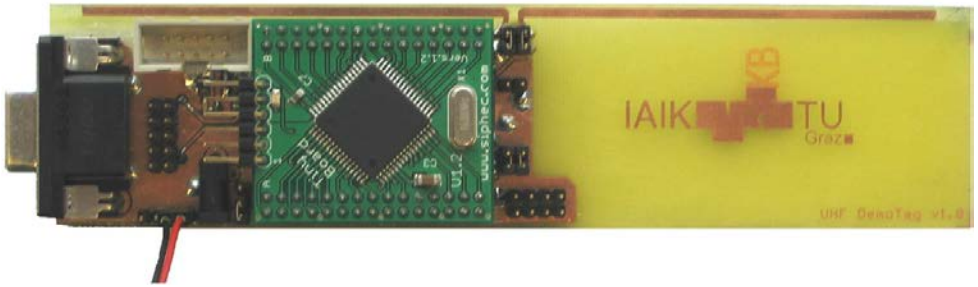
Measurement Setup (1)



(far-field measurement setup)

Measurement Setup (2)

Self-made prototype of an UHF RFID tag



Measurement probes

- Near field:

Far field:

Results (1)

DEMA successful on all examined UHF RFID tags

Measurements in the near field and far field

Self-made prototype of an UHF RFID tag

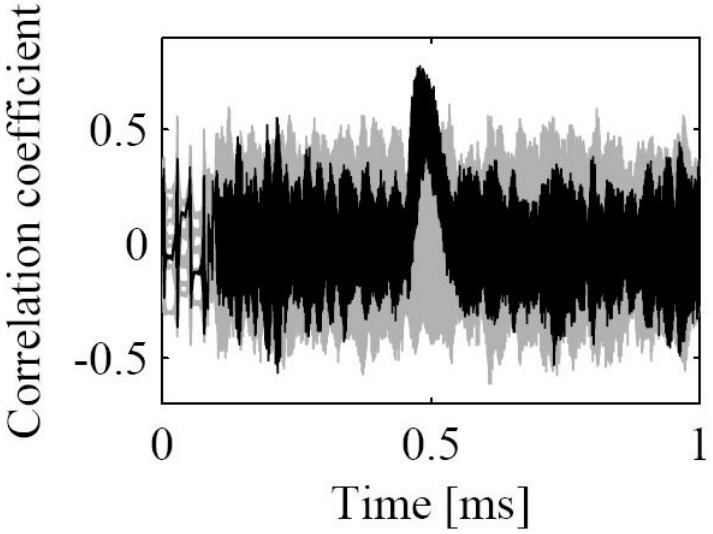
- Near field ✓
- Far field ✗

Commercially-available UHF RFID tags

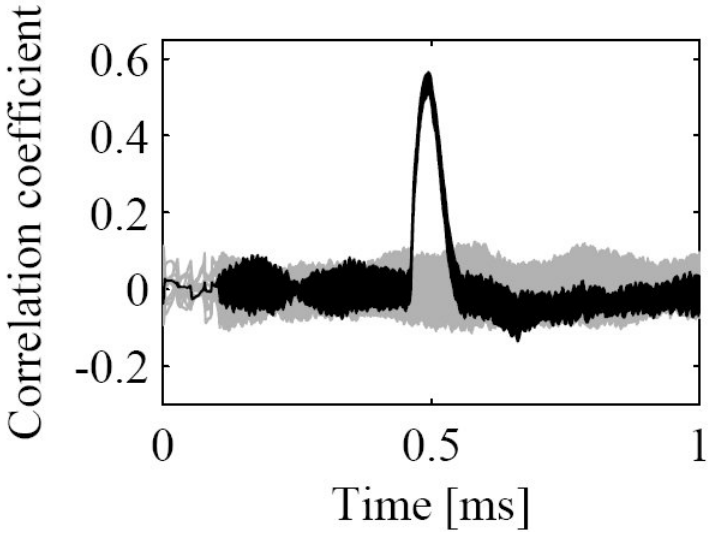
- Near field ✓
- Far field ✓

Results (2)

- Near-field measurements of a commercially-available UHF RFID tag



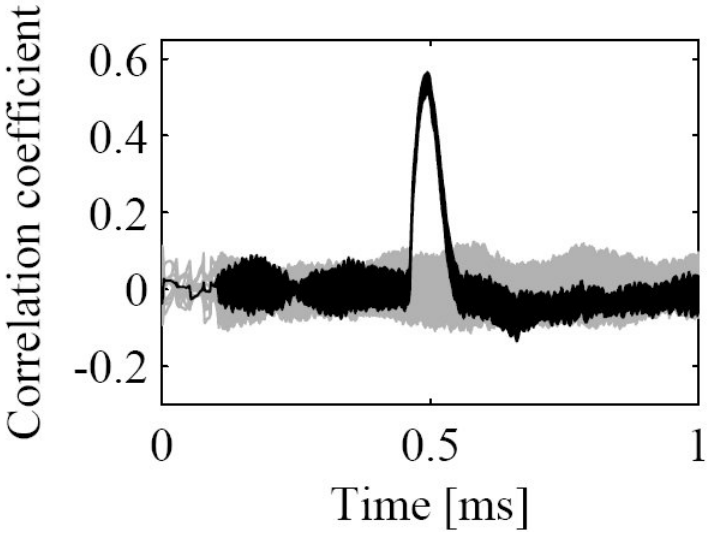
50 EM traces



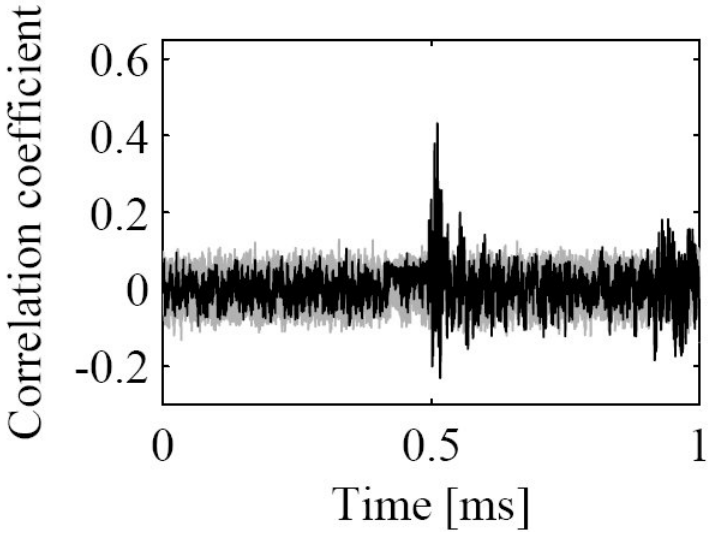
1000 EM traces

Results (3)

- Near-field measurements of commercially-available UHF RFID tags from different vendors



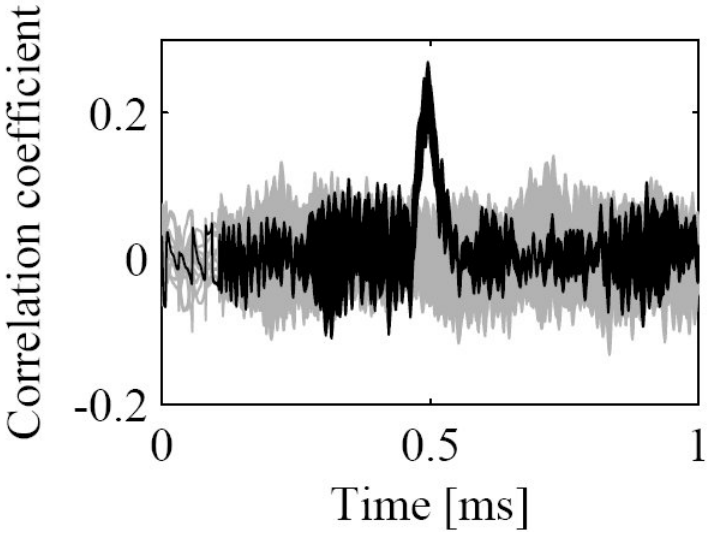
1000 EM traces / vendor A



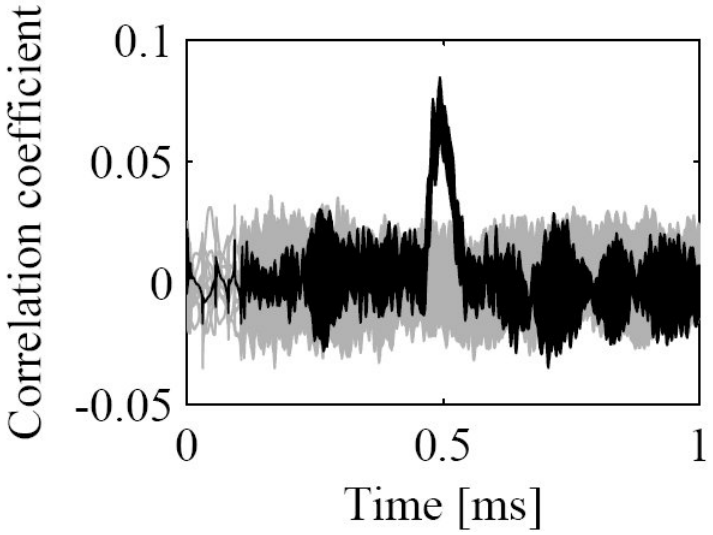
1000 EM traces / vendor B

Results (4)

- Far-field measurements of a commercially-available UHF RFID tag at different distances



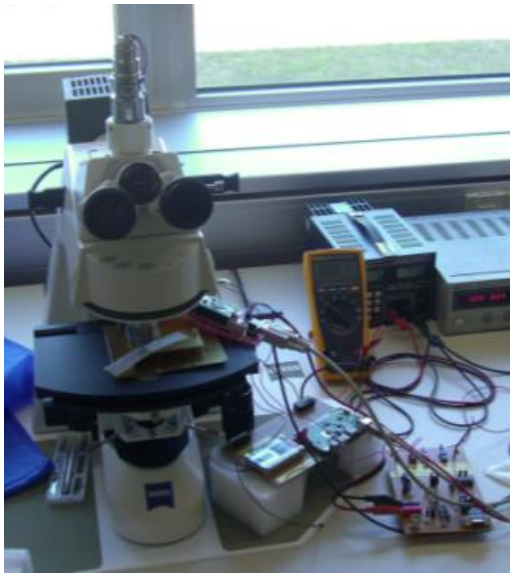
1000 EM traces / 20cm away



10000 EM traces / 1m away

Fault Analysis of RFID Tags (1)

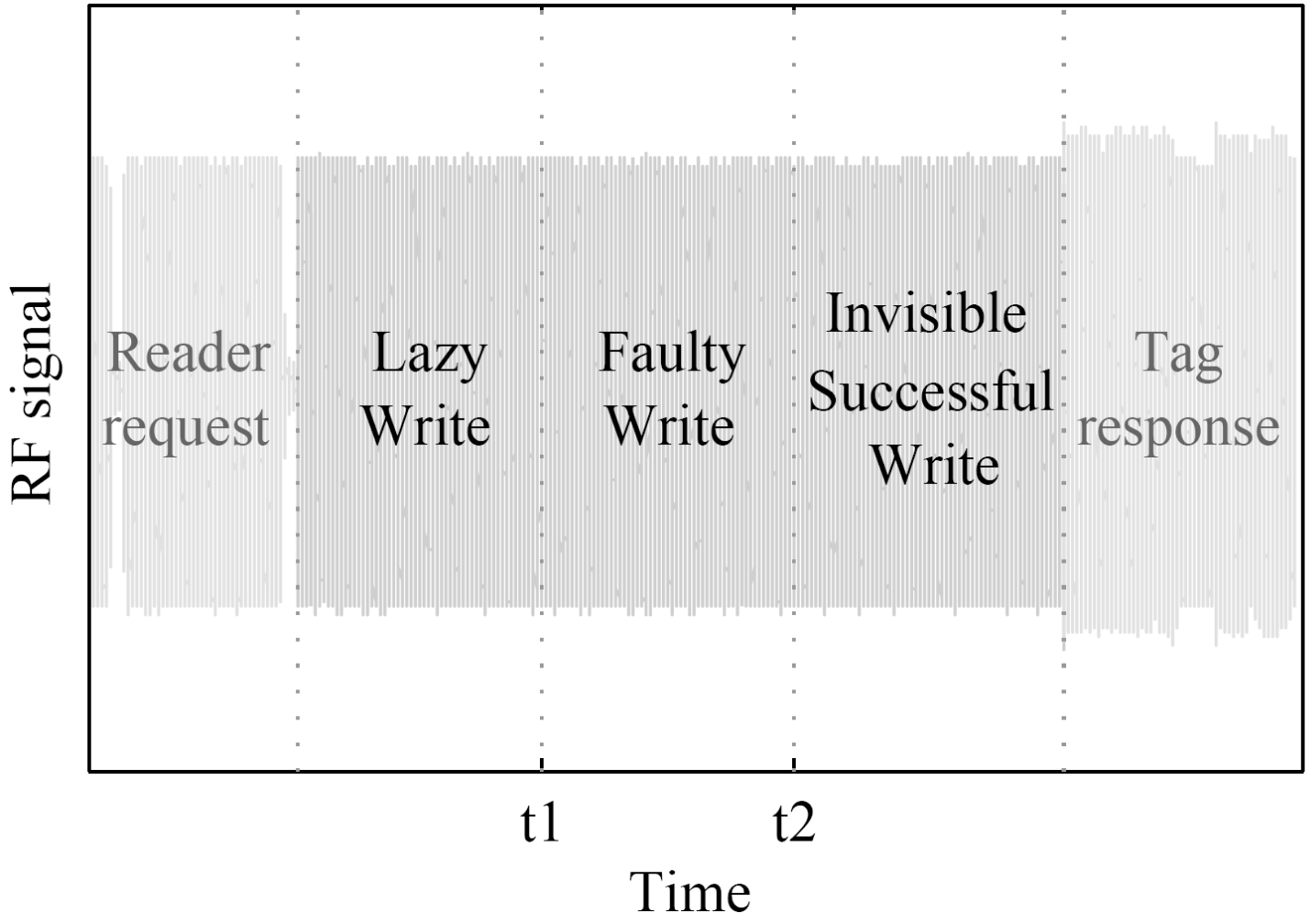
- Inducing faults globally and locally
- Global fault induction methods
  → affect whole tag IC at once
  - Temporarily antenna tearing
  - Electromagnetic interferences
  - Optical inductions
- Local fault induction methods
  → only parts of tag IC affected (more precise)
  - Optical inductions



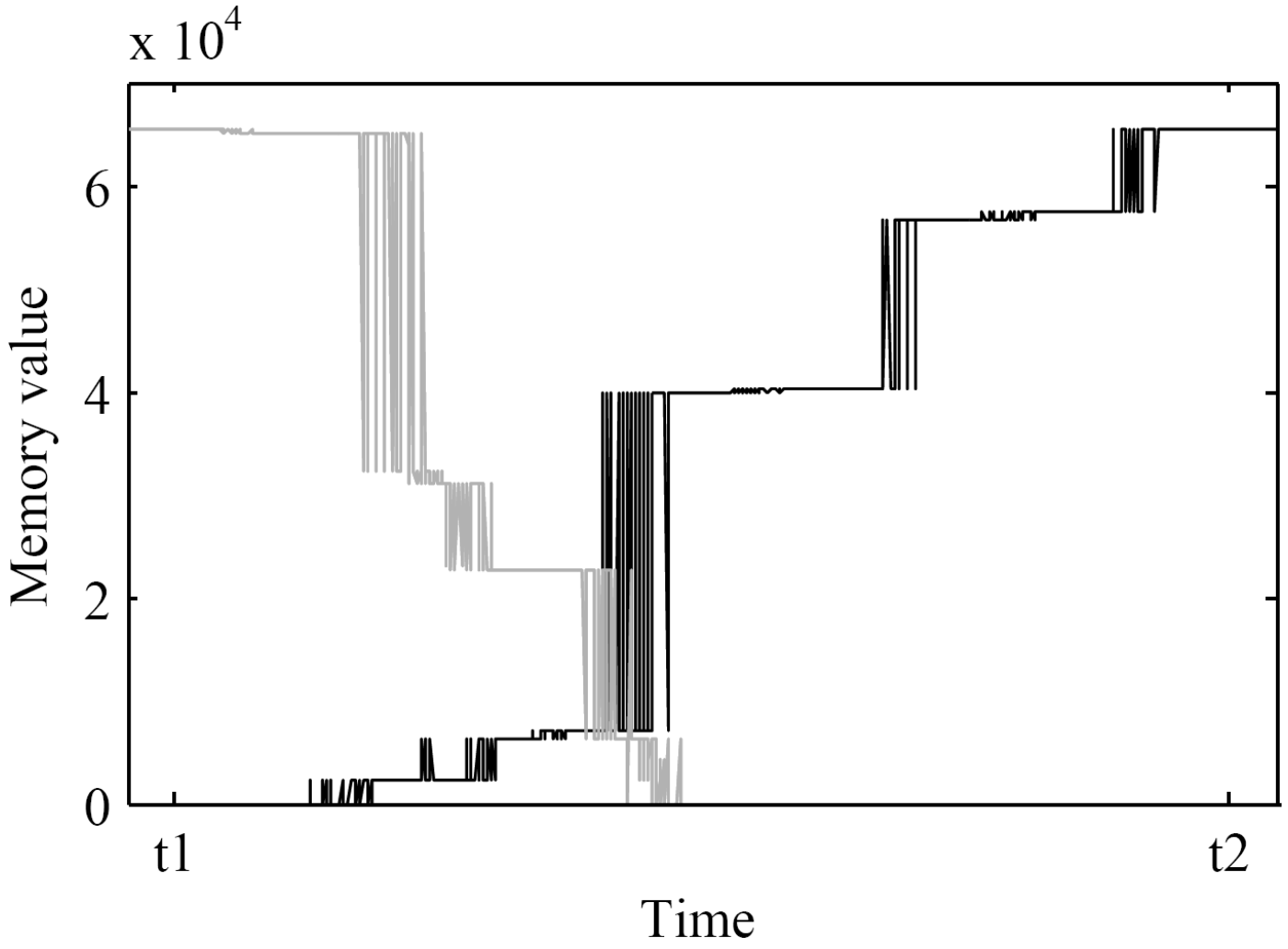
Fault Analysis of RFID Tags (2)

- Using EEPROM write operation of RFID tags
- Examining HF and UHF RFID tags
- RFID-tag prototypes deployed to trigger fault induction
- Automatic measurement sweep by varying offset and length of fault-injection trigger
- Various faulty behaviors can be achieved with low-cost equipment
  - Preventing the tag from writing to the EEPROM
  - Enforcing the tag to write a wrong value to the EEPROM
  - …

Fault Analysis of RFID Tags (3)



Fault Analysis of RFID Tags (4)



Conclusions

- Design of HF and UHF-tag prototypes
- Performed side-channel and fault analyses
- All attacks have been successful
- This emphasizes the need of appropriate countermeasures not also for security-enabled smart cards but also for low-cost passive RFID tags

Thanks for your attention!

Side-Channel Analysis Lab

PROACT